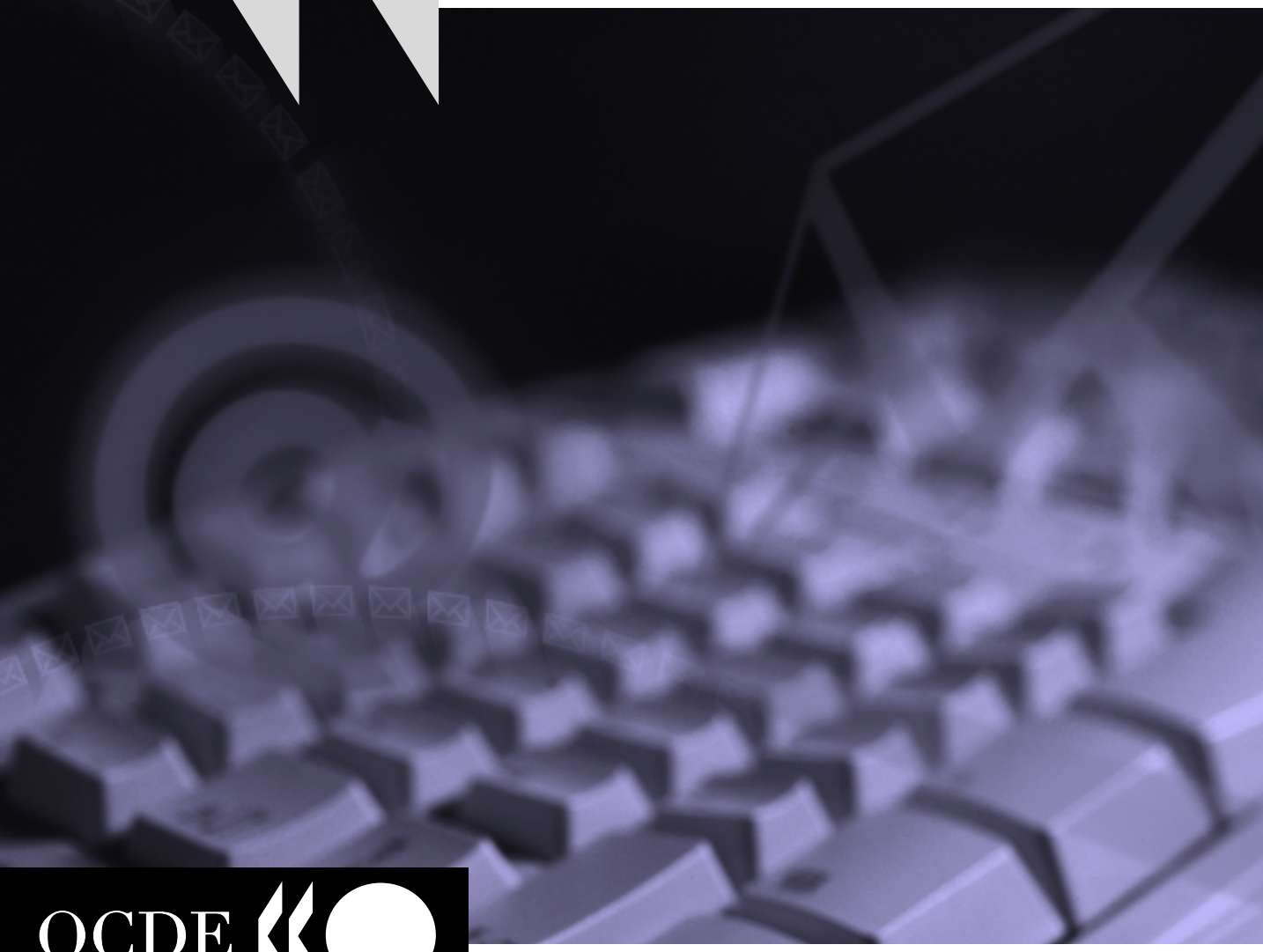
Boîte à outils anti-spam de l'OCDE et politiques et mesures recommandées



OCDE

ORGANISATION DE COOPÉRATION ET DE DÉVELOPPEMENT ÉCONOMIQUES

L'OCDE est un forum unique en son genre où les gouvernements de 30 démocraties œuvrent ensemble pour relever les défis économiques, sociaux et environnementaux que pose la mondialisation. L'OCDE est aussi à l'avant-garde des efforts entrepris pour comprendre les évolutions du monde actuel et les préoccupations qu'elles font naître. Elle aide les gouvernements à faire face à des situations nouvelles en examinant des thèmes tels que le gouvernement d'entreprise, l'économie de l'information et les défis posés par le vieillissement de la population. L'Organisation offre aux gouvernements un cadre leur permettant de comparer leurs expériences en matière de politiques, de chercher des réponses à des problèmes communs, d'identifier les bonnes pratiques et de travailler à la coordination des politiques nationales et internationales.

Les pays membres de l'OCDE sont : l'Allemagne, l'Australie, l'Autriche, la Belgique, le Canada, la Corée, le Danemark, l'Espagne, les États-Unis, la Finlande, la France, la Grèce, la Hongrie, l'Irlande, l'Islande, l'Italie, le Japon, le Luxembourg, le Mexique, la Norvège, la Nouvelle-Zélande, les Pays-Bas, la Pologne, le Portugal, la République slovaque, la République tchèque, le Royaume-Uni, la Suède, la Suisse et la Turquie. La Commission des Communautés européennes participe aux travaux de l'OCDE.

Les Éditions de l'OCDE assurent une large diffusion aux travaux de l'Organisation. Ces derniers comprennent les résultats de l'activité de collecte de statistiques, les travaux de recherche menés sur des questions économiques, sociales et environnementales, ainsi que les conventions, les principes directeurs et les modèles développés par les pays membres.

• • •

La Boîte à outils a été déclassifiée le 29 mars 2006 par les Comités PIIC et CPC, et la Recommandation du Conseil sur la question a été adoptée par le Conseil de l'OCDE à sa réunion du 13 avril 2006. Le mandat du Groupe de réflexion prend fin en juin 2006.

Les travaux du Groupe de réflexion ont été soutenus par des contributions financières volontaires de l'Australie, du Canada, de l'Italie, de la Norvège et de la République Tchèque.

Le Groupe de réflexion a bénéficié pour ses travaux du soutien de Dimitri Ypsilanti et de Claudia Sarrocco, du Secrétariat de l'OCDE.

Publié en anglais sous le titre :
OECD Anti-Spam Toolkit of Recommended Policies and Measures

AVANT-PROPOS

Compte tenu des préjudices économiques et sociaux que peut provoquer le spam et des risques de nouveaux problèmes liés à la convergence des technologies des communications, le Comité PIIC, en consultation avec le Comité de la politique à l'égard des consommateurs, a approuvé en avril 2004 la proposition de création d'un « Groupe de réflexion sur le spam » pour l'aider à poursuivre et à coordonner les travaux sur le spam et dégager plus rapidement un consensus sur un cadre d'action pour résoudre les questions posées par le spam. La création du Groupe de réflexion sur le spam, en tant qu'organe subsidiaire des deux Comités, a été approuvée par le Conseil de l'OCDE.

La Boîte à outils anti-spam de l'OCDE a été élaborée dans le cadre des travaux du Groupe de réflexion sur le spam et comprend une série de politiques et mesures recommandées qui couvrent les approches réglementaires, la coopération pour la répression du spam, les activités à l'initiative de l'industrie, les solutions techniques, les actions d'éducation et de sensibilisation, la mesure du spam et la coopération et les échanges au plan international.

Le présent document est constitué d'une synthèse, qui résume les mesures et politiques recommandées dans la Boîte à outils, et du rapport du Groupe de réflexion, divisé en huit sections principales reprenant les éléments présentés ci-dessus. Il est complété par la Recommandation du Conseil de l'OCDE relative à la coopération transfrontière dans l'application des législations contre le spam ; les pratiques et codes de conduite préconisés par le BIAC et le MAAWG pour les FAI et opérateurs de réseaux, et les pratiques exemplaires recommandées par le BIAC pour le télémarketing par courrier électronique. Dans les annexes, on trouvera également le formulaire de transmission des plaintes, proposé par le CNSA/LAP, et le Code de conduite concernant le spam mobile, élaboré dans le cadre de la GSM Association.

La Boîte à outils est également disponible en ligne, avec un certain nombre de ressources et documents, des informations actualisées sur les législations des pays à l'égard du spam et une liste des points de contact nationaux auprès des autorités chargées de l'application des législations anti-spam. Le site Web est en ligne à l'adresse : **www.oecd-antispam.org**.

TABLE DES MATIÈRES

Figures

Encadrés

SYNTHÈSE

Compte tenu du vaste impact du spam, et des risques de nouveaux problèmes liés à l'émergence des communications universelles et de l'Internet mobile, l'OCDE a réuni des décideurs et des professionnels pour former le **Groupe de réflexion sur le spam de l'OCDE** (ci-après dénommé « le Groupe de réflexion »), qui a été chargé d'élaborer un cadre pour lutter contre spam en s'appuyant sur un large éventail de solutions pluridisciplinaires.

Le Groupe de réflexion a élaboré la **Boîte à outils anti-spam** (la « Boîte à outils ») qui recommande un ensemble de politiques et de mesures qui devraient constituer des éléments clés d'un cadre global d'action publique pour s'attaquer au problème du spam. Ces politiques et mesures sont présentées succinctement ci-après.

Situation et évolution du spam

Pour que les plates-formes, les applications et les services de communications électroniques puissent contribuer au développement social et économique, ceux-ci doivent être fiables, efficients et dignes de confiance. Or, aujourd'hui, le courrier électronique et d'autres outils de communications électroniques peuvent être menacés par les messages électroniques non sollicités, non souhaités et préjudiciables, couramment appelés spam. Si ces menaces n'étaient pas contrées, elles pourraient éroder la confiance et l'assurance des utilisateurs.

Le phénomène du spam, qui se manifestait au début par des messages publicitaires vantant généralement des produits ou services commerciaux, a évolué au fil du temps, et aux simples messages publicitaires se sont ajoutés des messages potentiellement dangereux, susceptibles d'induire en erreur, encombrant les réseaux, pouvant déboucher sur certaines formes de fraude ou servant de vecteur pour la diffusion de virus et autres logiciels malveillants.

Une approche systématique et coordonnée à l'égard du spam

Il n'existe pas de solution simple pour enrayer le spam. Si le caractère ouvert et décentralisé d'Internet est l'une des principales raisons de son succès, il a également créé les conditions qui ont conduit à un certain nombre de vulnérabilités qui sont de plus en plus exploitées par les spammeurs et autres contrevenants en ligne. L'absence de contrôle centralisé permet aux utilisateurs de masquer leur identité. De plus, le faible coût de l'accès à Internet et des services de courrier électronique permet aux spammeurs d'envoyer quotidiennement des millions de messages de spam pour un coût marginal extrêmement bas, de sorte qu'il suffit d'un taux de réponse très faible pour dégager de gros profits. Toutefois, il apparaît important de lutter contre le spam et les autres menaces en ligne, pour maintenir l'ouverture, la flexibilité et l'innovation sur lesquelles repose l'Internet.

Dans ce contexte, le Groupe de réflexion, au début de son mandat, a décidé de la stratégie à suivre et du rôle des différents acteurs dans la lutte contre le spam. Il existait un consensus sur le fait que les pouvoirs publics devaient s'attacher à établir des politiques anti-spam nationales claires, en concertation avec les autres acteurs, collaborer avec le secteur privé et promouvoir la coopération au-delà des frontières. Il était également convenu que pour lutter contre le spam, il était important de mettre en place des groupes de coordination nationaux, et de créer des cadres réglementaires appropriés, fondés sur des objectifs politiques bien définis et soutenus par des mécanismes efficaces de sanction. Il était reconnu que le secteur privé a le premier rôle dans le développement de pratiques adéquates par les entreprises et la recherche de solutions techniques innovantes, et qu'il peut grandement contribuer à l'éducation des utilisateurs. La coordination et la coopération entre les acteurs publics et privés sont essentielles pour éradiquer le spam.

C'est dans ce contexte que le Groupe de réflexion de l'OCDE sur le spam a élaboré le concept de boîte à outils anti-spam, avec pour objectif de proposer aux Membres de l'OCDE une orientation politique globale et un cadre cohérent dans leur lutte contre le spam. Le Groupe était également convaincu que ce cadre serait également applicable par les pays non membres et qu'il leur serait utile. La Boîte à outils comprend huit éléments interdépendants qui couvrent :

Les approches réglementaires : il est essentiel d'élaborer une législation anti-spam afin de lutter contre le spam et les problèmes qui s'y rattachent. La législation doit fixer des orientations claires sur ce qui est autorisé et ce qui ne l'est pas.

Les problèmes de répression du spam : S'il est effectivement nécessaire de disposer d'une législation appropriée, la mise en oeuvre et l'application du droit sont fondamentales. Il est capital d'agir avec diligence et célérité pour décider et appliquer des sanctions, si l'on veut effectivement éliminer le spam, et les procédures traditionnelles de sanction qui peuvent prendre des semaines ou des mois ne sont pas pleinement efficaces dans l'environnement en ligne. Il convient tout particulièrement, dans le contexte du spam, de prendre en compte les questions de coordination nationale, de sanctions, d'habilitation des autorités chargées de faire appliquer la loi et de coopération transfrontière pour la répression du spam.

Les initiatives anti-spam du secteur privé : pour une action efficace contre le spam, les législations nationales anti-spam doivent être couplées avec des initiatives du secteur privé.

Les solutions techniques : les outils anti-spam agissent à plusieurs niveaux – au point d'origine du message électronique, sur le réseau de transport, sur le serveur de messagerie et sur l'ordinateur destinataire – et ils peuvent utilisées ensemble ou isolément. Tout effort pour lutter efficacement contre le spam passe par une utilisation et une administration rationnelles d'un certain nombre de ces outils et méthodes techniques. Aucune méthode ne permettra à elle seule d'obtenir un résultat complet. Quand plusieurs technologies anti-spam sont utilisées conjointement de façon efficace, le niveau de spam affectant un réseau peut être réduit de façon spectaculaire.

L'information et la sensibilisation : une stratégie globale anti-spam doit faire en sorte que l'utilisateur final, qui est le destinataire ultime du spam, la victime possible de virus et d'escroqueries, et dans le même temps, la personne qui a le contrôle sur son ordinateur et son information personnelle, soit suffisamment éduqué et sensibilisé à la façon de faire face au spam et aux autres menaces en ligne. Des activités d'information et de sensibilisation sont nécessaires dans les grandes entreprises, ainsi qu'auprès des PME, des particuliers et des établissements d'enseignement. Elles doivent avoir pour objet de créer une culture de la sécurité, et d'encourager une utilisation responsable du cyberespace.

Les **partenariats en coopération contre le spam** : le public et les acteurs privés ont collectivement intérêt à préserver la disponibilité et la fiabilité des outils de communications afin de promouvoir le développement de l'économie du numérique. La coopération entre les secteurs public et privé se développe de plusieurs façons innovantes. Les objectifs des partenariats stratégiques sont généralement la sensibilisation et l'échange d'informations. Des partenariats à caractère plus opérationnel contribuent également à l'éducation, au développement (et à la mise en oeuvre) de pratiques exemplaires et à l'échange d'informations et de données concernant les cas de spam transfrontières. De plus, comme le montrent les efforts déployés aux niveaux national et international, les partenariats sont un outil fondamental pour améliorer la communication et mieux comprendre les besoins, les attentes et les problèmes de chacun, et donc renforcer la coopération et l'implication mutuelle.

La mesure du spam : il est essentiel d'effectuer des mesures pour apprécier l'évolution du spam et l'efficacité des solutions anti-spam et des actions pédagogiques. La métrologie permet l'évaluation des stratégies nationales et de leur mise en oeuvre et elle éclaire sur les changements qui doivent être apportés aux cadres politiques, réglementaires ou techniques.

La coopération mondiale (Ouverture) : le spam, comme l'Internet, ne connaît pas de frontières, et il circule en provenance et à destination des économies développées et en développement. Dans ce contexte, la coopération mondiale est fondamentale pour promouvoir des cadres nationaux appropriés afin de contrer le spam dans tous les pays, et pour encourager la coopération entre les pouvoirs publics, le secteur privé, la société civile et les autres parties prenantes. La coopération est nécessaire pour assurer l'application harmonisée et généralisée des mesures techniques et le respect effectif des règles applicables.

Pour chacun des éléments précités, le Groupe de réflexion a recommandé un certain nombre de politiques et pratiques :

Élément I. Approches réglementaires

L'élaboration d'une législation anti-spam qui traite du spam et des problèmes qui s'y rattachent est fondamentale.

Les réglementations nationales anti-spam devraient s'attacher à :

1. **Préserver les avantages procurés par les communications électroniques**, en renforçant la confiance des utilisateurs dans l'Internet et les systèmes de messagerie électronique, et améliorer la disponibilité, la fiabilité et l'efficience des services, ainsi que le fonctionnement des réseaux de communications mondiaux.

2. **Interdire et sanctionner le spamming, tel que défini par la législation nationale.** La législation seule peut ne pas suffire à empêcher les spammeurs potentiels de tirer parti de cette technique de marketing, mais les lois et réglementations peuvent avoir un effet dissuasif en sanctionnant les individus et organisations qui choisissent d'utiliser le spam et d'en tirer profit. La force de la législation dépendra de la gravité des sanctions, et notamment du caractère inéluctable de leur application.

3. **Réduire le volume de spam**. Pour prévenir l'envoi de spam, une action doit être menée à différents niveaux, de manière à réduire le volume du spam transitant sur les réseaux, et réduire le nombre de messages de spam reçus par les destinataires.

Pour atteindre ces objectifs, le législateur doit prendre en compte quatre principes généraux :

- **Orientation de la politique publique** : La législation doit refléter une orientation claire de la politique publique. Les grandes lignes et les principaux objectifs de la politique anti-spam nationale et internationale doivent être esquissés très tôt et ils doivent guider l'ensemble de la stratégie gouvernementale.

- **Simplicité de la réglementation** : La législation doit être concise et simple.

- **Effectivité de l'application** : il est fondamental que la législation soit respectée, faute de quoi, elle perd toute utilité. C'est pourquoi il est important de mettre en place un régime de sanctions efficace et des modalités adéquates pour l'administration des preuves. De plus, les autorités chargées de faire appliquer la législation doivent être dotées de ressources et de pouvoirs suffisants.

- **Relations internationales** : le spam étant un problème international, la législation doit prévoir des dispositions adéquates au niveau international, et donner aux autorités nationales la possibilité de coopérer dans les enquêtes et d'échanger des informations avec les autorités étrangères (voir plus loin).

Lors de l'étude des meilleures pratiques pour la législation, les éléments suivants devraient être inclus dans toute la mesure du possible, en tenant compte du cadre institutionnel et juridique du pays :

	Questions	**Approche**
Champ d'application	Services concernés	Les formats des messages vont fusionner et évoluer, et des supports inédits pourront apparaître. Deux approches législatives sont envisageables : "Spécifique à telle ou telle technologie": Il s'agit de viser des technologies spécifiques de messagerie, en général celles qui posent actuellement un problème de spam. "technologiquement neutre": l'instrument réglementaire s'applique aux technologies de communications en général, et il est suffisamment flexible pour tenir compte des évolutions futures dans les technologies de messagerie sans avoir besoin d'être modifié. Les services en temps réel de voix à voix pourraient être réglementés à part.
	Finalité commerciale	Examiner si la législation ne devrait viser que les messages commerciaux au transactionnels, ou s'il faudrait aussi viser certains contenus non commerciaux, par exemple les messages politiques ou religieux. Des catégories spécifiques de messages peuvent être expressément exclues du champ de la loi (p.ex. messages des établissements d'enseignement à leurs anciens élèves).

	Questions	Approche
Consentement	Consentement	Le degré de consentement ou d'autorisation que les législateurs ou les autorités de régulation souhaiteront imposer peut varier selon l'approche choisie pour réglementer le spam. Il existe trois grandes approches en matière de consentement, qui sont souvent combinées dans la législation: Consentement exprès : forme de consentement par lequel un individu ou une organisation a activement donné son autorisation à une action ou une activité particulière (accord explicite ou opt-in). Consentement induit/implicite: consentement pouvant généralement être déduit du comportement et/ou des autres relations d'affaires du destinataire. Consentement supposé: il y a présomption du consentement jusqu'à ce que celui-ci soit retiré par le destinataire, par exemple par "désabonnement" (droit de refus ou opt-out).
Conditions à respecter pour les messages de marketing légitimes	Adresse de désabonnement	Les messages doivent toujours comporter un lien fonctionnel de désabonnement, permettant au destinataire d'indiquer qu'il ne souhaite plus recevoir de messages de la part de l'expéditeur. Il faut donc que le message indique une adresse de réponse valide, afin que le destinataire puisse aisément se désabonner. Une adresse postale pourrait également être exigée. La non fourniture d'un moyen de désabonnement, d'une adresse de réponse valide et d'une adresse postale valide, ou le fait de ne pas cesser les envois de messages dans les délais fixés par la législation devraient être sanctionnés.
	Information sur les origines du message	L'une des grandes difficultés que pose la réglementation du spam et le contrôle du respect des législations en la matière est de contrer la capacité qu'ont les spammeurs de falsifier l'origine des messages qu'ils envoient: • La législation doit interdire l'envoi de courriers électroniques dont l'origine est falsifiée ou dont les informations d'en-tête ou d'identification sont masquées. • La législation devrait également imposer que l'opérateur de marketing qui fait appel à l'expéditeur du courrier électronique soit clairement identifié.
	Pas d'envois en masse	La législation peut prévoir qu'un message électronique n'est considéré comme du spam que lorsqu'un certain nombre de messages a été envoyé sur une période donnée (en général plus de 50-100 sur 24 heures). Cet élément doit naturellement tenir compte du fait qu'il existe des envois en masse de courriers électroniques qui sont légitimes (p.ex. lettres d'information, etc.).
	Etiquetage	La législation peut comporter une disposition imposant l'utilisation d'une étiquette spécifique pour les courriers électroniques contenant de la publicité, des matériels pornographiques, etc.

	Questions	Approche
Éléments accessoires	Personne autorisant l'envoi du spam ou aidant/assistant le spammeur	La loi devrait sanctionner non seulement la personne physique qui envoie le message, mais aussi celle qui a demandé ou autorisé l'envoi des messages ou qui retire un gain financier des activités de spamming. Cette approche pourrait faciliter l'action de répression, car il est souvent difficile de déterminer l'identité de celui qui a effectivement envoyé le spam, et qu'il pourrait être plus aisé d'identifier l'opérateur de marketing bénéficiant du spamming.
	Logiciel de collecte de listes d'adresses et listes d'adresses collectées Attaques dictionnaire	La législation peut comprendre des dispositions spécifiques prévoyant des amendes ou des pénalités particulières en cas d'utilisation de ces outils pour envoyer des messages qui constituent une infraction à la législation anti-spam en vigueur: le fait de vendre, acheter ou utiliser des logiciels de collecte ou des listes d'adresses collectées, ou la génération automatique d'adresses de destinataires pourraient être sanctionnés.
Cybercriminalité et questions liées au contenu	Accès illicite	La législation devrait interdire l'utilisation non autorisée de ressources informatiques protégées. Quiconque s'introduit dans un ordinateur afin de s'en servir pour expédier des messages devrait être sanctionné.
	Contenu trompeur ou frauduleux	Cet aspect porte sur le contenu du message, laissant de côté beaucoup des problèmes systémiques concernant les messages de spam. Les spams utilisés pour l'escroquerie et pour l'hameçonnage peuvent être considérés comme relevant des délits informatiques, c'est-à-dire des délits ordinaires qui sont fréquemment commis en utilisant un système informatique. • La législation anti-spam pourrait comporter des dispositions interdisant les titres de message trompeurs ou frauduleux. De plus. • La législation à l'égard du spam pourrait couvrir le contenu des messages, surtout si les législations sur la lutte contre la fraude, la protection des consommateurs, etc. ne sont pas suffisamment claires.
	Menaces pour la sécurité	L'utilisation du spam pour la diffusion de logiciels malveillants est souvent considérée comme un délit par la loi et elle pourrait être incriminée en se fondant sur la Convention sur la cybercriminalité du Conseil de l'Europe.
Élément international	Juridiction transfrontière	La réglementation devrait spécifier que : • Les messages émis depuis la juridiction ou à destination de celle-ci sont couverts, de même que les messages dont l'expédition a été commandée à l'intérieur de la juridiction ainsi que les avantages financiers liés au spam. • Les spammeurs qui opèrent depuis la juridiction nationale, même si leurs spam sont adressés à d'autres pays, devraient être sanctionnés par la législation nationale. • Les autorités nationales chargées de faire appliquer la législation devraient être habilitées à engager des coopérations internationales, et les accords internationaux de contrôle de l'application des législations sont importants.

Le rôle des fournisseurs d'accès Internet et de services de messagerie électronique est également important, et pourrait être pris en compte dans la législation. Les pouvoirs publics et les autorités de régulation, en particulier, devraient soutenir l'élaboration de codes de conduite pour les FAI qui complètent la législation et soient compatibles avec elle. Les gouvernements devraient encourager les associations professionnelles à élaborer ce type de code et à adopter des pratiques exemplaires quand cela est dans l'intérêt du public et n'impose pas de charges financières ou administratives indues aux participants. Les Annexes II et III du Rapport final proposent une charte élaborée par le Comité consultatif économique et industriel auprès de l'OCDE et le Messaging Anti-Abuse Working Group (MAAWG) dans le cadre des travaux du Groupe de réflexion sur le spam.

Ces codes, suivant les pratiques et les dispositions législatives nationales, pourraient le cas échéant être déposés auprès de l'organisme national chargé de faire appliquer la législation. Ce dépôt pourrait permettre à l'autorité d'exiger d'un participant industriel qu'il se conforme au code, dans les cas où l'association professionnelle ne parviendrait pas à se faire entendre.

La législation pourrait également prévoir un cadre détaillé pour appuyer les activités des FAI destinées à bloquer ou limiter la circulation de messages de spam. Les FAI devraient pouvoir prendre des mesures défensives appropriées et équilibrées pour protéger leurs réseaux, et ils devraient être autorisés à engager des poursuites contre les spammeurs. Des résultats identiques pourraient être obtenus au moyen de dispositions contractuelles appropriées entre les FAI et les utilisateurs.

Élément II. Répression du spam

La législation doit faire en sorte que les organismes chargés de faire appliquer la législation disposent de pouvoirs adéquats pour fonctionner efficacement. Sur la proposition du Groupe de réflexion, une **Recommandation du Conseil de l'OCDE relative à la coopération dans l'application transfrontière des lois anti-spam** a été adoptée. Sur la base de cette recommandation, les gouvernements devraient améliorer leur législation pour :

a) Mettre en place un cadre national de lois, autorités et pratiques afin d'assurer la mise en application de la législation anti-spam.

b) Renforcer la capacité de leurs autorités à coopérer avec leurs homologues étrangers, en les dotant des moyens d'échanger des informations pertinentes et de collaborer avec ces dernières en matière d'enquêtes.

c) Améliorer les procédures de coopération, en donnant la priorité aux demandes d'entraide et en faisant usage des ressources et réseaux communs.[1]

d) Elaborer de nouveaux modes de coopération entre les organismes d'application des lois et les entités compétentes du secteur privé.

Élément III. Initiatives anti-spam du secteur privé

Pour lutter efficacement contre le spam, les législation anti-spam d'application générales doivent être conjuguées avec des initiatives engagées par des acteurs du secteur privé, comme les fournisseurs d'accès Internet et les fournisseurs de services de messagerie, les opérateurs de télécommunications, les opérateurs de marketing direct, les opérateurs en ligne, les éditeurs de logiciels et leurs associations.

Les initiatives du secteur privé constituent un volet important du cadre de l'action publique. Le Groupe de réflexion :

- Se félicite des efforts déployés par le BIAC et le MAAWG pour élaborer des pratiques exemplaires et il prend note des résultats accomplis à ce jour.

- Encourage la poursuite de leur élaboration, notamment à travers un dialogue avec les organismes politiques et réglementaires appropriés.

- Note que les pratiques exemplaires évolueront en fonction des développements réglementaires, techniques et commerciaux.

- Note que dans certaines juridictions, il existe des possibilités de reconnaissance officielle de ces pratiques exemplaires.

Les prestataires de services et de produits en ligne devraient, dans le cadre de leurs activités, prendre des mesures pour :

- Développer des méthodes et des normes de communication dans l'entreprise en ce qui concerne la vie privée de leurs clients, en gérant avec soin les informations et les adresses de courrier électronique personnelles. Les règles d'entreprise concernant les sites Web, l'utilisation des noms de domaine et la messagerie électronique contribuent à protéger les utilisateurs. Des politiques d'entreprise claires à l'égard du courrier électronique – comme le fait de ne jamais demander d'information de caractère personnel ou peut-être de ne jamais proposer de lien cliquable dans un message électronique – devraient être établies et mises en oeuvre de façon systématique. Une entreprise qui adresse des courriers électroniques à ses clients peut envisager la possibilité d'authentifier ces courriers ou d'utiliser des signatures numériques.

Agir préventivement de manière à créer des barrières aux escroqueries par courrier électronique, comme l'hameçonnage. On peut par exemple rendre le site web de l'entreprise moins vulnérable aux attaques ciblées en utilisant un nom de domaine explicite et en enregistrant les noms de domaine pouvant prêter à confusion (par exemple en enregistrant les noms de domaine présentant des similitudes avec celui de l'entreprise et qui peuvent être confondus avec lui), surveiller la fréquentation du site, contrôler les messages rejetés, surveiller les sites similaires, etc.

Informer et sensibiliser les consommateurs et assurer un service client. Les opérateurs en ligne devraient communiquer efficacement avec leurs clients. Ils devraient préciser quels sont les types de communications qui seront ou peuvent être assurés par courrier électronique, définir la façon dont les adresses de courrier électronique et autres informations correspondantes peuvent être consultées et modifiées par l'utilisateur, préciser qu'il ne sera jamais demandé à l'utilisateur de communiquer ses données personnelles par courrier électronique et répertorier les éléments que les utilisateurs doivent vérifier dans le message pour s'assurer qu'il émane bien de l'opérateur en ligne.

Les opérateurs de marketing direct devraient :

- Adopter et mettre efficacement en oeuvre un code de conduite sur les pratiques exemplaires en matière de marketing électronique, lequel englobe les messages commerciaux envoyés par courrier électronique, par messagerie instantanée et par téléphonie mobile. Ces associations, de même que les associations d'opérateurs en ligne, pourraient entretenir des relations plus rigoureuses avec les FAI et autres opérateurs de réseaux, afin de réduire le nombre de faux positifs, tout en garantissant dans le même temps la légitimité et la loyauté de leurs activités.

- Adopter des pratiques exemplaires ou des codes de conduite qui devraient viser à faciliter et compléter l'application de la législation anti-spam, aux niveaux national et international. Pour cette raison, des informations appropriées sur les différentes approches législatives devraient être communiquées par les gouvernements et les associations.

Le Groupe de réflexion de l'OCDE note que le BIAC a élaboré un ensemble de pratiques exemplaires recommandées pour le marketing par courrier électronique, qui est joint dans l'Annexe III au présent rapport.

Les Fournisseurs d'Accès Internet et les autres opérateurs de réseaux devraient :

- Adopter et mettre efficacement en oeuvre une politique d'autorégulation, sous la forme de pratiques exemplaires et de codes de conduite.

- Adopter et faire respecter des Conditions générales d'utilisation (CGU) qui interdisent le spamming, et les activités qui s'y rattachent, sur leurs réseaux. Ces Conditions feraient partie d'un accord contractuel entre le prestataire et l'utilisateur, et leur violation constituerait une cause de dénonciation du contrat, permettant la suspension du service et la résiliation du contrat.

- Donner aux abonnés des informations sur la disponibilité, l'utilisation et la configuration des logiciels de filtrage du spam et des virus. Des solutions et mises à jour pour le filtrage devraient être proposées à un prix raisonnable, et des liens vers des logiciels libres anti-virus et anti-spam devraient être indiqués aux utilisateurs.

Les Gouvernements devraient encourager les FAI et les autres opérateurs de réseaux nationaux à adopter et mettre en oeuvre efficacement des pratiques collectives exemplaires recommandées. L'OCDE note les pratiques exemplaires recommandées pour les FAI et les autres opérateurs de réseaux qui ont été élaborées par le BIAC et le MAAWG et qui figurent dans l'Annexe II du présent rapport.

Les **opérateurs mobiles** devraient adopter et mettre efficacement en oeuvre des mesures pour réduire le spam sur leurs réseaux. L'éventail des nouveaux services offerts via la téléphonie mobile crée de nouveaux problèmes assimilables à du spam pour les utilisateurs mobiles. Ces mesures préconisées pour les opérateurs mobiles devraient comprendre des outils contractuels, techniques et pédagogiques. Le Groupe de réflexion de l'OCDE prend note des pratiques exemplaires de la GSM Association à l'intention des opérateurs mobiles, qui figurent dans l'Annexe IV du présent rapport.

Élément IV. Mesures techniques

Les fournisseurs d'accès Internet et les autres opérateurs de réseaux devraient constamment améliorer leurs connaissances et leurs pratiques opérationnelles et actualiser leurs pratiques exemplaires techniques, comme celles à l'intention des FAI et autres opérateurs de réseaux mentionnées dans l'élément III, afin de pouvoir faire face aux nouveaux enjeux et à l'évolution technique, et promouvoir la mise en oeuvre et l'échange des solutions techniques disponibles entre les prestataires. Le fait de combiner efficacement plusieurs technologies anti-spam peut permettre de réduire dans des proportions considérables le niveau du spam qui encombre un réseau. Bien qu'important pour réduire le volume du spam dans les boîtes à lettre, le filtrage en lui-même est insuffisant pour réduire le volume du spam émis sur les différents réseaux, et il faut donc mettre en oeuvre un éventail de solutions techniques pour assurer une protection efficace.

Élément V. Initiatives en matière d'information et de sensibilisation

Particuliers :

- Les Gouvernements devraient :

  – Élaborer des campagnes d'information et de sensibilisation du public afin d'éduquer les utilisateurs sur les produits et services qu'ils utilisent et les risques associés auxquels ils peuvent s'exposer, afin de leur permettre de se protéger eux-mêmes contre le spam, les virus et autres codes malveillants. Cette information devrait également être rendue disponible sur les portails des FAI.

  – Organiser des campagnes nationales pour attirer l'attention des médias et de l'ensemble de la population.

  – Oeuvrer avec le secteur privé, la société civile et les autres parties intéressées pour lancer des campagnes d'information des utilisateurs.

- Étant donné leur capacité à toucher les utilisateurs individuels sur le Web , les FAI et les autres opérateurs de réseaux, y compris les opérateurs mobiles, devraient utiliser leurs canaux de communication avec leurs clients (site Web, portails, sms, lettre d'information) pour donner à ces derniers des informations sur :

  – La façon d'éviter le spam et les risques liés aux messages électroniques, SMS, MMS, etc. contenant du spam.

  – Les filtres anti-spam et anti-virus et les solutions en logiciel libre disponible pour la plate-forme en question.

  – Les modalités pour signaler les cas de spamming aux FAI ou à l'opérateur de l'utilisateur ainsi qu'aux autorités compétentes, et

  – L'adresse de courrier électronique ou le numéro de téléphone permettant de contacter le service des plaintes du prestataire.

Groupes d'utilisateurs :

Des classes informatiques pour **le troisième âge**, éventuellement financés par les pouvoirs publics ou les autorités locales, devraient donner des informations sur la sécurité informatique, ainsi que des exemples concrets sur la façon de se protéger du spam, des fraudes en ligne, des virus et des autres logiciels malveillants.

La sensibilisation aux menaces et aux questions de sécurité en ligne devrait faire partie du cursus des classes informatiques pour **les élèves et les enfants**. Des dessins animés et BD pourraient être utilisées pour toucher les jeunes.

Grosses entreprises et PME

- **Entreprises** : les services informatiques devraient remettre au personnel nouvellement recruté une brochure expliquant la politique de sécurité de l'entreprise en ce qui concerne le courrier électronique, les filtres existants et les pratiques exemplaires pour éviter le spam et s'en protéger. Le même type d'information devrait être disponible sur le site Web interne, et des mises à jour devraient être périodiquement adressées aux utilisateurs.

- **Petites et moyennes entreprises** : Les associations commerciales, les FAI et les éditeurs de logiciels de sécurité devraient fournir aux PME des informations spécifiques sur les pratiques de gestion de la sécurité, du matériel pédagogique, des logiciels en source libre, etc. Des exemples et de la documentation sont disponibles sur le site Web du Groupe de réflexion de l'OCDE à l'adresse www.oecd-antispam.org.

L'éducation des destinataires est aussi importante que celles des expéditeurs. Les autorités de réglementation et les associations professionnelles peuvent jouer un rôle important d'éducation des entreprises en diffusant des informations sur la façon dont elles peuvent communiquer avec leurs clients par message électronique, par exemple par courrier électronique, d'une manière qui respecte la législation nationale.

Les associations de **marketing direct** devraient informer leurs membres de la législation anti-spam en vigueur dans leur pays d'origine et dans le pays de destination des messages. Des pratiques exemplaires et des pages Web d'information sur le marketing en ligne devraient être élaborées et coordonnées au niveau international.

Élément VI. Partenariat pour la coopération

Toute stratégie anti-spam devrait être élaborée et mise en oeuvre dans le cadre de partenariats public-privé, avec la participation de représentants du public et du secteur privé. Les mesures anti-spam ne seront efficaces que si l'ensemble des acteurs sont associés à leur élaboration, les acceptent (en même temps que les effets indirects) et les jugent adaptées pour répondre à leurs besoins.

Les pratiques exemplaires recommandées, élaborées par les associations professionnelles avec la contribution des autorités publiques, devraient faire l'objet d'une large adoption. Ces pratiques exemplaires devraient être largement diffusées et mises en oeuvre. Elles devraient également être actualisées selon les besoins, de manière à prendre en compte l'évolution de la technologie et de l'environnement des services (voir également l'Élément III).

L'industrie et les autorités de justice devraient coopérer dans le contrôle du respect de la législation anti-spam. En particulier, les FAI et autres opérateurs de réseaux devraient être en contact avec les autorités pour signaler les cas possibles de spam, et ils devraient être autorisés à échanger avec ces mêmes organismes des informations sur les activités concernant le spam sur leur réseau.

Élément VII. Mesure du spam

Les pouvoirs publics et les acteurs du secteur privé devraient surveiller l'impact des mesures anti-spam, afin d'en évaluer l'efficacité. Les FAI, les autres opérateurs de réseaux et les organismes anti-spam nationaux devraient, dans toute la mesure du possible, échanger des informations et des données sur l'intensité et l'étendue des activités de spamming et leur évolution. Les méthodes de mesure devraient être détaillées et documentées, afin d'améliorer la lisibilité des résultats obtenus. Dans ce contexte, le MAAWG a développé son programme de métrologie du courrier électronique (Email Metrics). Le Groupe de réflexion se félicite de cette initiative et encourage sa poursuite et son développement.

Élément VIII. Coopération mondiale

Le Groupe de réflexion sur le spam recommande que la Boîte à outils et les pratiques exemplaires notées dans le présent document soient mises largement à la disposition des économies non membres tout autant que dans les pays de l'OCDE, et que les ressources qu'elles représentent soient rendues accessibles au plus grand nombre possible de personnes. Dans ce contexte, un site Web a été élaboré par le Groupe de réflexion, qui peut être consulté à l'adresse www.oecd-antispam.org. Afin que le site Web reste une ressource utile et à jour, les pays sont instamment invités à fournir régulièrement des contributions, de nouvelles ressources, ainsi que des informations sur leurs initiatives anti-spam nationales.

Les pays membres de l'OCDE devraient promouvoir et faciliter les activités anti-spam dans d'autres pays, à travers des partenariats – mécanismes bilatéraux ou multilatéraux, échange d'informations, etc. – pour aider à l'élaboration d'une législation anti-spam appropriée, épauler la mise en oeuvre de solutions techniques et faciliter la diffusion d'outils et de ressources didactiques.

INTRODUCTION

Le spam a un impact négatif sur l'économie du numérique et entraîne des coûts économiques et sociaux importants pour les pays de l'OCDE comme pour les autres économies. Face aux nouveaux problèmes qui pourraient se poser avec la convergence des technologies de la communication et l'émergence des télécommunications universelles et de l'Internet mobile, les pays membres de l'OCDE sont confrontés à la nécessité de trouver des solutions pour éliminer le spam. Pour relever ce défi, le Comité de la politique de l'information, de l'informatique et des communications (Comité PIIC) de l'OCDE, lors de sa réunion des 3 et 4 mars 2003, a décidé que des travaux prioritaires devaient être consacrés à cet important dossier, notant que le problème était d'ampleur mondiale. Le Comité de la politique à l'égard des consommateurs (CCP) a également exprimé son intérêt pour la poursuite de travaux sur ce thème dans le cadre de l'OCDE. Les problèmes liés au spam ont fait l'objet d'une première étude exploratoire dans un document de référence et dans le cadre d'un atelier sur le spam qui s'est tenu sous l'égide de la Commission européenne, à Bruxelles, en février 2004.[2]

Le spam a des conséquences sur plusieurs plans. Il pose ainsi des problèmes d'utilisation et de congestion des réseaux et des problèmes liés à l'Internet, des problèmes de respect de la vie privée et de sécurité des réseaux, et des problèmes de protection des consommateurs. Afin de mieux coordonner les travaux sur le spam et de parvenir plus rapidement à un consensus sur un cadre d'action pour la lutte contre les problèmes causés par ce phénomène, le Conseil de l'OCDE a décidé en juillet 2004 de créer un Groupe de réflexion transversal sur le spam. Ce Groupe de réflexion était invité à faire rapport aux comités CPC et PIIC d'ici juillet 2006.

L'objectif premier du Groupe de réflexion était de rassembler toutes les personnes chargées de coordonner les politiques de lutte contre le spam afin de préparer le plus efficacement possible les outils dont les pouvoirs publics avaient un besoin urgent pour lutter contre le spam, grâce à une approche plus large du problème et à l'expertise pluridisciplinaire de l'OCDE.

Le Groupe de réflexion avait pour mission d'étudier, de documenter et de faire connaître la gamme des stratégies anti-spam existantes et émergentes dans tous les secteurs. Sachant qu'il n'existe pas de remède miracle qui peut à lui seul venir à bout du spam, le Groupe de réflexion a élaboré une « Boîte à outils anti-spam » reposant sur le principe selon lequel il faut mobiliser de façon coordonnée plusieurs éléments différents pour favoriser le développement de stratégies et solutions de lutte contre le spam – techniques, réglementaires et d'application de la loi – et faciliter la coopération internationale face à ce problème. La Boîte à outils anti-spam de l'OCDE a donc pour but de rassembler une série cohérente de mesures complémentaires et d'autres initiatives (notamment coercitives). L'élaboration et la mise en oeuvre de la Boîte à outils s'appuient essentiellement sur les apports des parties prenantes dans les différents domaines concernés. Elle se compose de huit éléments interdépendants :

- Réglementation anti-spam.
- Coopération internationale pour la répression du spam
- Solutions anti-spam pilotées par le secteur privé
- Technologies anti-spam existantes et émergeantes
- Éducation et sensibilisation
- Partenariats de coopération contre le spam
- Mesure du spam
- Coopération mondiale (Ouverture)

Le Groupe de réflexion a rédigé des documents de référence sur plusieurs éléments de la Boîte à outils[3]. Le présent rapport final fait la synthèse des travaux menés par le Groupe de réflexion et de leurs conclusions. Il est complété par la recommandation du Conseil de l'OCDE relative à la coopération transfrontière dans l'application des législations contre le spam et par le site Web de l'OCDE sur la lutte contre le spam (www.oecd-antispam.org).

Les travaux du Groupe de réflexion ont déjà beaucoup contribué aux efforts de coopération pour lutter contre le spam. Le Groupe de réflexion a focalisé l'attention et les ressources internationales sur la question du spam, et les efforts concertés des gouvernements, de l'industrie et de la société civile ont certainement contribué à limiter ce problème. Une large diffusion et mise en oeuvre de la Boîte à outils peuvent continuer d'avoir un impact positif dans ce domaine.

Situation et évolution du spam

Fin 2004, on dénombrait au total dans le monde 380 millions d'internautes, dont environ 42 % disposaient d'un accès haut débit, en connexion permanente[4]. La plupart de ces internautes se trouvent dans les pays de l'OCDE, où le nombre d'abonnés aux services haut débit a augmenté de 118 millions à la fin de 2004 à 137 millions à la mi-2005.[5] Cependant, le développement des réseaux des TIC, en même temps qu'il crée tout un éventail de nouvelles possibilités, pose de nouveaux problèmes.

En particulier, comme le soulignent les *Lignes directrices de l'OCDE régissant la sécurité des systèmes et réseaux d'information : Vers une culture de la sécurité*, la fiabilité et l'efficacité des plateformes, des applications et des services, ainsi que la confiance des internautes dans leur utilisation revêtent une importance primordiale pour la concrétisation des avantages attendus des TIC en matière de

développement économique et social[6]. Cependant, la fiabilité du courrier électronique et des autres outils de communication électronique, et par conséquent la confiance des internautes dans ces technologies, sont aujourd'hui menacées par la multiplication de courriels non sollicités et indésirables (communément appelés « spam »), qui engorgent l'Internet et causent de graves préjudices aux personnes et aux entreprises.

Le phénomène du spam, qui se manifestait au début par des messages publicitaires pour des produits ou services commerciaux, a connu une croissance exponentielle, atteignant son point d'inflexion en 2004. En outre, les simples messages publicitaires ont été remplacés par des messages potentiellement dangereux, et non plus seulement importuns. Le spam est aujourd'hui de nature trompeuse, il peut perturber le fonctionnement du réseau et sert de vecteur de propagation des virus, ce qui sape la confiance des consommateurs, laquelle est un préalable indispensable à la société de l'information et au succès du commerce électronique. Cette évolution (voir la figure 1) peut se résumer à trois grands changements :

- Premièrement, les spammeurs ont adopté de nouvelles méthodes techniques et sociales pour dissimuler l'origine des messages qu'ils envoient, ce qui leur permet de contourner les mesures prises à leur encontre par les autorités chargées de l'application des lois, les FAI et les internautes. Ils ont ainsi recours notamment à la falsification de courriels, à l'utilisation de relais et de serveurs mandataires ouverts et, de plus en plus, à des réseaux d'ordinateurs zombies, ou « *botnets* ».

- Deuxièmement, ces derniers mois, le spam est devenu un vecteur pour la propagation de diverses menaces, facilitant la diffusion de virus et d'autres logiciels malveillants ou servant de support d'opérations frauduleuses comme l'hameçonnage[7].

- Troisièmement, naguère limité au courrier électronique, le spam gagne maintenant de nouvelles technologies de communication – notamment les appareils mobiles comme les assistants numériques personnels (ANP) et les téléphones intelligents, qui sont de plus en plus utilisés pour accéder aux courriels. En outre, le spam a envahi les services de messagerie instantanée, les blogs et menace le bon fonctionnement des applications de la téléphonie Internet (voir la figure ci-après).

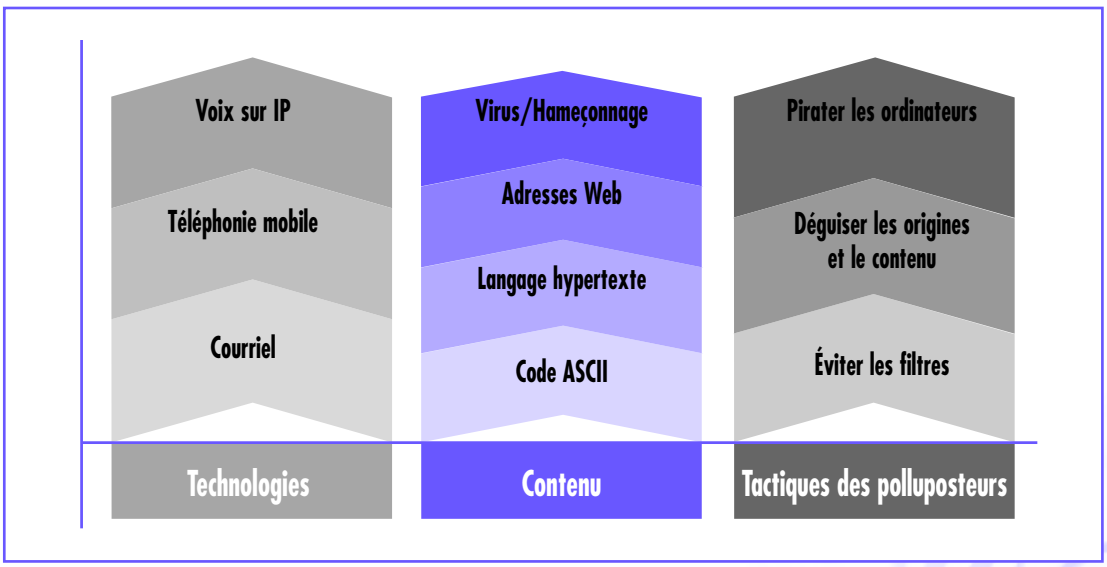


Figure 1. Évolution du Spam

- Du fait des différences d'approches juridiques d'un pays à l'autre, il n'existe pas de définition internationalement reconnue du spam. Pour cette raison, le Groupe de réflexion n'a pas entrepris de définir le spam. Il existe toutefois des caractéristiques communes que différents pays retiennent dans leurs définitions du spam :

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

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

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

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

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

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

En conclusion, on s'accorde sur un point : le spam représente une menace pour l'utilisation de l'Internet comme moyen de communication efficace et fiable, et pour l'évolution de la cyberéconomie dans son ensemble, d'où la nécessité d'une plus étroite coopération de toutes les parties prenantes en vue de trouver des solutions communes à ce problème.

Pourquoi le spam ? Comment s'articule ce phénomène ?

Pourquoi le spam constitue-t-il une telle menace ? Comme le coût d'envoi des courriels est extrêmement bas et n'augmente pas en fonction du nombre de messages envoyés, les spammeurs ont intérêt à envoyer autant d'exemplaires de leur message que possible. C'est ainsi que plusieurs milliards de spams sont envoyés chaque jour. Ce n'est donc pas le spammeur, mais le destinataire final qui supporte le coût du spam.

On retrouve les mêmes raisons à l'origine d'autres types de spams qui visent ou pourraient viser d'autres technologies et applications. La possibilité qu'offre la téléphonie Internet (voix sur IP) d'appeler n'importe où dans le monde pratiquement sans frais peut être exploitée par les spammeurs, qui seront en mesure d'envoyer des messages vocaux de marketing non sollicités sans qu'il leur en coûte un sou. Les nouveaux instruments comme les blogs, qui permettent aux internautes d'exprimer leurs idées et opinions sur le Web, sont déjà mis à profit par les spammeurs, qui affichent sur ces pages des quantités de commentaires non sollicités et hors de propos, engorgeant ainsi les sites et rendant toute discussion ou tout échange d'idées impossible. En ce qui concerne les téléphones mobiles, la situation a été jusqu'à maintenant moins préoccupante, du fait que le coût des SMS ou MMS, bien que bas, décourage le spam massif.
On trouvera ci-après une brève récapitulation des différents types de spam et de leurs effets.

Le spam dans le courrier électronique (« pourriel »)

Pour comprendre pourquoi le pourriel est le fléau qu'on connaît et comment fonctionnent les solutions possibles, il faut saisir le fonctionnement du courrier électronique sur l'Internet. En gros, le mécanisme standard de l'Internet qui est habituellement utilisé pour relayer les courriels est le protocole de transfert de courrier simple (protocole SMTP), lequel « soumet » au réseau le message à envoyer, amorçant ainsi un « dialogue en cinq étapes » qui se déroulera entre les différents ordinateurs concernés. L'ordinateur qui soumet le message est en général appelé « client SMTP ».

Selon le protocole SMTP, tous les courriels sont pourvus d'une enveloppe et d'un en-tête[8]. L'information d'enveloppe est destinée au système effectuant le transfert du message et n'est en général pas vue par l'utilisateur final. Elle fait l'objet d'échanges au cours du dialogue en cinq étapes ouvert par le protocole SMTP. Théoriquement, au moment de la transmission, l'information d'enveloppe est mémorisée dans les « en-tête » que le destinataire peut voir et qui occupent la partie supérieure du message, au-dessus du corps du texte.

Dans son état actuel, le processus d'authentification SMTP présente deux failles que les spammeurs peuvent exploiter[9] :

- aucune authentification n'est requise, de sorte qu'il est possible de dissimuler son identité, comme le font les spammeurs ;

- n'importe quelle information figurant dans un courriel (dans l'enveloppe que le destinataire humain ne voit pas, comme dans l'en-tête qu'il peut voir) peut être fausse.

L'une des conséquences de cette vulnérabilité du protocole SMTP est la falsification ou l'usurpation de courriel (« *spoofing* »), qui consiste à altérer l'en-tête et/ou le contenu d'un courriel afin de tromper le destinataire quant à l'objet du message ou de lui faire croire qu'il provient d'un correspondant digne de confiance (voir aussi le paragraphe ci-après concernant l'hameçonnage).

En outre, le coût de l'envoi du message est assumé à la fois par l'expéditeur et par le destinataire.

Le spam mobile

On entend en général par « spam mobile » les communications non sollicitées par SMS ou MMS. À ce jour, le spam mobile peut prendre les formes suivantes :

- Un SMS ou MMS annonçant un service ou un produit commercial ;

- Un SMS ou MMS sollicitant une réponse à un service kiosque ou vers un numéro à tarif international. Ces types de messages sont en général de nature trompeuse ou frauduleuse et relèvent de l'escroquerie.

Il importe de noter que s'il est désormais courant, avec le développement des services de troisième génération, de recevoir des courriels sur des appareils portables, une distinction est à faire entre les services mobiles spécifiques – tels que les SMS, qui sont des messages envoyés et reçus dans le cadre des réseaux de téléphonie mobile – et les autres services, comme le courrier électronique, qui ne sont pas propres à la téléphonie mobile mais émanent de l'Internet et sont le produit de la convergence des télécommunications fixes et mobiles.

Si la diffusion des pourriels sur l'Internet est devenu un fléau pour les internautes, le spam mobile, pour le moment, ne pose pas un problème de même ampleur, en raison essentiellement de l'environnement commercial et des modalités d'utilisation des services propres à la téléphonie mobile, qui offrent par définition une meilleure protection contre le spam, notamment grâce aux caractéristiques et mesures suivantes :

- Mesures économiques : principes de la tarification de l'appelant, blocage des paiements pour services kiosque proposés de façon frauduleuse, révision des accords relatifs à l'itinérance pour la couverture des SMS et MMS.

- Outils à la disposition de l'internaute : modalités de notification de spam ; mécanismes de désinscription.

- Initiatives techniques : lorsque la loi l'autorise, filtrage réseau ou analyse de trafic visant à détecter une activité inhabituelle couramment associée au spam mobile.

Dans la plupart des pays, il existe des lois qui s'appliquent aux SMS et MMS non sollicités, et les opérateurs ont en général mis en place des procédures pour détecter les messages frauduleux et y faire obstacle, notamment, indépendamment des mesures énumérées ci-dessus, par des activités de coopération avec les autorités publiques compétentes. Cependant, lorsque le spam mobile circule à travers différents réseaux ou à l'échelle internationale, il est parfois plus difficile à combattre. Des associations professionnelles, comme l'Association GSM (GSMA)[10], ont produit de l'information et recommandé des procédures pour aider les opérateurs à agir de façon concertée pour cerner le problème et y trouver une solution, et ont créé des groupes de travail internationaux sur le spam mobile qui facilitent la coopération internationale et la mise en commun des meilleures pratiques entre les opérateurs. L'élaboration d'un code de conduite à l'égard du spam mobile est également prévue.

Le spam sur la VoIP (« spit ») et sur les applications IP multimédias ?

Le spam ne se limite pas aux courriels, mais parasite également les nouvelles technologies qui font leur apparition, comme la téléphonie Internet (VoIP). Parmi les problèmes recensés, il faut désormais compter ceux qui sont habituellement associés aux réseaux IP, ainsi que des menaces plus insidieuses telles que la diffusion d'information trompeuse, l'écoute clandestine, les attaques entraînant un refus de service[11], les injections de paquets ou les messages indésirables ciblant spécifiquement la téléphonie Internet (« *spit* »). Ce type de spam s'explique principalement par la possibilité qu'offre la VoIP d'envoyer des messages vocaux à un coût très bas, ce qui pourrait conduire à la situation que l'on connaît déjà avec le courrier électronique : des quantités considérables de messages vocaux indésirables circulant sur la planète en quelques secondes et causant des problèmes analogues à ceux mentionnés plus haut.

La téléphonie Internet n'est que la première innovation d'une longue série de nouvelles applications et services que les réseaux de nouvelle génération mettront à notre disposition. De nouveaux services multimédias basés sur le SIP[12] et l'IMS[13], par exemple, sont en préparation. Ils permettront la messagerie instantanée et l'interphonie sur mobiles (Push To Talk over Cellular ou PoC), la partage de fichiers vidéo et les jeux multijoueurs. Encore là, il importera de prendre en compte l'aspect sécurité afin de protéger les applications multimédias IP contre de nouvelles formes de spam et toute autre nouvelle menace de façon générale.

Le spam ciblant les moteurs de recherche

Dans un cyberespace en expansion rapide, où l'on dénombre déjà quelque 83 millions de noms de domaine et 75 millions de sites Web enregistrés[14], le moteur de recherche fait partie des outils courants de l'internaute, qui l'utilise pour trouver sur le Web les pages et les contenus qui l'intéressent.

Cependant, comme cela s'est passé avec le courrier électronique, les nouveaux services et applications deviennent également très vite de nouvelles possibilités de fraude. Ainsi, le spam dirigé vers les moteurs de recherche tire parti du mécanisme de recherche pour imposer des pages Web spécifiques (à caractère pornographique, pour vendre du Viagra ou des services financiers, etc.) en tête des réponses que donnera le moteur. Les spammeurs disposent à cette fin de divers stratagèmes, plus ou moins complexes. Le « spam de recherche » consiste en pages produites automatiquement pour figurer dans les moteurs de recherche afin d'attirer du trafic (et en bout de ligne accroître les recettes) ; il arrive aussi que les webmestres dissimulent sur leur page Web des liens invisibles vers les sites d'annonceurs afin de rehausser le rang de l'annonceur dans la page, à l'insu de tous[15].

Le spam visant les blogs, ou « splog »

Une autre tactique à laquelle ont recours les spammeurs pour annoncer leurs sites Web consiste à utiliser des *bots* pour insérer des liens sur les pages commentaires des blogs. Parfois même, c'est une combinaison de spams et de blogs (les « splogs ») qui est composée de façon aléatoire à l'aide de programmes automatisés à partir de mots clés dont les occurrences sont importantes dans les moteurs de recherche. Ainsi, en octobre 2005, l'hébergeur de blogs « *Blogger* » a été submergé par une avalanche de 13 000 splogs créés en une seule semaine. Les moteurs de recherche comme Google et Yahoo ! s'efforcent d'affiner leurs paramètres de façon à exclure ces types de pages de leurs résultats[16].

La montée de phénomène porte atteinte à la fonctionnalité des blogs et aggrave le problème de la fiabilité de l'information sur l'Internet. Les blogs – instrument révolutionnaire qui permet à tous les internautes de s'exprimer et de confronter leurs points de vue sur le Web – risquent aujourd'hui d'être parasités par des « commentaires » indésirables, au point d'en devenir inutilisables.

Spam et hameçonnage

Le terme « hameçonnage » (*phishing*) désigne une pratique qui consiste à usurper une cyberidentité, par exemple en envoyant des courriels présentés comme provenant de sociétés établies et légitimes, pour tromper les destinataires et leur faire divulguer des données financières personnelles (numéro de carte de crédit, mot de passe). Fréquemment, ces messages ou les sites Web vers lesquels ils renvoient tentent d'installer sur l'ordinateur des codes malveillants[17].

Ce terme a été judicieusement choisi par les informaticiens à la fin des années 90 lorsque le phénomène qu'il désigne a fait son apparition. En effet, dans le hameçonnage, le « hameçonneur » se sert du courriel qu'il envoie comme « leurre » pour attirer l'internaute en plein cyberespace et lui faire divulguer de l'information sensible.

Le vecteur du hameçonnage est le courriel, expédié à des millions d'internautes. Ces dernières années, les attaques par hameçonnage se sont multipliées, tout en devenant plus sournoises[18], et les spammeurs élaborent avec le plus grand soin des messages grâce auxquels ils se font passer pour des institutions financières ou organisations connues et dignes de confiance. Les hameçonneurs ont recours aux techniques du spam pour donner à leurs courriels l'apparence de ceux émanant des sociétés visées ; ils peuvent facilement copier le logo et l'information figurant sur les sites de celles-ci et en utiliser le texte et le graphisme.[19] Les messages-hameçons sont aussi adaptés aux différents pays (langue, noms des banques et opérateurs nationaux, etc.).

Afin d'éviter d'être détectés, les hameçonneurs mènent en général leurs attaques sur de très courtes périodes[20], puis plient bagages. Pour la même raison, ils doivent faire preuve d'un grand dynamisme. Ils exploitent en général les faiblesses des logiciels des serveurs et des systèmes d'exploitation pour installer leurs contenus et doivent être capables de passer rapidement et facilement d'un serveur à l'autre pour brouiller l'origine de l'attaque ou si un site compromis est découvert et supprimé.

L'hameçonneur utilise l'information qu'il obtient pour accéder à des comptes bancaires et en retirer de l'argent ou pour ouvrir de nouveaux comptes bancaires ou de carte de crédit en usurpant l'identité de sa victime, à laquelle il cause un grave préjudice financier. Les techniques d'hameçonnage ont été utilisées récemment dans des opérations d'espionnage industriel et d'extorsion de données sensibles (voir encadré 1).

Encadré 1. L'harponnage ("*Spear-Phishing*")

Une nouvelle forme, plus ciblée, d'hameçonnage a fait son apparition au cours des derniers mois, suscitant une vive inquiétude dans le monde de l'internautisme. L' « harponnage » consiste à envoyer un message non plus à des millions d'internautes mais à un petit groupe – par exemple, une société ou un service public. La cible est choisie avec soin. Le faux courriel est personnalisé et destiné expressément aux personnes entretenant une relation établie avec l'expéditeur dont l'identité est usurpée, ce qui rend l'attaque plus difficile à détecter et à neutraliser. L'harponnage s'apparente à l' « ingénierie sociale » — une pratique qui consiste à obtenir de l'information confidentielle en manipulant des utilisateurs légitimes – qui sert notamment dans les opérations d'espionnage industriel. Le destinataire du courriel frauduleux révèle l'information et les mots de passe qui permettront à l'escroc d'accéder à des zones sécurisées du réseau interne de l'entité visée et d'éventuellement dérober des actifs intellectuels ou d'autres documents ou données sensibles.[21]

Quel est le coût du spam ?

Le spam impose aux internautes un coût direct lié au temps perdu à consulter, identifier et effacer les messages non souhaités, et il suscite des inquiétudes quant à la fiabilité des communications et au contenu des messages. Le spam fait obstacle aux nouvelles possibilités offertes par les connexions haut débit « permanentes » à l'Internet : messages trompeurs et frauduleux, contenu de mauvais goût, biens et services de nature douteuse proposés à la vente.

Pour les utilisations professionnelles et commerciales, le spam est synonyme de perte de productivité, et impose des coûts directs en accroissant le besoin d'assistance technique et de solutions logicielles comme les filtres. Le spam représente aussi un coût pour la société en général, en ce qu'il porte atteinte à la fiabilité du courriel en tant qu'outil de communication (des messages « légitimes » peuvent être bloqués par des filtres ou passer inaperçus parmi un trop grand nombre de messages non sollicités) et menace la sécurité des réseaux internes des entreprises.

Les autres grandes victimes du spam sont les fournisseurs d'accès Internet (FAI) et autres opérateurs de réseaux, qui doivent acheminer les courriels. La mise en oeuvre de solutions anti-spam – notamment de filtres – entraîne des coûts supplémentaires, notamment en termes d'expansion de l'infrastructure pour faire face au volume de messages, et un besoin accru d'assistance technique. De plus, lorsqu'ils sont utilisés par des spammeurs ou que des ordinateurs de leurs réseaux sont détournés, les FAI sont exposés à des risques supplémentaires, leur réputation est menacée et ils peuvent mettre être mis en quarantaine par leurs pairs. Une grande partie de ces coûts sera à terme supportée par le consommateur, qui paiera l'accès plus cher ou en aura moins pour son argent.

Il est difficile de calculer le coût véritable du spam, car certains des dommages causés par cette pratique sont indirects et parce que la question n'est pas encore tranchée de savoir s'il faut chiffrer le coût du temps que le spam fait perdre à ses victimes et, le cas échéant, de quelle façon. En outre, le caractère frauduleux du spam ou les logiciels malveillants dont il peut être porteur sont susceptibles de causer de graves préjudices financiers aux internautes et aux sociétés (voir par exemple les paragraphes sur le spam et l'hameçonnage).

Les messages non sollicités sont générateurs de problèmes et de coûts supplémentaires pour les pays de l'OCDE, mais aussi pour les pays en développement et les pays les moins avancés. Ces derniers ont une infrastructure Internet moins développée et disposent souvent de relativement peu de bande passante. Les internautes des pays en développement accèdent souvent à l'Internet par des liaisons commutées ou par des points d'accès collectif comme les cybercafés, où l'utilisateur paie en fonction du temps passé en ligne. Dans ces conditions, le spam accapare à l'évidence une part importante de ressources qui sont déjà limitées, alourdit la facture de l'accès à l'Internet et porte atteinte à la qualité du service.[22]

La suite du présent document donne un aperçu des travaux du Groupe de réflexion consacrés à chacun des éléments de la Boîte à outils anti-spam.

ÉLÉMENT I – RÉGLEMENTATION ANTI-SPAM

Considérations générales concernant la réglementation anti-spam

Depuis quelques années, de nombreux pays — essentiellement ceux de la zone OCDE — se dotent d'une législation spécifique pour circonscrire le problème grandissant du spam. Les travaux du Groupe de réflexion sur la réglementation anti-spam mettent en évidence les principaux éléments que peuvent prendre en considération les pays pour mettre en œuvre d'une législation efficace contre le spam. Le travail sur cet élément est inspiré du rapport « Réglementation anti-spam ».[23]

Le spam est un thème « transversal » c'est-à-dire qu'il touche à différents aspects : services de télécommunications, protection des consommateurs et vie privée, aux niveaux national et transnational. Par conséquent, le cadre législatif qui a été mis en place est complexe, particulièrement en raison des différentes instances nationales publiques et privées qui s'occupe de la répression, et de la nécessité de couvrir les différentes catégories de spam.

Avant de commencer cette section, il importe de noter que, du fait de la grande variété des environnements juridiques, politiques et culturels, il n'y a pas d'approche uniforme globale du spam ou de définition commune du spam acceptée au niveau international. Pour cette raison, la Boîte à outils se garde d'être l'expression d'une seule de ces approches, mais a pour but de mettre en évidence des points de décisions qui doivent être discutés dans l'élaboration de la législation de lutte contre le spam et d'examiner les questions de politique publique qu'elles posent.[24] Dans ce rapport, le terme de spam renvoie aux messages électroniques qui sont considérés comme illégaux dans leur législation nationale.

Les mesures prises pour empêcher le spam sont conçues de manière à répondre à un certain nombre de finalités et d'objectifs de politique publique :

- **Préserver les bienfaits des communications électroniques** en renforçant la confiance des utilisateurs dans les systèmes de messagerie et en optimisant la disponibilité, la fiabilité et le coût des services. Le niveau du spam a maintenant atteint un point où il ébranle sérieusement la confiance des utilisateurs dans l'utilisation du courrier électronique et d'autres supports de messagerie, et où il pénalise la performance des réseaux mondiaux de communication.

- **Interdire et sanctionner l'acte d'envoyer du spam, tel que défini par la législation nationale.** La législation à elle seule ne pourra empêcher les candidats spammeurs de se servir de cette technique de marketing, mais les lois et réglementations peuvent avoir un impact par leur effet dissuasif en sanctionnant les individus et organisations qui choisissent de recourir au spam. La force de la législation dépendra toutefois de la gravité des sanctions et du caractère inéluctable de leur application.

- **Réduire le volume de spam.** Les activités doivent être ciblées à différents niveaux : pour empêcher l'envoi du spam, pour réduire le volume de spam qui transite sur les réseaux, pour réduire le nombre de messages de spam reçus par les utilisateurs. Différents types de dispositions peuvent être prises pour atteindre ces trois objectifs : (1) interdire les techniques et les logiciels de collecte automatique d'adresses ; encourager les FAI à mettre en oeuvre des Conditions générales d'utilisation ; 2) permettre aux FAI de bloquer les utilisateurs qui envoient du spam ; (3) promouvoir l'usage des filtres.

En poursuivant ces objectifs, le législateur doit prendre en compte quatre principes généraux :

- **Orientation de la politique publique** : La législation doit refléter une orientation claire de la politique publique. Les tendances et les objectifs principaux de la politique nationale et internationale de lutte contre le spam doivent être définis à un stade précoce et doivent régir l'ensemble de la stratégie gouvernementale (y compris les initiatives de répression et de sensibilisation, par exemple) ;

- **Simplicité de la réglementation** : La législation doit être concise et simple.

- **Effectivité de l'application** : L'application effective de la législation est un point fondamental ; si on n'y veille pas, la législation aussi bien conçue soit-elle, ne sert à rien. Pour cette raison, il est important de mettre en place un régime de sanctions effectif et des modalités adéquates pour l'administration des preuves. De plus, il faut doter les autorités d'application de pouvoirs et de ressources adéquats (voir l'Élément II).

- **Relations internationales** : Le spam étant un problème international, la législation doit permettre des relations adéquates au niveau international et veiller à ce que les autorités nationales puissent coopérer et échanger des renseignements avec des autorités étrangères dans le cadre des enquêtes (voir l'Élément II).

Liste des questions à prendre en compte

Pour concevoir une approche réglementaire qui prenne en compte les objectifs et les principes énoncés précédemment de la politique de lutte contre le spam, il faut répondre à une série de questions :

- ✓ Nature du spam et objectifs de la législation ?

- ✓ Élément technique : description technologie par technologie, ou approche technologiquement neutre ?

- ✓ Consentement : explicite, supposé, implicite ? A qui incombe la charge de la preuve ?
- ✓ Élément commercial : objectif marketing / avantage financier ? Ne faut-il viser que les messages commerciaux ?
- ✓ Informations sur l'expéditeur : quelles informations doivent être incluses dans un message ?
- ✓ Envoi en masse – comment définit-on « en masse » ?
- ✓ Considérations liées à la vie privée : spam et utilisation abusive de données personnelles (adresse de courrier électronique, etc.)
- ✓ Contenu : la législation existante est-elle adaptée face aux contenus trompeurs ou frauduleux ?
- ✓ Éléments accessoires : la réponse réglementaire doit-elle également viser les activités accessoires à l'envoi de spam ?
- ✓ Critères supplémentaires: collecte d'adresses, attaques par dictionnaire, étiquetage ?

Nous allons examiner plus en détail les considérations qui doivent être prises en compte pour répondre à ces questions.

Approche réglementaire de la lutte anti-spam : éléments

Services concernés

Services concernés	• Message électronique : cibler un support de messagerie particulier (courriel) ou inclure les « messages électroniques » en général, c'est-à-dire aussi la messagerie instantanée, les SMS, MMS, les courriels sur mobiles et le spam sur VoIP ?
→ Élément technique : description technologie par technologie ou approche technologiquement neutre ?	

La définition légale du spam peut être limitée à un support particulier de messagerie, ou s'en tenir à une approche technologiquement neutre et énoncer un certain nombre de principes qui s'appliquent plus largement.

Si on définit de manière limitative le champ d'application des lois, on est amené à réactualiser la législation périodiquement face à de nouvelles menaces et pour protéger des technologies et applications émergentes. Mais même avec une approche technologiquement neutre, il est souhaitable d'évaluer quels supports de messagerie sont visés par des utilisations abusives ou sont fortement susceptibles de l'être un jour, et de veiller à ce que la législation y apporte une réponse adéquate.

L'une des raisons de cette approche législative est d'englober tous les moyens de communication dans lesquels le coût marginal d'un envoi est proche de zéro pour l'expéditeur, mais qui peuvent imposer une charge disproportionnée (frais, perte de temps, etc.) aux destinataires et au réseau dans son ensemble.[25]

Bien que pour de nombreux pays, le problème le plus urgent soit le spam par courriel, les pays dans lesquels la téléphonie mobile de troisième génération se développe largement sont de plus en plus préoccupés par le spam sur SMS et MMS. Dans certains pays, les spammeurs ont adoptés ces nouveaux modes de communication et ont aussi jeté leur dévolu sur toute une gamme de moyens de communication comme les wikis,[26] les blogs, et les communications sans fil à courte portée (dispositifs Bluetooth et réseaux sans fil).

En élaborant sa stratégie réglementaire anti-spam, le responsable public doit garder à l'esprit qu'avec la convergence des formats de messagerie permise par l'émergence de nouvelles technologies et applications comme la 3G, la 4G et la téléphonie IP (VoIP), de nouveaux supports de messagerie peuvent voir le jour de manière imprévisible. La nouvelle législation doit donc être suffisamment adaptable pour que les technologies de communication soient couvertes si elles se voient touchées par de nouvelles formes de spam. Dans le même temps, il ne faut pas oublier que toute action publique ou tout régime réglementaire imposé sur une technologie de messagerie a forcément un impact non seulement sur les messages de spam contre lesquels elle entend lutter mais aussi sur les envois légitimes.

Nature du message

Finalité commerciale → Nature du spam et objectifs de la législation ?	• Voir si la législation ne devrait viser que les messages commerciaux et transactionnels, ou si elle devrait aussi prendre en compte certains contenus non commerciaux, tels que les messages à contenu politique ou religieux

Une proportion importante du spam a pour but de faire un bénéfice financier en vendant des biens et services, ou par une action frauduleuse. Pour cette raison, de nombreuses définitions législatives du spam insistent sur la nature commerciale des messages. Certes en visant spécifiquement les messages commerciaux, on est assuré que la lutte contre le spam n'aboutit pas à restreindre les messages à caractère personnel, politique, religieux ou idéologique, et ne porte pas atteinte à la liberté de parole ou d'expression, mais il faut noter que tous les messages de spam n'ont pas un caractère commercial. En limitant la portée de la législation anti-spam aux seuls messages commerciaux, on peut passer à côté de spams particulièrement nocifs. Ainsi, un million de messages faisant la promotion d'une idée politique ou religieuse peuvent être aussi importuns et horripilants qu'un million de messages vantant les mérites de pilules aux plantes.

Aux États-Unis, la loi CAN-SPAM ne couvre que les messages électroniques à caractère commercial. Elle définit comme commercial tout courriel qui a comme principal objet de faire la publicité ou la promotion d'un produit ou d'un service commercial. Dans l'Union européenne, la Directive « Vie privée et communications électroniques » porte uniquement sur les messages envoyés « à des fins de prospection directe », alors que l'Australie, après avoir donné une définition du courriel commercial, précise que certains types de messages — notamment ceux qui sont envoyés par les organes gouvernementaux, des organisations religieuses ou des établissements d'enseignement à leurs anciens élèves — ne sont pas soumis aux restrictions envisagées par la section 16 de la loi (« les courriels commerciaux non sollicités ne doivent pas être envoyés »).

Consentement

L'un des principes fondamentaux qui sous-tendent de nombreux régimes réglementaires anti-spam est que les courriels à caractère commercial ne peuvent être adressés à des personnes ou à des organisations que si elles ont consenti à ces envois. Un certain nombre de cadres conceptuels sont utilisés en relation avec le consentement, notamment les modèles « opt-in » (consentement préalable) et « opt-out » (droit de refus), selon que l'activité est conditionnée par l'autorisation du destinataire (d'où le terme marketing autorisé) préalablement à la réception de message électronique – « opt in » – ou postérieurement à cette réception – « opt out » – ainsi que des dispositions permettant de considérer le consentement comme supposé en cas de relation commerciale préexistante.

Le concept de consentement, explicitement défini et prévu dans la législation, peut aussi être intégré dans l'application des régimes en matière de respect de la vie privée et des données personnelles, avec parfois une règle prévoyant que si elle n'a pas donné son consentement, une personne ne peut pas être contactée et les informations la concernant (notamment son adresse de courriel) ne peuvent pas être négociées ou échangées. Le fond du problème est le degré de consentement ou d'autorisation que l'on souhaite exiger dans la législation ou la réglementation dans les circonstances en question.

Le débat public au sujet du consentement tourne généralement autour de la dichotomie « opt-in » (consentement préalable) / « opt-out » (droit de refus). Si ce débat a pu être pertinent naguère, il apparaît maintenant dépassé car les approches en matière de réglementation du spam prévoient des méthodes plus complexes et plus subtiles distinguant entre consentement explicite, consentement induit, consentement supposé ou diverses combinaisons de ces nuances.[27] Nous allons examiner ces concepts plus en détail. Il importe de se rappeler que le consentement n'est qu'un élément de la définition ou de l'approche du spam. De fait, la plupart du spam reçu par les utilisateurs est en infraction avec plusieurs dispositions légales : informations d'en-tête masquées ou falsifiées, absence d'adresse de désabonnement, et souvent contenu trompeur ou porteur de virus.

Consentement : explicite, express, implicite, supposé ? Sur qui repose la charge de la preuve ?	Description	Avantages	Inconvénients
Consentement explicite	Forme de consentement dans lequel un individu ou une organisation a activement donné son consentement à une action ou activité particulière	– Protège la vie privée des utilisateurs en leur laissant davantage de contrôle sur leurs données personnelles ; – Peut produire des taux de réponse beaucoup plus élevés pour les expéditeurs de marketing légitimes car les messages proviennent de sources connues ou de confiance, et ils sont donc plus susceptibles d'être lus et d'être pertinents pour le destinataire. – C'est à l'expéditeur du message qu'il incombe de prouver que le consentement a été donné, non à son destinataire de prouver le contraire.	– Difficulté à garder la trace des consentements reçus. L'absence de traces peut diminuer considérablement la base potentielle de destinataires qui peuvent être visés par des messages par ailleurs légitimes. – Restriction de la « liberté de parole commerciale ». – Peut conduire à gaspiller des ressources dans des cas où il n'y a pas préjudice contre les consommateurs.
Consentement induit et implicite	Régime dans lequel le consentement peut généralement être induit d'après le comportement et/ou les autres relations commerciales du destinataire.	– Plus grande flexibilité	– Il peut être difficile de déterminer si un message donné peut être relié à une « relation commerciale » existante.
Consentement supposé	Il y a présomption de consentement jusqu'à ce que le consentement soit retiré, par exemple sous forme de « désabonnement » ou en inscrivant son adresse électronique sur liste rouge.	– Moins contraignant pour le fonctionnement du commerce électronique ; minimise le risque d'entrave dommageable à des envois légitimes. – Pas d'atteinte à la liberté de choix des bénéficiaires qui souhaitent recevoir des messages commerciaux.	– La charge (effort et coût) est transférée sur le consommateur. – Pour se désabonner, il faut ouvrir le message électronique et y répondre, ce qui est contraire aux bonnes pratiques en matière de sécurité informatique sauf lorsque le message provient d'une source connue et de confiance. – Il arrive souvent que les liens de désabonnement ne soient pas opérants. – La charge de la preuve repose sur le destinataire du message.
Approches hybrides en matière de consentement	Depuis peu certaines législations anti-spam reflètent une approche « mixte » ou situationnelle en matière de consentement.		

Le fait de savoir si l'expéditeur a ou non eu le consentement du destinataire pour envoyer le message peut être important pour limiter les pratiques de vente directe trop offensives, pour sanctionner les sociétés mal informées ou qui n'ont pas tenu compte de la législation anti-spam, et d'une manière générale pour protéger les consommateurs contre la publicité non sollicitée qui peut devenir, à mesure que de nouvelles technologies apparaissent, particulièrement envahissante. De plus, avec les règles de l' « opt-in », la charge de la preuve incombe à l'expéditeur, qui devra démontrer qu'il a obtenu le consentement préalable du destinataire, ou qu'il avait une relation commerciale antérieure avec l'intéressé. Si l'expéditeur est un annonceur légitime qui contrevient uniquement aux impératifs de l' « opt-in », il sera plus facile pour l'autorité publique ou privée d'intervenir, car l'expéditeur est connu, il peut être contacté facilement et il est généralement désireux de se mettre en conformité. Il convient de hiérarchiser les interventions afin d'affecter les ressources à la sanction des catégories de spam les plus nuisibles.

Retrait du consentement ou « désabonnement »

Adresse de désabonnement ➔ Le destinataire de messages électroniques doit toujours être en mesure de radier son adresse de la liste des destinataires et de demander l'arrêt des envois.	• Dans presque toutes les législations actuellement en place, les messages doivent comprendre **une adresse de réponse valide** (ou un numéro) afin que le destinataire puisse se désabonner facilement et sans coût supplémentaire. Dans certains cas, une adresse postale doit également être fournie. • L'expéditeur dispose d'une période donnée (par exemple 10 jours) pour obtempérer et mettre fin aux envois. • Toute transmission de messages effectuée après l' « opt out » est sanctionnée.

La possibilité pour le destinataire de retirer son consentement, souvent au moyen d'un « dispositif de désabonnement » est généralement un élément fondamental de la législation anti-spam car les utilisateurs et les consommateurs peuvent ne pas ou ne plus vouloir recevoir de messages d'un expéditeur donné. Pour leur permettre se désabonner, il faut que l'expéditeur indique une adresse de désabonnement que le destinataire peut contacter sans bourse délier. De plus, la loi doit prévoir un délai pour permettre à l'expéditeur de satisfaire la demande de radiation. Tout message envoyé après l'expiration de ce délai sera considéré comme du spam.

La législation australienne stipule que tout message électronique commercial doit contenir un dispositif fonctionnel de désabonnement, c'est-à-dire une adresse à laquelle le destinateur peut envoyer un message de désabonnement. Ces dispositifs doivent être utilisables facilement et instantanément par l'utilisateur. Des dispositions équivalentes sont incluses dans la Directive de l'UE et dans la loi CAN SPAM aux États-Unis.

Cette disposition a pour but de donner à l'utilisateur la possibilité de mettre un terme aux envois de messages ; toutefois, concrètement, son application pose quelques problèmes, notamment lorsque l'adresse fournie pour la désinscription est fausse, ou si la volonté de radiation n'est pas respectée par l'expéditeur. Dans ce dernier cas il se peut que le destinataire, en répondant à ce pourriel, ne fasse que confirmer que son adresse est active, ce qui risque plutôt de susciter un regain de messages de spam dans sa boîte de réception. Pour cette raison, s'il est essentiel de se doter des outils législatifs et de police adéquats, les pouvoirs publics doivent aussi informer les consommateurs des risques liés au courrier électronique et les aider à reconnaître un message de spam et à le traiter en conséquence.

Informations sur l'origine du message

Informations d'en-tête et identificateur de l'expéditeur → L'un des problèmes de la réglementation des activités de spam et de l'application des lois anti-spam est la possibilité qu'ont les spammeurs de masquer l'origine des messages qu'ils envoient.	• La législation doit **interdire l'envoi de courriels dont l'origine est falsifiée ou dont les informations d'en-tête ou d'identification sont masquées** • La législation doit aussi exiger que l'entreprise qui paye l'expéditeur soit clairement identifiée.

L'un des principaux problèmes du système tient au fait que le courrier électronique n'a pas été conçu au départ pour être sécurisé mais simplement efficace et d'emploi aisé.[28] Ce sont ces caractéristiques qui ont fait son succès et qui aujourd'hui se retournent contre le courriel. Les spammeurs peuvent envoyer des milliers de messages pour un coût négligeable, et en même temps ils peuvent dissimuler ou falsifier leur identité. Pour cette raison, l'interdiction d'envoyer des messages électroniques commerciaux en masquant ou en dissimulant les informations d'identité est présente dans tous les instruments anti-spam en vigueur actuellement.

Cet impératif est essentiel pour combattre l'utilisation du spam comme outil de propagation des escroqueries, des messages frauduleux ou des virus. Mais c'est aussi l'une des dispositions les plus difficiles à appliquer car si l'expéditeur a masqué ou falsifié les informations de l'en-tête, il est difficile à identifier pour une autorité de police ; les enquêtes sont généralement complexes et coûteuses, y compris en temps. Dans ces conditions, il faut que les autorités de police disposent d'expertise technique et que les preuves physiques et financières soient recevables pour l'application des législations anti-spam ou l'engagement de poursuites contre les auteurs de spam. De plus, il faut se doter d'instruments techniques de lutte pour compléter l'effort législatif ; des solutions d'authentification des courriels[29] sont en cours de développement et de mise en œuvre. Leurs avantages et leurs limites seront analysés plus en détail dans la section consacrée aux « mesures techniques ».

Éléments accessoires

Il est aisé de considérer que le spam est une manœuvre entreprise uniquement par la personne qui clique sur le bouton « Envoyer ». Pourtant, on peut en avoir une image plus large : le spam est souvent envoyé pour le compte d'un tiers qui espère ainsi vendre des biens ou des services aux personnes qui répondront aux messages. De plus en plus souvent, les campagnes de spam sont menées de manière à ce qu'il y ait plusieurs intermédiaires entre la personne (ou l'ordinateur contrôlé par un « cheval de Troie ») qui envoie le message et celle qui a décidé qu'il soit envoyé et espère tirer des bénéfices des réponses au spam. La réponse réglementaire pourrait cibler non seulement la personne qui est physiquement responsable de l'envoi du spam, mais aussi la personne qui a décidé de cet envoi, et celles qui y ont pris part. Il existe un certain nombre d'activités qui contribuent à permettre les campagnes de spam. Citons :

- L'utilisation de logiciels qui récoltent les coordonnées et adresses e-mail d'internautes sur l'Internet.
- La vente de listes d'adresses
- L'activité des FAI « complaisants » envers les spammeurs.

Il est important de remarquer que les logiciels collecteurs d'adresses ont une utilité légitime (les webmestres s'en servent par exemple sur leurs propres sites afin de recenser les adresses rendues publiquement accessibles). Une stratégie réglementaire concernant la collecte d'adresses, la vente de listes ou l'utilisation d'un fournisseur d'accès complaisant ne devrait restreindre ces activités que lorsqu'elles sont liées à l'envoi de spam.

Logiciels de collecte d'adresses et listes d'adresses collectées : Les logiciels de collecte d'adresse permettent de collecter les coordonnées de personnes à leur insu et sans leur consentement . **Attaques dictionnaire** : Les adresses sont automatiquement générées à partir des mots d'un dictionnaire de noms et de numéros fréquents.	• La législation peut comprendre des dispositions spécifiques prévoyant des sanctions particulières en cas d'utilisation de ces outils pour envoyer des messages qui constituent une infraction à la législation anti-spam en vigueur.

Les sanctions doivent viser non seulement les personnes qui envoient effectivement les courriers incriminés, mais aussi celles qui mandatent, autorisent cette activité ou qui en bénéficient de quelque manière que ce soit, et qui généralement reçoivent une part des bénéfices résultant du spam.

Personne qui autorise l'expédition du spam, ou qui aide ou assiste le spammeur	La loi doit sanctionner la personne qui envoie physiquement le message, et aussi celle qui a mandaté ou autorisé l'envoi des messages, ou qui a bénéficié financièrement de ces activités.

Outre qu'elle permet d'atteindre un malfaiteur supplémentaire, cette approche peut faciliter l'application de la loi, car il est souvent difficile de déterminer qui a effectivement envoyé le spam, mais il est souvent plus facile de déterminer quel est annonceur qui bénéficie du spam. Cette possibilité présente par conséquent deux grands avantages :

- Premièrement, les capitaux et les biens sont des actifs corporels et leurs flux sont plus faciles à suivre ;
- Deuxièmement, il est plus probable que le vendeur (ou l'annonceur) possède d'autres actifs qui peuvent être utilisés pour dédommager les destinataires du spam.

Cybercriminalité et questions liées au contenu

Si le spam constitue en lui-même un préjudice, les messages de spam véhiculent de plus en plus souvent des contenus malveillants. Des délits informatiques sont commis pour améliorer des techniques de spam – par exemple l'utilisation de logiciels « cheval de Troie » ou d'ordinateur zombies – et a contrario des techniques de spam sont utilisées pour perpétrer des délits en ligne (escroqueries en ligne, hameçonnage, etc.) et pour propager des atteintes à la sécurité (virus et logiciels espions). Comme pour les autres problèmes de contenu associés au spam, la décision d'appliquer la réglementation anti-spam à ces affaires doit être prise en fonction des circonstances nationales. Il faut toutefois reconnaître que dans de nombreux pays, l'envoi de logiciels malveillants est déjà considéré comme un délit par une loi ou peut être aisément incriminé dans le cadre de la Convention du Conseil de l'Europe sur la cybercriminalité.

Utilisation délictuelle de ressources informatiques ➔ Les spammeurs ont de plus en plus recours à des botnets ou à des ordinateurs « zombie » pour envoyer leurs messages, pour falsifier l'origine du spam et pour avoir une plus grande capacité de réseau et de traitement à leur disposition.	La législation **doit interdire l'utilisation non autorisée de ressources informatiques protégées**. Toute personne qui compromet des ordinateurs ou qui envoie des messages par l'intermédiaire d'ordinateurs compromis doit être passible de sanctions.

Dans le domaine du spam, un phénomène nouveau préoccupe les utilisateurs et les fournisseurs d'accès ; il s'agit des techniques que les spammeurs utilisent pour envoyer leurs messages, en exploitant des ressources informatiques et de réseau appartenant à des tiers. Ces systèmes utilisent des relais ouverts, et plus récemment des botnets ou des ordinateurs zombie, c'est-à-dire des ordinateurs qui ont été victimes d'un *cheval de Troie*[30] et peuvent être contrôlés à distance et utilisés pour envoyer du spam dont l'origine est masquée, de sorte qu'il est pratiquement impossible de retrouver le spammeur.

La Convention du Conseil de l'Europe sur la cybercriminalité prévoit dans son article 2 que « l'accès sans droit à tout ou partie d'un système informatique » doit être érigé en infraction pénale. Cette disposition a été mise en œuvre dans plusieurs pays.[31]

Contenu trompeur ou frauduleux

Le spam n'était au départ qu'une technique de vente agaçante, mais il est maintenant utilisé comme vecteur pour des escroqueries, des pratiques commerciales trompeuses, des contenus offensants et des virus dangereux, multipliant les coûts et les risques pour les utilisateurs.

Contenus trompeurs et frauduleux ➔ Contenus de nature douteuse. De nombreux messages de spam sont aujourd'hui utilisés comme vecteurs de manoeuvres frauduleuses (comme l'escroquerie par hameçonnage) ➔ Cet aspect porte sur le contenu du spam, laissant de côté beaucoup des problèmes systémiques concernant les messages de spam.	– Les spam utilisés pour l'escroquerie et pour l'hameçonnage pourraient constituer des délits à composante informatique, c'est à dire des délits ordinaires qui sont fréquemment commis en utilisant un système informatique. – Les lois anti-spam pourraient prendre en compte le contenu des messages, en particulier lorsque les législations sur la lutte contre la fraude, la protection du consommateur ou la pornographie, etc. ne sont pas suffisamment claires. – Certaines législations prévoient l'interdiction des titres de message trompeurs ou frauduleux.
Atteintes à la sécurité ➔ Le spam est très utilisé pour diffuser des virus, des vers et des logiciels espions : comme dans le cas précédent, l'accent est mis sur le contenu du message.	– Les logiciels malveillants associés au spam sont souvent visés par des lois pénales ou peuvent l'être en application de la Convention du Conseil de l'Europe sur la cybercriminalité.

Dans ces cas, l'accent n'est plus sur le vecteur (le spam) mais sur son contenu (fraude, virus par exemple). Beaucoup d'aspects sont déjà couverts par le droit national en matière d'escroquerie ou par des dispositions du droit pénal. Si certains pays préfèrent s'en tenir à des lois d'application générale et technologiquement neutres contre la fraude et des lois pénales, d'autres pourraient trouver justifié de remanier ces normes pour répondre aux nouvelles menaces sur l'Internet.[32] .

Au niveau international, l'une des initiatives les plus importantes est celle du Conseil de l'Europe avec la Convention sur la cybercriminalité.[33] Cette Convention a pour objet d'offrir un instrument général pour répondre à la cybercriminalité d'une manière plus harmonisée et coordonnée. En outre, la Convention soutient l'adoption au niveau national de lois pénales interdisant :

- L'accès sans droit à tout ou partie d'un système informatique (voir plus haut, utilisation abusive de ressources informatiques) ;
- L'interception sans droit, effectuée par des moyens techniques, de données informatiques, lors de transmissions non publiques, à destination, en provenance ou à l'intérieur d'un système informatique ;
- Le fait d'endommager, d'effacer, de détériorer, d'altérer ou de supprimer des données sans droit ;
- La fraude informatique ;
- Les infractions ayant trait à la pornographie enfantine.

Envois en masse

Envoi en masse	
→ L'envoi en masse doit-il être considéré comme un élément caractéristique du spam ? Comment le définir ? Comment répondre aux techniques courantes des spammeurs pour contourner les dispositions applicables à la livraison en masse ?	• La législation peut prévoir que le courriel n'est considéré comme du spam que si **un certain nombre de messages** ont été envoyés pendant un intervalle de temps donné (généralement plus de 50 à 100 sur 24 heures). • Cet élément doit être utilisé en combinaison avec les autres car tous les courriels envoyés en nombre ne constituent pas du spam (voir l'exemple des lettres d'information, etc.)

L'une des options de réglementation du spam consiste à déterminer le nombre de courriels au-delà duquel les messages sont désignés comme spam, donc interdits. Ce niveau est généralement fixé à environ 50 to 100 courriels.[34] Cette approche présente toutefois des inconvénients car elle est arbitraire. Tous les courriels envoyés en masse ne sont pas du spam, et on peut échapper à la classification d' « envoi en masse » par certaines manipulations techniques simples ou par des arguments juridiques (par exemple en envoyant plusieurs salves de messages ou en utilisant plusieurs adresses pour envoyer les messages).

Une personne qui reçoit un message commercial non sollicité ne prendra généralement pas la peine – si toutefois elle est en mesure de le faire – de déterminer si le message lui a été envoyé individuellement ou s'il a un million d'autres destinataires. Dans la plupart des pays, un message électronique unique peut toujours être qualifié de spam s'il est en infraction avec la législation anti-spam et il incombera au destinataire ou aux autorités de police de décider ou non d'intenter des poursuites contre l'expéditeur au cas par cas, en fonction de la gravité de l'atteinte et des ressources disponibles.

Étiquetage

Étiquetage	
→ L'étiquetage du courriel est l'inclusion d'un mot abrégé (par exemple [pub] pour qualifier le contenu d'un courriel donné. Ce système simplifie le filtrage, notamment le blocage de courriels contenant des données à caractère pornographique envoyés à des enfants.	• La législation pourrait comprendre une disposition imposant l'utilisation d'une étiquette particulière pour les courriels contenant de la publicité, des données à caractère pornographique, etc.

L'utilisation de mots spécifiques, ou étiquettes, pour permettre aux utilisateurs de distinguer entre les publicités et les autres courriels personnels ou professionnels, pourrait être vraiment utile pour lutter contre le spam. Dans le domaine du courrier électronique, l'étiquetage consiste à utiliser des mots standard dans l'en-tête ou dans le sujet du message qui identifient clairement le contenu du message. Par exemple la mention « PUB» pour la publicité ou « ADLT » pour les contenus réservés aux adultes. Grâce à un tel mécanisme, les destinateurs peuvent distinguer instantanément les publicités et les autres types de courriers. Les systèmes de filtrage s'en trouvent également plus efficients et plus effectifs.

Ce système présente plusieurs limites :

- Les variantes dans les étiquettes utilisées peuvent tromper les systèmes de filtrage, par exemple « P.U.B. » ou « p u b » au lieu de « PUB ».
- L'étiquetage ne sera une arme opérante dans la lutte contre le spam que si l'approche adoptée est harmonisée au niveau international.
- Il y a peu de chances que les spammeurs invétérés – surtout ceux qui masquent leur identité et ne donnent pas leur adresse – se conforment à cette règle.

Aspects transnationaux

Compétence transnationale	La réglementation doit créer un lien avec les entreprises nationales et les individus du pays :
→ Il est difficile d'imposer une législation aux messages de spam qui proviennent d'un autre territoire que celui du destinataire. Dans le même temps, les autorités nationales n'ont pas toujours compétence légale sur les messages de spam en provenance de leur territoire mais envoyés vers un autre pays.	• Dispositions d'application limitée précisant que les messages envoyés à destination ou en provenance du territoire sont concernés, de même que les messages mandatés depuis le territoire et les avantages financiers liés au spam (voir exemple ci-dessous). • Les spammeurs qui opèrent depuis le territoire national doivent pouvoir être poursuivis, même si leurs messages sont envoyés à destination de pays étrangers • Accords de coopération internationale et mécanismes transnationaux de police

L'un des principaux problèmes rencontrés par les autorités d'application dans leur lutte contre les spammeurs est la difficulté qu'il y a à imposer la législation interne aux spammeurs qui opèrent depuis un autre territoire que celui de la victime ; à l'inverse, les autorités ont parfois des facultés d'intervention limitées dans les cas où un spammeur opérant depuis leur territoire ne porte préjudice qu'à des utilisateurs situés à l'étranger. De même, dans de nombreux exemples, une partie des preuves se trouvent dans un autre pays, comme c'est le cas par exemple lors des enquêtes sur des comptes bancaires, des sociétés intermédiaires, des sociétés financières, des hébergeurs, etc.

La compétence extraterritoriale, c'est-à-dire la faculté légale de la puissance publique à exercer son autorité à l'extérieur de ses limites habituelles est un point juridique complexe qui relève de la doctrine générale d'une nation et peut varier d'un État à l'autre. Dans un nombre croissant de situations, des pays revendiquent une certaine dose de compétence extraterritoriale dans des domaines législatifs importants lorsque les circonstances le demandent.[35] Dans le contexte de la conception et de la mise en œuvre de la législation de lutte anti-spam, les points à considérer sont la nécessité d'inclure des mesures qui peuvent réellement être imposées par les tribunaux nationaux ; permettre des accords internationaux en la matière, et faciliter l'application transnationale au niveau opérationnel (échange d'informations, coopération dans les enquêtes). Ce point sera examiné plus en détail dans la prochaine section (Répression du spam).

Identifier les parties concernées

Le spam est un problème complexe qui fait intervenir un grand nombre de protagonistes : les internautes, les fournisseurs d'accès, les instances de répression, etc. Chacun de ces acteurs a ses droits et ses responsabilités, et la législation doit les prendre en compte.

Les victimes du spam sont le plus souvent des **internautes individuels** ou des consommateurs, dont les droits doivent être protégés par une législation adaptée et par l'existence de voies de recours. Cela signifie par exemple qu'il faut établir la manière dont les consommateurs peuvent signaler aux instances de répression les atteintes de type spam dont ils ont été victimes, ou créer une procédure de réclamation transparente et rapide. Lorsqu'un grand nombre d'individus reçoivent du spam, des groupes d'individus peuvent se former et intenter une action collective contre les spammeurs.[36] Mais il peut surgir des difficultés d'ordre administratif, notamment pour l'identification des individus affectés par une campagne de spam donnée, et pour la collecte, la rétention et la présentation des preuves. Étant donné ces problèmes, et la nature du spam qui fait qu'un grand nombre de parties civiles peuvent être touchées, cette solution est assez peu envisageable.

En matière de spam, les rôles des **fournisseurs d'accès** sont multiples. Ils sont des victimes du spam, qui engorge leurs réseaux et leurs serveurs, gaspille de la bande passante, et accapare de l'espace de stockage. Mais ils en sont aussi la source et les intermédiaires. En liaison avec ce dernier rôle, il est essentiel que les cadres législatifs et réglementaires de lutte anti-spam ne sanctionnent pas les FAI pour le simple fait d'avoir servi de canal de distribution des courriels incriminés. La présentation d'un message ne saurait être assimilée en soi à une responsabilité quant à son contenu ni au dommage causé par son envoi.

Les fournisseurs d'accès peuvent aussi constituer une importante source d'éléments de preuves susceptibles d'être vitales dans l'application des lois anti-spam. Il faut toutefois clairement définir la nature de ce rôle ; il peut être nécessaire et souhaitable de décrire le rôle des FAI dans la loi. Cela pourrait par exemple permettre aux fournisseurs d'échapper à des accusations de violation de la vie privée lorsqu'ils agissent au nom de la force publique. La publication par les fournisseurs d'accès de leurs Conditions générales d'utilisation est une autre méthode pour décrire les droits et les responsabilités des FAI. Des CGU bien conçues peuvent en effet permettre à un FAI de s'investir lui-même de fonctions d'application des politiques anti-spam et de devenir un partenaire majeur dans la lutte contre le spam.

Des codes de conduite peuvent aussi être élaborés par les FAI et les autres acteurs de l'Internet comme les sociétés de marketing direct. Les gouvernements et les autorités de réglementation peuvent faciliter et favoriser l'élaboration de codes qui vont dans le sens de la réglementation et la complètent (voir l'élément III).

La législation anti-spam, par exemple, peut aussi prévoir que des organismes et des associations du secteur des télécommunications élaborent des codes professionnels relatifs à leur activité. La législation peut aussi contenir des indications sur le contenu de ces codes, à condition de s'en tenir aux grandes orientations et de ne pas imposer de procédés ou de solutions spécifiques. Dans le cas des codes de conduite pour les fournisseurs d'accès et les opérateurs en ligne en matière de messages commerciaux non sollicités, le droit interne pourrait encourager[37] les entreprises à développer des codes de pratiques et des normes techniques volontaires lorsque cela va dans le sens de l'intérêt général et n'impose pas de charges financières et administratives indues aux acteurs du secteur. La loi peut prévoir que le code devra, par exemple[38] :

- Définir les procédures à suivre par les fournisseurs d'accès et les fournisseurs de services de messagerie électronique pour le traitement des courriels indésirables (notamment les procédures concernant l'utilisation ou la fourniture de mises à jours de logiciels de filtrage du spam) ;

- Informer les internautes des dangers liés au spam, des solutions technologiques existantes, de l'utilisation des filtres, etc. ;

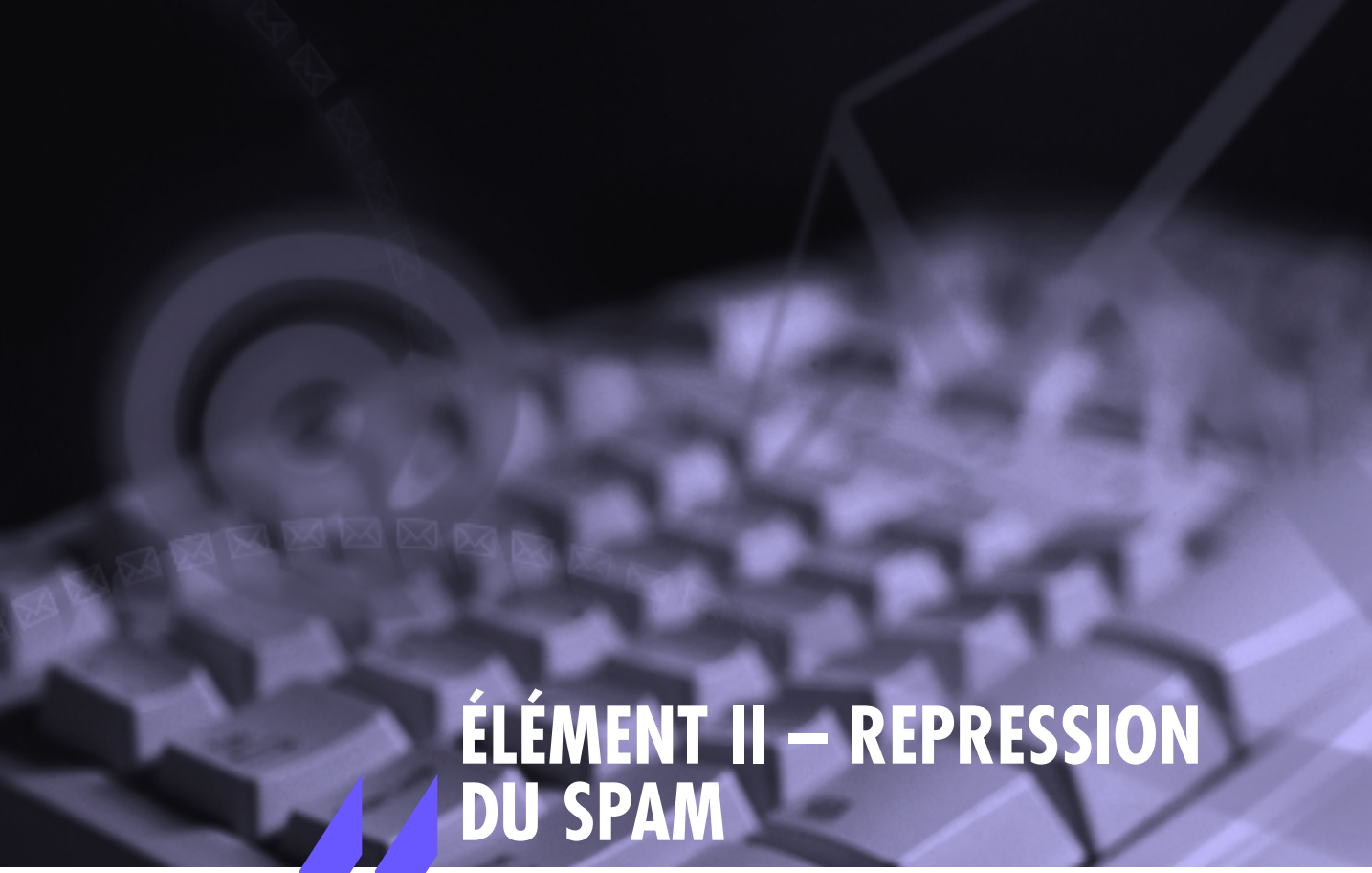
- Définir une liste de mesures à prendre pour minimiser ou empêcher l'envoi ou la livraison de courriels commerciaux indésirables, notamment la configuration correcte des serveurs pour minimiser ou empêcher l'envoi ou la livraison de spam, la fermeture des relais ouverts, etc.

Dans le cadre des activités du Groupe de réflexion de l'OCDE, un ensemble de bonnes pratiques a été rédigé à l'intention des FAI et opérateurs de réseaux par le BIAC et le MAAWG (Voir l'élément III – Initiatives anti-spam du secteur privé). De même, il convient de prendre note du code de pratique de la GSMA (Voir l'Annexe IV).

La législation peut aussi offrir un cadre global pour soutenir les efforts des fournisseurs d'accès pour bloquer ou limiter la circulation du spam par courriel. On peut citer l'exemple de la législation coréenne, qui autorise légalement les fournisseurs d'accès à définir leurs critères de blocage du spam et à développer des moyens d'empêcher sa circulation. Le texte dispose que, lorsque le spam provoque ou est susceptible de provoquer une interruption inacceptable de leurs services, ou lorsqu'un client ne souhaite pas recevoir du spam, les fournisseurs peuvent rejeter la transmission du spam en question. Des résultats analogues pourraient être obtenus par le biais de dispositions contractuelles adéquates entre les FAI et les internautes.

Acteurs	Rôle et besoins
Individus (personnes physiques).	Victimes du spam, ils ont besoin d'être protégés et d'avoir accès à des voies de recours Possibilité d'actions collectives ? Indemnités légales ?
Entreprises (personnes morales)	Définition de leurs droits Consentement (dans le cas de l' « opt-in ») : par un représentant autorisé
Fournisseurs de service Internet	Partie lésée – possibilité de recours ? Détenteurs d'éléments de preuve ; Appliquent les CGV ; Responsabilité ?
Fournisseurs de services télécom	(Comme pour les fournisseurs d'accès)
Autorités gouvernementales	Au niveau national, il doit exister une autorité publique ou privée chargée de l'application de la législation anti-spam (par exemple l'autorité de protection des consommateurs, ou l'autorité de protection de la vie privée) Dans le cas de spam constituant une infraction pénale, les autorités de police et de justice sont aussi concernées. La coopération entre les agences gouvernementales et les autorités judiciaires doit être encouragée.
Autres groupes d'intérêts :	
Associations de marketing direct	Code de conduite des associations de marketing direct
Associations de protection des consommateurs	Éducation et sensibilisation, répression.
Éditeurs de logiciels	Responsabilité des fournisseurs d'outils de CRM et de collecte d'adresses. Elle pourrait être prévue dans la législation en tant qu'élément accessoire.

Pour définir un cadre législatif adapté, un certain nombre de questions ne doivent pas être négligées : comment sera mise en œuvre la législation, comment elle peut être appliquée par les tribunaux nationaux et quelles dispositions peuvent être introduites pour faciliter la répression transfrontières au niveau opérationnel. Nous allons examiner ces questions dans la partie suivante de ce document.



ÉLÉMENT II – REPRESSION DU SPAM

Introduction

Une enquête réalisée par le Groupe de réflexion sur le spam de l'OCDE à la fin de 2004 révèle que la plupart des pays de l'OCDE ont mis en place au cours des dernières années un cadre législatif destiné à lutter contre le spam.[39] Les pays européens ont ainsi mis en application la directive 58/2002 dont l'article 13 concerne expressément les communications électroniques non sollicitées[40]. En Australie, la loi sur le spam (*Spam Act*) de 2003 a été considérée comme un exemple de bonne législation en raison de son caractère global[41]. La Corée et les États-Unis ont mis en application leurs législations respectives, qui sont fondées sur l'option de refus (*opt-out*)[42], en 2001 et 2003.
Au Canada, il n'existe pas encore de législation anti-spam spécifique, mais des textes y protègent la confidentialité des données et les droits des consommateurs. Ces textes s'appliquent également aux messages électroniques, et les messages qui enfreignent les normes sont considérés comme des spams[43]. Un groupe de réflexion canadien a présenté son rapport au Ministre de l'industrie et recommandé de prendre d'autres mesures législatives. Par ailleurs, quelques pays en sont encore au stade de l'élaboration de leur loi anti-spam. La Nouvelle-Zélande[44], par exemple, a publié un document de travail en 2004 et devrait adopter son projet de loi en 2006[45].

S'il est bien sûr nécessaire de se doter de la législation appropriée, un élément capital est l'application de cette législation, qui constitue la deuxième étape d'une stratégie anti-spam globale. La promptitude de la répression et de l'application des sanctions revêt une importance primordiale pour contrer efficacement le spam. En effet, les spammeurs peuvent aujourd'hui agir très rapidement et au besoin relocaliser l'ensemble de leurs activités en quelques jours, voire en quelques heures. La procédure de notification d'infraction, qui peut s'étaler sur une période de plusieurs semaines ou mois, n'a plus d'efficacité dans le cyberespace.

Les pouvoirs publics, dans le cadre de leur démarche visant à faciliter le répression du spam à travers les frontières, devront peut-être agir à quatre niveaux : coordination nationale, sanctions, octroi des moyens nécessaires aux autorités d'exécution et coopération internationale en matière de répression.

Coordination nationale

Le problème du spam concerne non seulement les droits des consommateurs et la confidentialité des données, mais également la sécurité et l'efficacité des réseaux. Par conséquent, dans de nombreux pays, ce sont plusieurs organismes — aux priorités et pouvoirs différents — qui sont chargés d'un ou de plusieurs aspects du spam. Par exemple, même si l'application de la législation anti-spam américaine incombe au premier chef à la *Federal Trade Commission* (FTC), elle fait aussi intervenir le ministère de la Justice, qui applique les dispositions pénales de la loi. En raison de ce partage de compétences, il est possible qu'un spammeur fasse l'objet de poursuites simultanées au civil et au pénal[46]. En Italie, si l'application de la législation anti-spam incombe avant tout à l'autorité de protection des données, c'est l'autorité de la concurrence qui est chargée des problèmes de courriels au contenu commercial frauduleux.

Les différents organismes chargés des enquêtes concernant le spam et/ou de l'application des diverses lois que les spammeurs sont susceptibles d'enfreindre n'ont pas toujours bien coordonné leur action pour tirer pleinement parti des synergies possibles et mettre en commun leur information et leurs ressources. Pour y remédier, plusieurs pays ont mis en place un mécanisme de coordination : en Australie, par exemple, quatre organismes sont convenus de coopérer pour les affaires liées au spam ; aux états-Unis, la FTC a mis sur pied un Groupe de réflexion national sur le spam pour faciliter la communication entre les organismes chargés de faire appliquer les législations anti-spam au niveau fédéral et dans les différents états ; en France, Le groupe de contact des acteurs de la lutte contre le spam comprend des représentants des pouvoirs publics, de l'autorité de régulation, du secteur privé et de la société civile ; en Allemagne, une « Alliance contre le spam » a été formée entre l'Association de l'économie Internet allemande (eco), la Fédération des associations de consommateurs allemande (vzbv) et l'Agence chargée de lutter contre la concurrence déloyale.

Certains pays devront peut-être intensifier leurs efforts pour renforcer la coopération inter-organismes et désigner un organisme pour assurer la liaison nécessaire. Pour les appuyer, le Groupe de réflexion a établi une liste de correspondants à l'intention des autorités nationales, que l'on peut consulter en ligne à l'adresse suivante : www.oecd-antispam.org.

Autorités d'exécution – Pouvoirs d'enquête

Le pouvoir d'enquêter et de recueillir de l'information et des éléments de preuve est le point de départ d'une politique de répression efficace. Dans les affaires de spam illégal, les preuves se présentent en général sous forme électronique et peuvent être stockées sur de nombreux ordinateurs, appareils ou réseaux situés dans un grand nombre de pays ou territoires.

Dans ce contexte, les autorités chargées de la répression du spam doivent disposer d'un pouvoir de perquisition et de saisie suffisant pour rechercher des éléments de preuve électroniques, y avoir accès, les saisir, les intercepter et les préserver. Idéalement, la collecte des preuves ne doit pas se limiter aux enregistrements de transmissions de messages. Les documents financiers et la correspondance peuvent aider à déterminer qui est à l'origine du spam ou y est associé. Le spam étant une activité à laquelle on peut se livrer facilement depuis son domicile, il pourrait être avisé de prévoir des contrôles et une supervision externe des autorités d'enquête pour les perquisitions. Dans certains pays, ces actions nécessiteraient l'obtention de mandats de perquisition.

Les mandats sont en général délivrés pour accéder à un site ou à un objet physique déterminé et ne sont guère adaptés à la recherche d'éléments de preuve électroniques, qui posent des problèmes très spécifiques pour les enquêtes judiciaires. Pour résoudre ces problèmes et aider les forces de l'ordre dans leur tâche, la Convention du Conseil de l'Europe sur la cybercriminalité propose un cadre procédural complet pour les enquêtes cybercriminelles, et contient des dispositions sur la préservation, la perquisition et la saisie d'éléments de preuve électroniques. De même, un guide a été publié sur la question par le Ministère américain de la justice (*Criminal Division, Computer Crime and Intellectual Property Section*) qui couvre tous les aspects de la perquisition et de la saisie des éléments de preuve électroniques.

Comme il est très facile pour des personnes soupçonnées de spam d'organiser la perte, la destruction ou la dissimulation d'enregistrements électroniques susceptibles de constituer des preuves, il peut être judicieux de prévoir des dispositions raccourcissant le délai de notification associé aux mandats de perquisition.

Procédures et sanctions

Étant donné que la principale motivation des spammeurs réside dans les gains économiques qu'ils comptent tirer de leur activité, la législation doit prévoir des sanctions suffisamment sévères pour décourager les spammeurs, en réduisant leurs profits ou en leur infligeant des sanctions pénales — l'incarcération, par exemple — pour certaines infractions.

Les sanctions sont fonction de la gravité du délit. En France, les sociétés de marketing et les cyberentreprises qui expédient des courriels non sollicités à plusieurs clients potentiels sont considérés comme des spammeurs, mais s'ils ne commettent pas d'autres violations, la CNIL se limitera à leur faire parvenir une lettre pour les informer du caractère illégal de leur démarche et leur demander de mettre un terme à leurs envois de spams, qui contreviennent aux lois sur la protection des données. Les organismes de protection des consommateurs peuvent en général solliciter des injonctions ordonnant aux spammeurs de cesser leur activité, sous peine de sanctions pour atteinte à l'autorité du tribunal lorsque le spam est vecteur de fraude.

Lorsqu'une simple injonction ou un avertissement ne semble pas suffisant, la législation prévoit en général des amendes. Les organismes chargés de l'application des lois, en particulier les autorités de protection de données et les régulateurs des télécommunications, sont habilités à infliger des amendes administratives, tandis que les amendes civiles relèvent des tribunaux civils. Les autorités peuvent également saisir une juridiction pénale, qui a le pouvoir d'infliger des amendes pénales. Les sanctions pénales sont infligées pour des délits plus graves, tels que le spam utilisé comme vecteur de fraude, l'utilisation non autorisée de ressources informatiques ou la propagation de virus. Elles vont de l'amende pénale à l'incarcération, mais l'application de cette dernière à un spammeur est jugée excessive dans certains pays, qui privilégient des sanctions pécuniaires.

L'un des problèmes actuellement à l'étude est de savoir si une personne physique ou morale possède un droit de recours privé lui permettant d'obtenir une réparation légale, et comment les recours civils peuvent s'exercer dans les affaires de spam. Cette question revêt une importance fondamentale compte tenu du fait qu'intenter une poursuite contre un spammeur exige beaucoup de temps et de ressources, et que les acteurs privés n'auront donc pas grand intérêt à le faire, à moins de pouvoir en escompter un résultat tangible. L'un des problèmes qui se pose dans le recours civil serait toutefois de chiffrer le préjudice causé par le spam. Si cela peut être assez simple en cas de spam frauduleux, qui occasionne une perte financière directe à son destinataire, il peut être en revanche difficile, faute d'assise législative, de démontrer que le spam a porté préjudice ou occasionné un coût substantiel à son destinataire, ou d'imposer au spammeur un dédommagement tel qu'il soit dissuadé de poursuivre son activité. Une loi pourrait être envisagée pour prévoir les dommages causés par le spam et faciliter le remboursement des coûts aux parties lésées.

Le montant des sanctions pécuniaires, qu'elles soient civiles, pénales ou administratives, peut être en rapport avec la nature et la gravité de l'infraction et tenir compte de son éventuelle répétition dans la durée et des conditions qui s'y rattachent (dissimulation ou falsification d'identité, utilisation d'adresses collectées, etc.)[47]. Les sanctions peuvent être infligées individuellement pour chaque infraction ou être déterminées en fonction d'une évaluation globale du comportement du spammeur. La législation australienne prévoit des amendes distinctes pour chaque infraction, c'est-à-dire pratiquement pour chaque courriel expédié[48]. La Corée et le Japon ont déjà relevé le plafond de la sanction qui peut être imposée aux spammeurs. En particulier, les autorités japonaises permettent maintenant d'infliger l'amende directement, sans avoir besoin d'émettre au préalable une "injonction administrative".

Le tableau ci-après récapitule certaines des réparations et sanctions qui existent dans les pays Membres de l'OCDE.

Nature	**Exemples***	**Commentaires**
Action civile	Sanctions monétaires : Amende civile – peut être un montant fixe, en fonction de la nature et de l'ampleur de l'infraction Recours des consommateurs Sanctions non monétaires: Lettres d'avertissement Injonctions	L'action civile peut généralement être intentée par des personnes physiques, par des autorités de police ou par des fournisseurs d'accès Internet. Amende : le produit de la sanction va dans les caisses de l'État. Recours des consommateurs : les fonds collectés sont restitués à la victime (le consommateur).
Actions pénales	Sanctions monétaires : Amende pénale Sanctions non monétaires : emprisonnement	Recours fort, surtout utilisé lorsque le contenu du spam est criminel, ou lorsque le spammeur n'a pas obéi à une injonction administrative. Problème : perte de temps, charge de la preuve plus lourde
Actions administratives	Sanctions monétaires : Amende administrative Sanctions non monétaires Lettres d'avertissement Injonctions	Les amendes administratives et les sanctions non monétaires sont les principaux instruments des autorités d'application dans de nombreux pays. L'application de recours administratifs peut éviter la nécessité d'ouvrir un procès civil ou pénal.

* Pour une analyse plus détaillée, se reporter au Rapport sur l'application des lois antispam, DSTI/CP/ICCP/SPAM(2004)3/FINAL, http://www.oecd-antispam.org/rubrique.php3?id_rubrique=8.

Coopération et mise en commun de l'information

Comme c'est souvent le cas quand il s'agit d'activités menées sur l'Internet, le spam soulève des problèmes d'application des lois nationales. Les spammeurs qui enfreignent apparemment les lois d'un pays peuvent en fait se trouver ailleurs.

La réglementation et l'application des lois relatives au spam sont compliquées par des difficultés liées à la collecte et à la préservation d'éléments de preuve dès lors que le spam franchit les frontières nationales, ce qui nécessite la coopération entre un organisme national et l'organisme étranger équivalent pour engager une poursuite.

Si la réglementation nationale anti-spam encourage explicitement les régulateurs à aider leurs homologues étrangers à collecter des éléments de preuve dans leurs enquêtes, l'efficacité des modalités de coopération s'en trouvera grandement renforcée. De même, l'élaboration de méthodes normalisées pour recueillir et fournir des éléments de preuve électroniques, qui prendraient dûment en compte les impératifs de protection de la vie privée dans la transmission transnationale d'éléments de preuve, pourrait contribuer à l'application non seulement de la législation anti-spam du pays ou territoire concerné, mais également d'autres lois relatives à la cybercriminalité.

Plusieurs protocoles d'accord et mécanismes informels de coopération ont été élaborés ces dernières années entre plusieurs pays de l'OCDE, mais principalement sur une base bilatérale. Il s'agit en général d'accords par lesquels un nombre limité d'entités s'engagent à tout mettre en œuvre pour améliorer la coopération. Les divers accords existants montrent que les régulateurs chargés de lutter contre le spam – dans les pays de l'OCDE comme dans les pays non membres – peuvent coopérer en faisant preuve de bonne volonté à un niveau opérationnel.

Certains mécanismes ont facilité la coopération, pour assurer une meilleure coordination entre les parties prenantes. Le plan d'action de Londres (LAP) associe les organismes d'application et les acteurs de l'industrie pour créer un réseau multilatéral de répression internationale du spam. Des réseaux francophones[49] travaillent actuellement à la mise en place d'un réseau multilatéral pour la coopération nationale contre le spam.

Par ailleurs, différents projets issus de centres de recherche, comme « Spotspam » et « Signal-spam » encouragent les efforts d'échange d'informations et de coordination entre les secteurs public et privé. Le projet français « Signal-spam » notamment assure la gestion technique et opérationnelle d'un logiciel de collecte, de marquage et d'analyse du spam. L'information ainsi obtenue est ensuite redirigée vers les organismes compétents pour qu'ils réagissent rapidement et mettent fin aux agissements du spammeur.

Au niveau de l'UE, le réseau de contact des autorités anti-spam (CNSA) a été créé à l'initiative de la Commission à la suite de sa communication de janvier 2004. Le CNSA facilite la mise en commun de l'information et des meilleures pratiques en matière d'application des lois anti-spam entre les autorités des états membres de l'Union. En outre, un accord volontaire a été conclu en février 2005 pour définir une procédure commune de traitement des plaintes transnationales relatives au spam.[50]

A la suite de discussions au sein de leurs organes respectifs, le LAP et le CNSA ont récemment élaboré un formulaire de transmission de plainte relative au spam (« Spam Complaint Referral » pro forma) accompagné d'une notice explicative (voir l'Annexe V) qui a été utilisé par certaines autorités[51] appartenant au LAP et/ou au CNSA. Le formulaire et la notice explicative sont des documents de travail qui facilitent la demande d'assistance et la transmission d'une demande d'enquête concernant un cas de spam à une autre autorité participante. Ces documents sont appelés à être modifiés et à évoluer.

Par ailleurs, les réseaux existants de coopération en matière d'application du droit pénal (comme le système 24/7 du G8) et les instruments d'entraide juridique (comme les traités d'entraide juridique et les lettres rogatoires) permettent déjà aux pays de coopérer et de partager de l'information aux fins d'enquêtes et de poursuites judiciaires relatives au spam ou à d'autres formes de cybercriminalité.

Coopération transnationale en matière de répression du spam

Sur la base des constatations exposées ci-dessus, il est évident que la répression au-delà des frontières serait facilitée par la mise en oeuvre d'une stratégie mondiale qui permettrait de résoudre certains problèmes, tels que la collecte et le partage d'informations, la définition des priorités en matière de répression et la mise en place d'un cadre d'action internationale efficace. À cette fin, une Recommandation du Conseil de l'OCDE a été adoptée pour donner des orientations et des conseils sur la façon d'améliorer la coopération transfrontière dans le contrôle de l'application des législations anti-spam (Annexe I).[52] Selon cette recommandation, les gouvernements devraient améliorer leur législation pour :

a) Mettre en place un cadre national pour habiliter leurs organismes nationaux d'application de la loi à instruire les affaires de spam et à réprimer cette activité ;

b) Renforcer la capacité de leurs autorités à coopérer avec les autorités étrangères, en les dotant des moyens d'échanger des informations pertinentes et de collaborer avec ces dernières en matière d'enquêtes ;

c) Améliorer les procédures de coopération, en donnant la priorité aux demandes d'entraide et en faisant usage des ressources et réseaux communs ;[53]

d) élaborer de nouveaux modes de coopération entre les organismes d'application et les entités compétentes du secteur privé.

ÉLÉMENT III – INITIATIVES ANTI-SPAM DU SECTEUR PRIVÉ

De par sa nature et son évolution rapide, l'Internet a entraîné une transformation des rôles respectifs des pouvoirs publics, de l'industrie et des utilisateurs dans la cyberéconomie, et a fait naître un intérêt pour la notion d'autorégulation.

Comme mentionné dans les précédentes sections, la réglementation et la législation revêtent certes une importance fondamentale pour la lutte contre le spam, mais elles ne sont souvent pas suffisamment flexibles pour suivre le rythme rapide du progrès technologique, ni toujours efficaces pour gérer la complexité de la répression transnationale ou résoudre les difficultés que posent notamment l'identification des spammeurs. Pour lutter efficacement contre le spam sur l'Internet, les lois anti-spam qui s'appliquent en général dans les pays devraient être jumelées à des initiatives d'autorégulation pilotées par des acteurs du secteur privé– fournisseurs d'accès à l'Internet, opérateurs de télécommunications, sociétés de marketing direct, cyberentreprises, sociétés de logiciels, ainsi que les associations professionnelles qui les représentent.

Fournisseurs d'accès à l'Internet (FAI)

Les pouvoirs publics et les régulateurs ont toujours été en faveur d'une stratégie d'autoréglementation, non interventionniste, des FAI, qui ne sont pas tenus responsables du contenu des données transitant par leurs réseaux, car on craignait, en imposant cette responsabilité aux FAI, d'ouvrir la voie à une dérive vers une surveillance plus stricte des contenus et par conséquent une censure plus sévère du cyberespace.

Néanmoins, les FAI jouent un rôle de premier plan dans la sécurité de l'Internet, et l'idée selon laquelle les fournisseurs de services de messagerie devraient intervenir activement pour prévenir la circulation de spams ayant pour origine leurs réseaux ou y transitant gagne du terrain. On constate en effet que si de nombreux FAI sont déjà résolument engagés dans la lutte contre le spam, certains tardent encore à les

suivre, et sans un ensemble de règles harmonisées (par exemple code de conduite, pratiques exemplaires), rien ne garantit qu'ils feront le nécessaire pour empêcher l'utilisation de leurs services par les spammeurs et fourniront à leurs clients l'information et les outils éducatifs et techniques devant leur permettre de se prémunir contre les menaces que constituent le spam, les logiciels espions, les botnets, la prise de contrôle d'ordinateurs, etc.

De façon générale, les instruments législatifs nationaux n'imposent aucune obligation aux FAI d'intervenir activement pour aider à faire échec au spam. Néanmoins, la plupart des fournisseurs ont un intérêt commercial à bloquer/limiter les spams entrants pour protéger leurs clients, car la présence massive de spams risque de perturber leur service, et par conséquent de compromettre sa disponibilité et sa fiabilité. La mise à disposition de filtres anti-spam pourrait donc devenir un avantage concurrentiel pour les FAI, qui seront en mesure d'offrir des services améliorés et d'attirer ainsi une clientèle plus nombreuse. Les fonctions anti-spam sont de plus en plus intégrées aux forfaits proposés par les FAI, en particulier sur les connexions haut débit. Bien qu'il soit important aux yeux des internautes, le blocage des spams entrants n'aidera pas forcément à réduire le volume global de spams créés et, de fait, pourrait même l'accroître car les spammeurs chercheront à maintenir leurs niveaux de recettes en contactant un plus grand nombre de clients potentiels.

S'agissant des spams sortants, ils affectent les clients plus indirectement, du fait qu'en accaparant une partie de la capacité du fournisseur, ils réduisent la qualité du service et allongent le temps de réponse du réseau. En outre, les autres fournisseurs peuvent décider de bloquer tous les messages provenant d'un FAI dont les services sont utilisés de façon répétée par les spammeurs et l'inscrire sur une « liste noire » publique d'adresses IP ou de domaines. Cette éventualité peut servir à dissuader les fournisseurs de conclure des contrats de complaisance (« *pink contracts* »)[54] et les inciter au contraire à prendre des mesures pour éviter un abus de leurs ressources. Les listes noires présentent toutefois plusieurs inconvénients, qui sont analysés dans la section consacrée aux solutions techniques.

Mesures techniques et autorégulation

Les FAI et les opérateurs de réseaux peuvent contribuer à lutter contre le spam sur deux fronts. D'abord technologique, en mettant au point et en appliquant des solutions technologiques pour limiter ou bloquer non seulement les spams entrants mais aussi, directement, les spams sortants. Ensuite opérationnel, puisque les FAI peuvent se conformer à un code de conduite et imposer à leurs clients des Conditions générales d'utilisation (CGU) interdisant le spam (encadré 2).

Le débat sur le rôle des FAI à l'égard du problème du spam a été lancé dans le cadre du groupe *Internet Engineering Task Force* (IETF) par un mémo intitulé "*Email submission between independent networks*"[55]. Ce document, qui vise à préciser les responsabilités en matière de contrôle des abus de services de messagerie sur l'Internet, propose une série de pratiques/comportements exemplaires aux FAI pour la gestion des courriels entrants et sortants.

Dans le même ordre d'idée, l'*Anti-spam Technical Alliance* (ASTA), active jusqu'en 2004 et qui regroupait certains des principaux FAI et autres acteurs de l'Internet, a été créée pour mettre au point des solutions techniques et non techniques au problème des courriels commerciaux non sollicités. L'Alliance a ainsi élaboré une proposition intitulée « Technology and Policy Proposal », rendue publique en juin 2004[56], qui comprend une série de pratiques exemplaires et de stratégies techniques que les FAI devraient adopter pour contrôler le trafic abusif et réduire ainsi les risques d'utilisation de leurs serveurs par les spammeurs. Ces techniques sont fondées sur des politiques de "bon voisinage". Autrement dit, les FAI sont responsables du contrôle du trafic qui provient de leurs réseaux.

Le problème du spam étant lié aux questions de sécurité des réseaux, les fournisseurs, en plus d'utiliser des filtres pour bloquer la réception de spams, devraient également améliorer la sécurité sur leurs réseaux, afin d'éviter d'être une source de spams. Ils sont nombreux à penser que le problème des « botnets »[57] et des ordinateurs « zombies » peut être résolu, ou tout au moins limité, en mettant en œuvre les meilleures pratiques en matière de sécurité, en appliquant des CGU et en formant les internautes à tirer parti des outils à leur disposition pour protéger leurs ordinateurs[58].

Encadré 2. Conditions générales d'utilisation (CGU)[59]

Plusieurs fournisseurs de services de messagerie incluent dans leurs conditions de service, qui sont acceptées par leurs clients, une série de règles sur la façon dont le service peut être utilisé, définissant ce qu'est un comportement inacceptable et les conséquences d'une éventuelle violation de ces règles. Les conditions d'utilisation type (appliquées de façon uniforme par un grand nombre de fournisseurs) comprennent notamment les dispositions suivantes :

- Il est interdit d'expédier, de transmettre, de diffuser ou de livrer des courriels non sollicités en masse ou des courriels commerciaux non sollicités (spams).
- Il est interdit de falsifier les en-tête de courriels ou d'effectuer toute autre manipulation d'identifiant afin de dissimuler l'origine de contenus transmis par le biais du service.
- Les conditions de service avertissent également les usagers qu'en cas de violation, le FAI se réserve le droit de prendre sans préavis les mesures qu'il juge appropriées, par exemple bloquer les messages émanant d'un nom de domaine Internet particulier, d'un serveur de messagerie ou d'une adresse IP ou de fermer immédiatement tout compte sur tout service qui a été utilisé pour transmettre un message contrevenant à cette politique. L'utilisation inacceptable comprend souvent l'établissement de listes d'adresses, les contenus illégaux et préjudiciables, les spams expédiés à des listes d'adresses et les bulletins.
- Certains fournisseurs ont adopté une stratégie plus globale et leur politique d'utilisation s'applique non seulement aux courriels mais à tout type de transmission ascendante, d'affichage, de courrier électronique, de transmission ou d'autres pratiques faisant intervenir de la publicité, de la documentation commerciale ou toute autre forme de sollicitation non autorisée (sauf dans les secteurs prévus à cette fin).
- L'envoi de messages contenant des virus ou tout autre code ou programme malveillant destiné à endommager la fonctionnalité de logiciels ou matériels informatiques ou d'équipements de télécommunications est interdit dans la plupart des cas.

La proposition technologique et stratégique de l'ASTA comprend une série de pratiques exemplaires et de technologies que les FAI devraient mettre en oeuvre pour aider à sécuriser l'infrastructure de courrier électronique et favoriser une responsabilisation accrue. Cependant, s'agissant des moyens techniques, le même document reconnaît qu'il ne faut pas y voir la solution unique au problème du spam et que les dispositions doivent être suffisamment flexibles pour pouvoir être adaptées à l'évolution rapide du cyberespace et à ses points vulnérables. C'est pour cette raison que les pouvoirs publics n'imposent pas de solutions technologiques aux FAI et que les associations et alliances formées par ces derniers préfèrent concentrer leurs efforts, dans une optique plus générale, sur le choix des meilleures pratiques et des

objectifs, plutôt que fixer des règles spécifiques. Un exemple typique à cet égard est le code de conduite adopté par le groupe de travail contre l'abus de la messagerie (MAAWG)[60], organisation qui regroupe désormais la quasi-totalité des anciens membres de l'ASTA et qui poursuit les travaux techniques mis en route par cette alliance.

Cependant, tous les FAI ne semblent pas conscients des problèmes de spam et de sécurité, ni particulièrement concernés. À cet égard, la *Federal Trade Commission*, avec d'autres partenaires de diverses régions du monde, a lancé en janvier 2004 l'opération « *Secure Your Server* » (Sécuriser votre serveur), qui a pour but d'informer les particuliers et les organisations que leur serveur de messagerie ou leur serveur mandataire peut être utilisé de façon abusive par les spammeurs, et de les renseigner sur les moyens de sécuriser les serveurs pour éviter ce genre de problème. Il existe encore des relais et des serveurs mandataires ouverts, mais d'autres techniques de spam ont fait leur apparition. À cet égard, la FTC et ses partenaires internationaux, dans le cadre des activités du Plan d'action de Londres, ont lancé en 2005 l'opération "*Spam Zombies*", destinée à faire échec au piratage d'ordinateurs (« zombies »).

Un « zombie » est un ordinateur – en général connecté à une liaison Internet haut débit – qui a été délibérément contaminé par un ver ou un virus à l'insu de son propriétaire et qui peut être utilisé à n'importe quelle fin, par exemple pour lancer des attaques entraînant un refus de service et expédier des spams ou des courriels d'hameçonnage. Les zombies constituent un réseau qui fournit aux spammeurs une capacité de traitement combiné plus grande tout en drainant les ressources des serveurs de messagerie. La société de conseil Sophos, dans son rapport de 2005, affirme que les ordinateurs zombies sont responsables de 40 % des spams diffusés dans le monde. En mai 2005, Ciphertrust affirmait qu'en moyenne 172 009 nouveaux zombies avaient été identifiés chaque jour, essentiellement aux États-Unis, en Chine et en Corée. Les pays européens connaissent également le problème des zombies, l'Allemagne, la France, et le Royaume-Uni comptant en mai 2005 pour 14 % de la population de zombies identifiés[61]. Les données d'octobre 2004 de MessageLabs indiquaient que 79 % des spams avaient pour origine des "mandataires ouverts" ou des botnets zombies. En février 2005, ce chiffre était tombé à 59 %, bien que dans le même temps, le volume de spams n'ait pas diminué dans les mêmes proportions.

Dans le cadre de l'opération "Spam Zombies"[62], une trentaine de pays ont contacté les FAI du monde entier pour les inciter :

i) à bloquer le port 25, sauf dans certaines circonstances ;

ii) à appliquer des contrôles de débit sur les relais de messagerie ;

iii) à identifier les ordinateurs qui expédient des volumes atypiques de courriels et à prendre des mesures pour déterminer s'ils servent de zombies à des spammeurs ; au besoin, à mettre en quarantaine les ordinateurs concernés jusqu'à ce que l'origine du problème soit supprimée ;

iv) à donner à leurs clients des conseils clairs ; et

v) à leur conseiller les outils devant leur permettre de supprimer les codes zombies.

La première mesure préconisée, à savoir le blocage du port 25, ne fait toutefois pas l'unanimité. Un certain nombre de FAI, tout en étant disposés à contribuer aux initiatives concertées, sont peu disposés à assumer la responsabilité de la surveillance et de la remise en état des ordinateurs piratés de leur réseau.

De par la position qu'ils occupent, les fournisseurs d'accès à l'Internet sont en mesure d'exercer un certain contrôle sur la transmission des données. Pour cette raison, le rapport du Groupe de travail canadien sur le pourriel leur attribue un rôle fondamental dans la lutte contre le spam[63]. Les FAI pourraient agir en prévoyant dans leurs PUA des dispositions spécifiques pour lutter contre le spam, mais aussi en adoptant des pratiques exemplaires et des solutions techniques pour limiter les spams entrants et sortants. Dans le cadre des travaux sur la boîte à outils anti-spam du Groupe de réflexion de l'OCDE, le BIAC et le MAAWG ont élaboré une série de recommandations de pratiques exemplaires à l'intention des FAI et autres opérateurs de réseaux (Annexe II).

Les solutions techniques ainsi que les problèmes de fond liés au spam sont également traités par le MAAWG et par EmailAuthentication.org, qui ont été créés pour améliorer la coopération parmi un groupe d'entreprises de communications et de technologie. Le MAAWG, qui regroupe notamment AOL, Bell Canada, Comcast, EarthLink, France Telecom, Microsoft et Yahoo, travaille sur la collaboration entre les FAI, ainsi que sur la technologie et la politique gouvernementale. L'association Emailauthentication.org a été créée conjointement par la Direct Marketing Association (DMA), l'Email Service Providers Coalition, Microsoft, Bigfoot, Symantec et Sendmail. Elle bénéficie également du soutien du groupe de travail sur la lutte contre l'hameçonnage, de Yahoo et d'autres organismes. L'association vise à faciliter le déploiement et la mise en œuvre de normes et de solutions d'authentification de courrier électronique. À cette fin, elle a organisé le sommet sur la mise en œuvre de l'authentification du courrier électronique, qui a eu lieu à New York en juillet 2005. Le MAAWG a également publié en juillet 2005 son livre blanc sur les principes directeurs pour le déploiement de SPF/SenderID et en novembre 2005 ses Recommandations sur la gestion du port 25.[64] Des lignes directrices pour les communications entre opérateurs ont également été proposées par le MAAWG, notamment en ce qui concerne les modalités de remontée d'information sur les cas de spam et les réseaux de contacts opérationnels.

Il a notamment été suggéré que les opérateurs de messagerie élaborent une série de mesures définissant les usages autorisés et interdits de leurs services. Ces mesures peuvent être intégrées aux conditions de service ou dans les conditions générales d'utilisation (CGU), auxquelles les clients adhèrent lorsqu'ils signent leur contrat avec le fournisseur. Le non-respect de ces conditions entraîne la rupture du contrat, ce qui confère à l'opérateur le droit de suspendre le service ou de fermer le compte.

Le code de conduite définit également la position des opérateurs de services de messagerie à l'égard des courriels entrants. Les opérateurs doivent de fait s'efforcer de limiter le volume de messages non sollicités sortant de leur serveur, mais ils sont également capables de protéger leurs serveurs, réseaux, usagers et autres ressources applicables contre l'abus par les systèmes d'autres opérateurs. Cela implique la possibilité de prendre des mesures protectrices destinées à empêcher un système de messagerie abusif d'accéder à leurs ressources.

Banques et autres opérateurs en ligne

S'agissant des spams frauduleux et trompeurs et de l'escroquerie par hameçonnage, les opérateurs en ligne ont également un rôle important à jouer. La fraude par hameçonnage (voir l'introduction), par exemple, a pour support des courriels qui ressemblent à des messages légitimes provenant d'un service en ligne tel qu'une banque ou une cyberentreprise. La confusion est facile car les entreprises en ligne, qui utilisent de plus en plus le courrier électronique pour communiquer avec leurs clients, appliquent rarement un ensemble de règles normalisées et bien définies concernant le type d'information que peuvent ou ne peuvent pas contenir ces messages, leur forme et les moyens dont disposent les usagers pour détecter et signaler les communications frauduleuses.

A cette fin, plusieurs entreprises ont élaboré ou sont en train d'élaborer des politiques et lignes directrices internes pour contrer et prévenir efficacement les attaques par hameçonnage. Les entreprises peuvent agir sur plusieurs plans, notamment :[65]

- **Méthodes et normes de communication d'entreprise** : l'application de normes d'entreprise pour les sites Web, l'utilisation des domaines et le courrier électronique complique la tâche des hameçonneurs, qui ont plus de mal à abuser leurs cibles. L'entreprise doit définir et appliquer systématiquement des politiques claires en matière de courrier électronique – par exemple, ne jamais demander d'information à caractère personnel ou même ne jamais inclure de liens cliquables dans un courriel. Elle peut également envisager d'authentifier les courriels qu'elle envoie à ses clients ou d'utiliser la signature électronique.

- **Activités de blocage** destinées à faire obstacle à l'hameçonnage et à compliquer les manoeuvres des escrocs, notamment par des mesures visant à rendre le site de l'entreprise moins vulnérable aux attaques de marques : utilisation de noms de domaine sans ambiguïté, enregistrement défensif de noms de domaine (c'est-à-dire de noms de domaine similaires à celui de l'entreprise et susceptibles d'être confondus avec lui), surveillance de la fréquentation du site Web, vérification des avis de non-livraison, surveillance de sites ressemblants, etc.

- **Éducation et sensibilisation des clients**, service-clients. Les opérateurs en ligne devraient entretenir des communications efficaces avec leur clientèle. Ils devraient clarifier les types de communications qui pourront ou seront acheminées par voie électronique, spécifier que le client ne sera jamais invité à fournir des données personnelles par courriel et énumérer les éléments que les clients doivent vérifier dans le message, pour s'assurer qu'il provient bien de leur opérateur.

Actuellement, les politiques en matière de courrier électronique varient, de même que la quantité des informations et la fréquence des avertissements fournis. C'est pourquoi il serait souhaitable pour les banques et institutions financières, mais également pour tous les opérateurs en ligne qui utilisent le courrier électronique pour communiquer avec leurs clients de dresser un inventaire de pratiques exemplaires harmonisées en matière de courrier électronique, qui devrait s'inscrire dans une stratégie de sécurité plus globale.

Associations professionnelles

Les codes de conduite et les pratiques exemplaires sont en général élaborés par les associations professionnelles, qui se multiplient dans le secteur des TIC. Les opérateurs de télécommunications, les fournisseurs de logiciels, les fabricants, les fournisseurs d'accès à l'Internet adhèrent souvent à des associations qui ont pour objectif de défendre leurs intérêts communs, d'harmoniser leurs stratégies et de mettre en commun les meilleures pratiques, de faciliter la coopération et de faire face de façon concertée à certains des principaux problèmes touchant la technologie ou le service faisant l'objet de leurs activités. Il existe plusieurs associations nationales de FAI, comme l'Association des fournisseurs d'accès (AFA), en France, l'Australian Internet Industry Association (IIA), l'association des FAI allemands ECO et l'Association canadienne des fournisseurs Internet, qui sont particulièrement actives dans ce domaine.

Au niveau régional, EuroISPA est la fédération européenne des associations nationales de FA[66]. Son objectif est d'adopter une stratégie coordonnée en matière de services Internet au niveau européen, de représenter les intérêts du secteur auprès des institutions européennes et d'assurer l'interface entre les fournisseurs et les autres secteurs de l'industrie, par exemple les associations de marketing direct. Eurolspa est associée à l'initiative "spotspam", financée dans le cadre d'un projet communautaire et proposée par ECO, le membre allemand de la fédération. Ce projet a pour but de faciliter la collecte d'éléments de preuve et l'échange d'informations lorsqu'une poursuite est engagée à l'encontre d'un spammeur, et de

mettre à disposition une source d'information supranationale pour suivre les plaintes relatives aux spams[67]. EuroISPA fournit également des ressources à ses membres, et encourage l'échange d'informations et l'adoption des meilleures pratiques.

C'est pour contrer les menaces étroitement liées aux spams qu'a été créé le Groupe de travail contre l'escroquerie par hameçonnage, une association professionnelle réunissant notamment des fournisseurs de logiciels, des développeurs de solutions de sécurité informatique, et des opérateurs en ligne, dont l'objectif est de diffuser de l'information sur le problème, d'alerter les publics/entreprises concernés et de suggérer des moyens de faire échec à l'hameçonnage et à la fraude par courriel[68]. Le site Web du Groupe de travail est une riche source de données sur les nouvelles attaques par hameçonnage et « *pharming* », de statistiques sur la croissance et l'évolution du phénomène, et comprend un espace « membres » où il est possible d'afficher des documents, de poser des questions et de débattre de nouveaux problèmes.

Les sociétés de marketing direct et les opérateurs qui ont recours à l'envoi massif de courriels publicitaires sont concernés au premier chef par les mesures anti-spam car ils doivent veiller à ce que leurs messages soient conformes à la législation anti-spam et puissent franchir les filtres, de plus en plus nombreux, pour atteindre la boite de réception du destinataire/client. À cette fin, les associations de marketing ont élaboré des codes de conduite qui offrent une garantie de pratiques loyales et de respect des dispositions législatives applicables de la part des sociétés qui y adhèrent. Tel est le cas notamment du code de conduite de l'association australienne de marketing direct, qui limite la publicité par courriel non sollicité, ou les codes de déontologie de ses homologues françaises (UFMD et SNCD), qui ont été approuvés par la CNIL. Les codes et les pratiques exemplaires non seulement fixent des règles que les membres doivent respecter, mais fournissent également un guide par étapes pour la planification et la mise en œuvre des activités de cybermarketing[69]. Dans le cadre des travaux sur la boîte à outils anti-spam du Groupe de réflexion de l'OCDE, le BIAC a élaboré un ensemble de recommandations de pratiques exemplaires à l'intention des opérateurs de marketing par courrier électronique, qui est reproduit dans l'Annexe III.

Bien que les activités de marketing sur le réseau de téléphonie mobile ne soient pas encore aussi développées que le marketing par courrier électronique — essentiellement en raison du coût d'envoi des SMS —, le phénomène se développe, faisant déjà appel à d'autres supports, comme les fichiers vocaux, les messageries SMS, MMS, WAP, Java et SyncML, ainsi que la messagerie vidéo et audio, et pourrait prendre de l'ampleur à l'avenir en profitant de l'amélioration des liaisons sans fil par Bluetooth et UWB (Ultra Wide Band). Ces nouveaux outils offrent de nouvelles possibilités et fonctions aux usagers, mais ils présentent également un risque plus important de violation de la vie privée des consommateurs et de la sécurité. Pour cette raison, par exemple, Vodafone K.K. Japan a instauré en 2005 des limites sur l'envoi de SMS[70]. La branche britannique de la *Mobile Marketing Association* (MMA), une association professionnelle d'entreprises liées au marketing mobile et aux technologies connexes, a élaboré pour la profession en 2003 un code de conduite et des lignes directrices fondées sur les meilleures pratiques[71].

Ce code fournit des éléments d'orientation pour le développement de l'activité dans le cadre de la législation en vigueur ainsi que des lignes directrices émanant d'autres organismes professionnels, tels que l'ASA, la DMA et l'ICSTIS. Il indique également l'information qui doit être incluse dans ces communications, ainsi que la façon dont elle doit être formulée, fixe des règles spécifiques pour le marketing de types particuliers de produits et services, et le marketing destiné aux enfants. En outre, il énonce les conditions d'exercice du marketing mobile géolocalisé, et du marketing utilisant des numéros kiosque. D'autres pays membres de la MMA élaborent leurs propres codes, en s'inspirant des principes retenus dans le document britannique[72].

Du côté des opérateurs de services mobiles, l'Association GSM, face aux problèmes liés aux pratiques inter-opérateurs et transnationales des spammeurs, a élaboré un code de pratique pour le spam mobile (voir l'Annexe IV) qui devrait proposer les mesures techniques et juridiques que les opérateurs de services mobiles pourraient envisager pour faire échec au spam (Voir l'encadré 3). Dans ce cadre, les opérateurs invitent également les pouvoirs publics et les associations de consommateurs à agir en soutenant l'élaboration de mécanismes d'autorégulation professionnelle et le développement d'industries du marketing mobile et des services kiosque qui soient responsables. Comme pour le pourriel, les pouvoirs publics ont un rôle important à jouer pour aider les opérateurs de services mobiles, par exemple en réexaminant la législation nationale susceptible d'entraver les activités anti-spam et en réfléchissant aux mesures qu'ils pourraient prendre pour empêcher les spammeurs de tirer des revenus de leurs activités. Les autorités nationales peuvent aussi appuyer les enquêtes sur les abus et la fraude liés au spam et lever les obstacles à la capacité de l'opérateur d'enquêter sur les affaires de spam mobile.

Encadré 3. Opérateurs de services mobiles[73]

Les mesures et stratégies que les opérateurs de services mobiles peuvent envisager pour lutter contre le spam mobile sont les suivantes :

- Élaborer une politique anti-spam explicite interdisant l'utilisation des réseaux mobiles pour concevoir des opérations de spam mobile ou envoyer ce type de messages.
- Inclure les conditions anti-spam dans les contrats avec des tiers.
- Fournir aux clients l'information, les conseils et les ressources nécessaires pour lutter contre le spam mobile, y compris des mécanismes leur permettant de signaler des incidents suspects s'y rapportant.
- Surveiller les réseaux mobiles pour pouvoir détecter des signes de spam mobile et établir des procédures pour hiérarchiser les incidents suspects et y remédier.
- Adopter les techniques recommandées pour détecter et contrer le spam mobile et les messages frauduleux.
- Coopérer avec les autres opérateurs de services mobiles pour limiter au minimum le spam mobile sur les réseaux et mettre en commun l'information sur les pratiques exemplaires.

Le rôle des acteurs du secteur privé

De toute évidence, les acteurs privés ont un rôle actif à jouer dans la réduction du spam, en mettant en oeuvre des politiques judicieuses et en appliquant des solutions technologiques empêchant la diffusion du spam sur le réseau.

La mise en œuvre de codes de conduite et de pratiques exemplaires du côté des opérateurs pourrait contribuer à garantir la livraison des messages légitimes, ce qui améliorerait la disponibilité du service et aiderait les usagers à faire la distinction entre un message réel et une tentative d'usurpation d'identité par courriel (hameçonnage). L'adoption de règles harmonisées par les différentes catégories d'acteurs pourrait grandement contribuer à la mise en place d'un cadre anti-spam global. La question n'est pas de savoir à qui il incombe d'agir, mais qui est le mieux placé pour le faire.

ÉLÉMENT IV – TECHNOLOGIES ANTI-SPAM

Introduction

Le spam pose aussi des problèmes techniques complexes et les solutions mises en œuvre pour en venir à bout doivent s'appuyer sur des mesures techniques appropriées. Si l'intervention de la puissance publique et le rôle de la législation sont essentiels, ils ne suffisent pas à répondre aux défis lancés par le spam, les virus et les logiciels espions. En outre, du fait de la structure même de l'Internet, il est excessivement difficile pour les autorités d'exécution d'identifier les spammeurs et donc de les sanctionner.

De par sa nature, le spam ne se prête pas aisément à l'exercice de la définition. Pourtant, il existe des technologies et des techniques qui peuvent être mises en œuvre pour limiter le phénomène des courriels inopportuns. L'objet de cette section est de faire un tour d'horizon neutre des différents types d'outils et de méthodes de lutte, ainsi que des éléments à prendre en considération avant de mettre en œuvre ces parades.[74] Nous faisons spécifiquement référence à des outils plutôt qu'à des solutions. La technologie est conçue pour répondre à une grande partie des problèmes posés par le spam, et elle pourrait effectivement « résoudre » une partie des problèmes spécifiques liés au spam, mais une solution globale au spam ne peut être atteinte qu'à travers une approche multifactorielle à base de technologie, de mesures publiques (notamment de réglementation s'il y a lieu), de pratiques et de sensibilisation.

Les outils de la lutte anti-spam interviennent à des niveaux multiples – au niveau du point d'origine, de la dorsale, du point d'entrée et dans la machine du destinataire – et peuvent être utilisés seuls ou en combinaison. On trouvera des informations actualisées et des ressources sur le site web de la Boîte à outils à l'adresse www.oecd-antispam.org.[75]

Cette section s'adresse en particulier aux gestionnaires de serveurs de messagerie et fait le point sur les forces et les faiblesses de chaque technique de filtrage afin de les aider à choisir leur solution logicielle en fonction de leurs impératifs et de leurs besoins en matière de messagerie et de l'architecture qu'ils prévoient. L'accent est mis ici sur les pratiques utilisables à l'encontre du courrier entrant, à l'exclusion de celles destinées à réduire le courrier sortant.

Les outils qui s'adressent au problème du spam doivent intervenir à la fois sur le courrier et sur le comportement des utilisateurs en matière de messagerie. Étant donné cette multiplicité de facteurs, de nombreux instruments et méthodes s'appuient sur des séries de règles ou d'hypothèses opérant séparément ou en combinaison afin d'identifier les messages électroniques suspects. Peu à peu, le spam a envahi de nouveaux espaces et il véhicule toujours plus de virus et de logiciels malveillants. Cela nécessite une technologie défensive qui ne se limite plus aux outils de type textuel mais fait appel à des outils qui analysent des facteurs comportementaux et contextuels pour déterminer s'il convient d'accepter ou de rejeter tel ou tel courrier ou même certaines tentatives de connexion. Compte tenu de la menace accrue que le spam représente pour la sécurité, nous pensons que les technologies antispam s'appuieront davantage sur des technologies avancées de sécurité et d'authentification soit devront être conjugués avec ce type de technologies.

L'importance de l'outil et du contexte technologique

Une partie des outils et des technologies examinés dans cette section sont spécifiquement conçus pour être mis en œuvre au point d'entrée de la plate-forme de messagerie ; d'autres peuvent être plus utilement déployés après la réception des message mais avant leur présentation au destinataire final. A chaque niveau d'application du filtre, l'objectif d'une règle peut être soit de refuser ou de rejeter le message électronique, soit de le marquer, soit de le placer dans la boîte de spam de l'utilisateur final.

L'opportunité et l'utilité de chaque règle ne peuvent donc être estimées qu'en fonction du contexte précis dans lequel elle est appliquée, du niveau auquel est appliquée dans le processus de distribution des messages, et de ce qu'il advient de la communication en bout de course.

Conjugaison de tests

L'application judicieuse d'instruments technologiques doit être à la base de toute stratégie visant à venir à bout du spam. Il faut savoir qu'aucune des technologies que nous examinerons ne constitue un remède miracle ou une solution universelle à tous les problèmes posés par le spam. Toutes les technologies sont complémentaires et leur efficacité sera optimale si elles sont employées en conjonction les unes aux autres. L'intégration d'un certain nombre de technologies est nécessaire pour réduire l'impact négatif du spam sur un système.

Il faut insister sur le fait que ces tests ne sont pas nécessairement destinés à être utilisés en mode « tout ou rien ». Il est préférable de les combiner afin de maximiser le nombre de messages de spam interceptés, tout en minimisant le nombre de courriels légitimes interceptés ou refusés à tort.

- Refus « tout ou rien » : c'est l'une des actions possibles pour les services qui utilisent une liste noire. Tout message qui ne passe pas le test est refusé. L'occurrence d'erreurs dépend toutefois du point où est appliquée la règle dans le processus de distribution.

- Privilège d'accès : c'est l'une des actions possibles pour les serveurs qui utilisent une « liste blanche ». Tout message qui passe le test est accepté. Pas de risque de rejet de messages légitimes, mais risque de faux négatifs. Par exemple, une liste blanche de domaines n'a pas vraiment d'intérêt si le domaine de l'expéditeur n'est pas authentifié (avec Sender Policy Framework ou DomainKeys Identified Mail, DKIM).

- De nombreux messages de spam ou vers se revendiquent de marques reconnues dans l'espoir de bénéficier de privilèges d'accès.

- Notation – c'est de cette façon que des programmes tels que SpamAssassin (de même que ProcMail) combinent plusieurs tests. La notation est vivement recommandée pour éviter les inconvénients du « tout ou rien » mais elle est coûteuse en ressources machines et demande une mise à jour permanente des facteurs de notation afin d'optimiser la détection tout en minimisant les « faux positifs ».

La méthode classique est d'appliquer plusieurs tests « tout ou rien », puis d'attribuer une notation aux messages qui ont été autorisés.

La pratique recommandée consiste à combiner plusieurs techniques, sans toutefois les multiplier de manière excessive car trop de complexité risque de pénaliser la fiabilité du système de livraison du courrier.

Types de technologies anti-spam

Authentification du courrier électronique

La première chose qu'il faut noter est que les méthodes d'authentification du courrier relèvent de la catégorie des règles qui, si elles contribuent à la lutte contre le spam, ne constituent pas des technologies spécifiques anti-spam.

Cet aspect est plus facile à comprendre si on a recours à une analogie. Une carte d'identité ne constitue pas une « marque de confiance », dans la mesure où les malfaiteurs peuvent aussi en avoir une. Mais l'obligation de la transparence est plus favorable aux expéditeurs légitimes qu'aux spammeurs.

SPF ou Sender-ID

L'un des principaux facteurs qui favorisent la prolifération du spam est la possibilité pour les spammeurs de masquer la véritable adresse de réponse de leurs messages. L'architecture du courrier électronique ne suppose pas qu'il y ait contact préalable entre l'expéditeur et le destinataire. Il n'est donc pas possible d'utiliser une authentification systématique. Le problème est de plus en plus préoccupant car des adresses falsifiées sont utilisées dans des escroqueries de hameçonnage qui trompent les destinataires afin de leur soutirer leurs numéros de cartes bancaires ou d'autres informations personnelles.

Cette technologie encore émergente souffre d'un manque de standardisation ; elle consiste à marquer ou bloquer les messages dont le véritable expéditeur ne peut être vérifié. Le principal avantage de l'authentification de l'expéditeur est qu'elle place la charge de la dissémination du spam sur l'expéditeur et non sur le destinataire, et qu'elle rend plus difficiles les opérations de hameçonnage. Le surcoût pour l'expéditeur est compensé par la garantie que le message sera livré si l'expéditeur est authentifié et fait un usage légitime du système. Les détails spécifiques du processus de vérification varient selon le modèle choisi et plusieurs modèles d'authentification des serveurs existent actuellement. Parmi les plus répandu, citons Sender Policy Framework (SPF) et Sender-ID.

Ces deux techniques peuvent être examinées ensemble parce qu'elles présentent un certain nombre de caractéristiques communes. Le choix de l'une ou de l'autre est toutefois moins évident.

SPF et Sender-ID peuvent être utilisées pour vérifier si un serveur de messagerie est bien autorisé à expédier du courrier pour le compte d'un domaine donné. Il faut pour cela publier un enregistrement dans le serveur de noms de domaines (DNS) qui donne la liste des serveurs de messagerie autorisés pour un domaine donné. Les deux techniques diffèrent essentiellement sur le choix de l'identité sur laquelle porte le test. SPF teste le champ MAIL FROM (2821) de l'enveloppe, alors que Sender-ID teste les en-têtes (2822).

Les administrateurs de serveurs prennent deux types de mesures : ils publient les enregistrements SPF dans le DNS et les testent à l'entrée.

Actuellement, rares sont les domaines qui publient des enregistrements SPF : l'intérêt pour ce système est donc limité. Certains administrateurs notent que Sender-ID est un concept nouveau qui n'a pas encore été expérimenté à grande échelle. Ces deux techniques ne s'appuient pas encore sur un standard stable.

L'authentification du courrier électronique par vérification de l'adresse IP du serveur de l'expéditeur contribuera à réduire et à gérer le spam dans l'avenir. Cela nécessitera probablement la création de services qui complètent l'authentification : listes blanches privées, services de réputation et services d'accréditation, par exemple.

A savoir : Les tests SPF et Sender-ID peuvent être appliqués à l'entrée. S'agissant d'outils émergents, les utilisateurs sont invités la prudence en les utilisant tant qu'ils ne seront pas plus largement adoptés, sauf en cas d'indication du serveur distant ou dans des contextes particuliers. L'authentification est une composante essentielle de toute procédure de sécurité du courriel. Le SPF est de loin la technique la plus répandue. Il est aussi recommandé de publier ses enregistrements SPF et Sender ID.

DKIM ou META

Les systèmes DKIM (DomainKeys Identified Mail) et META (Message Enhancements for Transmission Authorization) sont utilisés pour authentifier le domaine de l'expéditeur au moyen d'une signature cryptographique automatiquement ajoutée par le serveur de messagerie. Actuellement ces techniques présentent très peu d'avantages pratiques immédiats car peu de domaines signent leurs messages. De plus, les administrateurs noteront que ces trois techniques ne s'appuient pas encore sur un standard stable.

L'authentification du courriel par signature cryptographique pourrait contribuer à la réduction et à la gestion du spam dans l'avenir.

Le DKIM est le plus connu de ces modèles. Il fonctionne en imposant une signature numérique, ou clé privée, sur tous les messages sortants. Les messages entrants sont authentifiés au niveau du domaine et du serveur de messagerie en vérifiant que la clé privée correspond à la clé publique qui figure déjà sur le fichier. Cette méthode permet de s'assurer que le message vient forcément du FAI d'origine.

A savoir : Ces techniques peuvent être étudiées et testées. Il faut noter qu'il s'agit de technologies émergentes et tant qu'elles ne sont pas déployées à grande échelle, il est probablement prématuré de s'en remettre à elles à l'heure actuelle.

Existence du domaine de l'expéditeur et demande de réponse

Nombreux sont les spammeurs qui opèrent à l'aide d'une adresse d'expéditeur non existante. Une règle peut être utilisée pour refuser ces messages, comme la directive Postfix « reject_unknown_sender_domain » ou l'instruction BadMX de j-chkmail. Il est aussi possible de vérifier la validité de l'enregistrement du serveur entrant (MX) pour le domaine indiqué dans le champ « De : » du message. Certains spammeurs ont recours à un faux enregistrement MX pour éviter de recevoir des messages de protestation courroucées (par exemple, le MX pointe vers l'adresse 127.0.0.1, c'est-à-dire celle du PC local).

L'application de ces règles génère un volume modeste de trafic DNS, mais ce trafic aurait probablement existé du fait de la réponse ; elle permet aussi de rejeter un certain volume de spam.

A savoir : Cette technique n'est pas très répandue. La gêne provoquée est minimale, puisque si le domaine de l'expéditeur n'existe pas, il sera difficile (mais pas impossible grâce au mode automatique de la fonction « Reply to ») de répondre au message. Il ne faut pas envoyer de messages en utilisant un compte sans adresse de réponse.

Existence d'un enregistrement de ressource pointeur (PTR)

Un enregistrement PTR peut être inséré dans le DNS pour traduire sous forme de nom l'adresse IP du serveur de l'expéditeur, même s'il n'y a pas nécessairement vérification que ce nom correspond bien au domaine de l'expéditeur.

L'ajout de cet enregistrement n'est pas toujours contrôlé par le domaine de l'expéditeur (s'il n'y a pas délégation addr.arpa par l'IP, par exemple) et ce dernier, même s'il est légitime, peut ne pas être en mesure de satisfaire à cette obligation. Ces enregistrements peuvent être utilisés pour rechercher la source d'un courriel et déterminer dans quelle mesure on peut avoir confiance. Ils peuvent aussi servir à déterminer si un courriel provient d'une adresse IP résidentielle ou pour réexpédier un message d'erreur au bon serveur.

A savoir : Le test de ce critère peut être utile pour indiquer dans l'en-tête du courriel que le champ est vide ou suspect (par exemple s'il n'a pas abouti à une adresse IP suite à une requête directe). Le champ PTR peut toujours être utile (particulièrement si le serveur distant coopère) pour renvoyer certaines informations au destinataire. Toutefois, il faut éviter de se fonder sur ce test pour rejeter un courriel au seul motif que le champ PTR de l'IP qui se connecte n'a pas de contenu. Le rejet d'un courriel sur la base de ce test n'est recommandé que si les circonstances (par exemple si le champ peut être utilisé pour déterminer l'origine du message) ou le règlement de l'organisation (rejet de messages provenant d'adresses IP résidentielles particulières) le dictent.

Listes noires et listes blanches

Le filtrage traditionnel et le suivi des plaintes déposées au sein de groupes d'utilisateurs peuvent à terme aboutir à la création de listes blanches d'expéditeurs acceptés et de listes noires de suspects de spam. La méthode des listes blanches et listes noires est souvent une solution trop radicale pour être acceptée par la plupart des utilisateurs. Les listes blanches prennent du temps à créer et nécessiteront une mise à jour continuelle. Les listes noires exigent également un suivi permanent. Toutes les listes doivent être assorties de mécanismes et de procédures de mise à jour pour corriger les faux positifs et traiter les plaintes frauduleuses d'inscription sur la liste. L'usurpation d'identité (spoofing) et l'utilisation de relais ouverts peuvent aussi créer des problèmes liés à la source dont semble provenir le courriel.

Les listes noires consistent à recenser des sources de spam. Elles peuvent comprendre le nom des machines, les adresses IP et les adresses électroniques. Elles peuvent être tenues par une entité pour une utilisation partagée, à moins qu'elles ne soient créées et tenues à jour au niveau du serveur pour ses propres besoins.

Avec des agents de transfert de courrier (MTA) à jour, ce test peut être effectué au niveau de la session SMTP et peut donc aboutir à un rejet avant même que le message soit envoyé. Certaines listes contiennent des relais ouverts qui n'envoient pas seulement du spam. Leur configuration en relais ouvert peut être considérée comme un comportement illégitime par les plates-formes auxquelles sont envoyés les messages.

Les listes noires varient considérablement en qualité, selon le degré de professionnalisme de celui qui les tient. Beaucoup sont mal gérées, abandonnées ou d'intégrité douteuse : les noms peuvent être ajoutés hâtivement, les critères appliqués ne sont pas forcément clairs et la radiation de la liste peut être quasiment impossible ou soumise à paiement. Ce problème s'explique principalement par l'absence d'un code de conduite ou d'une autre forme de régulation pour organiser et limiter le fonctionnement des listes noires. Si cette solution doit être utilisée dans le futur, il faudra un effort coopératif pour établir une liste de bonnes pratiques, définir clairement les cas où des adresses peuvent être inscrites en liste noire et les modalités de leur radiation.

Les listes noires contiennent inévitablement des erreurs qui empêche certains messages légitimes de parvenir jusqu'au consommateur. Ce problème dit des « faux positifs » a donné lieu à des poursuites judiciaires, des expéditeurs légitimes estimant figurer par erreur sur la liste noire d'un FAI. De plus, le problème des faux positifs pour les utilisateurs individuels peut présenter l'inconvénient non négligeable de compter uniquement sur les technologies classiques de filtrage pour bloquer le spam.

Si leur utilisation pose de nombreux problèmes, les listes noires constituent une solution rapide pour bloquer la connexion avec des machines dont le comportement compromet la sécurité ou la qualité des services de la plate-forme à laquelle le courrier est envoyée, ou rejeter les messages provenant de certains expéditeurs.

A savoir : Il convient de faire preuve de discernement dans le choix de la liste à utiliser. Avant de choisir, il serait souhaitable de considérer un certain nombre de points :

- Utiliser des listes qui sont bien gérées.
- S'assurer que leur administrateur est un professionnel, qui répond et réagit.
- S'assurer que les critères d'inscription et de suppression sont clairs, raisonnables et accessibles.

  Lorsqu'on utilise une liste externe, son activité doit être suivie parce que la qualité peut évoluer au fil du temps. Si un administrateur tient sa propre liste noire (ce qui représente une certaine dépense de ressources), les critères de qualité ci-dessus vont bien sûr s'appliquer aussi. Comme il est difficile de produire une synthèse rapide des listes noires, étant donné leur variété, la prudence est recommandée.

Adresse du serveur expéditeur traitée comme « dynamique » ou « résidentielle »

Il s'agit d'une forme particulière de liste noire dans laquelle le critère d'inscription est le fait que l'adresse IP bloquée correspond à la machine d'un abonné individuel à un FAI et non au serveur de messagerie d'une organisation. L'idée est qu'un abonné ordinaire n'envoie pas de courrier directement au serveur SMTP, mais passe par le PTA de son fournisseur d'accès. Cela signifie que la machine bloquée envoie directement des messages pour le compte d'un spammeur, ou plus généralement que les messages sont envoyés à l'insu du propriétaire de la machine (la machine a été corrompue et transformée en « zombie » pour envoyer les messages).

Les listes d'adresses de ce type ne sont pas toujours fiables car la plupart d'entre elles ont été compilées en fonction de critères heuristiques, comme la présence du terme « adsl » dans le nom de la machine. La gestion de ces listes mobilise aussi d'importantes ressources.

En revanche, certaines de ces listes, notamment celles compilées par le serveur qui les utilise, peuvent être utilisées pour distinguer entre les serveurs autorisés pour un domaine et les listes résidentielles. De plus, certains domaines publient les plages d'adresses résidentielles pour leur domaine.

Ce test peut être considéré comme une source de discrimination entre les « consommateurs purs » et les fournisseurs. Ces derniers considèrent comme légitime la règle selon laquelle le propriétaire d'un domaine refuse de connecter ses machines aux adresses résidentielles, car celles-ci constituent actuellement la principale source de spam. Mais les consommateurs font valoir que le spam existe et qu'il faut protéger la liberté d'utiliser le courriel.

Les filtres

Le filtrage est la technologie anti-spam la plus répandue. Les principaux atouts des filtres sont la facilité de leur mise en œuvre et la latitude laissée aux utilisateurs de décider quels messages doivent être traités comme du spam. Les filtres heuristiques nécessitent que les utilisateurs donnent des critères, qui peuvent être des mots clés ou des adresses d'expéditeurs, qui déclenchent le filtre pour empêcher certains messages de parvenir jusque dans la boîte de réception du consommateur. Il est facile pour les spammeurs d'utiliser des graphies délibérément fautives ou d'écrire les mots dans une langue différente pour contourner le filtrage par mots-clé. Les filtres Bayesiens sont fondés sur l'expérience. Ils produisent des statistiques sur les messages dans une table de reconnaissance à laquelle les utilisateurs individuels pourront par la suite se référer pour distinguer entre le spam et les courriels légitimes. Le filtre ne laisse alors passer que les messages qui s'apparentent aux courriels légitimes que l'utilisateur a reçus par le passé.

Filtres heuristiques

Ces filtres consistent à tester la présence dans le message de certaines caractéristiques typiques du spam, comme l'utilisation exclusive du html ou le type de clients auquel le message est adressé. Le filtre attribue à chaque critère une pondération calculée par apprentissage par référence à une série de courriels connus comme des spams et une série de courriels connus comme légitimes (les scores ne sont donc pas calculés par un humain afin d'éliminer la subjectivité). L'un des filtres les plus connus et les plus utilisés est SpamAssassin. Yahoo!, Hotmail, et AOL, entre autres, utilisent des filtres heuristiques dans leurs systèmes de filtrage du junk mail.

Le risque de ces filtres est que certains messages présentant des caractéristiques de spam (les messages spectaculaires en html, par exemple), seront traités comme du spam. De plus, il faut noter que les filtres mobilisent d'importantes ressources machine.

Ces filtres permettent de détecter une importante proportion de spam, et ne nécessitent ni apprentissage ni configuration. Mais ils utilisent un grand nombre de tests, et mieux vaut savoir qu'il est possible de choisir quels tests sont pratiqués ainsi que les scores retenus pour déterminer qu'un message est du spam.

A savoir : D'une installation aisée pour l'utilisateur, ces filtres offrent un filtrage efficace et ne demandent que peu de travail à l'administrateur. Il faut prendre soin de mettre à jour régulièrement la base de tests, exactement comme pour un anti-virus. Une version d'un programme anti-spam qui date de 2 ans ne va pas bloquer beaucoup de spam, car le spam a évolué. Le risque de faux positifs doit être contrôlé et il faut ajuster les critères de filtrage. De même, certains des filtres mis en œuvre dans le B2B peuvent notifier au destinataire que certains messages ont été supprimés pour qu'il puisse voir si le filtrage a été fait à bon escient.

Filtres par mots clés

Il s'agit de filtres binaires qui recherchent un mot clé (par exemple « viagra »). Le risque de faux positifs est très élevé et ces filtres sont très faciles à contourner : il suffit de rajouter un espace entre chaque caractère, d'intervertir des caractères ou d'utilisant des graphies fautives.

A savoir : Ces filtres manquent de finesse d'analyse et d'efficacité, sauf dans des cas spécifiques au contexte.

Filtres sur empreinte

Les filtres sur empreinte de type Razor consistent à construire une empreinte du message qui leur est soumis et à indiquer s'il a déjà été identifié comme étant du spam. Cela produit de nombreux faux négatifs : plusieurs types de spam ne sont pas identifiés, même lorsque le serveur les analyse à l'aide de Razor. De plus, un message peut parfois varier suffisamment pour produire une empreinte différente. L'une des solutions à ce problème est de retenir le courriel (comme dans les listes grises). Cela produit peu de faux positifs.

Filtres Bayesiens

En guise d'introduction, il faut noter que les techniques décrites ne concernent pas la configuration individuelle de la machine d'un utilisateur mais celle d'un serveur de groupe.

Le principe de fonctionnement du filtre Bayesien est de préparer le moteur en lui présentant une série de courriels identifiés comme du spam et une série de courriers identifiés comme légitimes ; après un apprentissage du vocabulaire utilisés par les spammeurs à partir de cette série, le filtre utilise les probabilités Bayesiennes pour calculer si un message est du spam. Dans le cas d'un filtrage de groupe, l'apprentissage est généralement conduit par l'administrateur du système.

Ces filtres, qui s'appuient sur le concept de vocabulaire du spam, peuvent poser problème lorsqu'ils sont appliqués en environnement partagé. Dans un environnement d'échelle réduite et extrêmement uniforme (par exemple au sein d'une entreprise ou d'un département d'université, où chacun travaille dans le même domaine et utilise des vocabulaires voisins), cela peut fonctionner. Mais ce ne sera pas le cas pour un grand fournisseur de services de messagerie et particulièrement pour un FAI public, sauf si la base

partagée permet à chaque utilisateur individuel de personnaliser le filtre pour sa propre boîte de réception. Le problème est qu'un vocabulaire considéré comme acceptable par certains utilisateurs peut déclencher le filtre s'il a été qualifié de vocabulaire de spam au niveau du groupe.

Malgré les problèmes qu'ils peuvent poser au niveau du groupe, ces filtres sont extrêmement efficaces s'ils sont utilisés par des individus et constituent l'une des rares solutions qui, appliquée isolément, peuvent filtrer la quasi-totalité des courriels de spam après un apprentissage adapté. Microsoft propose un filtrage Bayesien personnalisable dans ses logiciels Outlook et Exchange Server. On peut citer également le programme gratuit Bogofilter (www.bogofilter.org).

A savoir : Ces filtres sont à utiliser au niveau individuel, ou doivent être personnalisables par les utilisateurs.

Filtres comportementaux

Ce type de filtres examine le comportement du serveur distant, en regardant par exemple le nombre de courriels envoyés dans un intervalle de temps donné. La limitation du débit constitue un exemple de ce type de filtrage. L'idée est que les courriels ordinaires sont expédiés individuellement ou en très petit nombre, alors que les spams sont envoyés en très grands nombres.

Ce type de filtrage est extrêmement délicat car il n'y a généralement aucun moyen de faire la distinction entre un spammeur et un serveur de listes de diffusion légitime comme un newsgroup.

D'après certains experts, il n'y a rien de choquant à ce qu'une plate-forme refuse certains volumes de courriels, essentiellement eu égard à ses propres dimensions ou au rôle de sécurité qu'elle doit assurer sur ses réseaux. Il n'est pas choquant de demander aux expéditeurs de courriel en grand nombre de respecter les ressources de la plate-forme distante en supportant une partie du coût de la distribution de leurs messages en leur demandant de ne pas les envoyer trop rapidement pour se défausser des coûts inhérents à l'utilisation du courriel comme mode de communication.

A savoir : Selon les règles appliquées par le destinataire, ce type de filtre peut être utilisé soit pour limiter les flux soit pour bloquer des courriels entrants. Dans ce dernier cas, le motif du rejet doit être accessible à l'expéditeur afin qu'il puisse se conformer aux règles de distribution.

HELO/CSV

Un ordinateur d'expédition s'identifie par son nom à un ordinateur de destination au début de chaque transaction SMTP. La commande SMTP qu'utilise l'ordinateur d'expédition pour s'identifier en donnant son nom à l'ordinateur de réception est appelée commande « EHLO » ou « HELO ».

Le service Certified Server Validation (CSV) offre un dispositif permettant à un serveur recevant du courriel d'évaluer un serveur d'expédition de courriels. Il s'appuie sur une pratique existante des fournisseurs de service qui accréditent les réseaux depuis lesquels les systèmes expéditeurs se connectent.

La fonction HELO vérifie que le MTA distant est bien configuré, mais ces tests ne permettent pas de déterminer si l'expéditeur est un spammeur ou non. Le test CSV ajoute un test de probabilité sur le nom : correspond-il vraiment à un domaine ? A la différence de SPF et de DKIM, CSV n'authentifie pas le domaine qui expédie le message, mais celui du serveur de courriel (ce peut être deux serveurs différents, par exemple dans le cas d'un FAI desservant un grand nombre de clients).

Les directives de configuration (par exemple la directive *reject_invalid_hostname* de Postfix) testent le nom annoncé par le serveur. L'utilisation de tests HELO classiques entraîne le rejet d'un très grand nombre de messages légitimes. En fait, actuellement seuls un très petit nombre d'administrateurs de sites savent modifier HELO pour qu'il fonctionne convenablement. Cette situation va probablement changer prochainement car des sites de plus en plus nombreux vont appliquer le test HELO, ce qui poussera à son amélioration.

A savoir : Ces solutions peuvent être envisagées lorsqu'elles concernent la configuration.

Listes grises

Il s'agit d'envoyer délibérément un code d'erreur SMTP 4xx (erreur temporaire, par opposition à l'erreur définitive 5xx, voir RFC 2821) lorsqu'on est en présence d'un nouvel expéditeur. Ce dernier, s'il s'agit d'un MTA normal, va réessayer l'envoi (généralement quinze minutes plus tard) et son message sera alors accepté. La plupart des logiciels de spam ne font pas de multiples tentatives d'expédition. Cette technique est extrêmement efficace et bloque tous les courriels de spam qui ne sont pas expédiés depuis un relais ouvert ou par le MTA d'un fournisseur. Elle empêche la réception de certains message envoyés depuis des serveurs mal configurés et se prête particulièrement bien à l'utilisation en conjonction avec une liste blanche.

A savoir : Cette technique est simple à mettre en œuvre mais son avenir demeure incertain : si tout le monde l'adopte, les spammeurs se remettront à faire des tentatives multiples. Son utilisation pourrait permettre à des techniques comme les filtres à empreintes de faire leurs preuves, avant qu'elle ne perde en efficacité suite aux ajustements des spammeurs.

Tokens et mots de passe

L'objet de ces techniques est d'inclure un mot de passe dans l'adresse à laquelle est envoyé le courriel ou d'utiliser un système défi-réponse de type test de Turing. Le logiciel du spammeur ne connaîtra pas le mot de passe et sera incapable de passer le test.

Ces techniques ne produisent pas de faux négatifs – sauf si les spammeurs décidaient d'employer des milliers de personne à de très faibles salaires pour faire ce travail.

Un certain nombre d'utilisateurs légitimes vont refuser de passer le test ou en seront incapables. Il y aura donc beaucoup de faux positifs. Ces techniques ne sont intéressantes que pour les destinataires très connus qui reçoivent déjà de grandes quantités de courriels en masse (dont une partie de courriels légitimes), ou pour des destinataires qui souhaitent réduire le nombre de messages qu'ils reçoivent, ce qui relève de la liberté de communication. Il faut savoir également que tous les expéditeurs n'accepteront pas le test imposé. En sensibilisant les utilisateurs sur les intérêts de cette technologie on peut les inciter à passer les tests pour réduire le taux de non acceptation.

A savoir : Ces filtres ne constituent pas tant une technique de filtrage qu'un élément d'une politique de liste blanche. Les utilisateurs de ces filtres doivent en être conscients. Voir le paragraphe précédent.

Techniques diverses

Dans cette section, nous allons passer en revues différentes techniques, pour la plupart expérimentales ou insuffisamment testées.

Tests de l'enveloppe (BATV, SES)

Ces techniques sont encore récentes et leur déploiement est insuffisant pour qu'elles soient envisagées.

Certification des courriels envoyés en masse

Réputation de l'expéditeur

Si une authentification efficace de l'expéditeur laisse aux fournisseurs d'accès Internet (FAI) un rôle beaucoup plus simple dans le traitement du spam, l'authentification n'est qu'une étape préliminaire vers l'élimination du spam. Une fois que l'expéditeur peut être identifié, des facteurs tels que la réputation et l'accréditation sont nécessaires pour déterminer si un message doit être considéré comme du spam avant d'atteindre le destinataire. Le processus de certification serait géré et les critères fixés par des autorités indépendantes. Un conseil de surveillance, comprenant une représentation plurisectorielle, superviserait les autorités de certification.

A cette fin, la norme TEOS (Trusted Email Open Standard) a été créée par le groupe ePrivacy. TEOS est le fruit du programme d'auto-régulation sectorielle ePrivacy, qui a pour but de séparer le courriel légitime du spam. TEOS va au-delà de l'authentification et crée une identité de confiance pour les expéditeurs de courriel à partir des signatures contenues dans les en-têtes. A la différence des signatures d'authentification du système DKIM, les signatures TEOS sont des « sceaux » visibles dans le message et certifient que l'expéditeur remplit les critères spécifiés.

Un certain nombre d'autres acteurs sont en train de mettre en place des dispositifs basés sur la réputation des expéditeurs. America Online (AOL) et EarthLink utilisent le système SPF pour vérifier leur courrier sortant. Brightmail et Microsoft utiliseront le modèle de Brightmail pour mener des tests conjoints sur l'efficacité des systèmes fondés sur la réputation de l'expéditeur. De plus, un fournisseur de systèmes de messagerie sécurisés, Sendmail, va travailler en collaboration avec Yahoo! pour tester DKIM.

A savoir : A la différence des services par authentification, qui fonctionnent de manière plus empirique, les services fondés sur la réputation et les autres services risquent d'avoir une composante subjective plus importante marquée par les règles et les pratiques du fournisseur. Seul le temps permettra d'évaluer le fonctionnement des différents services, leur crédibilité et leur utilité.

Pour atténuer le problème des courriels expédiés en masse qualifiés à tort de spam, les acteurs du secteur continuent d'examiner l'efficacité d'un mécanisme de certification pour le courriel expédié en masse. Par exemple, les courriels en masse légitimes pourraient être identifiés au niveau du FAI par une étiquette reconnue par le serveur, ce qui permettrait une utilisation plus fiable des filtres de courriels. Plusieurs critères pourraient être retenus dans le paramétrage du processus de certification, par exemple l'engagement à se conformer à des pratiques strictes en matière de respect de la vie privée. Par exemple, la France travaille avec son agence de protection des données, la Commission nationale de l'informatique et des libertés (CNIL), sur un projet de certification des expéditeurs qui notifient l'utilisation de fichiers clients.

Chaque FAI tiendrait une liste blanche de clients certifiés. Cette proposition exige un accord entre FAI sur le processus de certification et ne nécessite pas d'intervention extérieure. Mais pour que cette méthode soit efficace il faudrait une masse critique de FAI, et une confiance entre FAI, puisqu'il n'y a pas de supervision extérieure du processus de certification. De plus, il peut être délicat de fixer un nombre donné pour définir les envois de masse. Des spammeurs astucieux pourraient utiliser un grand nombre de comptes de messagerie gratuits pour envoyer des volumes importants de spam, en veillant à ce que le nombre de message envoyés depuis chaque compte soit tout juste inférieur au seuil prédéfini pour l'envoi en masse.

Systèmes de micro-paiement

Conceptuellement, la solution la plus simple au problème du spam serait de faire payer l'envoi de chaque message, exactement comme pour le courrier postal classique. Cette solution demanderait d'apporter des modifications structurelles au protocole SMTP et nécessiterait de créer un système garantissant la distribution de chaque message sans risque de rejet par un FAI sur la base d'un soupçon de spam « non standard ». L'argent est le premier moyen de paiement qui vient à l'esprit pour le paiement mais d'autres idées ont été proposées.

Par exemple, Microsoft propose une approche « computationnelle » qui consisterait à faire payer chaque courriel envoyé non en argent mais sous la forme d'un « impôt en temps de calcul ». Microsoft propose en effet de porter à dix secondes le temps de traitement nécessaire à l'envoi des courriers non sollicités. Ce projet n'affecterait guère les internautes qui envoient peu de courriels, mais ceux qui envoient des millions de messages par jour se verraient contraints à de lourds investissements en ressources informatiques supplémentaires, avec un effet dissuasif non négligeable contre l'envoi de spam. Avec cette approche, les utilisateurs pourraient choisir de tenir une liste blanche dont les membres seraient exemptés de l'impôt computationnel.

Autre variante, le programme Bonded Sender d'IronPort, qui est un programme de certification par liste blanche dans lequel l'expéditeur de courriels en masse doit fournir une garantie financière pour être accrédité. Si l'expéditeur enfreint les pratiques acceptables en matière de courriel, une amende est prélevée sur la garantie. Le montant de ces garanties peut aller de 500 USD à plus de 4000 USD selon le volume mensuel de courriel envoyé. Les infractions et les amendes sont basées sur les plaintes des utilisateurs. Microsoft a conclu un partenariat avec IronPort et va utiliser le programme Bonded Sender pour le courrier entrant sur ses comptes MSN et Hotmail.

Le serveur de l'expéditeur répond-il si vous essayez de répondre ?

Pas de recommandations particulières concernant l'usage de cette technique.

Signatures PGP

Cette technique est actuellement beaucoup trop peu utilisée pour être prise en considération ici.

Configuration du système

Les bonnes pratiques de sécurité pour les entreprises et les particuliers en matière de ports, de pare-feux, de réseaux, de routeurs, de proxies, d'accès, de mots de passe, de protection des clés d'autorisation et d'installation de logiciels constituent des exemples d'utilisation de la configuration du système comme technologie anti-spam. En configurant son système de manière à bloquer les courriels non sollicités, on n'intercepte qu'un certain pourcentage de spam. A mesure qu'un nombre croissant de systèmes se dotés de tels mécanismes, les spammeurs deviendront certainement de plus en plus ingénieux, mais en même temps, plus il y a d'obstacles à surmonter, moins il devient intéressant d'envoyer du spam. Aujourd'hui, les

gens envoient du spam parce que c'est simple, rapide et que cela ne coûte pas cher. Avec le temps cela le sera de moins en moins – des centaines de milliers d'administrateurs systèmes y travaillent – et il sera plus difficile d'atteindre son but par le spam.

Outils anti-virus

Les anti-virus sont des outils importants pour réduire le risque d'infection des systèmes informatiques par des courriels de spam. Généralement, les spams nocifs sont accompagnés de fichiers qui peuvent déclencher des virus. Les logiciels anti-virus analysent les boîtes de courriel et préviennent les infections virales.

Un certain nombre de FAI surveillent et actualisent en permanence les interfaces API (application programming interface) des anti-virus, ou VSAPI, avec Exchange Server. Cette technologie consiste à effectuer l'analyse anti-virus au niveau des boîtes de messagerie des utilisateurs, afin d'effectuer l'analyse hors du périmètre du réseau et prévenir ainsi l'impact des virus et des courriers infectants sur les infrastructures de réseau. Il est aussi possible d'empêcher les courriels infectés de quitter une organisation en analysant non seulement le courriel entrant, mais aussi le courriel sortant. Le système anti-virus Clam Antivirus http://www.clamav.net/ est un exemple de logiciel gratuit qui remplit la même fonction.

Outils anti-logiciels espions

Les logiciels espions sont une menace non négligeable pour les entreprises, car de façon subreptice, ils collectent des informations et déclenchent l'affichage de fenêtres « pop-up » publicitaires. Les logiciels espions et les enregistreurs de touches sont utilisés par des pirates malintentionnés pour capter des adresses e-mail, des mots de passe et des numéros de cartes de crédit. Globalement, les logiciels espions ralentissent le fonctionnement de l'ordinateur, prennent le contrôle des navigateurs web et envoient des informations personnelles aux annonceurs. Les outils anti-logiciels espions peuvent aussi détecter les courriels de spam dangereux, ce qui peut contribuer à la réduction du volume de spam.

Comment utiliser cette revue de technologies et quels facteurs prendre en compte ?

L'utilité d'un outil quel qu'il soit dépendra des besoins, de la capacité technique et de l'infrastructure de l'utilisateur de cet outil. Les outils sont conçus pour être mis en place en différents points du système et avec des finalités différentes. Les utilisateurs devront analyser en profondeur leurs besoins et leurs stratégies de défense pour choisir et mettre en œuvre leurs outils anti-spam. Les outils eux-mêmes ne sont pas non plus identiques en termes de maturité, d'efficacité, de fiabilité et de simplicité de mise en œuvre. Certains outils produiront davantage de faux positifs, certains sont particulièrement efficaces dans certains domaines et certains sont plus dispendieux que d'autres en termes de coût, d'utilisation de l'infrastructure, de bande passante ou de capacité et demandent davantage d'expertise technique. Nous avons énumérés quelques uns de ces facteurs, mais chaque utilisateur devra évaluer les outils dans le contexte de l'application spécifique envisagée.

Quelques uns des tests que nous avons évoqués ont pour but de lutter contre le spam, alors que d'autres visent à empêcher certains comportements qui représentent une menace contre la sécurité, qui ne respectent pas les ressources de la plate-forme de destination, ou simplement ne se conforment pas aux règles acceptées régissant l'envoi de messages électroniques. Lorsque la règle est appliquée après réception des données qui constituent le message expédié, il reste à déterminer comment sera traité le message. Cela dépendra bien sûr des résultats des tests pratiqués. Certains tests sont plus fiables que d'autres et peuvent donc justifier le recours à des mesures plus radicales. De plus, il peut être décidé de pratiquer de nouveaux tests plus onéreux sur certains messages.

Nous allons voir maintenant les différentes possibilités de traitement des messages en fonction du point où est appliquée la règle.

Rejet au niveau de la session SMTP

L'intérêt du rejet à ce niveau réside dans la non prise en charge du message électronique, dont la distribution reste sous la responsabilité du serveur distant, lequel est informé de la situation. De plus, cette solution économise de la bande passante, d'abord parce que le message n'est pas reçu, et ensuite parce que le serveur distant n'aura pas besoin d'envoyer la DSN (Delivery Status Notification, message généré en réponse à un rejet, voir RFC 3461) que peut générer le message. La tâche d'envoyer le message d'échec de l'envoi est transférée sur l'expéditeur.

Toutefois, avec ce type de rejet, il n'est pas possible de conserver une copie du message (et donc de récupérer un message légitime qui n'aurait pas été accepté, ou simplement d'enquêter sur un rejet).

De plus, tous les serveurs SMTP ne sont actuellement pas capables de pratiquer certains tests au cours de la session SMTP. Ce point est en passe de changer, avec la diffusion croissante de nouveaux produits et en particulier d'interfaces comme « milter », de SendMail, « policy server » de PostFix, et prochainement OPES, qui pourra faire fonctionner tous les programmes avec la session SMPT.

A savoir : Le rejet à ce niveau est recommandé.

Rejet muet

Cette méthode est souvent déconcertante pour l'utilisateur lambda qui s'attend à ce que son courriel soit distribué ou au moins à ce qu'un rejet lui soit notifié. Le principe « distribuer ou notifier » est une règle cardinale du courrier électronique, mais devra probablement être abandonné en raison du grand nombre de « joejobs ».[76]

Idéalement, il faudrait conserver une trace des courriels détruits de cette manière, afin de permettre l'application de techniques comme Message Tracking, par exemple en mettant en œuvre la RFC 3885, qui décrit le protocole de suivi des messages, permettant aux utilisateurs de connaître le parcours de leur message (comme les systèmes de suivi des colis des sociétés de transport).

A savoir : Il faut préciser que les plaintes d'utilisateurs concernant des « messages perdus » ne correspondent pas toutes à des rejets muets de la part du fournisseur. La cause de la perte peut être tout autre (suppression prématurée d'un message par le destinataire humain, ou suppression d'un DSN par l'expéditeur humain).

Rejet avec envoi de DSN (Delivery Status Notification ou « retour à l'envoyeur »)

C'est la méthode traditionnelle utilisée pour le courrier électronique Internet. Mais, en raison de l'existence de « joejobs », il existe un risque de pénaliser des expéditeurs innocents, comme avec les programmes anti-virus qui envoient des DSN à tort.

A savoir : Si un message a été qualifié de spam, l'adresse de son expéditeur est probablement fausse et l'envoi d'un DSN ne se justifie pas. En revanche, certains gestionnaires de serveurs ne veulent pas prendre le risque de ne pas informer l'expéditeur que le message n'a pas été distribué. Il est difficile de recommander une marche à suivre, étant donné les avantages et les inconvénients attachés à chaque solution.

Distribution dans une boîte de réception réservée au spam

Quand trop peu de messages sont interceptés au niveau de l'entrée sur la plate-forme, la boîte de spam peut contenir beaucoup de messages, ce qui dissuade les utilisateurs de les lire. Le message n'est pas détruit, mais l'utilisateur a la possibilité de rectifier les faux positifs.

A savoir :	Il s'agit d'un complément très utile au blocage à l'entrée de la plate-forme. L'utilisateur peut mettre en œuvre cette technique en complément des mesures prises par son fournisseur de services de messagerie si ce dernier ne propose pas une boîte de spam dans sa suite anti-spam.

Marquage

Le serveur ne prend pas de décision mais place simplement une note sur le courriel. Cette technique laisse le plein contrôle à l'utilisateur mais contraint aussi l'utilisateur à télécharger le spam.

Notons qu'un fournisseur de service de messagerie peut laisser l'utilisateur choisir si le courriel incriminé sera marqué ou distribué dans la boîte spam. Cette solution est relativement simple à gérer.

A savoir :	Le marquage du courriel en modifiant le champ « message » ou le champ « objet » est risqué tant du point de vue technique (parce que les signatures sont cassées) que du point de vue juridique. Il est préférable d'ajouter un en-tête (tel que « X-Provider-spamscanner: YES ») que tous les logiciels de messagerie savent utiliser pour filtrer le courriel.

Dans cette section, nous avons passé en revue les différentes technologies anti-spam et les fonctions qu'elles peuvent proposer, ainsi que les méthodes qu'il faut appliquer lorsque l'on reçoit du spam. Le meilleur moyen de combattre efficacement le spam est d'utiliser avec discernement une combinaison de plusieurs technologies. Utilisée isolément, aucune des méthodes décrites ne donnera entièrement satisfaction. Lorsque plusieurs technologies anti-spam sont mises en place et fonctionnent en collaboration, cela peut diminuer considérablement le volume de spam qui affecte un système.

ÉLÉMENT V – ÉDUCATION ET SENSIBILISATION

Introduction

Les gouvernements, les fournisseurs d'accès à Internet, les associations professionnelles et autres opérateurs en ligne peuvent contribuer à la lutte contre le spam, en créant le cadre législatif approprié, en assurant une application effective de la loi, en mettant en œuvre des solutions techniques et en appuyant des démarches concertées. Néanmoins, une stratégie anti-spam globale doit prendre en compte l'utilisateur qui est en dernier ressort le destinataire du spam, la victime potentielle des virus et des escroqueries, mais aussi celui qui a la maîtrise de son ordinateur et de ses données personnelles[77].

Étant donné que le spammeur peut tirer profit de son activité[78] même avec un très faible taux de réponse au spam, il est important dans une stratégie anti-spam globale de mettre en avant l'éducation et la sensibilisation, car l'une et l'autre contribuent à réduire le marché potentiel des spammeurs et, par là même, leur intérêt financier à poursuivre leur activité.

Malgré la masse d'informations et de documentation aisément disponibles, et l'opinion générale que le spam est négatif et potentiellement néfaste, il est clair que certains destinataires continuent d'ouvrir le pourriel, en cliquant sur les liens recommandés, voire en achetant le produit offert. En outre, en raison des progrès croissants des techniques d'hameçonnage, les utilisateurs continuent d'être adroitement amenés à dévoiler des informations personnelles et des mots de passe[79].

Pour les raisons susmentionnées, les initiatives visant à élever le niveau d'éducation et de sensibilisation demeurent nécessaires, et mériteraient peut-être d'être renforcées, pour changer le comportement des utilisateurs à l'égard du spam et d'autres menaces sur la sécurité en ligne. Il semble que la sécurité ne soit pas encore perçue comme un véritable enjeu et la plupart des utilisateurs ne sont pas conscients des risques liés à la messagerie instantanée, au courrier électronique, aux jeux d'argent et à la navigation sur Internet. Il faut créer une culture de la sécurité car l'essor de l'économie numérique est subordonné à une utilisation responsable du cyberespace.

Stratégies d'éducation et de sensibilisation : cibler les destinataires

Les activités d'éducation et de sensibilisation devraient s'adresser d'abord et avant tout aux utilisateurs, mais également aux grandes sociétés, aux petites et moyennes entreprises, aux entreprises de marketing direct et aux opérateurs en ligne. Tous ces acteurs jouent un rôle dans la société de l'information et contribuent aux activités en ligne. Dans ce contexte, la Boîte à outils anti-spam de l'OCDE vise à favoriser l'avènement d'une culture de la sécurité, en créant un accès en ligne aux ressources pédagogiques, ainsi qu'à la documentation de sensibilisation qui a été élaborée dans plusieurs pays utilisant des langues différentes. Il s'agit de mettre ces outils à la disposition d'autres organismes privés ou publics désireux de lancer des initiatives analogues et qui pourraient profiter de la documentation disponible. Cela permettrait de limiter les doubles emplois et de faciliter la mise au point d'une approche plus globale et plus uniforme, de promouvoir des pratiques exemplaires et de mettre en relief les succès remportés. Cette ressource sera particulièrement précieuse pour les économies en développement qui n'ont que des ressources limitées à consacrer au spam.

La page de la Boîte à outils anti-spam de l'OCDE relative à l'éducation comportera des liens et des documents organisés en fonction de la cible de l'initiative considérée : utilisateurs individuels ; enfants et étudiants ; entreprises utilisatrices ; et entreprises de marketing direct et associations. On trouvera sous chaque titre le lien aux ressources et à la documentation, et l'indication de la langue. Le Ministère des Affaires économiques des Pays-Bas a établi une brochure « *Sp@m : do's and don'ts* » (ce qu'il faut faire et ce qu'il ne faut pas faire) et l'a communiquée au Groupe de réflexion de façon à pouvoir la placer sous forme électronique sur le site de la Boîte à outils anti-spam de l'OCDE à l'adresse www.oecd.org/sti/spam/toolkit, et à la mettre à la disposition de toute entité souhaitant distribuer ou mettre à disposition des informations et des conseils aux utilisateurs sur la gestion du spam. La brochure existe en anglais et en français, mais grâce à la contribution des membres du Groupe de réflexion, il devrait être possible de la proposer également dans d'autres langues.

Utilisateurs individuels

Les entités les mieux placées pour toucher les utilisateurs individuels sur le web, sont les FAI et les fournisseurs de services électroniques. Grâce à leurs pages web, ils peuvent fournir des informations sur la façon d'éviter le spam, sur les filtres anti-spam et anti-virus et sur les bonnes raisons de les utiliser, ainsi que des conseils sur les modalités de signalement des abus de spam aux autorités. En outre, par le biais de politiques d'utilisation acceptables entérinées par le client dans un contrat d'abonnement, le fournisseur peut fixer une série de règles interdisant l'utilisation du service pour envoyer des spams, virus et autres contenus illicites.

Des activités de sensibilisation de portée générale peuvent être lancées via le web et d'autres médias tels que la télévision, les journaux et les magazines. Des brochures peuvent être distribuées dans les établissements scolaires, placées sur le site web de FAI, et également diffusées sous forme de dépliants dans des revues spécialisées. Des dessins humoristiques pédagogiques sur le spam et la sécurité en ligne ont été télévisés dans quelques pays européens. Des bandes dessinées populaires ont été utilisées pour promouvoir une navigation sécurisée des enfants sur Internet.

Les messages adressés aux utilisateurs doivent être clairs et harmonisés. Au Canada, par exemple, la campagne « Arrêtez le pourriel ici »[80] a mis l'accent sur « Trois conseils clés » : protégez votre ordinateur, protégez votre adresse électronique, protégez-vous. Des conseils sont prodigués aux utilisateurs sous ces trois rubriques. L'Australie a lancé le slogan accrocheur « Don't try, don't buy, don't reply to spam [81] (Pas d'essai ! Pas d'achat ! Pas de réponse au spam) qui, sans remplacer une éducation appropriée sur ces questions, contribue à sensibiliser à certaines astuces élémentaires pour échapper au spam.

En outre, des campagnes nationales peuvent également avoir un effet positif, en captant l'attention de la population et des médias. Le 7 février 2006, un total de 37 pays et une centaine d'organisations ont pris part au *Safe Internet Day* (Journée Internet de la sécurité), qui était organisé dans toute l'Europe et au niveau mondial sous les auspices de la Commission européenne.[82] Aux Etats-Unis, la FTC, le Department of Homeland Security, le Department of Commerce et d'autres acteurs des secteurs public et privé ont lancé un site web et une campagne d'éducation, pour inciter les internautes à la vigilance à l'égard de la fraude sur Internet. Cette campagne, qui s'intitule « OnGuard Online », est disponible sur le site http://www.OnGuardOnline.gov, en anglais et en espagnol. Elle s'appuie sur de la documentation simple, en langage de tous les jours, pour aider les internautes à se prémunir contre la fraude sur Internet, à sécuriser leurs ordinateurs et à protéger leurs informations à caractère personnel. La documentation sur OnGuard Online est à la disposition de quiconque souhaite l'utiliser, et les acteurs intéressés sont encouragés à envisager un partenariat avec le site web. Le Réseau international de contrôle et de protection des consommateurs (RICPC) a lancé une campagne annuelle de prévention de la fraude. L'un des principaux thèmes traités lors de la campagne de février 2006 a été le problème du spam.

Groupes d'utilisateurs

Il est possible de cibler un groupe d'utilisateurs avec des informations adaptées à leurs besoins. Ces groupes peuvent être les suivants:

- **Troisième âge** : les classes d'informatique destinées aux personnes du troisième âge sont le lieu le plus adéquat pour exposer le concept de sécurité appliqué à l'ordinateur et à l'information, et pour apprendre à ces nouveaux utilisateurs comment gérer le spam, éviter les virus et reconnaître les escroqueries.

- **Enfants et étudiants** : la sensibilisation aux dangers et aux questions de sécurité liés à Internet doit faire partie intégrante de leur programme d'enseignement. Il faudrait que les établissements scolaires inscrivent dans leurs cours d'informatique des sessions consacrées au spam, aux escroqueries en ligne et aux virus, au contenu illicite et à la nétiquette. Les parents jouent aussi un grand rôle en apprenant à leurs enfants à faire preuve de prudence en ligne, à leur faire comprendre les risques liés aux communications en ligne, et à se protéger (Voir Encadré 4).

Encadré 4. Education des enfants

Plusieurs initiatives pédagogiques s'appuient sur des personnages de bandes dessinées et des jeux interactifs pour apprendre aux enfants à se comporter prudemment sur Internet. On leur apprend en particulier à ne pas ouvrir les courriels provenant d'expéditeurs inconnus ou à ne pas y répondre, à ne pas divulguer d'informations personnelles en ligne et à alerter leurs parents à chaque fois qu'il reçoivent ou découvrent des informations en ligne qui les mettent mal à l'aise.

Source : http://www.cnil.fr ; http://www.saftonline.org/Education/ ; http://disney.go.com/surfswell/index.html.

Utilisateurs et hameçonnage

L'hameçonnage est un phénomène complexe qui présente à la fois des aspects sociaux et technologiques. C'est pourquoi toute solution suppose : la mise en oeuvre de mesures techniques visant à limiter le phénomène et à atténuer les dommages qu'il provoque ; un effort des opérateurs en ligne pour établir, appliquer et faire respecter des politiques efficaces et claires concernant leurs pratiques en matière de courrier électronique avec leurs clients (voir l'élément III, Initiatives anti-spam du secteur privé) ; et l'élaboration d'initiatives de sensibilisation des consommateurs.

Les campagnes de sensibilisation sont cruciales pour apprendre aux particuliers comment identifier les messages trompeurs et frauduleux, et y réagir. Les autorités publiques, les opérateurs en ligne et les FAI, mettent actuellement au point des outils pédagogiques destinés aux utilisateurs[83]. En l'occurrence, encore faut-il pour être efficace que le message transmis aux utilisateurs soit simple et uniforme, et qu'il ait le double effet de les sensibiliser et de les inviter à l'action. Il faudrait notamment mettre l'accent sur les points suivants :

- Recommander aux utilisateurs qui reçoivent un courriel sollicitant des informations personnelles d'appeler directement l'entreprise pour **demander confirmation** ou de taper l'adresse Internet exacte de l'entreprise, **tout en évitant de cliquer sur le lien proposé dans le courriel.**

- Recommander aux utilisateurs d'utiliser **un logiciel anti-virus et des pare-feu** pour protéger leur ordinateur et d'éviter d'accepter des fichiers non désirés susceptibles d'endommager un ordinateur ou de suivre à la trace les activités d'un consommateur sur Internet.

- Mettre en garde les utilisateurs contre l'envoi par courriel d'informations personnelles ou financières.

Grandes sociétés et petites et moyennes entreprises

Les grandes sociétés sont souvent victimes de spams et de maliciels, car leurs adresses électroniques figurent dans des sites Web publics, ou sont largement diffusées, et elles ont généralement des connexions à haut débit ouvertes en permanence. Il peut s'avérer nécessaire de faire une distinction entre sociétés de grande taille et petites et moyennes entreprises, car ces dernières ne peuvent pas s'offrir un soutien technique interne ou des politiques et des procédures de sécurité informatique individuelles, et doivent s'en remettre au sens de la discipline de leurs employés. Les besoins ne sont donc pas les mêmes en matière d'éducation :

- **Grandes sociétés** : il faudrait que les services administratifs remettent aux nouvelles recrues : une brochure expliquant la politique de sécurité de la société concernant le courrier électronique, les filtres existants et les meilleures pratiques pour gérer le spam (ne pas ouvrir, ne pas cliquer, etc.). Le même type d'informations devrait être disponible sur le site intranet et des mises à jour peuvent être adressées périodiquement aux utilisateurs par courrier électronique (voir Encadré 4).

- **PME** : il faudrait qu'elles fournissent des informations spécifiques sur les pratiques élémentaires de gestion de la sécurité, le matériel de formation, les logiciels, etc. En l'occurrence, les entités les mieux placées pour les aider seraient les FAI et les entreprises de logiciels de sécurité, mais également les associations (telles que les chambres de commerce et les associations professionnelles) qui pourraient participer à la sensibilisation de leurs membres aux problèmes et suggérer des solutions éventuelles.

Il est aussi recommandé de ne pas répondre aux courriers non sollicités. Souvent, les pirates et les spammeurs ne demandent pas mieux que d'avoir confirmation qu'une adresse électronique est valide pour rajouter un utilisateur imprévoyant à une liste de distribution. Cependant, cette pratique peut être difficile à employer dans les pays qui adoptent un système « opt-out », où les expéditeurs peuvent envoyer des messages sans le consentement préalable de l'utilisateur, qui a toutefois la possibilité de refuser l'envoi de messages.

Encadré 5. Conseils et astuces pour la sécurité en ligne : Exemple de politique anti-spam interne d'une entreprise[84]

Protégez votre adresse électronique :

- Efforcez-vous de ne pas afficher publiquement votre adresse, que ce soit sur des sites web, dans des groupes de discussion ou dans l'annuaire des membres de services en ligne.
- Lorsqu'il vous faut afficher une adresse électronique publique, rappelez-vous que vous pouvez demander au service informatique de créer un compte générique, par exemple : spam.project@oecd.org.
- Envisagez de « masquer » votre adresse électronique. Par exemple, l'adresse « jeandupont@monfai.com » peut être masquée et écrite comme suit : « jeandupont@halteauspam.monfai.com ». Cela peut éviter que votre adresse ne soit collectée automatiquement, mais ce n'est pas recommandé si vous avez besoin de recevoir une confirmation d'inscription à un service, par exemple.
- Décidez si vous souhaitez utiliser une ou plusieurs adresses électroniques. Vous pouvez avoir une adresse pour les messages professionnels et une autre par exemple pour les groupes de discussion et les annuaires. La plupart des FAI peuvent vous fournir gratuitement des adresses supplémentaires.
- Consultez la politique de confidentialité lorsque vous communiquez votre adresse à un site web. Regardez si elle autorise la société à revendre votre adresse ou pour quel type d'activités promotionnelles elle peut être utilisée.

Encadré 5. Conseils et astuces pour la sécurité en ligne : Exemple de politique anti-spam interne d'une entreprise (suite)

- Lisez et comprenez l'ensemble du formulaire lorsque vous communiquez des informations personnelles par l'intermédiaire d'un site web. Certains sites vous permettent de refuser que la société communique votre adresse à ses "partenaires" ; mais pour cela il vous faudra parfois décocher une case présélectionnée.
- Rappelez-vous qu'en application de la loi, vous devriez pouvoir refuser les messages non sollicités (système opt-out).

Protégez votre ordinateur :

N'oubliez pas, qu'un message spam peut contenir davantage qu'une offre spéciale pour du Viagra – il pourrait également héberger un virus, alors soyez extrêmement prudent si vous décidez de l'ouvrir. Si vous recevez un message suspect, le mieux est de le supprimer, ainsi éventuellement que ses pièces jointes. Ensuite, pensez à le supprimer du dossier Éléments supprimés. Si vous devez ouvrir une pièce jointe, suivez la procédure suivante :

- Assurez-vous que vos définitions de virus sont bien à jour.
- Sauvegardez le fichier sur votre disque dur.
- Soumettez le fichier à votre anti-virus.
- Si aucun virus n'a été détecté par l'anti-virus, vous pouvez ouvrir le fichier.

Vous pouvez utiliser des logiciels gratuits pour filtrer les spams, comme Spamassassin ou d'autres, qui déplacent automatiquement les messages signalés comme étant des spam vers un dossier pourriel.

Protégez vos données:

- Utilisez des mots de passe difficiles à deviner, changez-les fréquemment et ne les communiquez pas sur des moyens de communication non sécurisés, comme le courrier électronique.

Il existe encore d'autres moyens:

- « Fermez la porte à clé en sortant de la maison » –. Éteignez votre ordinateur et déconnectez-le du réseau quand vous ne l'utilisez pas.
- N'exécutez pas de programmes d'origine inconnue. Malgré leurs qualifications, ils peuvent installer des logiciels espions ou autres maliciels sur votre ordinateur, voire le transformer en machine zombie.
- Signaler les incidents sérieux.
- Aidez vos collègues de travail à protéger leur courrier électronique, leur ordinateur, et le réseau.

L'éducation des destinataires est aussi importante que celle des expéditeurs. Dans ce contexte, les sociétés qui utilisent le courrier électronique pour communiquer avec leurs clients devraient aussi recevoir des informations sur la façon d'utiliser correctement ce moyen de communication sans être considérées comme des spammeurs et se faire sanctionner en application de la législation nationale anti-spam. Il faudrait que toutes les entités respectent des pratiques d'envoi simples.

Par ailleurs, il faudrait que les sociétés surveillent de plus près la qualité de leurs entreprises affiliées et de leurs sous-traitants, en particulier s'agissant des contrats de publicité externalisés.

Sociétés de marketing direct

Il faudrait que les sociétés de marketing direct soient particulièrement attentives à la législation applicable au spam. Il leur faut connaître et respecter scrupuleusement la législation anti-spam en vigueur dans le pays d'origine et dans le pays de destination du message. Pour aider leurs membres à se conformer à la législation, les associations de marketing direct fournissent des listes de pratiques exemplaires de marketing en ligne, souvent sous la forme de listes de contrôle récapitulant les prescriptions auxquelles une société doit se conformer, depuis le moment où elle décide de lancer une campagne de publicité en ligne jusqu'à l'envoi effectif du message. La liste de contrôle contient des renvois aux dispositions applicables, des indications sur les modalités légales de collecte et d'utilisation des adresses électroniques, ainsi que des informations spécifiques et le libellé qui doit être inclus dans le texte du message (par exemple, la possibilité de refuser l'envoi de messages, ou l'adresse postale de la société), et des suggestions pour éviter de voir les messages arrêtés par inadvertance par un filtre en tant que spam. Dans ce contexte, le Groupe de réflexion a encouragé l'adoption par les représentants du secteur privé d'un ensemble de pratiques exemplaires visant le marketing direct que les membres du BIAC sont actuellement en train d'élaborer (voir l'élément III).

ÉLÉMENT VI – PARTENARIATS DE COOPÉRATION ANTI-SPAM

Conjuguée à l'essor d'Internet, la libéralisation du marché des télécommunications induite par les acteurs privés et peu réglementée, a contribué à façonner la société de l'information d'aujourd'hui dans laquelle toutes les parties prenantes – gouvernements, entreprises privées, société civile et utilisateurs – ont un rôle à tenir et au développement de laquelle elles peuvent contribuer.

Le spam et la cybersécurité sont des questions qui concernent les acteurs publics et privés ; les uns et les autres ont donc intérêt à préserver la disponibilité et la fiabilité des instruments de communication pour favoriser le développement de l'économie numérique. Si l'objectif est commun, des conflits peuvent surgir quant à la façon de le réaliser. Les gouvernements poursuivent des objectifs de politique publique et leur intervention est essentielle pour fixer des buts à long terme et élaborer une stratégie anti-spam cohérente. Toutefois, les instruments législatifs à eux seuls ne sont pas toujours efficaces et leurs mécanismes peuvent être trop rigides au regard de l'évolution rapide sur le front du spam et des maliciels. Les acteurs industriels sont souvent bien placés pour mener des actions concrètes au moment favorable. Nul ne conteste que certaines activités ne peuvent pas se justifier dans une perspective concurrentielle, mais il est des mesures d'incitation qui aideraient à assurer une meilleure prise en compte par les entreprises des intérêts de la collectivité au sens large.

Différentes stratégies peuvent être mises en œuvre pour remédier à cette situation, depuis l'approche réglementaire pilotée par les pouvoirs publics, dans laquelle l'autorité fixe les règles, en imposant certaines responsabilités aux entreprises privées, comme l'obligation d'appliquer des mesures de sécurité, par exemple, jusqu'à l'approche pilotée par le marché, dans laquelle les prestataires privés décident par eux-mêmes du niveau de leur engagement et de leur participation. Diverses possibilités intermédiaires sont possibles, notamment celles adoptées par plusieurs gouvernements de l'OCDE qui se sont attachés à établir un cadre réglementaire approprié et à utiliser des moyens d'action de portée générale pour encourager la participation du secteur privé.

Les secteurs public et privé ont trouvé plusieurs moyens variés et novateurs de coopérer : les pouvoirs publics cherchent à associer des entités du secteur privé, de même que des organismes non gouvernementaux, à l'étude de stratégies et d'activités anti-spam cohérentes. Le plus souvent les partenariats stratégiques ont pour objectif de renforcer les réseaux, de mener des actions de sensibilisation et de partager des informations. Des partenariats plus opérationnels contribuent également à l'élaboration de politiques anti-spam, à l'éducation des personnes concernées, à la mise au point (et à l'application) de pratiques exemplaires et à l'échange d'informations et de données sur les cas de spam transnationaux. En outre, comme le montrent les multiples efforts déployés aux échelons national et international, les partenariats sont un instrument fondamental pour améliorer la communication et la compréhension des besoins, des attentes et des problèmes réciproques, et ouvrent donc la voie à une coopération et un engagement mutuel accrus.

Parmi les partenariats public-privé qui s'occupent actuellement du problème du spam, ou plus généralement de la cybersécurité, on peut citer, l'ACMA (Australie), qui travaille avec l'Internet Industry Association (IIA) dans le but d'élaborer des codes de conduite à l'intention des FAI et des distributeurs directs en ligne[86]. Le Groupe de travail canadien sur le pourriel comprenait des représentants venant des secteurs public et privé, de la société civile et du monde universitaire[87], qui ont collaboré à l'élaboration d'une série de recommandations et de pratiques exemplaires anti-spam. Dans le cadre de son projet "Signal Spam"[88], la France mobilise les autorités publiques et les acteurs privés pour mettre au point un système destiné à simplifier le signalement du spam par les utilisateurs et à normaliser le traitement et l'analyse du spam de façon à renforcer l'efficacité et la coordination des actions anti-spam[89]. Au niveau de l'UE, l'initiative « SpotSpam » financée dans le cadre du programme Safer Internet Plus vise à faciliter le recueil d'éléments de preuve et l'échange d'informations lorsque des poursuites sont engagées contre un spammeur, et à constituer une source supranationale d'informations pour le suivi des plaintes concernant le spam.[90]

Plus pragmatique, le London Action Plan (LAP)[91], créé en octobre 2004, est actuellement particulièrement dynamique et attire un nombre croissant de participants venant des secteurs public et privé. Les activités du LAP comprennent des conférences régulières (trimestrielles), réunissant les différents membres pour examiner de nouvelles initiatives contre le spam, mettre en commun des informations et des pratiques exemplaires, étudier des initiatives ponctuelles sur un sujet déterminé, comme par exemple le « spam sweep day » (Journée coup de balai sur le spam), qui associe les autorités de différents pays, et le « projet zombies »[92], lancé récemment (voir l'Élément III : Initiative anti-spam du secteur privé). L'un des objectifs du Groupe est de faciliter les contacts entre les services chargés de faire respecter les mesures, de promouvoir l'échange d'informations dans les actions transnationales et d'intensifier la coopération avec les FAI et autres opérateurs privés.

Dans le domaine du spam, les partenariats public-privé sont nécessaires pour promouvoir l'interaction et la coopération entre les deux acteurs, surtout si l'on prend en compte le large éventail de parties concernées et la multiplicité de leurs besoins et perspectives. Tabler uniquement sur la législation pour imposer des obligations aux acteurs privés ne serait pas inefficace à moins d'être conjugué avec d'autres mesures. En effet, les lois ne peuvent pas suivre le rythme de l'évolution technique. En revanche, les pratiques exemplaires, si elles sont largement appliquées, peuvent être efficaces en liaison avec d'autres mesures notamment juridiques. Dans ce contexte, des partenariats stratégiques comme ceux qui se mettent en place dans les différents groupes de travail créés aux échelons national et international sont un outil fondamental pour améliorer la communication et mieux comprendre les besoins, les attentes et les problèmes réciproques et, ce faisant, permettre un renforcement de la coopération et de l'engagement mutuel.

Pour que le partenariat soit couronné de succès et débouche sur des résultats concrets, qui seront ensuite mis en œuvre par les différentes parties prenantes, les éléments suivants[93] semblent donc nécessaires :

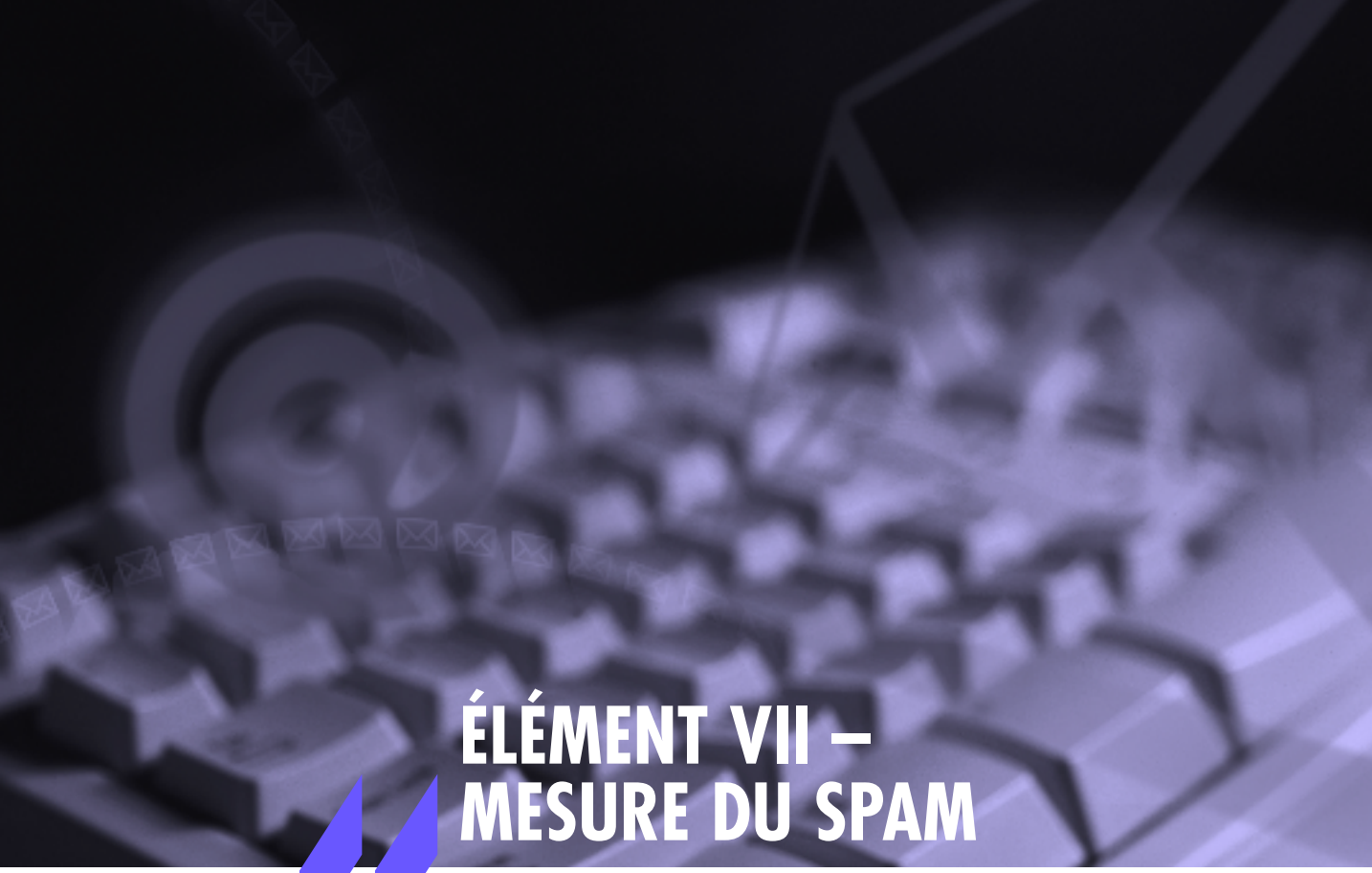
- Engagement et contribution véritable de toutes les parties ; appropriation du produit final.
- Objectif et horizon temporel bien définis.
- Un (ou plusieurs) éléments moteurs, qui investissent un surcroît de ressources et d'effort dans le projet.
- Un partenariat national qui alimente les initiatives et partenariats internationaux, pour compléter et harmoniser les solutions.
- Pour éviter les doubles emplois, il faudrait, autant que possible, que les partenariats s'appuient sur des liens et des organes représentatifs existants à la fiabilité reconnue.

Le Groupe de réflexion sur le spam de l'OCDE est en soi un partenariat en coopération, réunissant des représentants de différents secteurs et d'un grand nombre de pays. Le Groupe de réflexion fixe ses objectifs, qui sont stratégiques, impliquant la création d'un réseau d'information entre les différents acteurs, mais également opérationnels, car le Groupe vise à constituer une Boîte à outils qui devrait contribuer à la définition de stratégies anti-spam cohérentes aux échelons national et international. Toutefois, il faudrait dans le même temps renforcer et élargir le rôle du secteur privé, tandis que les acteurs gouvernementaux devraient tendre à faire leur le résultat de ces travaux, ce qui adresserait un message important à toutes les parties prenantes, dans les économies Membres et non-membres de l'OCDE, concernant la nécessité de lutter contre le spam et les maliciels, les meilleures solutions applicables et les efforts déployés à cet effet par les acteurs de l'OCDE[94].

La Recommandation du Conseil concernant la coopération dans la lutte transnationale contre le spam encourage expressément les gouvernements à coopérer avec les entreprises, les groupes industriels et les associations de consommateurs dans les actions contre les spammeurs, l'éducation des utilisateurs, le renvoi des données pertinentes pour les plaintes, et à partager les instruments et techniques d'enquête, les analyses et les données. La coopération public-privé est également jugée cruciale dans les efforts déployés à l'échelle internationale, pour faire respecter efficacement la législation, réduire l'incidence des informations erronées au sujet des titulaires de noms de domaines[95] et pour rendre l'Internet globalement plus sûr.

Le Groupe de réflexion a aussi encouragé l'établissement de pratiques exemplaires communes à l'intention des distributeurs en ligne et des FAI. Ces pratiques exemplaires ont été élaborées par un groupe intersectoriel d'acteurs privés et sont jointes en annexe au présent rapport (Annexes II et III). Dernier point, mais non le moindre, la mesure du spam est un outil important qui ne pourrait voir le jour sans le concours d'opérateurs du secteur privé, mais qui aiderait les décideurs et les autorités à évaluer l'impact de leurs initiatives réglementaires et de leurs efforts pour faire respecter les textes. Dans le cadre des travaux du Groupe de réflexion, le MAAWG a élaboré un Email Metrics Program (Programme de métrologie du courrier électronique) qui est mentionné dans l'Élément VII ci-dessous.

La coopération entre les secteurs public et privé sous-tend les multiples activités et initiatives anti-spam, aussi les différentes initiatives ont-elles été traitées plus en détail dans les éléments pertinents du présent Rapport.



ÉLÉMENT VII – MESURE DU SPAM

Métrologie du spam

On a fait observer au début du présent rapport que le spam évoluait. Bien que les données sur le volume de courrier électronique considéré comme du spam, le pourcentage de virus et le nombre de courriels hameçons adressés par le biais de messages électroniques proviennent d'une multiplicité de sources, les informations ne sont pas facilement comparables et les chiffres obtenus divergent. Cela tient à l'absence de définition internationale commune du spam, et aux différentes méthodologies utilisées pour mesurer le volume de spam qui dépend des différentes technologies de filtrage employées.

La plupart des données sur le spam sont communiquées par l'industrie, en particulier les fournisseurs de dispositifs anti-spam, mais aussi par les fournisseurs de services Internet (bien que ces dernières données ne soient généralement pas à la disposition du public). Les données réunies par ces acteurs sont difficiles à rapprocher car elles renvoient à des bases d'utilisateurs différentes et ne sont pas fondées sur les mêmes paramètres. On peut donc s'interroger sur l'exhaustivité de ces données, les éléments mesurés et l'opportunité d'encourager l'industrie à mettre au point une méthodologie unique pour la collecte des données. En outre, les FAI sont souvent peu enclins à divulguer des informations qui sont sensibles pour les entreprises, et pourraient compromettre leur compétitivité.

Les sociétés spécialisées dans le filtrage et les FAI (utilisateurs de filtres) recueillent auprès de leurs clients des données qui fournissent une mesure du volume du spam détecté par les filtres. Ces chiffres donnent une idée de l'augmentation relative du spam par rapport au volume total de courrier électronique, des différents contenus possibles et des pays touchés. Les organisations anti-spam et les organisations concernées par la protection des consommateurs et la confidentialité mesurent également le spam. En outre, certaines organisations gouvernementales ou publiques chargées d'élaborer des politiques ou des réglementations anti-spam collectent, dans des proportions limitées, des données sur le spam.

Il ressort des statistiques établies par les fournisseurs de solutions anti-spam, qu'en 2005, le pourcentage moyen de pourriel avait légèrement diminué, tombant à 68,6 % du courrier électronique total, contre 72,3 % en 2004.[95] Selon AOL, entre 2003 et 2004 déjà, le nombre de spams bloqués par leurs filtres avaient été divisé par deux, à l'instar du nombre de plaintes de leurs clients concernant le spam. Différentes sources observent que le spam affecte moins les utilisateurs, souvent en raison de l'utilisation de filtres anti-spam et d'une protection anti-virus, et des campagnes d'éducation et de sensibilisation, qui apprennent aux utilisateurs à gérer le problème. L'infléchissement de la tendance du spam, qui s'était accentuée au cours des années précédentes, démontre que la mise en œuvre de solutions techniques appropriées, conjuguée à une stratégie sans complaisance à l'égard des spammeurs (poursuites judiciaires, investigations), peut porter des fruits. D'après une étude de l'Institut finlandais des statistiques, les ménages finlandais sont dans l'ensemble modérément préoccupés par le spam. De même, selon une recherche du Pew Internet and American Life Project, 22 % des utilisateurs, au lieu de 29 % en 2004[96], indiquent consacrer moins de temps à leur courrier électronique à cause du spam.

Les statistiques peuvent aussi être une source d'information utiles pour les décideurs quant à la charge que le spam représente pour les opérateurs de réseaux. Ainsi, selon VeriSign, gestionnaire des domaines.com et .net, sur la période de trois mois comprise entre le 1er juillet et le 20 septembre 2004, le spam a représenté 80 % du trafic en volume, mais seulement 21 % de l'occupation de la bande passante pour le courrier électronique, car la taille moyenne d'un message de spam était de 3 Koctets, contre 40 Koctets pour un message légitime.[97] Ainsi, bien que le spam entraîne des coûts considérables pour les opérateurs de serveurs de messagerie, il ne semble pas que par son volume le spam déstabilise le système du courrier électronique.

La mesure est un élément clé pour évaluer l'évolution du spam et l'efficacité des mesures de répression et des efforts d'éducation, déterminer si une stratégie a des effets et, en dernière analyse, définir les changements requis dans les cadres administratifs, réglementaires et techniques.

Pour faire plus précisément le point de la situation du spam, et fournir des données sur la quantité de spam qui circule dans le réseau, le Messaging Anti-Abuse Working Group (MAAWG) a élaboré, dans le contexte des travaux du Groupe de réflexion, un programme de métrologie du courrier électronique et s'est mis d'accord sur une série d'indicateurs de spam destinés aux FAI pour mesurer:[98]

- Le nombre total de connexions interrompues en raison d'un blocage IP (bien que ce paramètre puisse être imprécis, il donne une idée de l'ordre de grandeur du volume de messages qui ne pénètre pas les réseaux) ;

- Le nombre total de courriels entrants bloqués ou étiquetés et le pourcentage de courriels transitant par les FAI (connexions bloquées exclues) identifiés comme spam ;

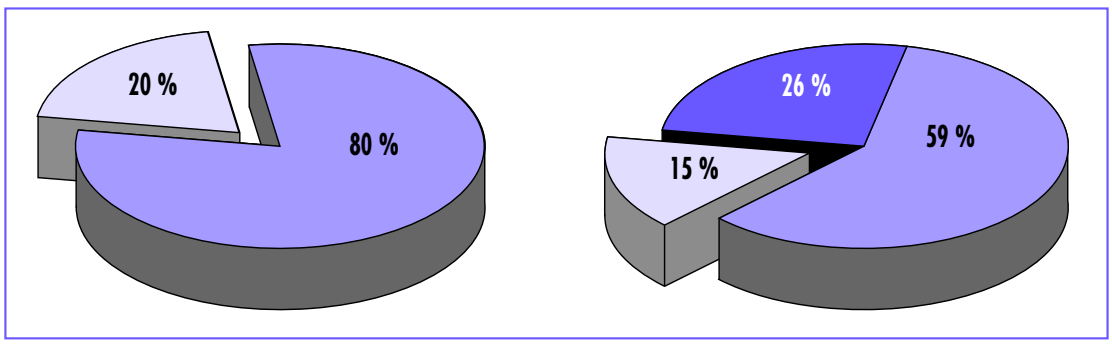
- La cible privilégiée est donc le courriel non "désiré", ce qui permettra de s'affranchir de la difficulté d'avoir à définir le spam.

Pour le dernier trimestre 2005, le nombre total de courriels entrants filtrés est d'environ 203 milliards. Sur ce chiffre, la distribution de plus de 61 milliards de messages a été refusée au moyen de RBL (Real Time Blacklists ou listes noires en temps réel) ou par d'autres méthodes, tandis que 142 milliards d'autres messages ont été dans un deuxième temps bloqués ou marqués au moyen d'un ensemble ASAV (Anti-Spam/Anti-Viral), de MTA (Mail Transfer Agents) ou d'autres règles appliquées au niveau destinataire ou du message. A cela il faut ajouter le filtrage effectué au niveau des MUA (Mail User Agents).

Cela signifie que pour le dernier trimestre 2005, on a dénombré :

- Quelques 500 connexions interrompues par boîte de messagerie ;
- Plus d'une connexion et demi interrompue par message électronique distribué sans altération ;
- Plus d'un millier des messages entrants marqués/bloqués, par boîte de messagerie ;
- Environ quatre messages entrants marqués/bloqués par message distribué sans altération, soit 80 % du nombre total de messages entrants.

Si l'on prend en considération par ailleurs le fait qu'il y a un message de courrier électronique abusif par connexion interrompue, le ratio des messages entrants bloqués/marqués par message distribué sans altération passe à 5.6 messages, soit 85 % des messages entrants (Voir la Figure 2).



Source : Programme de métrologie dus spam du MAAWG

Figure 2. Pourcentage de pourriels au niveau des FAI (4T2005)

Le rapport sera actualisé tous les trimestres pour essayer de mettre en évidence les évolutions dans le temps. Des opérateurs de messagerie ont volontairement décidé de participer et de s'engager à fournir des données confidentielles tous les trimestres pendant deux ans.[99] Les données seront disponibles sur le site du MAAWG (www.maawg.org) ou sur les pages anti-spam du site de l'OCDE (www.oecd-antispam.org) dans la rubrique « Statistiques ».

Les données provenant des FAI peuvent être comparées avec les mesures, dans leurs boîtes à lettres après l'intervention des filtres et autres solutions techniques, du courrier perçu comme du spam par les utilisateurs. Afin de procéder à une analyse plus détaillée du phénomène du spam, la France a procédé à une étude statistique basée sur le spam arrivant dans les boîtes à lettres. Les résultats préliminaires de l'étude, basée sur des règles statistiques publiques, complète bien l'information statistique existante. L'approche mentionnée se distingue par le fait qu'elle ne mesure pas le spam « dans le circuit », mais le spam qui parvient à l'utilisateur final et qui est considéré comme tel par ce dernier. Ce type de mesure fournit une analyse plus sociologique de ce que les utilisateurs définissent comme un spam et de l'importance qu'ils attachent au phénomène.

En ce qui concerne le premier point, environ 90 % des personnes interrogées considère comme du spam tout message commercial émanant d'un expéditeur qu'elles ne peuvent identifier ou un courrier électronique commercial émanant d'un expéditeur auquel elles n'ont certainement pas donné leur adresse de courrier électronique. De plus, 74 % considère les messages non sollicités (non commerciaux) émanant de partis politiques ou de syndicats comme étant du spam.

Malgré le fait que la plupart des utilisateurs peuvent aisément identifier les pourriels et les éliminer, il n'en reste pas moins que 8 % des déclarants ont affirmé avoir acheté un bien ou un service dont ils avaient vu la publicité dans un message de ce type. Une grande partie des personnes interrogées est consciente de la nécessité de prendre des précautions pour éviter de recevoir du spam. Parmi les méthodes les plus couramment utilisées figurent notamment la protection des adresses personnelles de courrier électronique et le recours à des services de filtrage anti-spam.

L'autre question est de savoir dans quelle mesure les personnes interrogées sont préoccupées par le spam. L'enquête a montré que si la plupart des internautes reçoivent peu de spam, et ne sont pas très préoccupés par le problème, environ 10 % des utilisateurs reçoivent 70 % du volume total de spam, et considère donc qu'il s'agit d'une nuisance majeure.

Des ressources et des données sont disponibles sur le site Web Anti-Spam de l'OECD, qui renvoie aux pages Web du MAAWG et à d'autres statistiques en ligne.

ÉLÉMENT VIII – CO-OPÉRATION (OUVERTURE)

Introduction

Le spam est une préoccupation pour les pays en développement comme pour les pays développés, car ceux-ci sont confrontés aux mêmes problèmes que les économies développées,[100] auxquels s'ajoutent des contraintes dues au manque de ressources techniques et financières et de compétences, en particulier :

- La bande passante disponible est souvent plus faible.
- La plupart des utilisateurs se connectent par téléphone ou dans des cybercafés, procédures plus coûteuses et plus lentes, ce qui a des répercussions quant à l'impact financier du spam.
- Souvent, les FAI ne sont pas conscients des dangers liés au spam et aux virus ou manquent de moyens pour les combattre.

L'application de solutions techniques (filtres, logiciels anti-virus, etc.) peut s'avérer difficile en raison de leur prix relativement élevé. De plus, le cadre législatif laisse parfois à désirer, car l'applicabilité à l'Internet des lois de portée générale sur la protection des consommateurs et sur la confidentialité des données n'est pas toujours évidente. Même lorsqu'il existe des textes, les ressources ou les autorités nécessaires font défaut pour veiller à l'application des lois anti-spammeurs.

De nombreux spammeurs — pour lesquels il est devenu difficile ou trop risqué d'opérer à partir d'un pays développé, ou qui sont considérés « *persona non grata* » par les FAI — peuvent exploiter les failles susmentionnées et migrer leurs opérations vers des pays où ils peuvent agir plus aisément et jouir d'un certain degré d'impunité. Cela tient aussi parfois à une politique sécuritaire et anti-spam laxiste de la part

des FAI. Certes, il ne s'agit pas là d'un problème propre aux pays en développement (les réseaux de machines zombies sont également une réalité dans les pays développés, de même que les « contrats roses » bien connus entre FAI et spammeurs), cependant ses conséquences peuvent être particulièrement redoutables, notamment du fait que dans de nombreux pays, comme l'Inde, où l'infrastructure des TI est relativement bien développée, les FAI sont souvent exploités par des spammeurs.

Si le plus souvent les FAI ne sont même pas conscients de ce qui se passe dans leur réseau, d'autres acceptent d'accueillir des spammeurs moyennant des contreparties financières. Cette tactique, qui peut sembler profitable à court terme, est catastrophique à long terme : les FAI peu regardants seront placés sur une liste noire par les autres fournisseurs et leurs clients légitimes, dans l'incapacité de communiquer avec d'autres utilisateurs dans d'autres pays, pourraient décider de changer de prestataires. Les listes noires, examinées dans l'Élément IV, sont particulièrement critiquées par les fournisseurs et les autorités publiques des pays en développement qui y voient un fardeau supplémentaire imposé à la population locale plutôt qu'une solution.

Rôle de la coopération internationale (Ouverture)

Quelle est la valeur ajoutée de la coopération internationale ? La coopération internationale poursuit deux grands objectifs : promouvoir des cadres nationaux appropriés pour combattre le spam ; et encourager la coopération entre les pays, le secteur privé, la société civile et d'autres parties prenantes de façon à appréhender le problème du spam dans toutes ses dimensions et à veiller à la mise en œuvre harmonisée et généralisée des mesures techniques et au respect effectif des règles applicables. En outre, compte tenu des problèmes particuliers qu'éprouvent les pays non membres de l'OCDE à gérer le spam, on est en droit de penser que la coopération internationale pourrait s'avérer très payante, notamment dans les domaines suivants :

- **Lois et réglementations, mesures d'application** : la coopération internationale dans le domaine législatif et réglementaire est fondamentale pour soutenir la mise en place d'un cadre réglementaire anti-spam approprié dans tous les pays — si possible en respectant un ensemble de principes de base harmonisés à l'échelon international. Il faudrait introduire dans la politique nationale des éléments destinés à faciliter la coopération internationale et le partage des informations et des pratiques. En outre, les mesures coercitives arrêtées dans quelques pays ont des répercussions à l'échelle mondiale ; d'où l'importance d'un renforcement de la coordination transnationale.

- **Éducation** : il faudrait que les outils d'éducation et de sensibilisation qui ont déjà été élaborés soient diffusés plus massivement à tous les utilisateurs, opérateurs, établissements scolaires et autorités publiques dans tous les pays. Etant donné que dans la plupart des pays en développement l'accès à Internet est souvent « collectif », autrement dit que les utilisateurs se connectent à partir de leur lieu de travail, d'un établissement scolaire ou en utilisant l'un des points d'accès collectif disponible, tels que les cybercafés et les bibliothèques publiques, il faudrait diffuser ces outils pédagogiques dans ces lieux, ce qui permettrait de toucher un grand nombre d'utilisateurs en même temps.

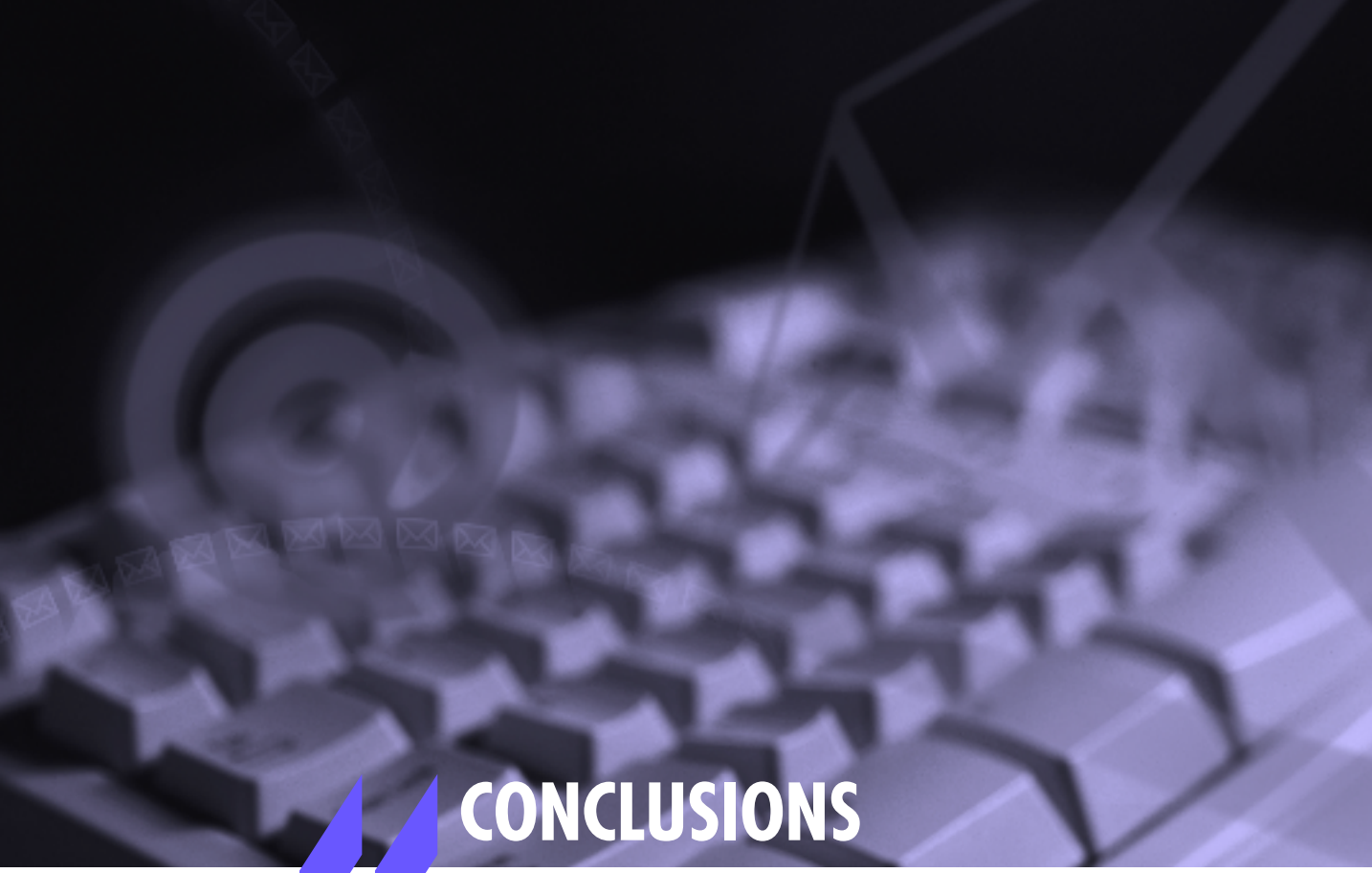
- **Faciliter la coopération de l'industrie** : la mise en place d'une série de pratiques exemplaires communes est un objectif mondial et il faudrait y associer tous les FAI. Les pratiques suggérées par diverses associations professionnelles, les initiatives public-privé ou les suggestions figurant dans le présent Rapport (voir Pratiques exemplaires à l'intention des FAI dans l'Élément III), pourraient constituer une bonne base de départ. L'engagement de l'industrie sera nécessaire pour aller plus loin. La coopération internationale serait particulièrement utile pour faire se rencontrer les FAI des économies développées, qui ont une expérience considérable dans le domaine, et leurs homologues dans les économies en développement, pour qu'ils partagent leurs connaissances, expériences et pratiques exemplaires.

Activités d'ouverture de l'OCDE

Dans plusieurs instances, les pays en développement ont réclamé un soutien accru des pays plus avancés sur le plan technique et de la communauté internationale pour affronter le problème du spam et de façon générale celui de la sécurité de l'Internet. La création d'un cadre pour une coopération transnationale efficace est vivement soutenue par les uns comme par les autres. Dans ce contexte, il apparaît que les travaux du Groupe de réflexion sur le spam de l'OCDE, et notamment sa boîte à outils anti-spam, pourraient constituer une ressource utile pour tous les acteurs intéressés.

Afin de promouvoir la coopération et l'échange d'informations et de faciliter la diffusion de la boîte à outils, le Groupe de réflexion a créé un site Web (www.oecd-antispam.org), où l'on peut trouver de la documentation sur les mesures éducatives, réglementaires et techniques, les coordonnées des services à contacter dans les différentes autorités chargées de faire appliquer la législation et un tour d'horizon de la législation anti-spam dans le monde. Le site Web est actualisé grâce aux contributions des pays participants. Les économies non membres de l'OCDE sont vivement encouragées à communiquer des données et informations sur leurs dispositifs nationaux.

Par ailleurs, l'OCDE prend aux initiatives anti-spam à l'échelle mondiale et y contribue, en partenariat avec d'autres organisations actives dans ce domaine, comme l'UIT, la CE et l'APEC.



CONCLUSIONS

Pour pouvoir contribuer au développement économique et social, les communications électroniques doivent être fiables, efficientes et dignes de confiance. La confiance actuelle des utilisateurs dans les outils de communications électroniques, et notamment dans le courrier électronique, pourrait être menacée par les messages non sollicités, non désirés et préjudiciables, autrement dit le spam.

L'ouverture et la décentralisation sont les facteurs clés du succès de l'Internet. Les applications et services créés ces dernières années – P2P, système vocal sur Internet – se sont tous généralisés rapidement sans qu'il soit besoin d'une quelconque autorisation ou formalité. Tout un chacun est libre d'utiliser le réseau comme il l'entend ou d'expérimenter de nouveaux moyens de le faire. Mais ces caractéristiques créent aussi de failles par où s'engouffrent aujourd'hui les spammeurs et autres délinquants informatiques. L'absence de contrôle centralisé permet aux utilisateurs de rester dans l'anonymat. En outre, le faible coût d'accès à l'Internet et aux services de courrier électronique permet aux spammeurs d'expédier quotidiennement des millions de pourriels. Il faut donc lutter contre le spam et les autres menaces, tout en prenant garde de ne pas porter atteinte au moyen de communication que l'on s'efforce de protéger.

La première question à laquelle devaient répondre les membres du Groupe de réflexion au début de leur mandat n'était pas de savoir si les Membres devaient ou non agir contre le spam, mais quelle était la bonne mesure à prendre. Une leçon importante à retenir est que le spam est un problème de nature complexe et qu'il faut impérativement une stratégie associant plusieurs acteurs et se déployant sur plusieurs fronts.

Il est clairement apparu dans les travaux du Groupe de réflexion que toutes les parties prenantes avaient un rôle important à jouer dans la lutte contre le spam. Il faudrait que les gouvernements définissent une politique nationale anti-spam lisible en concertation avec les autres acteurs, collaborent avec les opérateurs privés, et encouragent le coopération transnationale. La constitution de groupes de coordination nationaux et la création d'un cadre réglementaire approprié – fondé sur des objectifs d'action bien définis – complété par des mécanismes de répression efficaces, peut contribuer puissamment au combat anti-spam. S'appuyant sur ce cadre, le secteur privé est le mieux placé pour élaborer des pratiques commerciales appropriées et des solutions techniques novatrices, et il peut jouer un rôle considérable dans l'éducation des utilisateurs. La coordination et la coopération entre les acteurs publics et privés sont cruciales pour marquer des points dans la bataille contre le spam.

Compte tenu du rythme rapide de l'évolution technique, et par conséquent des changements qui interviennent dans les pratiques frauduleuses et illégales, la présente Boîte à outils ne prétend pas apporter de réponses spécifiques, mais des orientations. Par ailleurs, la complexité du problème restera la même après l'expiration du mandat du Groupe de réflexion, d'où l'importance de mettre sur pied et de maintenir une stratégie claire de lutte contre le spam. Dans cette entreprise, la coordination nationale, la coopération public-privé, et le dialogue sont déterminants.

L'Internet est défini dans la Déclaration de principes du SMSI comme "*une ressource publique mondiale*". Autrement dit, il incombe aussi à l'ensemble du public de le préserver et de contribuer à sa facilité d'emploi et à sa fiabilité. Tous les acteurs doivent apprendre à gérer le spam et, à cette fin, la méthodologie de la boîte à outils doit être mise en oeuvre à l'échelon national et elle devrait être revue à intervalles réguliers pour faire face aux nouvelles menaces et activités illégales auxquelles le spam sert de vecteur.

ANNEXES

Annexe I :
Recommandation du conseil relative à la coopération transfrontière dans l'application des legislations contre le spam

LE CONSEIL,

Vu la Convention relative à l'Organisation de Coopération et de Développement Économiques, en date du 14 décembre 1960, en particulier son Article 5 b) ;

Reconnaissant que le spam sape la confiance des consommateurs, qui est une condition préalable à la société de l'information et au succès du commerce électronique ;

Reconnaissant que le spam peut faciliter la propagation des virus, servir de support pour des tentatives traditionnelles de fraude ou de tromperie mais aussi pour d'autres menaces liées à l'Internet, comme l'hameçonnage, et que ses effets peuvent influer négativement sur la croissance de l'économie du numérique, avec pour conséquences d'importants coûts économiques et sociaux pour les pays Membres et les économies non membres ;

Reconnaissant que le spam pose des problèmes spécifiques pour les autorités chargées de l'application de la loi dans la mesure où les expéditeurs peuvent aisément masquer leur identité, falsifier la trace électronique de leurs courriels et les envoyer de n'importe quel endroit du monde à n'importe qui dans le monde, ce qui fait du spam un problème international particulier contre lequel il n'est possible de lutter efficacement qu'à travers une coopération internationale ;

Reconnaissant le besoin d'une coopération mondiale afin de surmonter un certain nombre de difficultés pour la collecte et le partage de l'information, pour l'identification des priorités de lutte et pour l'élaboration de cadres de lutte internationaux efficaces ;

Reconnaissant que des dispositifs en vigueur, comme de nombreux instruments de coopération bi- et multilatérale pour l'application du droit pénal, fournissent un cadre pour une coopération en matière de lutte contre les conduites frauduleuses associées au spam, telles que l'utilisation de logiciels malveillants et l'hameçonnage ;

Vu la *Recommandation du Conseil concernant des Lignes directrices régissant la protection des consommateurs contre les pratiques commerciales transfrontières frauduleuses et trompeuses* (ci-après dénommées « *Lignes directrices sur la fraude transfrontière* »), qui définit des principes pour une coopération internationale entre organismes chargés de faire appliquer les dispositions de protection des consommateurs dans la lutte contre les pratiques transfrontières frauduleuses et trompeuses [C(2003)116] ;

Vu la *Recommandation du Conseil concernant les Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel* [C(80)58] (ci-après dénommées « *Lignes directrices sur la vie privée* »), et la *Déclaration des Ministres relative à la protection de la vie privée sur les réseaux mondiaux* [C(98)177] ;

Reconnaissant que, dans certains cas, les *Lignes directrices sur la fraude transfrontière et les Lignes directrices sur la vie privée* peuvent s'appliquer directement à la coopération pour la lutte transfrontière contre le spam et que même lorsque cela n'est pas le cas, nombre des principes exprimés dans ces Lignes directrices peuvent être utilement adaptés pour élaborer des cadres nationaux appropriés et faciliter la coopération internationale pour faire appliquer les lois contre le spam ;

Rappelant que, bien que la coopération pour la lutte transfrontière contre le spam soit un élément important pour faire face au problème mondial du spam, il est nécessaire à cet égard d'adopter une approche nationale globale qui prenne également en compte les questions de réglementation et de politique générale, facilite l'élaboration de solutions techniques appropriées, améliore l'information et la sensibilisation de tous les acteurs et encourage les initiatives pilotées par l'industrie ;

Sur la proposition conjointe du Comité de la politique de l'information, de l'informatique et des communications et du Comité de la politique à l'égard des consommateurs :

CONVIENT que :

Aux fins de la présente Recommandation, et sans préjudice des autres instruments de coopération existants « les Autorités de lutte contre le spam » désignent tout organisme public national, tel que déterminé par chaque pays, qui est chargé de faire appliquer les dispositions législatives en relation avec le spam et est habilité à (a) coordonner ou mener des investigations ou (b) engager des procédures d'exécution, ou (c) les deux.

Aux fins de la présente Recommandation, « les dispositions législatives en relation avec le spam » désignent (a) les dispositions législatives visant spécifiquement les communications électroniques ; ou (b) les dispositions législatives générales, telles que celles relatives à la vie privée, à la protection des consommateurs ou aux télécommunications, qui peuvent s'appliquer aux communications électroniques.

La présente Recommandation s'adresse principalement aux organismes publics nationaux, habilités à faire appliquer les dispositions législatives en relation avec le spam. Il est reconnu que certains pays Membres disposent d'un grand nombre d'organismes compétents, certains à caractère régional ou local, qui peuvent prendre ou engager des actions contre le spam. Il est également reconnu que dans certains pays Membres, des organismes de lutte privés peuvent jouer un rôle très important pour assurer le respect des dispositions législatives en relation avec le spam, notamment dans un contexte transfrontière.

La présente Recommandation vise la coopération pour la lutte transfrontière contre le spam uniquement dans les domaines pour lesquels le comportement interdit par les dispositions législatives en relation avec le spam dans le pays Membre recevant une demande d'entraide, est assimilable pour l'essentiel à un comportement interdit par les dispositions législatives en relation avec le spam du pays sollicitant l'entraide. La coopération en vertu de la présente Recommandation n'affecte pas la liberté d'expression protégée par les législations des pays Membres.

La coopération en vertu de la présente Recommandation est circonscrite aux violations les plus graves des dispositions législatives en relation avec le spam, comme celles qui (a) provoquent ou sont susceptibles de provoquer des préjudices (financiers ou autres) pour un nombre significatif de destinataires, (b) affectent des groupes particulièrement nombreux de destinataires ou (c) causent d'importants préjudices aux destinataires.

Dans tous les cas, la décision de fournir ou non une entraide en vertu de la présente Recommandation appartient à l'Autorité de lutte contre le spam recevant la demande d'entraide.

Les pays Membres sont par ailleurs encouragés à utiliser les possibilités de coopération en la matière offertes par tout autre instrument, accord ou arrangement.

RECOMMANDE que :

Les pays Membres s'attachent à élaborer des cadres pour une coopération plus étroite, plus rapide et plus efficiente entre Autorités de lutte contre le spam prévoyant, selon les besoins :

a) La mise en place d'un cadre national.

Les pays Membres devraient à cet égard :

(i) Mettre en place et entretenir un cadre efficace de dispositions législatives, d'Autorités de lutte contre le spam et de pratiques pour l'application des dispositions législatives en relation avec le spam.

(ii) Prendre des mesures pour que les Autorités de lutte contre le spam disposent du pouvoir nécessaire pour recueillir des preuves suffisantes pour enquêter et agir dans les meilleurs délais contre les violations de dispositions législatives en relation avec le spam qui sont commises sur leur territoire ou provoquent des effets sur leur territoire. Ce pouvoir devrait notamment comporter la capacité d'obtenir l'information nécessaire et les documents pertinents.

(iii) Améliorer la capacité des Autorités de lutte contre le spam à prendre les mesures appropriées contre (a) les émetteurs de communications électroniques qui violent des dispositions législatives en relation avec le spam et (b) les particuliers et entreprises qui tirent profit de l'émission de telles communications.

(iv) Revoir périodiquement leurs propres cadres nationaux et s'efforcer d'assurer leur efficacité pour une coopération transfrontière destinée à faire respecter les dispositions législatives en relation avec le spam.

(v) Etudier les moyens d'améliorer les voies de recours en cas de préjudice financier causé par le spam.

b) Le renforcement de la capacité à coopérer.

Les pays Membres devraient améliorer la capacité de leurs Autorités de lutte contre le spam à coopérer avec les Autorités de lutte contre le spam étrangères.

Les pays Membres devraient à cet égard :

(i) Doter leurs Autorités de lutte contre le spam de mécanismes pour échanger, sur demande, avec des autorités étrangères les informations pertinentes relatives à des violations de leurs dispositions législatives en relation avec le spam, dans les cas appropriés et sous réserve de garanties adéquates.

(ii) Permettre à leurs Autorités de lutte contre le spam de fournir à des autorités étrangères, sur leur demande, une entraide en matière d'enquête sur des violations de leurs dispositions législatives en relation avec le spam, dans les cas appropriés et sous réserve de garanties adéquates, notamment pour ce qui est d'obtenir des informations auprès de certaines personnes, d'obtenir des documents ou des pièces ou de localiser ou identifier des personnes ou des biens.

(iii) Désigner un point de contact pour la coopération en vertu de la présente Recommandation, et communiquer au Secrétariat de l'OCDE des informations à jour concernant leurs dispositions législatives en relation avec le spam et l'Autorité de lutte contre le spam désignée comme point de contact. Le Secrétariat de l'OCDE consignera ces informations et les mettra à la disposition des parties intéressées.

c) L'amélioration des procédures de coopération.

Avant d'effectuer des demandes d'assistance telles que prévues dans les paragraphes précédents, les Autorités de lutte contre le spam devraient :

(i) Procéder à certains travaux préliminaires d'enquête pour déterminer si une demande d'entraide se justifie et si elle est conforme au champ d'application et aux priorités énoncés dans la présente Recommandation.

(ii) S'efforcer de hiérarchiser les demandes d'entraide et, dans toute la mesure du possible, utiliser des ressources communes telles que le site de l'OCDE sur le spam, les canaux informels, les réseaux internationaux existants ainsi que les instruments existants de coopération pour la mise en application du droit, en vue de mettre en œuvre la présente Recommandation.

d) La coopération avec les entités compétentes du secteur privé.

Les Autorités de lutte contre le spam, les entreprises, les fédérations industrielles et les groupements de consommateurs devraient coopérer dans la poursuite des violations des dispositions législatives en relation avec le spam. Les Autorités de lutte contre le spam devraient notamment coopérer avec ces groupes pour l'information des utilisateurs, et les encourager à communiquer les données utiles dont ils disposent en matière de plaintes et à partager avec les Autorités de lutte contre le spam leurs outils et techniques d'enquête, leurs analyses, leurs données et leurs informations sur les évolutions en cours.

Les pays Membres devraient encourager la coopération entre les Autorités de lutte contre le spam et le secteur privé pour faciliter la localisation et l'identification des spammeurs.

Les pays Membres devraient également encourager la participation du secteur privé et des économies non membres dans les efforts de coopération pour la lutte au plan international, dans les efforts pour réduire l'incidence des informations erronées sur les détenteurs de noms de domaine et dans les efforts pour mieux sécuriser l'Internet.

Lorsqu'il y a lieu, les Autorités de lutte contre le spam et le secteur privé devraient continuer d'explorer de nouvelles voies pour réduire le spam.

INVITE les économies non membres à tenir dûment compte de la présente Recommandation et à collaborer avec les pays Membres pour sa mise en œuvre.

CHARGE le Comité de la politique de l'information, de l'informatique et des communications et le Comité de la politique à l'égard des consommateurs de suivre l'avancement de la coopération pour la lutte transfrontière contre le spam dans le cadre de la présente Recommandation dans un délai de trois ans suivant son adoption, puis par la suite en fonction des besoins.

Annexe II :
Pratiques exemplaires preconisées par le BIAC et le MAAWG à l'intention des fournisseurs d'acces internet et opérateurs de réseaux[1]

Contexte

Les FAI et opérateurs de réseaux ont un rôle important dans la lutte contre le spam.

En raison de ce rôle important qu'ils jouent, les FAI, les opérateurs de réseaux, les groupes techniques et les alliances continuent d'échanger leurs pratiques exemplaires pour prévenir le trafic émis ou transitant sur leurs réseaux.

Bien que ces pratiques exemplaires ne sauraient, en elles-mêmes, constituer une solution globale au spam, elles s'inscrivent dans une stratégie sur plusieurs fronts pour s'attaquer au problème du spam. Plus les entités qui adoptent et appliquent des pratiques communes seront nombreuses, plus leur action sera efficace.

Si ces pratiques exemplaires volontaires sont adoptées par les FAI et opérateurs de réseaux, il appartiendra aux utilisateurs, pour démultiplier leur impact positif, de prendre aussi les mesures nécessaires pour protéger la sécurité de leurs ordinateurs, logiciels et réseaux, et notamment de veiller à protéger leur identité personnelle en ligne.

Finalité

Les pratiques exemplaires du BIAC à l'intention des FAI et opérateurs de réseaux représentent un ensemble de principes volontaires élaborés par les milieux d'affaires dont la finalité est de renforcer la sécurité des infrastructures de réseaux dans la lutte contre le spam. Le secteur privé continuera de collaborer à l'élaboration de mesures techniques et de procédure additionnelles pour promouvoir la mise en oeuvre de ces principes.

Le BIAC considère ses pratiques exemplaires à l'intention des FAI et opérateurs de réseaux comme un outil important pour combattre le spam. Ces pratiques exemplaires et les mesures qui seront appelées à les compléter ont un caractère **volontaire**, et en toutes circonstances, elles sont subordonnées aux cadres juridiques et réglementaires applicables.

1 Le Comité consultatif économique et industriel auprès de l'OCDE (BIAC) a été créé en mars 1962. C'est un organisme indépendant reconnu par l'OCDE comme le représentant officiel des milieux d'affaires de ses pays Membres (http://www.biac.org). Le BIAC regroupe les principales fédérations de l'industrie et des employeurs des 30 pays Membres de l'OCDE, représentant plus de 8 millions d'entreprises. À travers ses 31 comités permanents et groupes de politique, le BIAC reflète toutes les questions économiques traitées par l'OCDE, et examine leurs conséquences potentielles pour les milieux d'affaires à la fois dans les pays Membres, mais aussi dans un nombre croissant de pays non-membres tels que la Russie, la Chine et l'Inde.

Le Messaging Anti-Abuse Working Group (http://www.maawg.org) est une organisation mondiale ayant pour mission de protéger les messages électroniques des attaques et utilisations abusives en ligne de manière à renforcer la confiance et l'assurance des utilisateurs, tout en garantissant la distribution des messages légitimes. Bénéficiant d'une large assise de Fournisseurs d'accès Internet (FAI) et d'opérateurs de réseaux représentant plus de 600 millions de comptes de messagerie, de grands équipementiers et d'expéditeurs, le MAAWG s'attache à lutter contre les utilisations abusives de la messagerie en encourageant les solutions technologiques, la collaboration entre professionnels et les initiatives des pouvoirs publics.

La mise en oeuvre de ces pratiques exemplaires et des éventuelles mesures additionnelles sera fonction des configurations techniques des réseaux des différents fournisseurs et opérateurs, ainsi que des impératifs et des enjeux commerciaux qui leur sont propres. Nous notons que la flexibilité dans la mise en oeuvre de ces pratiques exemplaires est la clé pour que ces pratiques soient largement et efficacement adoptées par les fournisseurs de service grands et petits.

Etant donné la rapidité du changement technologique, ces pratiques exemplaires seront périodiquement revues et actualisées.[2]

Pratiques exemplaires

Contexte/définitions

Quelle que soit la juridiction nationale considérée, il est entendu que chacune des pratiques exemplaires ci-dessous n'est recommandée que si elle ne contrevient pas à la législation nationale en vigueur.

Dans le contexte de ces pratiques exemplaires, les « FAI et opérateurs de réseaux » désignent toute entité exploitant un serveur SMTP relié à l'Internet.

Le BIAC formule à l'intention des FAI et opérateurs de réseaux les recommandations suivantes :

1. Dans les limites du cadre juridique applicable, les FAI et opérateurs de réseaux devraient prendre en compte le problème des équipements d'utilisateur compromis en mettant en place des procédures rapides permettant de gérer ces équipements d'utilisateurs et éléments de réseau de manière à ce qu'ils n'émettent plus de spam ;

2. Les FAI et opérateurs de réseaux devraient utiliser la technologie standard de l'industrie pour authentifier leur courrier électronique et/ou leurs sources ;

3. Les FAI et les opérateurs de réseaux devraient bloquer les fichiers joints au courrier électronique susceptibles d'être une source d'infection. S'agissant du filtrage du courrier électronique ou des fichiers en pièce jointe d'un courrier électronique fondé sur les propriétés du contenu, il convient si la législation l'impose d'obtenir le consentement préalable du client ;

4. Les FAI et opérateurs de réseaux devraient surveiller activement le volume de courrier entrant et sortant afin de repérer toute activité inhabituelle sur le réseau et sa source, et prendre des mesures en conséquence ;

5. Les FAI et opérateurs de réseaux devraient établir des processus interentreprises adéquats pour donner suite aux rapports d'incidents des autres opérateurs de réseaux, et également pour recueillir les plaintes des utilisateurs ;

6. Les FAI, les opérateurs de réseaux et les prestataires de services de courrier électronique aux entreprises devraient communiquer à leurs utilisateurs leurs politiques et procédures en matière de sécurité ;

2 Les pratiques exemplaires seront tenues à jour par le BIAC et le MAAWG. Des versions actualisées ou améliorées seront disponibles en ligne sur les sites Web du BIAC et du MAAWG. Pour plus de précisions, voir le site : http://www.oecd-antispam.org.

7. Les FAI et opérateurs de réseaux devraient s'efforcer de n'envoyer des avis de non distribution que pour les messages émis par leurs propres titulaires de comptes ;

8. Les FAI et opérateurs de réseaux devraient prendre des mesures pour s'assurer que seuls leurs titulaires de comptes utilisent leurs serveurs d'expédition de courrier électronique ;

9. Les FAI et opérateurs de réseaux devraient veiller à ce que tous les noms de domaine, les fichiers DSN (Domain Name System) et les fichiers d'enregistrement d'adresses IP (Internet Protocol) applicables soient tenus de manière responsable, sur la base d'informations exactes, complètes et à jour. Ces informations devraient comprendre les coordonnées des services à contacter pour résoudre les problèmes d'utilisation abusive et inclure, sans que la liste soit limitative, les adresses postales les numéros de téléphone et les adresses de courrier électronique ;

10. Les FAI et opérateurs de réseaux devraient veiller à ce que toutes leurs adresses IP routables publiques et visibles sur Internet disposent d'enregistrements DNS pour le routage direct et inverse et d'enregistrements WHOIS et SWIP adéquats et à jour ; tous les exploitants de réseaux locaux devraient se conformer à la RFC (Request for Comments) 1918 – « Classes d'adresses privées » ; les réseaux locaux en particulier ne devraient pas utiliser l'espace IP enregistré globalement au nom d'autrui ou l'espace IP non enregistré au nom de quelqu'un, à titre d'espace IP privé.

Annexe III :
Pratiques exemplaires du BIAC[3] pour le marketing par courrier électronique[4]

Contexte

Il s'agit en élaborant une série de pratiques exemplaires volontaires de donner des orientations aux entreprises de marketing en ligne afin qu'elles puissent adopter des techniques de communication qui soient à la fois non polluées par le spam et plus efficaces. Ces règles devraient clairement énoncer que le spam n'a aucune place dans le marketing légitime.

La plupart des organismes responsables appliquent déjà des codes professionnels ou ont adopté des pratiques exemplaires. On trouvera dans le présent document un ensemble de pratiques exemplaires volontaires qui empruntent à des codes existants afin d'offrir à tous une base pour l'utilisation du courrier électronique à des fins commerciales ou de marketing.

De plus en plus, les Fournisseurs d'accès Internet (FAI) et les fournisseurs de services de courrier électronique cherchent à stopper le spam en utilisant des méthodes de filtrage et des listes blanches et listes noires. Ce faisant, ils bloquent par inadvertance des messages légitimes avant que ceux-ci ne parviennent à leurs destinataires. Les pratiques exemplaires volontaires du BIAC pour le marketing par courrier électronique ont été élaborées pour aider les entreprises à faire en sorte que leurs messages de courrier électronique commerciaux légitimes parviennent bien à leurs destinataires.

Finalités

Les pratiques exemplaires volontaires du BIAC pour le marketing par courrier électronique sont un ensemble de recommandations volontaires élaborées par les milieux professionnels, qui visent à améliorer les communications commerciales légitimes sur l'Internet tout en luttant contre le spam.

Le BIAC considère ses pratiques exemplaires pour le marketing par courrier électronique comme un outil important pour combattre le spam. Ces pratiques exemplaires ayant un caractère volontaire, en toutes circonstances, elles sont subordonnées aux cadres juridiques et réglementaires applicables. A ce titre, elles visent à compléter les législations existantes qui régissent le spam, la vie privée, le marketing par courrier électronique et le marketing en direction des enfants.

Ces pratiques exemplaires, qui sont des suggestions de pratiques commerciales responsables en matière de marketing, proposent une vision globale par les milieux d'affaires de pratiques de marketing responsables qui à la fois protègent les intérêts des consommateurs et donnent aux entreprises la souplesse nécessaire pour répondre aux besoins de leurs clients et explorer de nouveaux types de débouchés commerciaux. Conscient toutefois du fait que certains cadres juridiques nationaux/régionaux ou les

3 Le Comité consultatif économique et industriel auprès de l'OCDE (BIAC) a été créé en mars 1962. C'est un organisme indépendant reconnu par l'OCDE comme le représentant officiel des milieux d'affaires de ses pays Membres. Le BIAC regroupe les principales fédérations de l'industrie et des employeurs des 30 pays Membres de l'OCDE, représentant plus de 8 millions d'entreprises. À travers ses 31 comités permanents et groupes de politique, le BIAC reflète toutes les questions économiques traitées par l'OCDE, et examine leurs conséquences potentielles pour les milieux d'affaires à la fois dans les pays Membres, mais aussi dans un nombre croissant de pays non-membres tels que la Russie, la Chine et l'Inde.

4 Following the Task Force discussion BIAC is proposing to modify the wording of these best practices.

pratiques de certaines entreprises peuvent être avoir un caractère plus restrictif que les propositions ci-après, le BIAC n'entend pas suggérer que ces recommandations soient appliquées quand celles-ci peuvent être moins restrictives que les prescriptions légales.

Etant donné le rythme rapide du progrès technologique, ces pratiques seront revues périodiquement pour s'assurer qu'elles gardent leur pertinence pour l'utilisation de l'Internet comme un support de communication viable pour les expéditeurs de courriers électroniques commerciaux légitimes.

Pratiques exemplaires recommandées

1. **L'expédition de messages commerciaux électroniques devrait respecter les prescriptions en matière de consentement de la législation nationale en vigueur dans le pays d'où opère l'expéditeur, à moins que celui-ci ne cible délibérément et en connaissance de cause des consommateurs résidant dans un autre pays.**

2. **Les organismes devraient garder trace des demandes d'inscription ou désinscription afin que les listes d'adresses électroniques puissent être nettoyées avant les campagnes promotionnelles.**

Les organismes devraient s'assurer qu'ils ont les moyens d'honorer dans des délais raisonnables les demandes d'inscription/désinscription et de nettoyer leurs listes en conséquence.

Un processus interne devrait être en place pour enregistrer les preuves de consentement, quand cela est nécessaire, notamment la date et l'heure. Les autres informations dont la trace pourrait être conservée sont notamment l'adresse IP et le lieu d'origine de la demande (notamment l'URL), l'endroit où le recueil d'adresse a été effectué et le support par lequel le consentement a été obtenu s'il n'a pas été obtenu via Internet (par exemple, carte de visite professionnelle, bulletin de participation, téléphone, communication verbale ou carte de crédit [p.ex. par paiement d'un abonnement à une liste]. Les organismes devraient pouvoir fournir ces informations à un destinataire qui en fait la demande, sous réserve qu'un délai raisonnable se soit écoulé pour permettre la saisie dans la base de données.

3. **Dans tous les courriers électroniques de marketing (à l'exception des courriers de transaction), il conviendrait de proposer aux destinataires un moyen évident, clair et efficace de refuser, par courrier électronique ou par le Web, de recevoir d'autres messages électroniques commerciaux ou de marketing de la part de l'expéditeur.**

Dans tous leurs courriers électroniques à des clients existants ou potentiels, les organismes devraient offrir au destinataire une possibilité de désinscription. Cette option ne devrait pas être cachée dans le message et devrait, au minimum, être accessible par le Web et/ou courrier électronique. Les termes utilisés devraient être aussi simples que : « Si vous ne souhaitez plus recevoir nos offres promotionnelles, **cliquez ici** ou adressez un courrier électronique à **info@ABCsociété.com** ».

Le processus de désinscription devrait être simple et explicite, et les organismes devraient confirmer par courrier électronique ou par une annonce sur le web que la demande de désinscription a été ou sera prise en compte sans autre démarche du consommateur.

4. **Toute communication marketing par courrier électronique devrait clairement mentionner l'identité de l'expéditeur. La ligne « sujet » et le corps du texte du message devraient fidèlement refléter le contenu, l'origine et le but de la communication.**

Les identités de l'expéditeur et de la source du message électronique devraient être indiquées de façon claire et visible, et chaque fois que possible figurer dans le premier écran du message (c'est-à-dire dans la partie du message visible sans avoir à dérouler la page avec l'ascenseur).

Exemple A : communication directe d'un organisme à un abonné

Date: Tue, 5 Oct 2004 07:32:02 -0400; From: Bell Canada - Electronic bill bill.presentment@bell.ca TO: JOE CONSUMER " joe@consumer.com Subject: Your Bell e-bill is ready / Votre facture électronique est prête

Exemple B: D'un prestataire tiers de courrier électronique à un abonné pour le compte d'un autre organisme

From: "peteMOSS PUBLICATIONS <bounces@peteMOSS.com>" v2user-13990-IXoyuP..CahrNet _0bkttg@mailer.whitehat.com Subject: SpamNEWS 07/21/04 To: joe@consumer.com
Date: Sat, 24 Jul 2004 18:50:17 -0700

Même dans les cas où la ligne « Sujet » reflète avec fidélité le contenu, il convient de mettre en garde les organismes contre l'utilisation dans les lignes « Sujet » d'expressions comme « Offres gratuites » ou « Prix à gagner ». En effet, certains filtres anti-spam utilisent ce type de mots clés pour classer les messages dans la catégorie spam.

L'adresse postale principale de l'expéditeur doit figurer dans les messages de courrier électronique. Tous les organismes sont vivement encouragés à se familiariser avec les dispositions de la législation nationale des pays qui ont légiféré sur ce point.

5. **Tous les courriers électroniques devraient proposer un lien pointant vers la charte de protection de la vie privée de l'expéditeur**

Les organismes devraient rendre aisément consultables les informations concernant leurs procédures de recueils d'informations en ligne, en les regroupant dans une charte générale relative à la protection de la vie privée sur leurs sites Web. Cette charte sur la vie privée devrait également préciser la marche à suivre ou proposer un lien pour indiquer que l'on ne veut plus recevoir de communications commerciales à l'avenir.

6. **Les entreprises de marketing, les courtiers de listes et les détenteurs de listes devraient prendre des mesures pour s'assurer que les adresses figurant dans leurs listes d'adresses électroniques ont été obtenues de façon licite**

Parmi les mesures raisonnables qu'un organisme pourrait prendre pour s'assurer que les listes qu'il utilise sont convenables on peut mentionner le fait :

- d'examiner la politique en matière de vie privée du vendeur ou détenteur de la liste ;
- d'examiner les procédures qui ont pu être utilisées pour obtenir les adresses électroniques.

- D'obtenir l'assurance que les adresses de courrier électronique ont été obtenues d'une manière conforme aux lois en vigueur.

- De faire signer au vendeur ou au propriétaire de la liste une convention certifiant qu'il s'est conformé aux prescriptions de la législation sur la vie privée.

7. Les entreprises de marketing devraient agir avec beaucoup de discernement lorsqu'elles adressent des courriers électroniques de marketing à des enfants et des adolescents, pour tenir compte du degré de connaissance, d'expérience et de maturité de ce public.

La façon dont les personnes qui ne sont pas encore majeures perçoivent les communications de marketing par courrier électronique et réagissent dépend de l'âge et de l'expérience, de même que du contexte du message. Ainsi, des communications de marketing par courrier électronique qui sont acceptables pour des adolescents ne le seront pas nécessairement pour des enfants plus jeunes. Il en va de même pour le marketing par courrier électronique de contenus pour adultes, lesquels englobent aussi bien les contenus à caractère sexuellement explicite que ceux qui ont trait aux jeux de hasard, au tabac, à l'alcool, aux armes à feu et autres armes.

Par exemple, tout courrier électronique renfermant un contenu sexuellement explicite devrait inclure la balise de préface « SEXUELLEMENT EXPLICITE » dans la ligne « Sujet ».

Bien qu'il n'existe aucun moyen de s'assurer de l'âge d'une personne qui s'inscrit sur une liste de distribution de courrier électronique, lorsque les messages ont un contenu pour adulte, il conviendrait préalablement à l'envoi de la communication de s'efforcer de vérifier que le destinataire a bien l'âge autorisé pour recevoir et lire ce type de contenu. Les organismes devraient donc faire preuve de jugement et de retenu dans leurs activités de marketing en direction des mineurs et devraient s'efforcer de recueillir un accord parental pour ce type de communication. Si un opérateur de marketing cible délibérément un pays donné, les entreprises devraient consulter les éventuelles dispositions législatives ou prescriptions nationales concernant l'autorisation parentale et s'assurer qu'elles sont respectées.

8. Les organismes devraient mettre en place un système de traitement des plaintes juste, efficace, confidentiel et facile à utiliser.

Toutes les plaintes des particuliers concernant l'utilisation de leur adresse de courrier électronique devraient être traitées avec courtoisie et dans un délai raisonnable.

9. Les organismes peuvent divulguer les adresses de courrier électronique de leurs clients à des tiers affiliés ou au sein d'une famille de sociétés :

i. s'ils utilisent les adresses aux fins pour lesquelles elles ont été recueillies (c'est-à-dire pour un marketing relié à l'achat original ou à la prestation de services associés à cet achat) ;

ii. s'il existe un moyen facile de refuser de recevoir d'autres communications par courrier électronique ;

iii. ou s'ils ont obtenu un consentement à cet effet.

Lorsqu'elles partagent des bases de données d'adresses électroniques au sein d'une organisation ou d'un groupe industriel, les entreprises doivent garder à l'esprit que les consommateurs peuvent ne pas comprendre que différentes marques peuvent être détenues par une seule et même entreprise, et que différentes entreprises peuvent entretenir des liens et échanger des adresses de courrier électronique, et elles doivent donc être transparentes vis-à-vis des consommateurs sur les raisons pour lesquelles ceux-ci reçoivent d'autres offres marketing apparentées (par exemple sous une autre marque).

Conseils techniques à l'intention des entreprises de marketing électronique

1. **Les expéditeurs devraient mettre en oeuvre les spécifications techniques standard suivantes :**

   - Tous les serveurs (par exemple serveurs entrants, serveurs sortants, sites Web) doivent disposer de pointeurs de système de noms de domaine (DNS) inverse — rDNS PTR — dans les enregistrements DNS, les valeurs de recherche directe et inverse de l'hôte doivent correspondre et les machines sources doivent indiquer ce nom dans la commande HELO/EHLO.

   - Les fichiers Sender Policy Framework (SPF) (par exemple http://spf.pobox.com) et clef de domaine (domain-key) (par exemple http://antispam.yahoo.com/domainkeys) devraient être publiés par les expéditeurs et les sites tiers associés à un publipostage (par exemple sites Web, fournisseurs de services de messagerie, etc.) et tenus à jour en permanence. L'adoption de technologies similaires doit être envisagée au fur et à mesure qu'elles sont mises au point et sont normalisées.

   - Les adresses IP qui sont distinctes des autres serveurs du site doivent être assignées à des serveurs de courrier sortant.

   - Les enregistrements dans la base de données WHOIS de tous les domaines expéditeurs doivent toujours être exacts et complets.

   - Les comptes techniques (par exemple postmaster@ et abuse@) doivent être fonctionnels et activement surveillés pour tous les domaines expéditeurs, y compris les sites Web, mentionnés dans le contenu du courrier électronique.

2. **Les expéditeurs doivent traiter les messages refusés comme suit :**

   - Ils doivent promptement retirer les adresses faisant l'objet d'un refus permanent « hard bounced » (5xx : Utilisateur non existant / boîte aux lettres non disponible, etc.) des listes qu'ils contrôlent lorsque le nombre total de refus excède 3 en 14 jours. Si un refus 5xx indique un blocage pour spam, l'adresse peut être réactivée si le blocage pour spam est levé.

   - Ils doivent retirer les adresses faisant l'objet d'un refus temporaire « soft bounced » (4xx : Échecs isolés) lorsque le nombre total de refus est supérieur à 5 lors de campagnes consécutives à partir d'une même liste ou totalise 5 à partir de plusieurs listes en 10 jours.

Les politiques de traitement des messages refusés sont expliquées en détail sur les sites suivants :

- http://help.yahoo.com/help/us/mail/defer
- www.isipp.com/standards.php
- http://postmaster.info.aol.com/guidelines/bestprac.html

Annexe IV :
GSM Association mobile Spam code of Practicec[5]
Version 1.0 February 2006

1. Executive Summary

1.1 About this document

The Mobile Spam Code of Practice ('the Code') is a voluntary non-legally binding document reflecting a commitment by operators and the GSMA to act against mobile spam and minimise the impact it has on customers.

Some of the principles and commitments within the Code are already contained in the laws of various countries. However, against a background of disparity in national legal environments, the mobile industry has identified the need to work together to adopt consistent approaches to dealing with spam and share best practice.

1.1.1 Scope

The Code applies to unsolicited communications sent via SMS and MMS and includes: commercial messages sent to customers without consent, commercial messages sent to customers encouraging them directly or indirectly to call or send a message to a premium rate number, and bulk fraudulent messages sent to customers (e.g. faking, spoofing or scam messages).

1.1.2 Purpose

Under the Code, the mobile operators that are signatories commit to:

- Include anti-spam conditions in all new contracts with third party suppliers.
- Provide a mechanism that ensures appropriate customer consent and effective customer control with respect to mobile operators' own marketing communications.
- Work co-operatively with other mobile operators to address spam issues.
- Provide customers with information and resources to help them minimise the levels and impact of mobile spam.
- Undertake other anti-spam activities to minimise the level and impact of mobile spam.
- Encourage governments and regulators to support industry.

5 Any update of this version will be available on the GSMA Web site at: www.gsmworld.com.

The signatories will work in good faith to implement the commitments highlighted above and the GSMA will monitor the adoption and implementation of the Code. The GSMA and signatories to this Code of Practice will continue to examine issues associated with other types of spam and unsolicited communications and will update the Code as appropriate.

2. The code of practice

This Code of Practice demonstrates mobile operators' commitment to fight proactively mobile spam and minimise the impact that it has on customers.

This Code of Practice applies to unsolicited communications sent via SMS and MMS (referred to as 'mobile spam') and specifically includes[6]

i) Commercial short messages or multimedia messages sent to customers without consent as required by national law (e.g. marketing messages).

ii) Commercial short messages or multimedia messages sent to customers encouraging them directly or indirectly to call or send a short message or other electronic communication to a premium rate number.

iii) Short messages or multimedia messages sent to customers in bulk and which are fraudulent (e.g. faking, spoofing or scam messages).

For the purpose of this Code of Practice, "commercial short messages or multimedia messages"[7] means SMS or MMS messages designed to promote, directly or indirectly, the goods, services or image of any person pursuing a commercial activity or exercising a regulated profession.

The mobile operators that are signatories to this Code of Practice commit to:

1. Include anti-spam conditions in all new contracts with third party suppliers. In these third party supplier contracts, conditions should include:

- A commitment to not send or initiate mobile spam.
- A commitment to respect the consent requirements set by relevant national legislation or selfregulatory mechanisms in force.
- A commitment to provide customers with obvious, clear and efficient means to opt-out of receiving further SMS or MMS marketing communications.
- Potential penalties for breaching the anti-spam commitments, including possible suspension and/or termination of contracts.

11. Provide a mechanism that ensures effective customer control with respect to mobile operators' own marketing communications via SMS or MMS, in line with consent requirements set out in national legislation.

The means of enabling consent could include providing customers with prior 'opt-in' consent mechanisms (where customers opt-in to receive communications) and/or 'optout' mechanisms (where customers are given the opportunity to opt-out of any future communications).

Operators also commit to:

- Ensure that the processes they use to obtain consent are clear and transparent and that records are kept of the type of consent obtained from customers, including how and when consent was received.

- Provide customers with obvious, clear and efficient means to opt-out of receiving further operator mobile marketing communications sent via SMS or MMS.

12 Work co-operatively with other mobile operators to investigate cases of mobile spam transmitted across networks and take action where appropriate.

13. Provide customers with information and resources to help them minimise the level and impact of mobile spam. These should include:

- Provision of information on operators' anti-spam policies, relevant legislation and local codes of practice.

- Advice on how to handle incidents of suspected spam, through their customer services contacts, in print and/or on their websites.

- Provision of mobile spam reporting facilities. For example, through their customer services contacts, website and/or via a 'shortcode' for customers to forward suspected mobile spam to.

14. Undertake activities designed to minimise the level and impact of mobile spam, including:

- Ensure that they have an anti-spam policy that prohibits the use of the mobile network for initiating or sending mobile spam.

- Review customer contracts, Terms & Conditions and/or Acceptable Use Policies, to ensure that up-to-date and relevant anti-spam conditions are included. For example, conditions indicating that complaints may be investigated (including co-operation with relevant public authorities as appropriate) and that the operator may terminate its service to a customer who originates mobile spam.

- Prioritise and investigate customer complaints regarding mobile spam, as appropriate, take action and report cases to the relevant public authorities, where appropriate.

- Monitor networks for signs of mobile spam and take proactive action to eliminate mobile spam, subject to the requirements of national legislation.

- Share information on best practice and co-operate with other mobile operators, nationally and internationally, to minimise mobile spam sent across networks. This should include considering the adoption of GSMA recommended techniques for detecting and dealing with the international transmission of fraudulent mobile spam and/or unsolicited SMS and MMS, which encourage a premium rate response and taking measures to ensure that the operators originating SMS and MMS are correctly identified i.e. to prevent "spoofing" of the sender's identification.

15. Encourage governments and regulators to:

- Support industry self-regulatory mechanisms.

- Support the development of responsible mobile marketing and premium rate industries. For example, through support for codes of practice that promote effective consent principles, transparency and clear pricing.

- Support investigation of spam abuses and fraud. For example, by addressing any data protection / privacy law issues or premium rate payment issues that may hamper mobile operators' ability to investigate mobile spam abuses.

- Support mobile operators in their efforts to combat mobile spam at the network level. For example, by permitting the use of network level filtering to identify and prevent mobile spam reaching customers.

- Create/support an environment that penalises those that send unsolicited SMS or MMS messages that encourage a premium rate response. For example, allow mobile operators to withhold payments to suspected mobile spam destinations, pending investigation of their spam activities by the relevant public authorities.

3. Implementation and review

The signatories to this Code of Practice will work in good faith to implement the commitments and measures listed above. Implementation timescales may vary for the different commitments and measures, depending on their technical complexity and the duration of existing contracts. The Code of Practice constitutes the intention of the GSMA and signatories to implement the measures as soon as practical in order to serve their customers interests.

The GSMA commits to:

- Monitor the adoption and implementation of the Code of Practice and the need for any further action.

- Invite signatories periodically to provide more detailed information on the effectiveness and proportionality of the measures taken.

- Assist operators in resolving inter-network mobile spam issues and in dealing with cases of persistent illegal or fraudulent activity, related to mobile spam.

Annexe V :
London Action Plan/Contact Network of Spam Authorities Pro Forma for the Referral of Spam Investigations and Accompanying Guidance (Working Document)

The "Spam Complaint Referral" *pro forma* and accompanying guidance, have been created by the London Action Plan (LAP) and the EU Contact Network of Spam Authorities (CNSA).

The *pro forma* and guidance are flexible working documents to be used by spam enforcement agencies. They were created to *i*) serve as a checklist for agencies investigating and bringing cases, *ii*) ensure that the investigating agency provides adequate information in a referral/request for the receiving agency to evaluate whether pursuing action would have merit; and *iii*) establish guidelines to help members limit referrals to those that are most likely to result in successful enforcement actions.

London Action Plan/Contact Network of Spam Authorities Pro Forma for the Referral of Spam Investigations (Working Document)

**Please see accompanying guidance prior to providing the information*

1. Contact Details

From:	Referring Authority, Country
	Contact Person, Title
	Telephone
	Email Address
To:	Receiving Authority, Country
	Contact Person, Title
	Telephone
	Email Address

2. Status of investigation/ background to request

3. Confidentiality Requirements

☐ The Receiving Authority has agreed to maintain this referral as required by the Referring Authority, and any necessary documents regarding confidentiality have been completed prior to transmission of this referral.

4. Other Authorities Involved

5. Consequences of Spamming Activity

6. Known history (e.g. search engine references of the alleged spammers)?

7. Description of Spam

Category of Spam

☐ Phishing (forged emails from banks or other institutions asking for personal information)

☐ "So called" Nigerian Scam (appears to come from person in foreign country, offers to share hidden funds)

☐ Lottery and Other Prizes

☐ Pharmaceutical (vitamins, alternative health, pain killers, arthritis)

☐ Pharmaceutical – adult (Viagra etc)

☐ Body Enhancing (diet, weight loss, bodybuilding)

☐ Miracle Cures (AIDS, arthritis, cancer, etc.)

☐ Merchandise (Jewellery, watches)

☐ Computer software, hardware

☐ Mortgages, loans, financial services

☐ Business opportunities, work-at-home, job offers

☐ Pornographic content

☐ Online Gambling

☐ Dating services

☐ Educational, degrees, grants

☐ Charity (disaster appeals,etc)

☐ Other _____

Spam Details

Approximate Volume of Spam Sent	
Time Frame in Which Spam Was Sent	
Breaches of Legislation (if known)	

8. Spam Transmission Information

Attach 10 sample spam messages, if possible. Be sure to include the message's extended headers and complete message body, including any images.

Number of messages attached: _____

Spam Att. #	Originating IP Address	ISP (or entity that IP address assigned to)	Contacted? Information Obtained?
1			
2			
3			
4			
5			
6			
7			
8			
9			
10			

Provide any impediments to obtaining IP user information.

Indicate whether based on available data, spam appears to be sent from any of the following:

1) open relay/proxy ☐ 2) zombie drones/botnets ☐ 3) headers appear to be forged ☐

Explanation/Basis

9. Parties Identified

Sender(s) The Sender is the entity that pays "Initiator" to spam on its behalf. Include individual or company name, physical address, country, website, telephone, email address, etc. Note if additional senders have been identified, but are not listed here.	Sender 1
	Sender 2
	Sender 3
	Sender 4
	Other Senders identified but not listed here?
Initiator(s) The Initiator is the spammer. Include individual names, physical address, country, website, telephone, email address, online usernames, aliases, etc. Note if additional initiators have been identified, but are not listed here.	Initiator 1
	Initiator 2
	Initiator 3
	Initiator 4
	Other Initiators identified but not listed here?

Physical postal address provided in the spam (if any)	
Websites, company names, or products being advertised by spam	

10. Spamvertized URLs, Purchase Page URLs, and related Whois information

Spamvertised URLS

	Spamvertised URL	Whois Information (provide payment info. if known)	Whois Source	Registrar and Country Where Domain Name Registrar Located (Contacted?)
S1				
S2				
S3				
S4				
S5				
S6				

(If applicable) Provide the reason why Domain Name Registrar was not contacted. Should Receiving Agency attempt to contact Domain Name Registrar? Is there other relevant information regarding Whois information?

Purchase Page URLS

	Purchase Page URL	Whois Information (provide payment info. if known)	Whois Source	Registrar and Country Where Domain Name Registrar Located (Contacted?)
P1				
P2				
P3				
P4				
P5				
P6				

(If applicable) Provide the reason why Domain Name Registrar was not contacted. Should the Receiving Authority attempt to contact Domain Name Registrar? Is there other relevant information regarding Whois information?

11. Additional Sources of Information

12. Other information related to URLs used

URL # from previous pages	Hosting provider/ Location of host	Information obtained (if any)	DNS provider	Information obtained (if any)
S1				
S2				
S3				
S4				
S5				
S6				
P1				
P2				
P3				
P4				
P5				
P6				

13. Email addresses used by target

	Email address	Source	ESP (Email Service Provider) contacted?	Result (information obtained, incomplete or appears fake)
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				

14. Forensic software used in the investigation

15. Financial data found during the investigation or deemed necessary

16. Summary of contacts made and available evidence

Using the check list below, please indicate which third-party entities have been contacted as well as whether information from such entities is either available or attached to pro forma. Please use the space provided to include the name and contact details of the organisation or person.

Entity	Entity contacted?	Evidence available?	Evidence attached?
Bank/Financial	☐	☐	☐
Domain Registrar(s)	☐	☐	☐
ISP/ESP	☐	☐	☐
Telephone company	☐	☐	☐
Postal authority	☐	☐	☐
Consumers	☐	☐	☐
Other: _____	☐	☐	☐
Other: _____	☐	☐	☐

London Action Plan/Contact Network of Spam Authorities Protocol for the Referral of Spam Investigations and accompanying guidance (Working Document)

Contents

Introduction

This protocol is designed to assist with the completion of the accompanying LAP/CNSA Spam Referral Template. It outlines some procedures that could greatly facilitate the referral of a spam investigation to another LAP/CNSA participating authority [or member].

Given the highly technical nature of spam investigations, a uniform referral method can greatly facilitate the referral of spam investigations to the appropriate authority. This referral method is the accompanying Spam Referral Template. The template should be completed to the fullest extent possible by the Referring Authority before referring any spam investigation to another LAP/CNSA participating authority. The main advantage of the template is that it will allow spam investigations to reach the correct authority in a uniform manner. According to its national law, the Receiving Authority can then process the information and consider pursuing the action in a timely fashion without having to do a great deal of additional investigation.

This protocol will assist you in completing the template.

Instructions for completing the template

1. Contact details

Include the contact details for your authority, the Referring Authority, and the authority to which the investigation is being referred, the Receiving Authority. See *Annex A* to this template for contact information for LAP/CNSA participating authorities.

Where there is more than one authority in any particular country, one authority will act as the main point of referral for that country.

2. Status of investigation/ background to request

Provide a brief summary of the investigation, including why the matter is being referred to the Receiving Authority. Please make it clear if the Referring Authority is taking any further action, and if co-ordinated action is required. Please mention if caution is needed in continuing the investigation due to offensive content of the spam or related internet pages (e.g. pornographic content).

3. Confidentiality requirements

Provide any procedural or evidentiary requirements impacting how the information contained in the template should be used. Additionally, indicate whether the referral or any part of the referral should be treated as confidential or used only for a specified purpose.

Prior to sending the referral, the Referring Authority should contact the Receiving Authority to determine whether the Receiving Authority will maintain the confidentiality from documents to be completed and signed by the Receiving Authority, this should be completed before the referral is made. Please check box in this section of the template to verify that any confidentiality requirements of the Referring Authority have been met.

4. Other authorities involved

Please include any other authorities that have provided assistance with the investigation.

5. Consequences of spamming activity

If known, outline the consequences or anticipated consequences of the spamming activity. This could include the number of complaints received by your agency about the spam, the number of consumers impacted, any loss of productivity caused by the spam, and the total monetary loss.

6. Known history

Please include a summary of any known history about the alleged spammers (e.g. search engine references, Rokso, blacklists, etc).

7. Description of spam

In this section, please summarize key aspects of the spam that is the subject of the referral:

- Category of the spam. Using the checkboxes, select the category or categories of spam to which the spam applies.

- Indicate the volume of spam sent.

- Indicate the time period in which the spam was sent.

- Provide the legislation that the spam appears to violate.

8. Spam transmission information

Attach to this form 10 sample spam messages, including the message's extended headers and message body. The sample spam messages may be attached on paper or in electronic format. Give each spam message an Attachment Number, and provide information about each sample spam message as requested on the template. Spam messages in addition to the 10 samples that are requested can be provided in electronic format as an attachment to the template.

The lack of copies of complete spam messages can significantly hamper the ability of a Receiving Authority to act upon a referral. The Receiving Authority can investigate and determine the identities of the sender and the initiator more easily if it has a wide sampling of messages to review.

This section solicits detailed transmission information about the spam you are attaching.

- Using the attachment numbers, for each spam message you have attached, list the IP address where the spam appears to originate. Using an IP Whois service (such as www.DNSstuff.com, Cygwin, etc) indicate the ISP (or other entity) that the IP address has been assigned to. Finally, indicate whether the ISP was contacted and if so, whether that contact resulted in additional information.

- Explain any impediments to obtaining information about the sending IP addresses, for example, if the ISP is located in another country; the ISP would not keep the request confidential; or whether the headers appeared to be forged.

- If applicable, indicate whether spam appears to be sent through an open relay or open proxy, via a zombie drone or botnet, or whether the headers appear to have been forged, and provide the basis for that determination.

9. Parties identified

Identify the parties involved in the spamming activity. For the purposes of this template, the "Sender" is the company that pays the spammer(s) to send email on its behalf, and is typically the company whose product or service is being advertised by the spam. The "Initiator" is the actual spammer who sends the spam.

- Sender(s) – list any identifying information known about the "sender," including company name, physical address, website, etc. Be sure to include the country where the sender is located. Multiple senders can be listed.

- Initiator(s) – list any identifying information known about the "sender," including name, physical address, email address, online usernames or other identities or aliases. Be sure to include the country where the initiator is located. Multiple initiators can be listed.

- Physical postal address – provide postal addresses, if any, listed in the spam.

- Company names and/or products being advertised by spam.

10. Spamvertised URLs, purchase pages, and related Whois information

The "**Spamvertised URL**" (the URL that is advertised by the spam) is the hyperlink that consumers would click if they wanted to purchase the offer being advertised by the spam. These URLs can change frequently. Many times, these URLs may redirect the consumer to a different URL where the offer or product can be purchased. The website where the offer or product can be purchased will be referred to as the "Purchase Page URL." The "Spamvertised URL" is usually a domain name registered by the "initiator" and the "**Purchase Page URL**" is usually a domain name registered to the "sender."

- In the tables, list the "Spamvertised" and "Purchase Page" URLs. In each table, codes will accompany each URL listed, where "S" will represent a Spamvertised URL and "P" will represent the Purchase Page URL. These codes will help to easily reference a particular URL throughout the template.

- List the URLs' Whois Information and any information about who paid for the domain name's registration, if that information is obtained (can require a judicial order or subpoena).

- In the "Whois Source" field, include whether the Whois information being provided was obtained from either an online Whois database (such as from www.betterwhois.com or www.whois.sc) or whether the Whois information was obtained from the Domain Name Registrar directly (such as from a subpoena).

- Provide the name and country of the Domain Name Registrar, and whether Registrar was contacted for information.

- If there are many different URLs used, provide only those with a unique domain names. Additional information related to these URLs may be attached to the Pro Forma.

- For the Spamvertised and the Purchase Page URLs, if the domain name registrar was not or could not be contacted for any reason, indicate the reason why in the text boxes provided (*i.e.* Registrar is located in another country, Registrar would not keep the request confidential, etc.). This text box can also be used for any notes about the Whois information, such as whether it appears to fake, or any other relevant information.

11. Additional Sources of Information

Provide details of any additional sources of information, which may assist with this investigation (e.g. websites, news links etc).

12. Other relevant information related to URLs used

Using the codes from the previous tables, list other information related to each URL. This would include information related to Hosting provider, where Host is located, or who provides DNS services.

13. Email addresses used by target

List the email addresses related to the spamming activity. During the course of an investigation, email addresses may be identified in places other than in the actual headers of spam messages. For example, an email address may be listed on a website or on that website's Whois information. Identification of the owners of these email addresses can help to identify the individuals behind the spam activity.

- For the "source" of the email address, identify where the email address was located (in spam, on a website (which one?), or in whois information (for which domain?).

- List whether the Email Service Provider (the "ESP") was contacted and what, if any, information was obtained from the ESP. If the email address is spammer@yahoo.com, the ESP would be Yahoo! Inc. The ESP can be contacted for additional information related to an email address. Note that free email services such as Yahoo or Hotmail may not have complete or accurate information. They do, however, record and keep for a short period of time the IP address of the computer that was used most recently to log into the email account. Using this IP address, the ISP that owns the IP address can be contacted to obtain additional information about which computer was used to log into the email account.

14. Forensic software used

Please provide a list of any forensic software that was used in the investigation (*e.g.* dd-copies, encase, etc).

15. Financial data found during the investigation

Please provide brief details of any financial data that has been gathered during the investigation or that will be needed.

16. Summary of contacts made and available evidence

Using the check list provided, indicate which third-party entities have been contacted for further information. Please provide the name of the organisation or individual, and contact details in the appropriate box. For those that were contacted, indicate whether evidence from those entities is available and whether that evidence has been attached with the template.

Notes

1 Voir également dans l'Annexe V le formulaire de soumission de plainte du LAP/EU CNSA visant à faciliter les demandes d'assistance et la soumission d'une demande d'enquête pour spam à l'autorité d'un autre participant.

2 Atelier de l'OCDE sur le spam, Bruxelles, 2-3 février 2004. Voir le document de référence, à http://www.oecd.org/document/47/0,2340,en_2649_22555297_26514927_1_1_1_1,00.html.

3 La documentation de référence a été établie par les membres du Groupe de réflexion et par le Secrétariat de l'OCDE : "Anti-Spam Regulation Report", A. Maurer, DCITA, Australia (2005); "Report on spam cross-border enforcement", J. Radish, OCDE/PIIC (2004); "Anti-SPAM Initiatives: Alliances and Self Regulation", BIAC (2005); "Anti-Spam Techniques for Incoming Mail", Direction du développement des médias (France), US Federal Trade Commission, BIAC; "Report on Education and Awareness initiatives", Mina Park, OCDE (2005); "Spam Issues in Developing Countries", S. Ramasubramanian. Ces documents sont accessibles en ligne à l'adresse : www.oecd-antispam.org

4 "World Telecommunication Indicators 2004/2005", UIT.

5 OCDE, Statistiques 2005 sur le haut débit, voir www.oecd.org/sti/telecom.

6 Lignes directrices de l'OCDE régissant la sécurité des systèmes et réseaux d'information : Vers une culture de la sécurité, voir http://www.oecd.org/dataoecd/16/22/15582260.pdf

7 On trouvera une définition de l'hameçonnage dans les paragraphes suivants.

8 L'information de l'enveloppe SMTP est définie dans : J. Klensin, "Simple Mail Transfer Protocol", IETF Network Working Group, Standards Track, avril 2001, http://www.ietf.org/rfc/rfc2821.txt, <consulté en juillet 2004>. Les autres renseignements relatifs à l'enveloppe, à l'en-tête, au corps du message et aux extensions de format MIME sont définis dans : Pete Resnick, "Internet Messsage Format", IETF Network Working Group, Standards Track , avril.

9 Le contenu de cette section est extrait de *Anti-Spam Research Group Discussion Archive – Date Index*, http://www1.ietf.org/mail-archive/web/asrg/current/maillist.html, <consulté en janvier 2005>.

10 Pour des précisions sur la GSM Association, voir http://www.gsmworld.com/index.shtml.

11 Voir par exemple "Scientists warn Skype ideal for hackers", 26 janvier 2006, : http://today.reuters.co.uk/news/newsArticle.aspx?type=internetNews&storyID=2006-01-26T193207Z_01_L2671747_RTRIDST_0_OUKIN-UK-SECURITY-INTERNET.XML

12 Le protocole d'ouverture de session (protocole SIP), mis au point par l'IETF (et accepté par le 3GPP in 2000 comme élément de l'architecture IMS), propose une norme pour l'ouverture, la modification et la fin d'une session interactive faisant intervenir des éléments multimédias tels que vidéo, téléphonie, messagerie instantanée, jeux en ligne et réalité virtuelle. C'est l'un des principaux protocoles de signalisation pour la téléphonie Internet, avec le H.323. Voir http://en.wikipedia.org/wiki/Session_Initiation_Protocol.

13 Le sous-système multimédia IP (IMS) est une architecture normalisée de réseaux de prochaine génération destinée aux opérateurs de télécommunications qui veulent fournir des services multimédias mobiles et fixes. Voir www.wikipedia.org.

14 Netcraft, enquête d'octobre 2005, voir http://news.netcraft.com.

15 Pour plus d'information, voir "The Secondary Market for Domain Names", online at http://www.oecd.org/dataoecd/14/45/36471569.pdf.

16 Pour plus d'information sur les blogs, voir les Perspectives des technologies de l'information de l'OCDE, édition 2006 (à paraître).

17 On trouvera la définition que le Ministère américain de la Justice donne du hameçonnage dans "*Special Report on Phishing*" 2004, voir http://www.usdoj.gov/criminal/fraud/Phishing.pdf (consulté pour la dernière fois le 19 octobre 2004). Voir aussi la définition de Wikipedia, à l'adresse http://en.wikipedia.org/wiki/Phishing.

18 Voir Netcraft "Phishing attacks evolved steadily through 2005", http://news.netcraft.com/archives/2005/12/29/phishing_attacks_evolved_steadily_throughout_2005.html

19 Cette pratique, qui a pour nom « *pharming* », se définit comme l'exploitation d'une vulnérabilité dans le logiciel du serveur DNS qui permet à un cyberpirate d'acquérir le nom de domaine pour un site et rediriger, par exemple, le trafic de ce site vers un autre site. Voir Wikipedia http://en.wikipedia.org/wiki/Pharming

20 Selon l'*Anti-Phishing Working Group*, la durée de vie moyenne d'un site-hameçon est de 5.3 jours.

21 Voir MessageLabs "2005 Annual Security Report", à http://www.messagelabs.com/. Voir aussi "Online Scammers go Spear-phishin'", New York Times, 4 décembre 2005. Pew Internet Report on Spam and Phishing, à http://www.pewinternet.org/PPF/r/155/report_display.asp

22 Voir le document de référence du Groupe de réflexion sur le spam de l'OCDE « Le spam dans les pays en voie de développement », consultable en ligne à www.oecd.org/sti/spam/toolkit.

23 Accessible en ligne (aux formats HTML et PDF) à http://www.oecd-antispam.org/article.php3?id_article=1

24 Le rapport sur « La réglementation anti-spam » présente une analyse plus détaillée des différents éléments inclus dans la législation contre le spam dans les pays de l'OCDE, de leur importance, et de leur impact probable. Ce document, ainsi que la présente section de la Boîte à outils, a pour but de contribuer à l'élaboration et à l'examen des stratégies réglementaires et des dispositifs de lutte anti-spam.

25 La Directive 2002/58/CE de l'Union européenne s'applique en particulier aux « automates d'appel , télécopies et courriers électroniques, y compris les messages courts (SMS) » mais exclut explicitement de son champ d'application les appels téléphoniques de personne à personne, laissant les États Membres libres de les réglementer ou non. En Australie, la loi anti-spam suit la même approche, sauf qu'elle exclut les fax, et la loi prochainement adoptée par la Nouvelle Zélande devrait faire de même. Le Japon et la Corée sont beaucoup plus attentifs au spam sur mobiles, compte tenu de la forte diffusion dans ces pays des téléphones mobiles Internet, qui servent à se connecter à l'Internet, à recevoir des courriels et à « clavarder » par messagerie instantanée (IM).

26 Un « wiki » est une application web permettant aux utilisateurs d'ajouter du contenu comme sur un forum Internet, mais dans laquelle quiconque peut aussi modifier le contenu existant. voir http://en.wikipedia.org/wiki/Wiki.

27 Dans les pays européens et en Australie par exemple, c'est l' « opt-in » (consentement explicite) qui est généralement requis, mais le consentement induit suffit en cas de relation commerciale préexistante. De plus, de nombreux pays européens adoptent l'approche « opt-in » pour les personnes physiques mais l'opt-out pour les messages adressés à des personnes morales (entreprises, etc.). Cette approche est contestée car elle laisse le champ libre aux personnes qui veulent adresser des messages commerciaux non sollicités aux adresses des entreprises, lesquelles notent que leurs adresses de courriel sont des cibles faciles pour les spammeurs. L'avantage de ce régime est que le marketing en ligne légitime de B2B n'est pas entravé.

28 Voir US National Do Not Email Registry Report, page 9, en ligne à http://www.ftc.gov/reports/dneregistry/report.pdf.

29 Voir le rapport de la FTC « Do Not Spam Registry », et le document « Effectiveness and enforcement of the CAN-SPAM Act », FTC, décembre 2005.

30 En informatique, un cheval de Troie est un programme malveillant qui possède l'apparence d'un logiciel légitime. Voir http://en.wikipedia.org/.

31 Le code pénal italien, par exemple, sanctionne des actes tels que l'accès non autorisé à des ressources informatiques protégées, la diffusion de virus, les atteintes aux systèmes et réseaux informatiques, etc. Aux États-Unis, la loi CAN-SPAM interdit la transmission de courriels commerciaux à partir d'ordinateurs protégés utilisés sans autorisation. Cette loi prohibe en outre l'utilisation d'ordinateurs protégés pour relayer ou faire suivre de tels courriels dans le but de tromper ou d'induire en erreur les destinataires ou le fournisseur d'accès Internet quant à l'origine de ces messages.

32 La législation française offre un bon exemple d'approche globale du spam et de tous les enjeux qui s'y rattachent – cybersécurité et protection des consommateurs notamment. La Loi 2004-575 pour la confiance dans l'économie numérique comprend des dispositions qui modifient en même temps le code de la consommation, la réglementation des télécoms et le code pénal, insérant des termes spécifiques pour traiter le spam, les contenus trompeurs et illégaux, la cybercriminalité, la cryptographie, etc. Avec la *Loi pour la Confiance dans l'Economie Numérique*, la France a simplifié des instruments existants, les a reliés entre eux et les a actualisés de manière cohérente et globale afin de mieux répondre aux nouveaux défis et aux évolutions technologiques encore inconnues.

33 Cette convention est entrée en vigueur en juillet 2004. Pour le moment, seuls 10 pays ont ratifié le texte, qui a par ailleurs été signé par 32 pays, notamment quelques pays non européens comme le Canada, l'Afrique du Sud, les Etats-Unis et le Japon. Voir également la Décision cadre de l'UE de 2005 sur les attaques contre les systèmes d'information : 2005/222/JHA, JOCE L.69, du 16 mars 2005.

34 Concernant des infractions caractérisées, comme l'envoi sans autorisation de courrier par l'intermédiaire d'un ordinateur protégé, la loi CAN-SPAM des États-Unis fait référence à des messages « multiples ». (CAN-SPAM Act of 2003, Section 4).

35 En Australie, la loi sur le spam de 2003, par exemple, établit que la législation est applicable à tous les messages « ayant un lien avec l'Australie », c'est à dire en provenance d'Australie, envoyés par des individus ou des organisations situées physiquement en Australie ou par des organisations dont la direction centrale et le contrôle se trouvent en Australie, etc. (Section 7, Spam Act 2003). Des dispositions similaires sont incluses dans la législation anti-spam de certains pays européens comme la Loi sur les télécommunications des Pays-Bas, qui donne à l'OPTA (autorité de régulation des télécommunications) la possibilité d'engager des poursuites contre les spammeurs basés aux Pays-Bas ou opérant depuis ce pays, ou si les produits dont il est fait la publicité sont vendus par une société basée aux Pays-Bas, etc.

36 Les actions collectives peuvent être particulièrement adaptées dans les cas où un grand nombre de clients ont chacun subi une faible perte. Elles offrent une voie de recours aux consommateurs qui, du fait de la faible valeur de leur plainte, ne souhaiteraient pas supporter individuellement la charge et le coût d'une action en justice. Voir l'Atelier de l'OCDE sur le règlement des litiges avec les consommateurs et la réparation sur le marché mondial, Rapport de référence, avril 2005. En ligne à www.oecd.org/sti/consumer-policy .

37 Par exemple, en Australie, ces codes professionnels peuvent être enregistrés auprès de l'autorité nationale des télécommunications (l'ACA). Cet enregistrement permet à l'ACA d'exiger d'un acteur du secteur qu'il se conforme au code et d'appliquer ses dispositions par la contrainte si l'association professionnelle ne le fait pas.

38 Voir la loi sur les télécommunications (Telecommunication Act) australienne de 1997 (amendée), sections 112 et 113.

39. Voir le rapport sur l'application des lois anti-spam (www.oecd-antispam.org), qui analyse la situation actuelle et présente une série de recommandations destinées à améliorer les activités de répression transnationale.

40 S'agissant de l'état de mise en oeuvre de la directive, voir le site de la CE à l'adresse suivante : http://europa.eu.int/information_society/topics/ecomm/doc/all_about/implementation_enforcement/annualreports/10threport/sec20041535VOL1fr.pdf.

41 La loi Spam Act de 2003 est consultable en ligne à l'adresse : http://scaleplus.law.gov.au/html/pasteact/3/3628/top.htm.

42 États-Unis: "Controlling the Assault of Non-Solicited Pornography and Marketing Act"- 117 Stat. 2699 Public Law 108- 187- 16 décembre 2003, voir : http://frwebgate.access.gpo.gov/cgi-bin/useftp.cgi?IPaddress=162.140.64.88&filename=publ187.108&directory=/diskb/wais/data/108_cong_public_laws. République de Corée: "Act on Promotion of Information and Communication and Communications Network Utilization and Information Protection" (2001) et la loi révisée de 2002, voir : http://www.spamcop.or.kr/eng/m_2.html.

43 Voir M. Geist "Untouchable?: A Canadian perspective on the anti-spam battle", http://www.michaelgeist.ca/geistspam.pdf.

44 Document de travail "Legislating against spam", IT & Telecommunications Policy Group, Ministry of Economic Development, New Zealand. Voir http://www.politechbot.com/docs/new.zealand.spam.051804.pdf.

45 Le projet de loi du gouvernement a été annoncé le 24 février 2004. Voir : http://www.med.govt.nz/pbt/infotech/spam/index.html.

46 Voir « OCDE : Tableau des poursuites engagées », annexe B du rapport sur l'application des lois anti-spam ; voir www.oecd-antispam.org.

47 Selon la loi australienne sur le spam (Spam Act), pour déterminer la sanction appropriée, le tribunal doit prendre en compte toutes les questions pertinentes, à savoir la nature et l'ampleur de l'infraction et de toute perte ou de tout préjudice en découlant, ainsi que les circonstances dans lesquelles l'infraction a été commise et le fait qu'il ait déjà été établi ou non, au cours d'une procédure engagée en vertu de cette loi, que la personne a déjà mené une activité similaire. Voir Spam Act 2003, article 24, http://scaleplus.law.gov.au/html/pasteact/3/3628/top.htm.

48 La prudence est toutefois de rigueur lorsqu'il s'agit d'un régime en vertu duquel une sanction peut être infligée pour chaque infraction, sachant qu'un seul spammeur peut expédier des millions de messages en une seule journée, ce qui donnerait lieu à des sanctions d'une ampleur irréaliste.

49 *Conférence administrative des postes et télécommunications des pays d'expression française (CAPTEF), Réseau francophone de la régulation des télécommunications (FRATEL) et Institut francophone des nouvelles technologies de l'information et de la formation (INTIF).*

50 Ressources de la Commission européenne relatives au spam : http://europa.eu.int/information_society/policy/ecomm/todays_framework/privacy_protection/spam/index_en.htm

51 Le formulaire et la notice explicative ont été adoptés par le LAP pour servir d'instrument de signalement en février 2006.

52 Le texte de la Recommandation est reproduit dans l'Annexe 1 : « Recommandation du Conseil de l'OCDE sur la coopération transfrontière dans l'application des législations contre le spam ».

53 Pour faciliter la coopération, l'OCDE a établi une liste de correspondants des organismes d'application, qui est en voie d'être élargie aux économies non membres.

54 Un « contrat rose » est un contrat en vertu duquel le spammeur s'engage à payer un montant forfaitaire pour le volume de pourriels qu'il expédie via les serveurs de messagerie du FAI, ce dernier s'engageant de son côté à permettre ce type d'envoi. Il semble que l'expression vienne de la couleur de la viande que contient la fameuse conserve dont les pourriels tirent leur nom (le « spam »).

55 Voir « Email submission between independant networks », à http://www.ietf.org/internet-drafts/draft-hutzler-spamops-04.txt

56 Voir http://www.google.com/url?sa=U&start=3&q=http://docs.yahoo.com/docs/pr/pdf/asta_soi.pdf&e=9797 ou http://postmaster.info.aol.com/asta/ ou http://www.microsoft.com/presspass/press/2004/jun04/06-22ASTAPR.asp.

57 Le terme botnet désigne un groupe de robots logiciels (« bots ») qui sont autonomes. La personne ou l'entité à l'origine d'un botnet peut contrôler le groupe à distance, habituellement par des moyens comme l'IRC et à des fins malveillantes. Un botnet peut être composé d'un ensemble d'ordinateurs piratés exécutant des programmes (en général appelés « vers », « chevaux de Troie » ou « trappes ») pilotés par une même infrastructure de commande. Les botnets sont souvent utilisés par les spammeurs pour envoyer leurs courriels.

58 Voir également les Lignes directrices de l'OCDE régissant la sécurité des systèmes et réseaux d'information : Vers une culture de la sécurité, OCDE 2002, accessible en ligne à : http://www.oecd.org/document/42/0,2340,en_2649_34255_15582250_1_1_1_1,00.html. "Three ways phishers are hooking you", 24 mai 2005, consultable à : http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci1090307,00.html. C'est également l'opinion exprimée par S. Ramabrasubramanian, dans le rapport de l'OCDE sur les problèmes de spam dans les pays en développement.

59 Voir, par exemple, la politique anti-spam de Microsoft à : http://privacy.msn.com/anti-spam/, les conditions d'utilisation de Yahoo à : http://docs.yahoo.com/info/terms/ , Tiscali (en Italien) à : http://abbonati.tiscali.it/pop-up/internet-gratis/condizioni_contrattuali.html, l'Association française des fournisseurs d'accès à Internet et de services en ligne (AFA) : http://www.afa-france.com/déontologie.html

60 Voir le code de conduite du MAAWG, à : http://www.maawg.org/about/CodeofConduct.pdf

61 Voir http://www.spamdailynews.com/publish/index.asp.

62 FTC Opération Spam Zombies, http://news.zdnet.com/2100-1009_22-5716576.html.

63 "Freinons le pourriel: Créer un Internet plus fort et plus sécuritaire", rapport du Groupe de travail canadien sur le pourriel, accessible à http://e-com.ic.gc.ca/epic/internet/inecic-ceac.nsf/fr/h_gv00317e.html

64 http://www.maawg.org/port25.

65 Voir "Best Practices for Businesses to Avoid Being Phished", élaborées par *l'Anti-Phishing Working Group, the Mail Anti-Abuse Working Group, et le US Homeland Security Identity Theft Technology Consortium*, novembre 2005, à https://antiphishing.kavi.com/events/2005_11_fallconferencenotes/20051108_BestPracticesWorkingDoc.pdf. Voir aussi R. Rasmussen, "Phishing Prevention: Making Yourself a Hard Target", et "Online Identity Theft: Phishing Technology, Chokepoints and Countermeasures" à www.antiphishing.org/Phishing-dhs-report.pdf

66 Voir le site Web d'EuroISPA : http://www.euroispa.org/.

67 Voir l'exposé de M. Rotert lors de la réunion du Groupe de réflexion de l'OCDE, http://www.oecd.org/dataoecd/52/5/34594094.pdf

68 Voir http://www.antiphishing.org.

69 Voir le site web de la *Direct Marketing* Association : http://www.the-dma.org/.

70 Voir le communiqué de presse "Vodafone K.K. adopts anti-spam measure for SMS", accessible à http://www.vodafone.com/assets/files/en/E-NoticeAnti-spamSMS.pdf

71 MMA Code for responsible mobile marketing: A code of conduct and guidelines to best practice. Voir http://www.mmaglobal.co.uk/imgs/MMA-Code-of-Conduct_Dec03.pdf

72 Pour plus de renseignements sur la MMA, voir : www.mmaglobal.com.

73 L'Association GSM, http://www.gsmworld.com/using/public_policy/mobile_content.shtml; le code de conduite du Royaume-Uni pour l'autorégulation des nouvelles formes de contenus sur les services mobiles, en ligne à : www.imcb.org.uk/assets/documents/10000109Codeofpractice.pdf, et « Insights on Mobile Spam », en ligne à : http://www.mobilespam.org/ . Voir aussi la politique spam de Vodafone à : http://www.vodafone.com/section_article/0,3035,CATEGORY_ID%253D30407%2526LANGUAGE_ID%253D0%2526CONTENT8ID%253D265596,00.html

74 Cette section est le fruit d'une étude préliminaire réalisée par le Groupe de contact anti-spam français, à laquelle ont participé différents acteurs, notamment des experts de l'Internet et des représentants de la société civile. L'étude a été ensuite enrichie grâce aux contributions du BIAC et des Etats-Unis, avant d'être soumise comme contribution au Groupe de réflexion.

75 Cette section présente un éventail de technologies classées par type ou par catégorie ; si une application spécifique est mise en valeur au sein d'une catégorie donnée, ce n'est pas pour indiquer une préférence mais simplement à titre d'illustration. De plus, compte tenu de l'évolution rapide des technologies, cette section doit être vue comme un simple aperçu des mesures techniques disponibles au moment de sa préparation (deuxième trimestre 2005).

76 Courriel qui se revendique d'une personne qui en réalité n'y est pour rien.

77 La présente section s'inspire du document de référence intitulé "Education and Awareness Raising", Mina Park, OCDE (2005).

78 Le coût marginal de l'envoi d'un courriel pour le spammeur est extrêmement faible, un taux de réponse de seulement 0,025 % ou moins suffit pour permettre au spammeur de tirer un profit de son investissement.

79 Une étude réalisée par le Pew Internet & American Life Project en mars 2004 indique que 9 % des destinataires disent avoir répondu à un courrier électronique dont ils ont découvert par la suite qu'il était frauduleux, 3 % avoir communiqué des données personnelles en réponse à un courrier électronique non sollicité et 5 % des utilisateurs ont commandé un produit ou un service en réponse à un courrier électronique non sollicité. Le IPSOS Trend Report Canada pour mai-juin 2004 indiquait que plus d'un tiers des Canadiens en ligne ouvraient leurs courriels par curiosité.

80 En ligne à l'adresse suivante http://stopspamhere.ca/.

81 En ligne à l'adresse suivante http://www.iia.net.au/spamvt.html.

82 Programme Safer Internet en ligne à l'adresse suivante http://www.safer-internet.net/.

83 Par exemple, la Federal Trade Commission des Etats-Unis a créé une « carte électronique » qui donne aux utilisateurs des conseils sur la façon de se prémunir contre les fraudes par hameçonnage. Cette carte est disponible en ligne à l'adresse : http://www.ftc.gov/bcp/conline/ecards/phishing/index.html.

84 Tiré des Lignes directrices anti-spam de l'OCDE destinées aux agents.

85 En ligne à l'adresse suivante http://www.iia.net.au/.

86 De plus amples informations sur le Groupe de travail canadien sur le pourriel sont disponibles en ligne à l'adresse suivante: http://e-com.ic.gc.ca/epic/internet/inecic-ceac.nsf/en/h_gv00248e.html.

87 Signal-spam, http://www.signal-spam.fr.

88 Voir *Direction du Développement des médias* : http://www.ddm.gouv.fr/rubrique.php3?id_rubrique=63.

89 SpotSpam a reçu le soutien de la Commission dans sa Communication 2004/28.

90 En ligne à l'adresse suivante http://www.londonactionplan.org/.

91 « Operation spam zombies », voir le communiqué de presse de la FTC sur http://www.ftc.gov/opa/2005/05/zombies.htm/.

92 Voir DDSI "Roadmap: public-private partnerships", novembre 2002, en ligne sur www.ddsi.org/Documents/final%20docs/DDSI_D3_PPP_Roadmap_f.pdf.

93 Cet élément est étroitement lié aux autres éléments de la Boîte à outils, par exemple les solutions techniques et les initiatives pilotées par l'industrie.

94 Sur la question de l'inexactitude des informations sur les contacts concernant les noms de domaines enregistrés, voir US GAO « Internet Management : Prevalence of False contact Information for Registered Domain Names », en ligne sur http://www.gao.gov/docsearch/abstract.php?rptno=GAO-06-165.

95 MessageLabs Security Report 2005. En ligne à l'adresse suivante www.messagelabs.com.

96 Pew Internet and American Life Project: http://www.pewinternet.org/PPF/r/155/report_display.asp.

97 VeriSign Internet Security Intelligence Briefing, nov 204, v.2, Issue 2, p. 5-6, disponible à l'adresse http://www.verisign.com/static/017574.pdf

98 Les chiffres sont fondés sur le nombre de boîtes à lettres de chaque FAI participant. Dans le cas où seul le nombre d'abonnés est communiqué, on estime qu'il y a 1,5 boîte à lettres par abonné.

99 Si de nouveaux participants se joignent au programme, il leur sera demandé de fournir des données à partir d'octobre 2005, pour assurer la cohérence des chiffres.

100 Voir le document de référence « Spam issues in developing countries » disponible sur le site www.oecd-antispam.org

LES ÉDITIONS DE L'OCDE, 2, rue André-Pascal, 75775 PARIS CEDEX 16
IMPRIMÉ EN FRANCE
(93 2006 06 2 P) ISBN 92-64-02718-1 – n° 55246 2006

Boîte à outils anti-spam de l'OCDE
POLITIQUES ET MESURES RECOMMANDÉES

Compte tenu du vaste impact du spam, et des risques de nouveaux problèmes liés à l'émergence des communications universelles et de l'Internet mobile, l'OCDE a réuni des décideurs et des professionnels pour former le Groupe de réflexion de l'OCDE sur le spam. Ce Groupe a été chargé d'élaborer un cadre pour lutter contre le spam en s'appuyant sur un large éventail de solutions pluridisciplinaires.

Le Groupe de réflexion a élaboré la « Boîte à outils anti-spam » qui recommande un ensemble de politiques et de mesures qui devraient constituer les éléments clés d'un cadre global d'action publique pour s'attaquer au problème du spam.

www.oecd.org/sti/spam

OCDE

ÉDITIONSOCDE

ISBN 92-64-02718-1
93 2006 06 2 P

9 789264 027183