

Non classifié

DSTI/CP/ICCP/SPAM(2004)3/FINAL



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

30-Aug-2005

Français - Or. Anglais

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

Groupe de réflexion sur le spam

RAPPORT SUR L'APPLICATION DES LOIS ANTISPAM

JT00188581

Document complet disponible sur OLIS dans son format d'origine
Complete document available on OLIS in its original format

**DSTI/CP/ICCP/SPAM(2004)3/FINAL
Non classifié**

Français - Or. Anglais

AVANT-PROPOS

Le Groupe de réflexion sur le spam a examiné le présent document lors de sa réunion tenue en mars 2005 et a recommandé sa déclassification au Comité de la politique à l'égard des consommateurs et au Comité de la politique de l'information, de l'informatique et des communications (PIIC). La procédure écrite correspondante a été achevée le 23 avril 2005.

Le rapport, préparé par Jack Radisch, du Secrétariat de l'OCDE, est publié sous la responsabilité du Secrétaire général de l'OCDE.

© OCDE 2005.

Les demandes de reproduction ou de traduction de tout ou partie du présent document doivent être adressées au :

Chef du Service des publications, OCDE, 2, rue André-Pascal, 75775 Paris Cedex 16, France.

TABLE DES MATIÈRES

RAPPORT SUR L'APPLICATION DES LOIS ANTISPAM	4
Principaux points.....	4
INTRODUCTION	6
I. Le questionnaire de l'OCDE sur l'application transfrontière des lois antispam	7
II. Types d'organismes publics chargés de faire respecter les lois relatives au spam.....	8
III. Cadres nationaux d'application des lois	14
IV. Obstacles à une application transfrontière efficace	22
V. Efforts en cours pour surmonter les obstacles à la collecte et au partage d'informations.....	28
VI. Conclusions	34
ANNEXE A QUESTIONNAIRE DE L'OCDE SUR L'APPLICATION TRANSFRONTIÈRE DES LOIS ANTISPAM	37
Instructions	37
Section I : Description du cadre national d'application des lois	38
Section II : Aspects transfrontières de l'application des lois antispam.....	39
ANNEXE B OCDE : TABLEAU DES POURSUITES ENGAGÉES	40

RAPPORT SUR L'APPLICATION DES LOIS ANTISPAM

Principaux points

Le présent rapport est une synthèse instantanée des réponses transmises par les pays membres de l'OCDE concernant la nature et l'ampleur des pouvoirs dont disposent les organismes publics ou financés par des fonds publics chargés de veiller au respect des lois utilisées pour lutter contre les spammeurs (ou polluposteurs). Il est destiné à fournir une base de discussion permettant de déterminer les moyens d'améliorer la capacité des organismes d'application de répondre aux plaintes relatives au spam (ou pollupostage) et de coopérer avec leurs homologues étrangers.

Types d'organismes publics chargés de faire respecter les lois relatives au spam

Les réponses montrent la multiplicité des organismes d'application exerçant un rôle dans le domaine du spam, dont la collaboration reste à peaufiner. Dans les pays dotés d'une législation antispam spécifique comme dans ceux qui n'en ont pas, les autorités compétentes comprennent des organismes de protection des consommateurs, des organismes de protection des données, des organismes de régulation des communications et des autorités pénales. Le rapport fournit des informations générales sur les missions de chaque type d'organisme, ainsi que des explications plus détaillées concernant leurs pouvoirs. Des tableaux présentent également pour chaque pays les différents organismes responsables dans le domaine du spam.

Cadres nationaux d'application des lois

Les réponses font apparaître que les organismes chargés des questions relatives au spam ont des pouvoirs variés en vertu desquels ils réalisent des enquêtes, prennent des mesures d'exécution et obtiennent des sanctions. Le présent rapport fournit des informations concernant les différentes procédures d'exécution dont disposent ces organismes, et sur leurs diverses pratiques en matière de traitement des plaintes, de collecte de preuves, d'établissement des priorités, ainsi que d'amendes, de sanctions et de recours disponibles. Dans l'ensemble, des actions peuvent être engagées dans les cadres administratif, civil ou pénal. Une fois qu'une procédure est entamée, les sanctions et recours applicables sont les suivants : les lettres d'avertissement, les injonctions, les peines de prison, les amendes, les réparations financières et la révocation d'une licence d'exploitation.

Obstacles à une application transfrontière efficace

A partir des réponses reçues et de travaux de recherche indépendants, le rapport souligne les principaux problèmes auxquels se heurtent les organismes d'application lorsqu'ils souhaitent coopérer avec leurs homologues étrangers pour prendre des mesures contre les spammeurs. Il montre que les outils dont disposent les organismes d'application ne sont pas toujours appropriés pour permettre une coopération efficace, et il fournit une liste non exhaustive des obstacles rencontrés, à savoir :

- Les restrictions de l'étendue des pouvoirs de l'organisme d'application.
- Les limitations pesant sur la collecte et le partage d'informations.

- La force exécutoire limitée des décisions au niveau international.
- Les différentes priorités d'exécution parmi les organismes d'application.

Le rapport comprend également des exemples de types de plaintes relatives au spam qui sont prioritaires pour une application transfrontière des lois.

Efforts en cours pour surmonter les obstacles à la collecte et au partage d'informations

Le rapport montre que plusieurs initiatives ont été prises pour surmonter les obstacles à l'application des dispositions antisipam au niveau international, et il fournit des informations concernant des protocoles d'accord multilatéraux ou bilatéraux portant spécifiquement sur la lutte contre le spam, des accords internationaux dans des domaines d'action connexes, des mesures adoptées par d'autres organisations internationales, et des efforts déployés par le secteur privé. Des organismes de plusieurs pays ont conclu des protocoles d'accord avec des homologues étrangers en vue d'améliorer la coopération. En Europe, la récente « procédure de coopération relative à la transmission d'informations et renseignements sur les plaintes » a été approuvée par 16 organismes d'application de la législation antisipam dans 13 pays membres. Dans un cadre plus multilatéral, 27 organismes et 12 professionnels du secteur ont signé le Plan d'action de Londres, une initiative visant à tout mettre en œuvre pour favoriser la coopération internationale dans la lutte contre le spam. D'autres initiatives internationales pertinentes dans des domaines étroitement liés, telles que les Lignes directrices de l'OCDE régissant la protection des consommateurs contre les pratiques commerciales transfrontières frauduleuses et trompeuses ou la Convention du Conseil de l'Europe sur la cybercriminalité sont aussi mentionnées. Le rapport souligne enfin que le secteur privé peut également jouer un rôle essentiel en matière d'aide aux organismes publics responsables de l'application des législations antisipam, notamment en fournissant une assistance technique et les preuves nécessaires pour identifier les spammeurs.

Conclusions

Tout en constatant les progrès réalisés jusqu'à présent, le rapport conclut que des étapes importantes doivent encore être franchies pour renforcer l'efficacité des efforts nationaux et internationaux de lutte contre le spam. Pour étayer le débat sur des travaux complémentaires de l'OCDE en vue de faciliter la coopération en matière d'application de la législation antisipam, les conclusions mettent en évidence des aspects de la situation actuelle que les autorités pourraient examiner et traiter.

INTRODUCTION

Le présent rapport a pour objectif d'analyser la nature et l'ampleur des pouvoirs dont disposent les organismes publics ou financés par des fonds publics chargés de faire respecter les lois utilisées pour sanctionner les spammeurs. Il est destiné à servir de base de discussion pour le Groupe de réflexion de l'OCDE sur le spam afin de déterminer les moyens d'améliorer la capacité des organismes d'application de répondre aux plaintes relatives au pollupostage et de coopérer avec leurs homologues étrangers. Il présente également des exemples de mise en œuvre réussie de mécanismes d'application nationaux et internationaux (voir le tableau des poursuites engagées, annexe B). Les projets entrepris par des organismes d'application en vue d'améliorer les solutions techniques permettant de lutter contre le spam (telles que la sécurisation des serveurs ou l'authentification des courriers électroniques) ne sont pas examinés dans ce rapport. Les informations concernant les initiatives du secteur privé destinées à combattre le pollupostage par des moyens techniques et des actions en justice ne rentrent pas non plus dans le cadre de ce rapport.

Les décideurs reconnaissent à l'unisson que le spam nuit à l'économie numérique et que l'application des lois joue un rôle important dans la stratégie pluridimensionnelle destinée à lutter contre cette pratique. Dix-neuf pays membres de l'OCDE ont soit promulgué des législations spécifiques soit modifié les législations existantes pour réglementer et sanctionner le spam, et des législations en la matière sont en préparation dans trois autres pays membres. En outre, cinq pays membres utilisent les règles et principes juridiques présents dans la législation existante pour s'attaquer à toute la gamme de pratiques abusives perpétrées au moyen des technologies des communications électroniques telles que le courrier électronique, les SMS (service de messages courts), la messagerie instantanée, les télécopies et la téléphonie sur Internet (VoIP). L'ensemble de ces législations constitue le corpus de la réglementation antispam.

Une application efficace de la législation antispam sert de désincitation économique pour les spammeurs dont les bénéfices sont entamés par les amendes et les sanctions imposées : elle fournit aux victimes de fraudes à la consommation liées au spam un mécanisme de protection et de recours sous la responsabilité de l'État, et défend les droits en matière de préservation de la vie privée des destinataires de spam. En outre, une mise en lumière du renforcement de l'application de la législation en la matière pourrait contribuer à restaurer la confiance dans les systèmes de courrier électronique qui a été ébranlée par le pollupostage.

Toutefois, les organismes chargés de faire respecter la loi se heurtent à d'importants obstacles dans l'accomplissement de leurs fonctions, en raison des difficultés et des dépenses liées au dépistage des spammeurs, à la collecte de preuves suffisantes pour engager des poursuites et au recouvrement des indemnités pour les victimes.

Les polluposteurs par courriels peuvent facilement dissimuler leurs véritables identité et localisation en falsifiant les informations qui figurent dans l'en-tête du message, en acheminant les courriels par l'intermédiaire de serveurs mandataires et de serveurs relais ouverts, en se servant de programmes zombies ou de connexions Internet impossibles à retracer. Même lorsqu'un suspect peut être identifié, il convient de faire la preuve de sa responsabilité dans l'envoi des messages électroniques. Une récente affaire jugée aux Pays-Bas montre que la simple possession d'ordinateurs et de logiciels utilisés dans le cadre de pollupostage n'est pas considérée dans toutes les juridictions comme une preuve de la participation à

l'envoi répréhensible de spam. En Australie, en revanche, l'inférence valide découle du fait de tirer un avantage financier du spam, indépendamment de la question de savoir si la personne concernée a envoyé le message ou a favorisé sa transmission. Une fois le suspect identifié et reconnu comme étant l'expéditeur du spam, il reste encore à récupérer les sommes versées par les victimes de fraudes portant sur des biens ou des services. Même si ces sommes peuvent être déterminées et localisées, les organismes chargés de l'application des lois n'ont pas toujours les moyens nécessaires pour les recouvrer si elles se trouvent dans un pays étranger.

De nos jours, les spammeurs envoient des milliards de courriels à destination d'adresses électroniques et de téléphones mobiles dans le monde entier, sans s'interroger sur la capacité du marché ou l'aptitude des destinataires à comprendre la langue dans laquelle le message est rédigé, et en se souciant encore moins des incidences des envois massifs sur les opérateurs de réseaux. Par ailleurs, dans la plupart des pays membres de l'OCDE, les spam reçus proviennent davantage de sources étrangères que de sources nationales. Les enquêtes sur les spammeurs aux fins de l'application des lois ont permis de découvrir d'autres aspects internationaux de leur mode de fonctionnement. Par exemple, les entreprises qui commercialisent des produits frauduleux grâce au spam sont généralement inscrites à des registres relevant de juridictions étrangères, et leurs bénéficiaires sont souvent transférés sur des comptes à l'étranger où leurs actifs sont détenus en trust et échappent donc à tout recouvrement en vertu d'éventuels jugements d'exécution de paiement. Le spam est manifestement un problème international, et seules des mesures d'application des lois tenant compte de ses aspects transfrontières fourniront les instruments juridiques nécessaires pour y mettre un terme au niveau international.

Le fait que les spammeurs s'efforcent de dissimuler leurs identités et placent leurs actifs à l'étranger montre qu'ils sont conscients des difficultés d'exécution transfrontière des mesures d'application. Les organismes d'application doivent surmonter de nombreux obstacles à une application transfrontière, concernant la non-extraterritorialité de la législation nationale sur le spam, le traçage de l'identité du spammeur, la collecte et le partage d'informations provenant d'organismes d'application étrangers et la saisie effective d'avoirs déposés dans une banque étrangère. En conséquence, les organismes d'application nationaux — notamment ceux de pays qui ne sont pas habituellement producteurs de spam — ont intérêt à coopérer au niveau international s'ils veulent obliger les spammeurs à rendre compte de leurs activités.

I. Le questionnaire de l'OCDE sur l'application transfrontière des lois antis spam

Le Plan de travail révisé de l'OCDE sur le spam pour 2004-2006 prévoit la réalisation d'une enquête sur les possibilités d'amélioration de la coopération transfrontière en matière d'application de la législation antis spam. En particulier, le plan de travail propose de se baser sur l'étude des législations antis spam (réalisée avant l'atelier de l'OCDE sur le spam organisé à Bruxelles en février 2004), qui a porté essentiellement sur la question de savoir si les pays membres ont adopté une législation antis spam et, si tel est le cas, s'ils ont choisi le système de consentement préalable explicite (*opt-in*) ou celui de liste de refus (*opt-out*). A cet effet, un questionnaire a été diffusé en juillet 2004 (voir annexe A) pour obtenir des informations en vue de : repérer les organismes publics responsables de l'application des législations antis spam, analyser leurs pouvoirs et leurs procédures pour recevoir les plaintes, mener des enquêtes et prendre des mesures contre les spammeurs, et déterminer les principales difficultés faisant obstacle à la coopération transfrontière. Vingt-huit réponses au questionnaire ont été reçues de la part des pays membres de l'OCDE suivants : Allemagne, Australie, Autriche, Belgique, Canada, Corée, Danemark, Espagne, États-Unis, Finlande, France, Grèce, Hongrie, Irlande, Italie, Japon, Mexique, Norvège, Nouvelle-Zélande, Pays-Bas, Pologne, Portugal, République tchèque, Royaume-Uni, Slovaquie, Suède, Suisse et Turquie. A l'occasion d'une réunion des organismes d'application tenue à Londres le 11 octobre 2004, Chypre et le Pérou, deux pays non membres, ont transmis leurs réponses au questionnaire.

Dans plusieurs pays, une législation antispam spécifique accorde expressément à certaines entités privées le droit d'entamer des poursuites civiles en dommages-intérêts contre les spammeurs. De fait, les principaux fournisseurs d'accès à Internet (FAI) qui gèrent des services de comptes de courrier électronique ont mis en œuvre une stratégie coordonnée pour engager des poursuites civiles à l'égard des polluposteurs les plus prolifiques. Les contentieux privés ont joué un rôle dans l'efficacité globale de la législation antispam en rendant le modèle économique des spammeurs moins rentable. Les travaux réalisés au sein de l'OCDE se concentrent toutefois sur les activités des organismes publics ou financés par des fonds publics, responsables de l'application des dispositions antispam au niveau national.

Pour recueillir des informations concernant chaque phase d'une mesure d'exécution, le questionnaire a porté sur les pouvoirs et les limites de tout organisme disposant d'un « rôle d'application ». Le rôle d'application s'entend ici comme englobant l'une quelconque des trois fonctions suivantes : réception des plaintes, réalisation d'enquêtes ou engagement de poursuites devant une cour ou un tribunal. Même si certains organismes ne sont pas habilités à obtenir des sanctions ou former des recours contre les spammeurs, ils peuvent néanmoins jouer un rôle important dans le cadre de la coopération internationale en ce qui concerne la réception des plaintes ou la collecte et le partage d'informations. Les destinataires des questionnaires ont été encouragés à consulter le secteur privé et certaines autres organisations non gouvernementales actives en matière d'application des dispositions antispam, et il leur a été demandé de signaler les obstacles au partage d'informations à des fins d'enquête.

Le rapport présente une synthèse des pouvoirs et pratiques des organismes d'application des lois, tels qu'ils ressortent des réponses au questionnaire. Tous les organismes remplissant un rôle d'application en matière de spam n'ont pas été mentionnés dans les réponses au questionnaire. Les membres du Groupe de réflexion sont invités à transmettre des informations afin de compléter les réponses fournies par leur pays, qui sont affichées sur le site du Groupe de discussion électronique de l'OCDE consacré au spam.

II. Types d'organismes publics chargés de faire respecter les lois relatives au spam

Il ressort des réponses au questionnaire que les principaux types d'organismes publics responsables de l'application des législations antispam sont les suivants : organismes de protection des consommateurs (19) ; organismes de protection des données (18) ; organismes de régulation des communications (12) ; unités de police chargées de la lutte contre la cybercriminalité ou services de poursuites pénales (9) ; et divers autres organismes (4) (les tableaux 1, 2 et 3 ci-après regroupent les différents organismes de chaque pays). Les 29 pays qui ont répondu au questionnaire ont donc désigné 62 organismes d'application. Dans les pays qui ne disposent pas d'une législation antispam spécifique, plusieurs organismes sont chargés de l'application des différentes mesures dont relèvent les actions réalisées par polluspostage. Ainsi, au Canada, le Bureau de la concurrence est habilité à engager des poursuites contre des spammeurs si des arguments commerciaux figurant dans un courrier électronique sont faux ou trompeurs, tandis que le Commissariat à la protection de la vie privée peut prendre des mesures lorsque des renseignements personnels, par exemple une adresse électronique, sont utilisés sans le consentement de la personne concernée.

La pluralité des organismes d'application responsables dans le domaine du spam s'explique par plusieurs raisons. La compétence peut être partagée au niveau territorial entre des bureaux régionaux de même type (par exemple, bureaux régionaux du *Fernmeldbüro*, une autorité chargée des télécommunications en Autriche). Toutefois, la principale raison tient au fait que les diverses pratiques abusives commises au moyen des communications électroniques peuvent enfreindre les protections prévues en vertu de plusieurs législations, dont chacune attribue une compétence à un organisme différent. Les spammeurs peuvent en effet commettre des infractions concernant :

- **La législation sur la protection des consommateurs**, en incitant de manière trompeuse les destinataires à acheter des marchandises sans valeur ou en les attirant dans différents types d'escroqueries et de fraudes (ce qui peut également aboutir à des infractions au droit pénal – voir ci-dessous).
- **Le droit pénal**, lorsque les courriels sont utilisés pour envoyer des virus ou de grandes quantités de messages électroniques vers un même compte de courrier électronique en restreignant ou perturbant la capacité du destinataire de s'en servir, ou en cas de comportement frauduleux, s'il correspond à une infraction au droit pénal (pêche aux données personnelles, par exemple).
- **La législation sur la protection des données**, lorsque les spammeurs envoient des courriels commerciaux non sollicités à des fins de marketing, sans le consentement préalable du destinataire, c'est-à-dire en utilisant des renseignements personnels (adresses électroniques) sans l'autorisation de la personne concernée.
- **La législation sur les télécommunications et la protection des données**, lorsque les courriels contiennent de fausses adresses de retour et des mentions d'objet trompeuses ou omettent de proposer une option de refus ou de la respecter quand elle est exercée.

Même lorsqu'une législation antispam spécifique a été promulguée, les compétences sont réparties entre plus d'un organisme d'application dans tous les pays sauf sept (Chypre, Danemark, Espagne, Irlande, Pérou, République tchèque et Suède). Néanmoins, bien que différents organismes puissent être responsables en matière de spam dans un même pays, dans plusieurs cas, une autorité spécifique joue le rôle de chef de file, et consacre davantage d'efforts et de ressources à la lutte contre les spammeurs. Cet organisme chef de file est important au niveau tant national qu'international, car il sert de point de contact et prend part aux forums internationaux. C'est le cas, par exemple, de la Commission fédérale du commerce (FTC, organisme de protection des consommateurs) aux États-Unis, qui a une plus grande responsabilité en la matière que la Commission fédérale des communications (FCC), chargée principalement du spam mobile, ou de la Commission nationale de l'informatique et des libertés (CNIL, s'occupant notamment de la protection des données), très active dans le secteur en France, alors que ça n'est pas le thème sur lequel l'autre autorité concernée, la Direction générale de la concurrence, de la consommation et de la répression des fraudes (DGCCRF), organisme de protection des consommateurs, fait porter l'essentiel de ses travaux.

En Australie, par exemple, l'Autorité australienne des communications (ACA) veille au respect de la loi sur le spam (*Spam Act*), et peut enquêter sur une plainte en matière de pollupostage. Cependant, lorsque les messages relevant de cette pratique ont un contenu qui est lui-même interdit, l'expéditeur peut également faire l'objet de poursuites pénales ou civiles. En règle générale, l'ACA signale les pourriels à l'instance d'exécution pénale ou civile compétente et collabore à toute enquête menée à ce sujet. Si le pourriel contient des éléments trompeurs ou fallacieux, la Commission australienne de la concurrence et de la consommation (ACCC) intervient, en appliquant la loi sur les pratiques commerciales (*Trade Practices Act*), qui contient des dispositions civiles et pénales. Les infractions particulièrement graves, par exemple des messages se rapportant à la pornographie infantile, comprenant des contenus frauduleux ou constituant des actes de criminalité informatique, relèvent directement de la responsabilité du Centre australien de lutte contre la criminalité technologique (AHTCC), service de la police fédérale australienne, tandis que les affaires concernant les marchés financiers sont également suivies par la Commission australienne des valeurs mobilières et des investissements (ASIC). Lorsqu'il est fait référence à un site Web dans un pourriel, c'est l'Autorité australienne de radiodiffusion (ABA) qui est compétente pour exiger des fournisseurs d'accès à Internet (FAI) qu'ils ferment les sites Web correspondant au contenu illégal ou offensant diffusé dans le pourriel (notamment éléments pornographiques illégaux).

Organismes de protection des consommateurs

Il ressort des réponses aux questionnaires que 19¹ organismes de protection des consommateurs jouent un rôle en ce qui concerne l'application de législations antispam spécifiques ou d'autres législations susceptibles d'être utilisées contre les polluposteurs (voir le tableau 1). En général, les responsabilités de ce type d'organisme portent notamment sur la prise de mesures contre les fournisseurs de biens ou de services trompeurs ou frauduleux. Les organismes de protection des consommateurs engagent communément des actions contre les spammeurs qui envoient des courriers électroniques contenant des publicités trompeuses ou frauduleuses, ou sont liés à un site Web par l'intermédiaire duquel une escroquerie commerciale est réalisée. Du point de vue de l'action des pouvoirs publics, ces activités sont jugées particulièrement insupportables car elles sapent la confiance des usagers dans les services en ligne.

Les réponses au questionnaire montrent que presque tous les organismes de protection des consommateurs ont le pouvoir d'obliger toute entité qui fait l'objet d'une enquête à fournir les renseignements nécessaires à la bonne marche des investigations. Ils disposent de plusieurs pouvoirs d'exécution, notamment la capacité de solliciter des injonctions, d'imposer des amendes administratives, d'engager des poursuites contre les spammeurs devant un tribunal civil, et de renvoyer les spammeurs devant des instances de poursuites pénales (voir les tableaux 4 et 5).

¹ En Allemagne, plusieurs organisations de consommateurs privées jouent un rôle semblable à celui des organismes publics de protection des consommateurs mentionnés dans cette section. Le rapport comptabilise ces organisations privées (bien que financées par des fonds publics) parmi les organismes publics de protection des consommateurs, en raison du fait qu'elles peuvent, en vertu du droit allemand, intenter des poursuites légales contre les spammeurs.

Tableau 1. Organismes de protection des consommateurs chargés de faire respecter les lois relatives au spam

Pays	Organisme de protection des consommateurs	Lien
Allemagne	Fédération allemande des organisations de consommateurs (vzbv)	www.vzbv.de/start/index.php?page=franzoesisch
Australie	<i>Australian Competition and Consumer Commission</i> (Commission australienne de la concurrence et de la consommation)	www.accc.gov.au/content/index.phtml/itemId/54073
Belgique	Direction générale du contrôle et de la médiation	www.mineco.fgov.be/redir_new.asp?loc=/protection_consumer/complaints/complaints_fr_001.htm
Canada	Bureau de la concurrence Canada	http://competition.ic.gc.ca/epic/internet/incb-bc.nsf/en/Home
Corée	Commission coréenne des pratiques commerciales loyales <i>Korea Consumer Protection Board</i> (Conseil coréen de la protection du consommateur)	www.ftc.go.kr/eng/ http://cpb.or.kr/eng/index.html
Danemark	Ombudsman des consommateurs	www.consumerombudsman.dk
États-Unis	<i>Federal Trade Commission</i> (Commission fédérale du commerce)	www.ftc.gov/
Finlande	Administration de protection des consommateurs et ombudsman des consommateurs	www.kuluttajansuoja.fi
France	Direction Générale de la Concurrence, de la Consommation et de la Répression des Fraudes	www.finances.gouv.fr/DGCCRF/
Hongrie	Direction Générale de la Protection du Consommateur	www.fvf.hu/
Italie	Autorité garante de la concurrence et du marché Conseil national des consommateurs et des usagers (ministère des activités productives)	http://www.agcm.it/ http://www.minindustria.it/organigramma/index.php?sezione=organigramma&tema_dir=tema2&nodo=63
Japon	Commission pour l'équité des pratiques commerciales du Japon Ministère de l'économie, du commerce et de l'industrie	www.jftc.go.jp/ www.meti.gov.jp
Mexique	Profeco	www.profeco.gob.mx/html/inicio/inicio.htm
Norvège	Ombudsman des consommateurs	www.forbrukerombudet.no/index.db2?id=490
Pologne	Bureau de la concurrence et de la protection du consommateur	www.uokik.gov.pl
Royaume-Uni	<i>Office of Fair Trading</i> (Bureau de la concurrence)	www.oft.gov.uk/default.htm
Slovaquie	Inspection slovaque du commerce	www.soi.sk
Suède	Administration suédoise de protection des consommateurs/ Ombudsman des consommateurs	www.konsumentverket.se/mallar/en/startsidan.asp?lngCategoryId=646
Pérou	INDECOPI	www.indecopi.gob.pe/

Organismes de protection des données

Il ressort des questionnaires complétés que 18 organismes de protection des données jouent un rôle en matière d'application des législations antispam (voir le tableau 2). L'Agence coréenne pour la sécurité de l'information (KISA), bien qu'elle ne soit pas un organisme de protection des données à proprement parler, est responsable de l'application de dispositions semblables aux législations relatives à la protection des données. Dans bon nombre de pays membres de l'OCDE, il incombe aux autorités de protection des données de veiller au respect des réglementations qui limitent la collecte et l'utilisation de données personnelles. Les États membres de l'Union européenne (UE) considèrent notamment que les adresses électroniques qui désignent un particulier sont des données personnelles. La directive « vie privée et communications électroniques » (2002/58/CE), transposée par tous les États membres de l'UE dans leur législation nationale, interdit l'envoi de courrier électronique commercial non sollicité à des fins de prospection sans le consentement préalable du destinataire. En outre, la législation en matière de protection des données accorde généralement à la partie intéressée un contrôle sur les renseignements qui la concernent et prévoit qu'elle dispose d'un droit de rectification des informations. Conformément à ce principe, la directive exige de l'expéditeur de courrier électronique qu'il fournisse une adresse valable à laquelle le destinataire pourra envoyer des demandes visant à ne plus recevoir de tels messages et interdit à l'émetteur de dissimuler son identité. En dehors de l'Union européenne, ce sont des Commissaires à la protection de la vie privée qui, au Canada, en Nouvelle-Zélande, en Suisse et à Chypre, sont chargés de l'application des lois relatives au spam.

Les réponses au questionnaire montrent que le principal pouvoir d'enquête détenu par les autorités de protection des données est celui de demander que les renseignements soient fournis volontairement ; en l'absence de cette communication volontaire, certaines autorités peuvent exiger la transmission de pièces justificatives. Les autorités de protection des données entament généralement une action en rédigeant des lettres d'avertissement demandant aux spammeurs de modifier leurs pratiques commerciales. Si ces avertissements restent sans effet, la plupart des autorités publiques sont habilitées à imposer des amendes administratives aux spammeurs, d'autres peuvent réclamer des amendes auprès d'un tribunal civil, tandis que certaines n'en demandent qu'auprès d'un tribunal pénal (voir le tableau 4).

La Commission nationale de l'informatique et des libertés (CNIL), active en France, est un exemple d'autorité de protection des données disposant de nouveaux pouvoirs. En vertu d'une nouvelle législation, la CNIL peut non seulement s'informer et mener des enquêtes avant de décider s'il sera nécessaire de renvoyer un contrevenant devant le ministère public qui peut engager une poursuite pénale, mais aussi appliquer l'une des sanctions administratives relevant de ses compétences, par exemple en émettant un avertissement éventuellement rendu public ou en demandant au contrevenant de cesser l'envoi de courriers électroniques jugés illégaux. Si ces avertissements sont sans effet, la CNIL peut infliger à l'expéditeur une amende administrative — pouvant aller jusqu'à EUR 150 000 ou EUR 300 000 en cas de récidive — ou lui adresser une injonction pour qu'il stoppe son activité.

Les mesures les plus communément utilisées par les autorités de protection des données contre les spammeurs sont notamment les lettres d'avertissement et le renvoi d'affaires relatives au spam devant les autorités pénales. L'Agence coréenne pour la sécurité de l'information (KISA) a été particulièrement active en la matière ; elle indique avoir envoyé 15 462 lettres d'avertissement à des entreprises et adressé 1 463 affaires au ministère public, mais les autorités pénales n'ont pas encore porté d'accusations formelles correspondantes.

Tableau 2. **Organismes de protection des données chargés de faire respecter les lois relatives au spam**

Organisme de protection des données		
Belgique	Commission de la protection de la vie privée	www.privacy.fgov.be/
Canada	Commissariat à la protection de la vie privée	www.privcom.gc.ca/
Corée	Agence coréenne pour la sécurité de l'information	www.kisa.or.kr/english/
Espagne	Commissaire à la protection des données	www.aepd.es
Finlande	Ombudsman de la protection des données	www.tietosuoja.fi
France	Commission Nationale de l'Informatique et des Libertés	www.cnil.fr/
Irlande	Commissariat à la protection des données	www.dataprivacy.ie/
Italie	Commission de protection des données	http://www.garanteprivacy.it/
Norvège	Inspection de la protection des données	www.datatilsynet.no/
Nouvelle-Zélande	Commissaire à la vie privée	www.privacy.org.nz/top.html
Pays-Bas	Commission de protection des données	www.dutchdpa.nl
Pologne	Inspecteur général de protection des données personnelles	www.giodo.gov.pl/168/i/en/
Portugal	Commission nationale de protection des données	www.cnpd.pt/
République tchèque	Bureau de protection des données personnelles	www.uoou.cz/
Royaume-Uni	Commissariat à l'information	www.informationcommissioner.gov.uk/
Suède	Conseil à la protection des données	www.datainspektionen.se/in_english/start.shtml
Suisse	Préposé fédéral à la protection des données	www.edsb.ch/e/aktuell/index.htm
Chypre	Commissaire à la protection des données personnelles	www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/index_en/index_en?opendocument

Organismes de régulation des communications

Les organismes de régulation des communications sont généralement responsables de la réglementation des communications nationales et internationales par radio, télévision, fil, satellite et câble. Pour mener à bien ces tâches, il leur incombe d'ordinaire de traiter les demandes de licences, d'analyser les plaintes des consommateurs, de procéder à des enquêtes et d'élaborer et de mettre en œuvre des programmes de réglementation. Dans plusieurs pays, le spam est considéré comme un problème qui doit être réglé aussi par les autorités de régulation des communications qui, dans certains cas, ont un rôle d'application essentiel en la matière, compte tenu du fait que de nos jours, les courriels commerciaux non sollicités inondent les réseaux de communication, en ralentissant la distribution de courriers électroniques et le fonctionnement d'Internet dans son ensemble (voir le tableau 3). Les réponses données au questionnaire ont mis en lumière divers pouvoirs d'exécution, dont : la capacité de procéder à des inspections impromptues auprès d'un établissement, de formuler des demandes écrites de renseignements

et, en cas de procédure civile, d'assigner des témoins et de sommer de transmettre des documents. Huit autorités de régulation des communications peuvent imposer des amendes administratives aux spammeurs, et une peut engager une procédure à leur égard auprès d'un tribunal civil.

Tableau 3. **Organismes de régulation des communications chargés de faire respecter les lois relatives au spam**

Organisme de régulation des communications		
Australie	Autorité australienne des communications	www.aca.gov.au/consumer_info/spam/consumerinformation.htm
	Autorité australienne de radiodiffusion	www.aba.gov.au/
Autriche	Bureau des télécommunications (notamment pour Vienne, le Burgenland et la Basse Autriche)	
États-Unis	Commission fédérale des communications	www.fcc.gov/
Finlande	Autorité finlandaise de régulation des communications	www.ficora.fi
Hongrie	Autorité nationale des communications	www.hif.hu/english/index1.html
Italie	Autorité pour les garanties dans les communications	www.comunicazioni.it/
Japon	Ministère des affaires intérieures et des communications (MIC)	http://www.soumu.go.jp/joho_tsusin/eng/index.html
Mexique	COFETEL	www.cft.gob.mx/
Pays-Bas	OPTA	www.opta.nl/
Portugal	Autorité nationale des communications	www.anacom.pt
Slovaquie	Bureau des télécommunications	www.teleoff.gov.sk
Turquie	Autorité des télécommunications	www.tgm.gov.tr/

III. Cadres nationaux d'application des lois

Les réponses au questionnaire montrent que les différents types d'organismes d'application décrits précédemment disposent d'une vaste gamme de pouvoirs, procédures et sanctions. La présente section vise à mettre en lumière certains éléments majeurs afin de déterminer comment améliorer la capacité des organismes d'application de répondre aux plaintes, de réunir des preuves suffisantes, de prendre des mesures efficaces contre les spammeurs et de renforcer la coordination.

A. Pouvoirs d'enquête

Notification adressée aux organismes d'application

La première phase de l'application des lois concerne la réception des plaintes relatives au spam, qui nécessite la mise en œuvre d'activités de communication et de transmission d'informations avec les destinataires des pourriels et les opérateurs des réseaux servant à leur diffusion. Il ressort des questionnaires que tous les organismes qui jouent un rôle en matière d'application de la législation relative au spam fournissent au moins un moyen permettant aux destinataires d'avertir l'autorité concernée, par

exemple par courriel, en complétant un formulaire sur le site Web de l'organisme, ou par téléphone, télécopie ou courrier. Seuls quelques organismes d'application proposent un formulaire de plainte en ligne, dispositif pourtant très efficace pour collecter les plaintes et les preuves. Généralement, les utilisateurs doivent envoyer leur plainte par écrit, soit par la poste, soit par courrier électronique, en joignant directement à la plainte dans ce dernier cas le pourriel supposé illégal, pour permettre à l'autorité de vérifier s'il y a infraction.

Aux États-Unis, la FTC (organisme de protection des consommateurs) déploie des efforts importants pour communiquer avec les destinataires de spam en utilisant plusieurs ressources en matière de plainte ou par interaction avec celles-ci. Les consommateurs peuvent, à partir du service en ligne de la FTC, présenter une plainte contre une entreprise ou une organisation dont ils s'estiment victimes, en s'adressant au *Consumer Response Center* ou en utilisant une adresse électronique créée spécifiquement pour recueillir les plaintes concernant le spam. Cette boîte aux lettres électronique consacrée au spam a été instaurée en 1998 pour encourager les consommateurs à transmettre les pourriels en vue d'extraire des données et d'étayer les futures mesures d'application des lois. Elle a reçu plus de 140 millions de pourriels et permet à la FTC de repérer des tendances en la matière et de déterminer quels spammeurs il convient de poursuivre. La FTC reçoit également des plaintes transmises par *Consumer Sentinel*, une base de données sur les plaintes, à laquelle les organismes d'application des lois peuvent accéder après avoir passé un accord avec la FTC concernant le maintien de la confidentialité des plaintes. Cette base de données rassemble les plaintes déposées par les consommateurs par l'intermédiaire du site e-consumer.gov (voir la section V), une initiative organisée sous les auspices du Réseau international de contrôle et de protection des consommateurs (RICPC).

L'idée de l'utilisation d'un tel dispositif a également été appliquée en France, où la CNIL gère le projet « Boîte à spam ». La boîte à lettres électronique a été utilisée pour recevoir des pourriels retransmis par leurs destinataires en vue d'étudier le problème. Les messages n'ont pas été traités comme des plaintes, mais simplement comme une source d'informations, permettant à la CNIL de mieux cerner l'ampleur du phénomène. Actuellement, les plaintes peuvent être adressées à la CNIL par courrier.

L'obligation d'enquêter sur chaque plainte faisant état d'une supposée infraction à la loi est assez répandue. Seules six entités interrogées ont répondu que leur organisme d'application avait la liberté d'enquêter ou non sur une plainte, tandis que douze ont précisé que toute plainte, si elle indique une violation à première vue de la loi, doit faire l'objet d'un examen. Cette responsabilité serait impossible à assumer si un organisme d'application recevait des millions de courriels retransmis, chacun constituant une plainte. En Italie, l'autorité de protection des données (*Garante per la protezione dei dati personali*) établit une distinction entre les notifications reçues des destinataires de spam, et les plaintes officielles portant sur la violation des droits de la personne concernée par les données détournées. Depuis mai 2002, 1 754 plaintes officielles concernant le spam ont été présentées à la *Garante*. Les plaintes officielles doivent être examinées, mais la personne concernée doit transmettre sa plainte par courrier recommandé ou par courriel authentifié par signature électronique.

Les réponses montrent que les autorités de protection des données sont plus souvent amenées à examiner des plaintes que les autres organismes d'application, parfois dans le cadre d'une procédure plus officielle, comme l'envoi d'une lettre écrite. Le Canada, par exemple, ne dispose pas d'une loi antispam spécifique, mais un pourriel peut enfreindre certaines dispositions de sa loi sur la protection des renseignements personnels et les documents électroniques. Les plaintes adressées au Commissariat à la protection de la vie privée du Canada doivent l'être par écrit et comprendre le texte du courriel incriminé. Comme en Italie, les plaintes *officielles* doivent faire l'objet d'une enquête. En revanche, le Bureau de la concurrence du Canada n'est pas obligé d'examiner toutes les plaintes concernant des fraudes liées au spam, et peut donc agir conformément à ses priorités en matière d'application.

Instruction des plaintes

Comme indiqué précédemment, les organismes d'application n'ont pas toujours la liberté de décider d'enquêter ou non sur des plaintes. Compte tenu des ressources limitées dont ils disposent, ils adoptent différentes méthodes pour instruire les plaintes selon les activités illicites à examiner. Certains organismes d'application des lois font une distinction entre les spammeurs contre lesquels ils engageront des poursuites en vertu de leurs pleins pouvoirs et ceux contre lesquels une lettre d'avertissement est suffisante. Il est généralement aisé de reconnaître les polluposteurs professionnels et les entreprises honnêtes qui ont omis de respecter la loi, car ces dernières ne cherchent pas à masquer leur véritable identité, et n'envoient généralement pas des quantités considérables de courriels.

La possibilité d'adopter ces deux types d'attitude à l'égard des spammeurs vise à favoriser le respect de la loi, sans devoir engager des procédures judiciaires ou administratives à forte intensité de ressources contre des parties qui n'ont simplement pas conscience de ne pas se conformer à la loi. L'Australie a indiqué que l'ACA a envoyé 150 lettres d'avertissement à des entreprises depuis l'adoption de la loi sur le spam (*Spam Act*) en avril 2004, mais sa ligne de conduite consiste à réserver les amendes pour les spammeurs professionnels (en règle générale, ceux qui envoient des centaines de milliers de courriels proposant des biens ou services frauduleux) et les entreprises qui enfreignent la loi sur le spam de manière répétée. La France a précisé que la CNIL adresse systématiquement une lettre de rappel aux sociétés qui font l'objet d'une plainte si elles sont situées en France ou dans l'Union européenne, afin de renforcer la sensibilisation des citoyens et des entreprises et de les former — en particulier pour ce qui est des petites entreprises — en expliquant les obligations prévues par la loi. L'Autriche a adopté une méthode différente en imposant une amende à une centaine d'entreprises, dont la plupart ne savaient pas qu'elles étaient hors la loi et avaient seulement envoyé des centaines de courriels sur un marché ciblé. Cette stratégie initiale vise à adresser un message fort au public pour prévenir que le spam, qui représente une utilisation illicite des communications électroniques, ne sera pas toléré ; toutefois, le droit administratif autrichien prévoit un mécanisme de lettres d'avertissement auquel les autorités de régulation des communications peuvent recourir à l'avenir. Les différences constatées dans les lignes d'action adoptées sont sans doute le reflet de ce que chaque société a recours à des méthodes originales pour assurer le respect de la loi.

Ces diverses méthodes sont adaptées et appliquées en prenant en considération les différents types de pourriels reçus au quotidien par les usagers. Chaque infraction appelle une réponse appropriée. En particulier, plusieurs petites et moyennes entreprises ne sont pas pleinement avisées des obligations légales qui pèsent sur l'utilisation des données personnelles — telles que les adresses électroniques — ou sur l'envoi de messages commerciaux. En pareille occurrence, il convient de compléter les mesures par des actions de formation. La formation et la diffusion de l'information peuvent favoriser la prévention des infractions. Aussi les autorités nationales signataires du Plan d'action de Londres mettent-elles en œuvre plusieurs activités destinées à améliorer leurs compétences internes, à accroître la coopération entre organismes, et à sensibiliser davantage les usagers et les entreprises au problème du spam. Lors d'une opération conjointe de « balayage » de l'Internet organisée sous l'égide du Plan d'action de Londres et du Réseau international de contrôle et de protection des consommateurs en 2004, les membres ont fait un état des lieux du problème du spam dans leurs juridictions. Les messages considérés comme des pourriels illégaux feront l'objet d'un examen et de mesures d'exécution, en partenariat avec le secteur concerné le cas échéant dans les mois à venir.

Compétences en matière de collecte de preuves

Comme indiqué précédemment, l'identification de la source du spam et la collecte de preuves pour relier une personne donnée à l'envoi du spam figurent parmi les obstacles majeurs auxquels sont confrontés les organismes d'application. C'est pour cette raison que les organismes d'application doivent

disposer des outils nécessaires pour obtenir des éléments probants suffisants permettant de passer des enquêtes à la phase suivante de l'exécution, celle des sanctions.

Il ressort des réponses au questionnaire que 16 organismes d'application peuvent émettre des demandes portant sur la fourniture volontaire de renseignements tels que des registres commerciaux pertinents aux fins de l'enquête et des déclarations de témoins. Ce type de méthodes informelles de collecte des preuves peut être utile pour obtenir des informations concernant l'identité de spammeurs auprès de tierces parties telles que les FAI et les registres des noms de domaine, sans que les spammeurs soient alertés. Les polluposteurs qui enfreignent la loi involontairement se conformeront à ces requêtes mais il est peu probable que ceux qui se prêtent à des activités frauduleuses y répondent par peur des poursuites.

Aussi les organismes d'application ont-ils besoin de disposer de moyens contraignants leur permettant d'obtenir des informations, par exemple par assignation de témoin ou mandat d'amener. Les renseignements transmis dans le cadre des questionnaires portent sur à peu près la moitié des organismes d'application recensés. Il en ressort que la majorité des organismes ont le pouvoir d'exiger que leur soient fournies des pièces justificatives et des dépositions de témoins, et de réaliser des inspections sur place dans les entreprises. Les organismes d'application semblent être suffisamment à même de réunir les preuves nécessaires pour constater des irrégularités. Par exemple, aux Pays-Bas, l'organisme de régulation des communications (*Onafhankelijke Post en Telecommunicatie Autoriteit* : OPTA) peut délivrer une assignation à témoigner pour information à laquelle le destinataire est légalement tenu de répondre, en satisfaisant au critère juridique relativement simple selon lequel l'ordre de transmettre les renseignements est raisonnable dans le cadre d'une enquête.

En revanche, la Suisse, qui est dans une période de transition pour ce qui est de la législation antispam, ne prévoit pas pour l'instant que le Préposé fédéral à la protection des données dispose de pouvoirs contraignants lui permettant d'obtenir des informations. Au Mexique, l'autorité de régulation des communications (*Comisión Federal de Telecomunicaciones* : COFETEL) n'est pas habilitée à exiger la fourniture de renseignements de la part des FAI, sauf s'ils enfreignent par leurs actions les lois et règlements en vigueur dans le domaine des télécommunications. L'organisme de protection des consommateurs (*Procuraduría Federal del Consumidor* : Profeco), néanmoins, peut recourir à une procédure obligatoire pour collecter des informations dans le cadre d'enquêtes concernant des fraudes à la consommation. De même, au Royaume-Uni, le Commissariat à l'information, autorité de protection des données (*Information Commissioner's Office* : ICO) ne peut contraindre une tierce partie à fournir des informations, mais le Bureau de la concurrence, organisme de protection des consommateurs (*Office of Fair Trading* : OFT) peut émettre des demandes de renseignements, qui sont exécutoires par ordonnance judiciaire.

Coopération avec d'autres organismes d'application des lois au niveau national

Les compétences en matière de collecte de preuves ne sont que le point de départ d'une politique d'exécution des lois efficace. Étant donné que, selon la nature du spam considéré, les responsabilités en matière d'application sont souvent partagées entre plusieurs organismes, pour que les actions contre les spammeurs soient un succès, il peut s'avérer utile que les plaintes soient traitées et les informations partagées entre les organismes tant au niveau national qu'avec les homologues dans d'autres pays. S'il semble y avoir des restrictions au partage d'informations entre organismes d'application d'un même pays, le renforcement de l'efficacité de la coordination entre les différents organismes est un défi qu'un certain nombre de pays ont commencé à relever. (Remarque : les restrictions qui pèsent sur le partage d'informations avec des homologues étrangers sont évoquées dans la section consacrée à la coopération en matière d'application transfrontière des lois).

Le questionnaire posait précisément la question de savoir s'il y avait dans chaque pays des protocoles ou des systèmes d'organisation pour échanger les dossiers des plaintes en matière de spam ou partager des informations entre les organismes. Seules cinq parties concernées ont répondu que des protocoles existaient au niveau national ou étaient en cours d'élaboration à ces fins. Douze réponses ont fait état d'une coopération informelle entre organismes, mise en œuvre sans qu'un protocole ait été convenu. C'est par exemple le cas de l'Autriche ou de la Belgique, où les différents organismes coopèrent de manière informelle. Le transfert de plaintes ne relevant pas de leurs compétences à d'autres organismes d'application ne pose pas de difficulté particulière. Dans de nombreux pays, les renvois sont le résultat d'une obligation juridique administrative, indépendamment du fait que les plaintes portent sur le spam ou tout autre sujet.

L'Australie a surmonté les obstacles susceptibles de découler de l'absence d'un organisme d'application unique en affectant du personnel de l'Autorité australienne des communications (ACA) aux travaux du Centre australien de lutte contre la criminalité technologique (AHTCC), assurant ainsi une excellente communication entre les deux entités. En outre, il y existe des accords avec trois organismes afin de coopérer pour l'application de la loi sur le spam (*Spam Act*), et des pourriels contenant des éléments illégaux ou offensants sont régulièrement transmis à l'autorité compétente. Au Mexique, un accord bilatéral entre l'autorité de régulation des communications (COFETEL) et l'organisme de protection des consommateurs (Profeco) prévoit une assistance mutuelle pour l'examen de pratiques publicitaires frauduleuses ou trompeuses, qui peut s'appliquer aux cas de spam. Au Royaume-Uni, l'OFT a mené une stratégie nationale de coordination des autorités britanniques de régulation des communications concernées par le spam. Il a présidé deux réunions au cours desquelles des représentants d'instances telles que le Commissariat à l'information (*Information Commissioner's Office*), l'Autorité des normes publicitaires (*Advertising Standards Authority*), le ministère du commerce et de l'industrie (DTI), l'Office des Télécommunications (OFTEL), l'organisme de régulation des services avec numéros surtaxés (*Independent Committee for the Supervision of Standards of Telephone Information Services : ICSTIS*), des pouvoirs publics locaux, du ministère de l'intérieur et des autorités judiciaires ont approuvé une matrice indiquant leurs responsabilités respectives et un système de transmission pratique.

L'exemple de coopération entre organismes d'application au niveau national le plus communément cité est celui mis en place entre les organismes d'application qui reçoivent les plaintes et les services de police ou les instances responsables des poursuites pénales qui traitent les plaintes. Au Japon et en Corée, la coopération avec les responsables des poursuites pénales est la procédure d'exécution normale si les spammeurs ne se conforment pas aux demandes administratives de cesser leur activité, car les organismes d'application n'ont pas à proprement parler de compétences en matière de sanctions. En revanche, le *Forbrug* au Danemark et la CNIL en France (respectivement organisme de protection des consommateurs et autorité de protection des données) peuvent imposer des amendes administratives aux spammeurs, mais ont aussi transmis des dossiers de spam à des instances judiciaires afin que des mesures soient prises en vertu du droit pénal ; ces deux organismes peuvent également comparaître comme témoin dans le cadre d'une procédure pénale engagée contre un spammeur. Les plaintes reçues par le Bureau de la concurrence du Canada qui portent effectivement sur des fraudes sont transmises, conformément à des accords informels, aux services de police ou à des organisations telles que Phonebusters — un centre d'appel national qui collecte des informations sur les pratiques commerciales frauduleuses. Le Bureau de la concurrence transfère environ 250 plaintes concernant des pourriels frauduleux par mois à Phonebusters. Aux États-Unis, la FTC n'a pas de pouvoir en matière d'application du droit pénal, mais elle peut transmettre des affaires aux autorités pénales le cas échéant. Lorsque la FTC décide d'examiner une affaire relevant de la loi CAN-SPAM (*CAN-SPAM Act*) en cherchant à obtenir uniquement des sanctions civiles (c'est-à-dire sans chercher de réparation équitable car aucune fraude n'est alléguée), elle transfère le dossier au ministère de la justice (*Department of Justice : DOJ*) pour qu'il soit traité par un tribunal.

En outre, pour renforcer l'efficacité de l'application des lois et la communication entre organismes responsables dans le domaine du spam, la FTC a créé un groupe de réflexion sur le spam réunissant 136 membres représentant 36 pays, plusieurs services du DOJ et la FTC elle-même. Elle a par ailleurs tenu pour son groupe de réflexion deux séances de formation sur les techniques d'enquêtes et elle organise des téléconférences mensuelles pour partager les informations sur les tendances, technologies, techniques d'enquête, objectifs et affaires en matière de spam. Les avantages de ces efforts coordonnés aux États-Unis sont illustrés par le nombre de poursuites civiles engagées par les organismes d'application contre les spammeurs : plus de 60, soit beaucoup plus que tout autre pays. Cela reflète également le fait que la plupart des pourriels proviennent des États-Unis.

Nonobstant les efforts de coordination des activités au moins au niveau national, il est toujours difficile de repérer un unique point de contact dans chaque pays. Comme indiqué précédemment, le spam est un problème aux multiples facettes, et plusieurs aspects liés aux activités y afférentes peuvent déjà être traités avec les instruments existants, notamment les législations en matière de protection des données ou de lutte contre la fraude. C'est pourquoi une coopération à l'échelle nationale serait particulièrement importante pour éviter la redondance des activités, et permettre l'optimisation des ressources et l'exploitation de synergies entre les différents acteurs. Il est souvent plus facile de poursuivre un spammeur pour fraude ou utilisation abusive de données personnelles que pour l'envoi d'un pourriel. En France, par exemple, la CNIL joue un rôle fondamental dans la procédure, en fournissant les éléments de base au ministère public. Il en est de même en Belgique où la Direction générale du contrôle et de la médiation réalise les enquêtes nécessaires et comparait à titre de témoin. La coordination permettra une utilisation plus efficace des renseignements collectés et partant une économie de ressources essentielles.

Plusieurs instances reconnaissent que si une coopération informelle est de fait une première étape, des canaux de communications plus clairement établis simplifieraient la procédure, augmenteraient la transparence et renforceraient l'efficacité du système. Les spammeurs agissent de nos jours à l'échelle internationale² ; il serait illusoire d'espérer pouvoir faire face à ce phénomène sans disposer d'un cadre précis aux niveaux national et international.

B. Procédures utilisées pour prendre des mesures d'exécution

Une fois qu'une plainte concernant des pourriels a été déposée ou, si nécessaire, retransmise à l'organisme d'application approprié, la phase suivante de l'exécution consiste à engager une action. La présente section du rapport fournit des renseignements concernant les procédures utilisées à l'égard des spammeurs. Cette description doit être distinguée de celle des réparations et sanctions recherchées, qui sont abordées dans la section suivante. Il ressort des réponses au questionnaire que les organismes d'application peuvent utiliser trois types généraux de procédures :

- Mesures administratives ;
- Procédures civiles ;
- Procédures pénales.

2. Par exemple, les spammeurs utilisent des serveurs à l'étranger pour héberger leur site Web, empêchant ainsi leur démantèlement en cas de poursuite. Ces services, également appelés « bullet-proof Web host services » sont accessibles sur le Web. Sur ce sujet, voir l'article « Law barring junk email allows a flood instead », du NYT, 01/02/2005, à l'adresse suivante : <http://www.nytimes.com/2005/02/01/technology/01spam.html?ex=1108270800&en=fad6b058565b5287&ei=5070>.

Il a été précisé dans quelques cas que des juridictions ou administrations spécialisées, telles que le Tribunal de commerce en Suède et l'Autorité des normes publicitaires au Royaume-Uni, géraient les procédures.

L'analyse de l'ensemble des questionnaires fait apparaître que 34 des 62 organismes d'application signalés peuvent engager leur propre procédure administrative aboutissant à une sanction contre un spammeur. L'émission de lettres d'avertissement, les ordonnances de se conformer à la loi et les amendes sont les mesures les plus fréquemment utilisées à ce titre par les autorités de protection des données, puis les autorités de protection des consommateurs et les autorités de régulation des communications. Le recours aux juridictions pénales est la deuxième solution la plus souvent mise en œuvre par les organismes d'application : 12 autorités de protection des consommateurs, 9 autorités de protection des données et 4 autorités de régulation des communications peuvent transmettre des plaintes directement aux ministères publics ou leur transférer des affaires quand les polluposteurs ne respectent pas une ordonnance administrative. Les plaintes sont également renvoyées directement au ministère public lorsque le contenu du pourriel est criminel (notamment pornographique ou, dans certains cas, frauduleux). Enfin, 13 organismes d'application peuvent engager des poursuites contre les spammeurs au civil : neuf autorités de protection des consommateurs, 3 autorités de protection des données et 1 autorité de régulation des communications peuvent recourir à cette option. Dans certains pays, comme l'Autriche par exemple, seuls les simples particuliers peuvent poursuivre un polluposteur au civil, tandis qu'aux États-Unis, outre les autorités d'application (telles que la FTC ou le DOJ), les fournisseurs d'accès Internet peuvent tenter une action à l'égard des spammeurs au titre de la *CAN-SPAM Act*.

Le recours aux procédures administratives présente plusieurs avantages. Un organisme d'application qui intervient de sa propre initiative n'a pas à compter sur le pouvoir d'appréciation d'une instance distincte pour tenter une action contre des spammeurs. Par ailleurs, les poursuites au civil ou au pénal peuvent prendre un temps considérable pendant lequel les consommateurs et les utilisateurs de technologies de communications électroniques restent à la merci de fraudes ou d'utilisations abusives de données personnelles. En outre, les procédures pénales peuvent nécessiter une charge de la preuve plus importante, rendant plus difficile l'obtention de la réparation ou de la sanction recherchée. Toutefois, la gamme des réparations et sanctions dont disposent les organismes d'application est plus large lorsqu'ils s'adressent aux tribunaux. Dans certains pays, l'organisme d'application ne peut recourir à une injonction que si elle est accordée par un juge, ce qui est aussi le cas des réparations civiles ou des sanctions accompagnées d'une peine d'emprisonnement.

Des règlements négociés peuvent fournir une solution de remplacement rapide et bon marché pour assurer le respect des lois, par rapport à l'une des trois procédures mentionnées précédemment. Il est indiqué dans neuf questionnaires que les organismes d'application du pays concerné ont engagé contre des spammeurs des actions ayant abouti à un règlement avant qu'une audience contradictoire ne soit nécessaire. Par exemple, l'ACA (autorité australienne de régulation des communications) prévoit la possibilité de prendre un « engagement exécutoire » (*enforceable undertaking*) avec un spammeur. En Belgique, la Direction générale du contrôle et de la médiation peut proposer au contrevenant un accord transactionnel, avec paiement d'une certaine somme. En règle générale, ce type d'accord exige des spammeurs qu'ils cessent leur activité et, en cas de préjudice, qu'ils dédommagent les consommateurs et/ou restituent les gains mal acquis. Si le spammeur ne respecte pas les conditions de l'accord, l'ACA peut s'adresser à un tribunal fédéral pour obtenir un jugement constatant ce non-respect, et l'autorité belge peut de même déférer le cas au ministère public. Deux pays, toutefois, ont indiqué qu'une audience devant un tribunal est une garantie procédurale fondamentale dans toute poursuite engagée.

C. Sanctions et voies de recours

Alors que la précédente section présentait les procédures que les organismes d'application peuvent engager contre les spammeurs, la présente section porte sur les voies de recours et sanctions concrètes utilisables contre les contrevenants. Les instruments dont disposent les organismes d'application pour lutter contre le spam vont de la coercition douce des lettres d'avertissement à la privation de liberté par incarcération.

Il ressort des réponses au questionnaire que les organismes d'application peuvent recourir aux sanctions non pécuniaires suivantes : lettres d'avertissement, injonctions, incarcération suite à une procédure pénale, révocation de licence d'exploitation, interdiction d'accès à Internet, fermeture des locaux professionnels, confiscation du matériel utilisé pour envoyer des pourriels et destruction de fichiers de données. Les deux voies de recours non pécuniaires les plus communément utilisées sont les lettres d'avertissement et les injonctions. Il existe une différence marquée en la matière entre les compétences des autorités de protection des données et celles des organismes de protection des consommateurs : 9 des 18 autorités de protection des données répertoriées dans les réponses sont habilitées à avertir les spammeurs de l'illégalité de leurs actions et à leur demander d'interrompre leurs envois de pourriels effectués en violation des lois sur la protection des données ; tandis que 12 des 19 autorités de protection des consommateurs signalées peuvent solliciter des injonctions ordonnant au spammeur de cesser son activité illégale, sous peine de sanctions pour outrage lorsque le spam est vecteur de fraudes. Les autorités de régulation des communications ont recours presque de façon égale à ces deux sanctions non pécuniaires.

Tableau 4. Voies de recours et sanctions non pécuniaires

Recours/sanction	Autorité de protection des données (18)	Organisme de protection des consommateurs (19)	Autorité de régulation des communications (12)
Lettre d'avertissement	9	3	4
Injonction	2	12	3
Incarcération (suite à une procédure pénale)	9	8	2
Révocation de licence d'exploitation	4	-	3
Interdiction d'accès à Internet	2	1	1
Fermeture des locaux professionnels	1	1	1
Confiscation de matériel	2	1	1
Destruction de données	3	-	-

D'après les réponses au questionnaire, les organismes d'application disposent des voies de recours pécuniaires suivantes : amendes administratives, amendes civiles, amendes pénales, réparation des préjudices subis par les consommateurs, restitution des gains mal acquis et gel des actifs. Les amendes sont des sanctions monétaires dont le produit revient généralement à l'État. La réparation des préjudices subis par le consommateur vise à replacer ce dernier dans la situation qu'il avait avant d'être victime de pratiques frauduleuses, aussi, contrairement à une amende, les sommes récupérées auprès du spammeur sont reversées au consommateur. La restitution des gains mal acquis se traduit par la confiscation des produits d'activité illégale identifiables et leur versement au fisc. Un gel des actifs est une mesure préliminaire, d'ordinaire une ordonnance d'un tribunal, qui exige d'une tierce partie telle qu'une banque qu'elle saisisse les actifs du spammeur pour l'empêcher de les transférer dans un autre pays où ils pourraient ne pas être accessibles. Cet instrument d'application conservatoire, lorsqu'il est autorisé, améliore la possibilité des organismes d'application de garantir l'exécution de tout jugement de paiement

éventuellement délivré. Pour que cette mesure soit efficace, toutefois, il faut qu'elle soit ordonnée ou mise en œuvre dans le pays où se trouvent lesdits actifs.

Les autorités de protection des données et les autorités de régulation des communications sont habilitées à rechercher des voies de recours pécuniaires contre les spammeurs principalement par le biais d'amendes administratives. Pour obtenir la fixation d'amendes, les organismes de protection des consommateurs peuvent également recourir à des tribunaux civils et pénaux, presque aussi souvent qu'à une procédure administrative. Cela peut s'expliquer dans un souci d'économie judiciaire, puisque bon nombre des organismes de protection des consommateurs doivent déjà rechercher des sanctions non pécuniaires auprès de tribunaux civils. Les solutions consistant à solliciter la réparation des préjudices subis par les consommateurs et la restitution des gains mal acquis sont relativement rares et le gel d'actifs n'a été mentionné qu'une fois.

Tableau 5. Voies de recours et sanctions pécuniaires

Recours/sanction	Autorité de protection des données	Organisme de protection des consommateurs	Autorité de régulation des communications
Amendes administratives	10	11	8
Amendes et/ou réparations civiles	3	9	1
Amendes pénales	5	9	3
Réparation des préjudices subis par les consommateurs	-	2	2
Restitution des gains mal acquis	-	3	1
Gel des actifs	-	1	-

IV. Obstacles à une application transfrontière efficace

Le but des sections ci-après est de donner un aperçu des principaux problèmes auxquels sont confrontés les organismes d'application qui souhaitent coopérer avec des homologues étrangers dans la lutte contre les spammeurs. Les problèmes signalés, les exemples d'obstacles rencontrés par les organismes d'application et les efforts entrepris pour les surmonter sont tirés des réponses au questionnaire et de travaux de recherche indépendants. Cependant, ils ne sont pas supposés constituer une liste exhaustive ni des problèmes ni des solutions possibles.

Restrictions de l'étendue des pouvoirs des organismes d'application

Lorsqu'un spammeur et le destinataire du message sont situés dans des pays différents, les organismes d'application sont confrontés à de nombreux obstacles, tant pratiques que juridiques, lorsqu'ils veulent prendre des mesures contre les polluposteurs. Comme indiqué précédemment, l'application de la législation antispam est pour l'essentiel l'apanage de pouvoirs publics qui tirent leurs compétences du droit public. Dans certains cas, les lois mises en œuvre pour lutter contre le spam ne sont pas applicables à des messages provenant d'une source étrangère, ce qui peut empêcher les organismes d'application du pays où un message est reçu de s'adresser à un homologue étranger ne serait-ce que pour lui demander d'agir en vertu de sa propre législation. L'autre difficulté de ce type de situation apparaît lorsque le message considéré est illégal là où il est reçu, mais ne l'est pas d'où il a été expédié, si bien que l'homologue

étranger ne peut pas prendre de mesures au titre de sa législation. En dernier lieu, même lorsque des organismes d'application sont habilités de par la loi à rechercher une assistance étrangère et que leurs homologues ont la volonté de les aider, il peut exister des conditions et/ou des restrictions pesant sur la collecte et le partage d'informations.

Pour vérifier les capacités juridiques actuelles (par rapport aux capacités pratiques) des organismes d'application concernant la mise en œuvre d'actions transfrontières contre les spammeurs, le questionnaire posait la question de savoir si la législation nationale s'applique aux polluposteurs étrangers visant des utilisateurs de courrier électronique nationaux. Si tel est le cas, certains organismes d'application peuvent entamer des actions contre une présence ou une activité se rapportant au spammeur sur leur territoire (par exemple en confisquant des stocks ou en interdisant le transit de marchandises). En outre, des organismes d'application peuvent chercher une assistance auprès d'un homologue étranger dans le pays où le spammeur est installé. Dans 15 questionnaires, il a été répondu que des mesures d'exécution peuvent en théorie être engagées contre des spammeurs indépendamment de l'origine du message électronique, dès lors que le message a un lien national, notamment s'il est envoyé sur une adresse électronique consultée sur le territoire national³.

Il convient de tenir compte de certaines nuances précisées dans les réponses. Les Pays-Bas ont transposé la directive 2002/58/CE en modifiant leur loi sur les télécommunications, et ne prévoient pas la mise en œuvre de mesures d'exécution à l'égard de sources étrangères de spam sur cette base. Toutefois, l'envoi de courriers électroniques commerciaux non sollicités est susceptible d'impliquer le traitement automatisé de données personnelles, et d'enfreindre les lois néerlandaises en vigueur en matière de protection des données. La situation est semblable dans d'autres pays de l'Union européenne, où des mesures d'exécution peuvent être engagées contre des polluposteurs étrangers pour autant que ces derniers soient installés en dehors de l'UE, tandis que les spammeurs situés dans l'UE relèvent de la législation nationale du pays d'origine du pourriel. En Belgique, l'organisme de protection des consommateurs ne peut poursuivre des spammeurs basés à l'étranger que s'ils sont extracommunautaires, alors qu'en Finlande, l'autorité de régulation des communications ne peut engager de telles poursuites, mais les autorités de protection des consommateurs et de protection des données sont habilitées à le faire. Ainsi, même si la loi antis spam spécifique ne s'applique pas au spam provenant de l'étranger, d'autres dispositions juridiques peuvent permettre de prendre des mesures contre le spammeur ou de solliciter l'aide d'un homologue étranger.

Dans 13 questionnaires, il a été indiqué que les mesures d'exécution soit ne pouvaient pas être engagées contre des spammeurs installés à l'étranger, soit n'étaient pas entamées à leur égard dans la pratique, en raison des difficultés à enquêter dans un pays étranger et des problèmes liés en dernier ressort à l'application d'une condamnation. Dans certains pays, la loi limite expressément l'application de ses dispositions aux activités concernant des pourriels provenant du territoire national. Dans d'autres, l'utilisation des ressources requises pour repérer et localiser un spammeur ne peut être justifiée par la nécessité de répondre à une plainte étrangère. Il peut donc sembler que les spammeurs installés à l'étranger ne risquent aucune action de la part des organismes d'application de ces pays. Cependant, presque tous ceux qui ont répondu au questionnaire ont indiqué qu'il est possible de signaler à des homologues étrangers des pourriels provenant de leur territoire.

Bien que le spam soit souvent reçu hors du pays d'où il a été émis, il est probable que le spammeur ait également adressé ses pourriels à des destinataires dans son pays, de sorte que l'organisme d'application local peut engager des actions à partir de preuves y afférentes. Un obstacle juridique à la coopération internationale peut surgir si le spammeur fait attention de n'envoyer des spams qu'à des destinataires situés

3. La loi sur le spam (*Spam Act*) en Australie, par exemple, prévoit explicitement qu'elle s'applique à tous les pourriels envoyés ou reçus dans le pays ou ayant un lien avec le pays.

en dehors de son pays d'installation. Dans six questionnaires (réponses émanant de trois organismes de protection des consommateurs et de trois autorités de régulation des télécommunications), il a été indiqué que des spammeurs adressant leurs courriels non sollicités à des utilisateurs étrangers ne pouvaient pas être poursuivis en l'absence d'un autre lien national. Pour ces organismes d'application, l'envoi de spam à partir de leur territoire ne constitue pas un fondement juridique suffisant pour engager une action, le spam doit être reçu par un utilisateur de courrier électronique situé sur le territoire national.

Collecte et partage d'informations entre organismes d'application

Les organismes d'application qui souhaitent prendre des mesures contre les spammeurs installés dans un pays étranger sont gênés par le fait qu'ils ne peuvent pleinement exercer leurs pouvoirs au-delà des frontières nationales. Toutefois, ils peuvent localiser et identifier les spammeurs, et rassembler contre eux des éléments de preuves susceptibles d'être ensuite utiles pour leurs homologues étrangers. Il convient d'apporter quelques précisions au sujet de la collecte et du partage d'informations dans le contexte d'une application transfrontière. Tout d'abord, un organisme d'application peut chercher à obtenir des renseignements auprès de particuliers et d'entreprises nationaux, notamment les FAI, dans le cadre d'une procédure obligatoire ou d'une coopération volontaire. Lorsque les enquêtes permettent de repérer un spammeur installé à l'étranger, l'organisme d'application peut, comme indiqué précédemment, faire appel à un homologue étranger dans le pays d'installation du spammeur. Cependant, le pays qui demande de l'aide peut être limité par sa propre législation nationale pour ce qui est du type d'informations qu'il peut partager avec l'homologue étranger sollicité. Deuxièmement, l'homologue étranger peut être freiné dans sa capacité de prendre des mesures et/ou de rassembler des informations en réponse à la demande d'un organisme étranger si le spammeur n'a pas enfreint sa propre législation nationale.

Seules deux parties concernées ont répondu dans le questionnaire que la collecte et le partage d'informations pour et avec un organisme d'application étranger n'étaient pas autorisés ; cela étant, dans les pays où le partage d'informations est possible, il peut être soumis à de nombreuses conditions. Les renseignements fournis en réponse au questionnaire n'étaient pas assez précis pour permettre une analyse comparative entre pays des possibilités de collecte et de partage d'informations. Le tableau 6 montre que la plupart des réponses ont porté essentiellement sur les conditions et restrictions relatives au partage d'informations avec un organisme d'application étranger. Une telle comparaison à l'échelle internationale serait extrêmement utile pour déterminer avec précision les lacunes existant dans les capacités des organismes d'application de rassembler et de partager des informations pour et avec des homologues étrangers. Néanmoins, une synthèse des renseignements contenus dans les réponses au questionnaire fournit au Groupe de réflexion un aperçu des types de conditions et restrictions auxquelles les organismes d'application sont confrontés lorsqu'ils cherchent à partager les informations dans le cadre d'une coopération transfrontière.

La condition la plus fréquente mentionnée dans les réponses au questionnaire était l'obligation de partager les informations dans le cadre d'un accord international sous une forme ou sous une autre. Parmi ces réponses, six pays n'ont pas indiqué d'accord en vigueur pour la coopération internationale, ce qui suppose que le partage d'informations concernant des affaires de spam est en théorie possible, mais qu'un accord international sous une forme ou sous une autre est toujours requis. Plusieurs réponses opèrent également une distinction entre les informations collectées de manière informelle et celles obtenues en vertu d'une procédure obligatoire. Les premières peuvent être partagées avec des organismes d'application étrangers, sous réserve de prévenir la source initiale des informations et d'obtenir son autorisation, tandis que les deuxièmes ne peuvent pas être partagées avec des organismes d'application étrangers.

Six réponses, toutefois, ont mentionné des accords en vigueur concernant le partage d'informations, notamment entre organismes de protection des consommateurs. En Europe, le Réseau de contact des autorités antispam (*Contact Network of Spam Authorities* : CNSA) a été évoqué dans plusieurs réponses. Ce réseau a été créé pour améliorer le partage d'informations et l'échange des meilleures pratiques entre les autorités européennes responsables en matière de spam. Dans le prolongement de cette initiative, une « procédure de coopération relative à la transmission d'informations et renseignements sur les plaintes en relation avec l'application de l'article 13 de la directive sur la vie privée et les communications électroniques » a été préparée⁴. La procédure a été approuvée, jusqu'à présent, par 16 organismes d'application des dispositions antispam dans 13 pays européens. La nature de l'accord est telle que d'autres organismes peuvent le signer au fil du temps. L'accord — initialement élaboré par l'OPTA en coopération avec la CNIL — instaure une procédure commune pour le partage des informations et le traitement des plaintes au-delà des frontières afin de repérer et de poursuivre plus facilement les spammeurs partout en Europe⁵.

Tableau 6. **Conditions et restrictions relatives au partage d'informations avec des organismes d'application étrangers**

Condition ou restriction	Nombre de réponses
Doit être réalisé dans le cadre d'un accord international sous une forme ou une autre	12
Doit respecter les législations en vigueur en matière de protection des données et de la vie privée	5
Doit être effectué conformément aux missions de l'organisme	4
Les informations ne doivent pas avoir un caractère confidentiel	4
Les informations partagées ne doivent pas avoir été rassemblées dans le cadre d'une procédure obligatoire de l'organisme	2
L'organisme qui partage les informations peut demander que l'organisme qui les reçoit s'engage à les traiter sous le sceau du secret	1
Si l'État qui émet la demande souhaite être informé des plaintes relatives à un spammeur donné, l'autorité étrangère qui partage les informations doit demander l'autorisation de la partie à l'origine de la plainte initiale	1
Le code de procédure pénale ne permet pas le partage d'informations concernant un défendeur une fois qu'une enquête judiciaire est lancée	1

Force exécutoire des décisions au niveau international

Aucun pays membre de l'OCDE n'a conclu d'accord portant expressément sur la reconnaissance et la force exécutoire des jugements obtenus par des organismes d'application étrangers contre des spammeurs. Neuf réponses font état de la signature d'un accord multilatéral ou bilatéral prévoyant la reconnaissance et la mise en œuvre de décisions en matière civile et commerciale, susceptible d'être appliqué dans certains cas aux jugements contre les spammeurs. Toutefois, lorsque le créancier poursuivant devant un tribunal civil est un organisme d'application public, certains tribunaux étrangers peuvent considérer que les jugements rendus ont un caractère pénal ou administratif, et ne sont donc pas soumis à l'accord. Ce raisonnement pourrait être utilisé pour exclure l'ensemble des trois conventions européennes concernant la

4. Les conclusions du Conseil peuvent être consultées à l'adresse suivante : <http://register.consilium.eu.int/pdf/en/04/st15/st15481-re01.en04.pdf>.

5. Voir le communiqué de presse à l'adresse suivante : <http://europa.eu.int/rapid/pressReleasesAction.do?reference=IP/05/146&format=HTML&aged=0&language=EN&guiLanguage=en>.

reconnaissance et l'exécution des décisions étrangères en matière civile et commerciale : le règlement (CE) n° 44/2001 du Conseil⁶, la Convention de Lugano de 1988⁷ et la Convention de Bruxelles de 1968⁸, qui s'appliquent aux jugements en matière civile et commerciale, et ne concernent donc pas les sanctions administratives. En l'absence d'accord particulier conclu entre pays concernant la compétence judiciaire et l'exécution des décisions, les règles nationales du droit international privé régissant la reconnaissance et l'exécution de jugements étrangers pourraient s'appliquer ; de sorte que la reconnaissance et l'exécution pourraient être accordées en vertu du principe de courtoisie internationale, avec des conditions telles que, par exemple, la réciprocité judiciaire et le respect de règles de procédure appropriées.

L'Accord de libre-échange entre les États-Unis et l'Australie contient une disposition concernant les jugements obtenus par la FTC, la Commission des valeurs mobilières (*Securities and Exchange Commission* : SEC), et la Commission des opérations à terme sur les produits de base (*Commodities Futures Trading Commission* : CFTC) des États-Unis, la Commission australienne de la concurrence et de la consommation (ACCC) et la Commission australienne des valeurs mobilières et des investissements (*Australian Securities and Investment Commission* : ASIC). Il y est prévu que les tribunaux aux États-Unis et en Australie ne peuvent pas refuser d'exécuter des décisions de réparation financière obtenues par ces organismes dans des affaires de fraudes au seul motif que ces décisions sont de nature pénale. Cette disposition pourrait s'appliquer à un jugement obtenu dans une affaire de spam portant sur des opérations commerciales trompeuses ou des fraudes. Bien qu'elle n'impose pas aux tribunaux d'appliquer ces décisions, elle précise la situation en ce sens que leur exécution doit être considérée sous l'angle des règles de droit international privé sur l'exécution des jugements.

La Conférence de La Haye de droit international privé prépare une Convention sur la compétence et les jugements étrangers en matière civile et commerciale⁹ dans laquelle chaque pays adhérent s'engagera à appliquer les jugements des autres, quel que soit le lieu de la cause de la procédure. Selon l'article 2, paragraphe 5, de l'actuel projet de Convention, « un litige n'est pas exclu du champ d'application de la Convention au seul motif qu'un gouvernement, une agence gouvernementale ou toute autre personne agissant pour le compte d'un État y est partie. » Les travaux relatifs à cette Convention ont toutefois été laissés en suspens quand il est devenu évident qu'il serait difficile de parvenir à un accord. Le texte a donc été révisé, et la version actuelle de l'avant-projet de la Convention, officiellement désignée comme le Projet relatif aux accords exclusifs d'élection de for¹⁰, s'applique dans des affaires internationales aux accords exclusifs d'élection de for conclus en matière civile ou commerciale. La Convention vise à établir un régime juridique international apportant la sécurité et assurant l'efficacité des accords exclusifs d'élection de for conclus entre des parties à des opérations commerciales pour donner effet à des jugements étrangers en matière civile et commerciale à la suite d'un litige concernant une clause d'élection de for. Il

-
6. Règlement (CE) n° 44/2001 du Conseil du 22 décembre 2000 concernant la compétence judiciaire, la reconnaissance et l'exécution des décisions en matière civile et commerciale. Journal officiel L 12 du 16 janvier 2001, consultable à l'adresse suivante : <http://europa.eu.int/scadplus/leg/en/lvb/l33054.htm>.
 7. Convention concernant la compétence judiciaire et l'exécution des décisions en matière civile et commerciale, consultable à l'adresse suivante : <http://www.curia.eu.int/common/recdoc/convention/en/c-textes/lug-textes.htm>.
 8. Convention concernant la compétence judiciaire et l'exécution des décisions en matière civile et commerciale, Bruxelles 1968, consultable à l'adresse suivante : <http://www.curia.eu.int/common/recdoc/convention/en/c-textes/brux-idx.htm>.
 9. Le texte de l'avant-projet de 1999 peut être consulté sur le site Web de la Conférence de La Haye de droit international privé à l'adresse suivante : http://www.hcch.net/upload/wop/jdgm_draftf.pdf.
 10. Dernier projet (avril 2004) disponible en ligne à l'adresse suivante : http://www.hcch.net/upload/wop/jdgm_wd110_f.pdf.

est donc hautement improbable que des affaires intentées contre des spammeurs par des organismes d'application rentrent dans son champ d'application.

Malgré les efforts entrepris au niveau européen pour harmoniser les législations, dans la pratique, l'application des lois varie d'un pays à l'autre, et la coopération transfrontière est toujours limitée par des difficultés d'ordre juridique ou juridictionnel. Au niveau international, la situation est encore plus marquée : même si les autorités d'exécution essaient de travailler ensemble, il n'y a pas de mécanisme mis en œuvre automatiquement quand une affaire est engagée contre un spammeur installé dans un autre pays. Étant donné la rapidité d'action des contrevenants dans ce domaine, la réaction doit être immédiate et non le résultat d'accords conclus au cas par cas.

Établissement de priorités en matière de coopération internationale

Le questionnaire demandait de signaler les types de plaintes qui devraient être traités prioritairement dans le cadre de la coopération transfrontière en matière d'application des lois ou s'y prêteraient le mieux. L'objectif de cette question était de déterminer s'il existait un accord quelconque parmi les pays concernant les types de pollupostage qui devraient être les premiers visés par des mesures d'exécution transfrontières. Sept réponses ont indiqué qu'il n'y avait pas de degré de priorité attribué aux plaintes selon le type de spam ; sur ces sept réponses, cinq ont précisé que tous les courriels commerciaux non sollicités étaient traités avec la même priorité, et deux qu'aucune priorité n'était appliquée. Vingt et une réponses ont mentionné au moins un type de spam prioritaire aux fins d'une application des lois transfrontière. Le tableau 7 récapitule les types de plaintes concernant le spam auxquels les organismes d'application accordent une priorité en vue d'une coopération transfrontière.

Un grand nombre de motifs possibles ont été cités pour juger du caractère prioritaire d'une plainte relative au spam ; les plus courants sont fondés sur le type de dommage que le message peut causer, par exemple en mettant en péril les intérêts financiers ou la santé des consommateurs, en portant atteinte à la vie privée des utilisateurs, aux réseaux ou aux biens. Le type de spam le plus souvent désigné comme se prêtant prioritairement à une coopération transfrontière est le courriel qui contient des affirmations fausses ou trompeuses nuisant au destinataire. Cette constatation traduit une préférence accordée à la protection des intérêts des consommateurs en ligne avant ceux des FAI, des entreprises, des particuliers concernés par l'utilisation de leurs données personnelles ou d'autres parties dont les intérêts sont mis à mal par le spam. Les FAI et les entreprises subissent clairement un préjudice économique du fait du spam qui est synonyme de diminution de la capacité du réseau et de la productivité des travailleurs, mais leur bien-être ne rentre pas dans les intérêts publics en tant que tel, c'est-à-dire qu'une institution publique ne peut pas accorder la priorité à leurs plaintes par rapport à celles d'un concurrent sans être accusée de fausser la libre concurrence. Le même raisonnement ne peut pas servir à expliquer pourquoi la protection des droits de protection des données n'est pas aussi prioritaire que celle contre les fraudes dans des affaires transfrontières.

La responsabilité en matière d'application des législations antispam incombant le plus souvent à plusieurs types d'organismes d'application, on pourrait s'attendre à constater des priorités différentes selon les types d'organismes. Or, sur les 22 pays comptant plusieurs organismes d'application, seules 4 réponses font état de modification du caractère prioritaire en fonction de la mission de chaque organisme. Cela signifie que même lorsque les responsabilités sont partagées, il y a généralement un accord au niveau national concernant le type de spam à traiter en priorité dans le cadre d'une coopération transfrontière en matière d'application des lois.

Tableau 7. Types de plaintes relatives au spam à traiter en priorité dans le cadre d'une application transfrontière

	Organismes de protection des consommateurs	Autorités de protection des données	Autorités de régulation des télécommunications	Autorités pénales
Critère de priorité				
Message contenant des affirmations fausses ou trompeuses (par ex. pêche aux données personnelles, escroqueries, allégations portant sur des questions de santé)	8	7	4	1
Message contenant un virus	3	3	2	3
Courriel commercial non sollicité	3	1	-	-
Message au contenu offensant ou illicite (par ex. pornographie infantine)	1	1	2	1
Ampleur des dommages subis (aucun exemple précis n'a été donné)	1	1	-	-
Volume de messages envoyés	-	1	-	-
Récidive	-	-	1	-
Spam par téléphonie mobile	-	-	1	-
Message émis en dehors de l'UE	-	1	-	-

V. Efforts en cours pour surmonter les obstacles à la collecte et au partage d'informations

Protocoles d'accord multilatéraux ou bilatéraux se rapportant expressément à l'application de la législation antispam

Actuellement, quatre pays membres de l'OCDE (Australie, Corée, États-Unis et Royaume-Uni) ont conclu divers protocoles d'accord sur le spam pour améliorer la coopération entre organismes d'application dans les affaires transfrontières. L'Australie (ACA et ACCC), les États-Unis (FTC) et le Royaume-Uni (OFT et ICO) ont signé en juillet 2004 un protocole d'accord multilatéral sur le spam qui prévoit que les organismes d'application responsables en matière de lutte contre le spam coopéreront pour ce qui est de : la détection et les enquêtes relatives à des infractions liées au spam, la poursuite des spammeurs, l'échange de preuves et la coordination dans le domaine de l'application des lois contre le pollupostage transfrontière. En octobre 2003, l'Australie (ACA) et la Corée (KISA) ont ratifié un protocole d'accord bilatéral sur le spam permettant l'échange de renseignements concernant le spam originaire de l'un ou l'autre de ces deux pays, collectés à l'occasion d'enquêtes relatives à la mise en application des lois. Le protocole d'accord entre l'Australie et la Corée prévoit également l'échange d'informations concernant les efforts déployés pour instaurer et mettre en œuvre des cadres réglementaires en matière de lutte contre le spam et les utiliser efficacement. L'Australie est aussi partie à une Déclaration commune avec la Thaïlande sur la coopération dans les domaines des technologies de l'information et des télécommunications au niveau ministériel, qui comprend notamment des dispositions relatives à l'échange de renseignements sur les politiques et stratégies de lutte contre le spam.

Le Réseau international de contrôle et de protection des consommateurs (RICPC) participe à la lutte contre la fraude transfrontière par Internet en gérant un site Web multilingue, econsumer.gov, qui fournit des informations concernant la protection des consommateurs dans ses pays membres, les coordonnées d'organismes de protection des consommateurs dans ces pays et un formulaire de plainte en ligne pour collecter et partager les plaintes liées aux activités de commerce électronique transfrontières. Au cours du premier semestre 2004, 3 502 plaintes ont été transmises à econsumer.gov, dont 54 % portaient sur des offres communiquées par courriel. Lors d'une réunion organisée en octobre 2004, le Bureau de la concurrence britannique (OFT) et la Commission fédérale du commerce américaine (FTC) ont présenté le Plan d'action de Londres sur le spam, un accord non contraignant ouvert à la signature d'organismes d'application chargés de faire respecter les législations antispam, et de certains acteurs du secteur privé concernés par la lutte contre le spam.

En substance, le Plan d'action de Londres prévoit que les gouvernements et les organismes publics participants s'efforcent de renforcer la coopération internationale en matière d'application des lois antipourriel en : désignant un point de contact national afin de communiquer avec les organismes d'application étrangers sur les affaires de spam ; promouvant la coordination nationale entre les différents organismes compétents en matière d'application de la législation antispam ; priorisant les cas selon le tort causé aux victimes lors de la sollicitation d'une aide internationale ; préconisant et appuyant la participation des pays moins développés à l'application des lois antipourriel ; prenant part à des audioconférences tenues périodiquement afin de passer les cas en revue et de faire le suivi des développements en matière de législation et d'application ; partageant des techniques d'enquête et des stratégies de mise en application efficaces. Un site Web sera créé pour permettre aux membres d'examiner et d'échanger des informations et leurs meilleures pratiques en ligne de manière sécurisée. Les projets en cours portent sur des actions de « balayage » du spam ainsi que sur un projet éducatif sur les ordinateurs zombies. Le Plan d'action de Londres regroupe 27 organismes de 19 pays et 12 acteurs majeurs du secteur industriel (dont 5 associations de FAI). Diverses provenances géographiques et compétences (organismes de protection des consommateurs, autorités de protection des données, autorités de régulation des télécommunications) sont représentées.

Accords internationaux dans des domaines d'action connexes

En juin 2003, les gouvernements des pays membres de l'OCDE ont approuvé les *Lignes directrices de l'OCDE régissant la protection des consommateurs contre les pratiques commerciales transfrontières frauduleuses et trompeuses* (2003). Le spam relève de ces Lignes directrices lorsqu'il est utilisé comme vecteur de pratiques commerciales frauduleuses et trompeuses. Le cadre créé par ces Lignes directrices traite des systèmes nationaux et des principes propres à faciliter la coopération internationale, de la notification, de l'échange d'informations, de l'entraide en matière d'enquêtes, de la confidentialité, des pouvoirs en matière de protection des consommateurs, de la réparation financière des préjudices subis par les consommateurs et de la coopération avec le secteur privé. Les Lignes directrices peuvent être consultées à l'adresse suivante : www.oecd.org/sti/crossborderfraud.

Le Danemark, la Norvège, la Finlande et la Suède ont instauré des relations de travail transfrontières en matière de protection des consommateurs dans le cadre d'un Accord de coopération entre les Ombudsmen des consommateurs des pays nordiques. L'Accord prévoit que les Parties peuvent engager des poursuites au nom de chacune d'entre elles et échanger des informations concernant les pratiques commerciales internationales (sous réserve de respecter les règles nationales sur la confidentialité et d'une demande de traitement confidentiel des informations). L'Accord peut s'appliquer aux cas d'activités frauduleuses ou trompeuses menées grâce au spam émis depuis le territoire de l'une des parties contractantes et reçu sur celui d'une autre partie contractante. Il comprend également des dispositions prévoyant la consultation des entreprises affectées ainsi que le paiement des dépenses et des traductions.

Dans le domaine du droit pénal, la Convention sur la cybercriminalité du Conseil de l'Europe, entrée en vigueur le 1^{er} juillet 2004, prévoit que les États qui l'ont ratifiée mettent en œuvre une législation pénale relative notamment à la fraude informatique et aux violations de la sécurité des réseaux. Ces dispositions pourraient être utilisées pour engager des actions contre les spammeurs qui se servent de messages électroniques pour commettre une fraude (comme les « fraudes 419 ») et/ou diffuser des virus. La Convention agit comme un catalyseur encourageant à prendre des mesures contre les polluposteurs dans des pays où les capacités font actuellement défaut, en renforçant les pouvoirs d'enquête des autorités compétentes, et en leur fournissant les outils nécessaires pour obtenir des preuves de malversations (par exemple., injonction de produire des données, perquisition et saisie de données informatiques stockées, collecte en temps réel des données relatives au trafic et interception de données relatives au contenu) [articles 18-21]. En ce qui concerne la coopération internationale, la Convention est particulièrement intéressante pour l'examen par le Groupe de réflexion des mesures d'exécution transfrontalière car elle prévoit des principes relatifs à l'extradition [article 24] et un système détaillé d'entraide pour la collecte et le partage d'informations entre les Parties [articles 25-34]. Jusqu'à présent, huit pays ont ratifié la Convention, dont un, la Hongrie, est membre de l'OCDE.

Récemment, le Conseil de l'Union européenne a adopté le règlement (CE) n° 2006/2004¹¹ relatif à la coopération en matière de protection des consommateurs. L'objectif du règlement est d'établir des relations entre les autorités nationales chargées de l'application de la législation et de leur permettre de prendre des mesures coordonnées contre les opérateurs commerciaux malhonnêtes qui détournent à leur profit la liberté du marché intérieur pour tromper les consommateurs. Il supprime les obstacles existants à l'échange d'informations et à la coopération et il habilite les autorités d'application à rechercher et à obtenir des actions de leurs homologues dans d'autres États membres. Le nouveau réseau d'autorités d'application à l'échelle de l'UE sera opérationnel en 2006.

Au sein de l'Union européenne, la directive 98/27/CE (directive « Actions en cessation »)¹² est une nouvelle réponse apportée aux problèmes que pose l'application transfrontière des dispositions en matière de protection des consommateurs. Elle vise précisément à fournir une solution pour lutter contre les opérateurs qui réalisent dans un État membre des activités qui portent préjudice aux intérêts collectifs des consommateurs d'un autre État membre. Elle établit une procédure commune en vertu de laquelle une action en cessation pourra être intentée par une « entité qualifiée » auprès d'un tribunal ou d'une autorité administrative désignés en cas d'infractions aux dispositions nationales transposant les directives communautaires énumérées en annexe. Lorsque l'objet d'un message électronique commercial contient, par exemple, des termes trompeurs, les entités qualifiées (telles que les organismes d'application publics, les organismes de défense des consommateurs ou les associations professionnelles) peuvent demander à l'instance appropriée une injonction de cessation immédiate (*stop now order*). L'objectif de la directive est de veiller à ce que les actions collectives visant à protéger les consommateurs puissent être engagées là où les entreprises sont implantées et donc là où les voies de recours sont le plus susceptibles d'être efficaces.

11 Règlement (CE) n° 2006/2004 du Parlement européen et du Conseil du 27 octobre 2004 relatif à la coopération entre les autorités nationales chargées de veiller à l'application de la législation en matière de protection des consommateurs (« Règlement relatif à la coopération en matière de protection des consommateurs »), JO L 364, p. 1, consultable en ligne à l'adresse suivante : http://europa.eu.int/comm/consumers/prot_rules/admin_coop/index_fr.htm.

12 Directive 98/27/CE du Parlement européen et du Conseil du 19 mai 1998 relative aux actions en cessation en matière de protection des intérêts des consommateurs, JO 166, p. 51, consultable en ligne à l'adresse suivante : http://europa.eu.int/comm/consumers/policy/developments/acce_just/acce_just09_fr.pdf.

Initiatives engagées dans d'autres organisations internationales

Plusieurs autres organisations internationales telles que la Commission européenne (CE), l'Union internationale des télécommunications (UIT) et l'Organisation de coopération économique Asie-Pacifique (APEC) ont lancé des projets orientés vers l'action en vue de trouver des solutions au problème du spam, avec notamment des travaux consacrés aux activités d'application des lois.

Au sein de la Commission européenne, la Direction générale « Société de l'information » a constitué un Réseau de contact des autorités antispam dans le but d'améliorer la coopération et d'envisager des stratégies coordonnées en matière d'application (voir également page 25 ci-dessus). Les deux organismes d'application à la tête de ce groupe, la CNIL (autorité française de protection des données) et l'OPTA (autorité de régulation des communications des Pays-Bas) ont diffusé un questionnaire aux autres organismes d'application de l'UE, en demandant comment l'article 13 de la directive 2002/58/CE avait été mis en œuvre, s'il s'appliquait aux personnes physiques ou morales, quelle était l'autorité nationale compétente en la matière et quelles étaient les sanctions prévues par les législations nationales de chaque pays. De son côté, la Direction générale « Société de l'information » a étudié les questions précitées et a collecté des informations concernant : la question de savoir si les organismes d'application européens disposaient de ressources suffisantes pour enquêter et assurer le respect des dispositions législatives transposant la directive 2002/58/CE ; le suivi des boîtes de courriers électroniques spécialisées (boîtes à spam) ; la coopération entre les ministères et les mesures permettant d'éviter les chevauchements et les répétitions inutiles entre les différentes autorités chargées de l'application des lois ; les plaintes et la coopération transfrontières relatives à l'application des lois au sein de l'UE et la coopération avec des pays tiers.

L'Union internationale des télécommunications (UIT) a mené une série d'activités de lutte contre le spam pour favoriser la mise en place de cadres d'actions harmonisés, encourager la coopération internationale et apporter un soutien aux pays en développement dans ce domaine¹³. L'UIT a coopéré avec l'OCDE dans le but de rassembler des éléments pour sa base de données sur les législations antispam dans le monde entier et d'établir une liste des autorités d'application compétentes avec indication des coordonnées permettant de les contacter¹⁴. En outre, l'UIT a accueilli des conférences virtuelles au cours desquelles les représentants d'organismes d'application responsables en matière de lutte contre le spam ont examiné les principaux obstacles à une coopération internationale et ont envisagé des cadres possibles pour les surmonter. Elle gère sur son site Web des pages qui fournissent des informations actualisées sur des questions non confidentielles relatives à la politique en matière de spam, notamment l'application des lois et la coopération au niveau international.

Le Groupe directeur sur le commerce électronique de l'APEC¹⁵ a entrepris de faire rapport sur plusieurs points liés à l'application des lois dans son Programme de travail sur le spam. Tout d'abord, il a prévu de déterminer les moyens disponibles pour favoriser la coopération transfrontière afin de lutter contre les pratiques de spam trompeuses et frauduleuses, en renforçant la mise en œuvre des Lignes directrices de l'APEC pour la protection du consommateur. Les travaux dans ce domaine visent à établir des points de contact, encourager le partage d'informations entre représentants d'organismes de protection

13 Voir les pages du site Web de l'UIT consacrées aux initiatives de lutte contre le spam, accessibles en ligne à l'adresse suivante : www.itu.int/spam.

14 Voir la page Web concernant les autorités et législations antispam : <http://www.itu.int/osg/spu/spam/law.html>.

15 Groupe directeur sur le commerce électronique de l'Organisation de coopération économique Asie-Pacifique (APEC-ECSG), page en ligne à l'adresse suivante : http://www.apecsec.org.sg/content/apec/apec_groups/som_special_task_groups/electronic_commerce.html.

des consommateurs et d'autres organismes d'application des lois, accroître les compétences en matière d'enquêtes, et favoriser des transferts de plaintes/affaires appropriés entre pays membres de l'APEC. Deuxièmement, le Programme de travail sur le spam entend évaluer l'efficacité des mesures de lutte contre le spam en utilisant des éléments quantifiables.

Assistance du secteur privé

Le secteur privé a été extrêmement actif dans le domaine des actions en justice introduites contre les spammeurs, de même que dans la mise au point des meilleures pratiques et de recommandations techniques destinées aux fournisseurs d'accès à Internet et de services de courrier électronique, en particulier l'Alliance technique antispam (*Anti-Spam Technical Alliance* : ASTA) qui réunit Yahoo, Earthlink, Microsoft et AOL. En outre, les FAI, les bureaux d'enregistrement des noms de domaines, les opérateurs de téléphones portables et les associations professionnelles entretiennent avec les organismes d'application des lois des partenariats concernant la lutte contre le spam. Dans les réponses au questionnaire, l'exemple le plus fréquemment cité d'une assistance du secteur privé allant aux organismes d'application est la communication d'informations servant de preuves de l'activité illégale de spammeurs ou permettant de les identifier. Une autre forme d'aide du secteur privé souvent mentionnée est celle fournie par les dépositions de témoins dans le cadre de procédures judiciaires introduites contre des spammeurs. Dix des responsables interrogés ont fait savoir que les acteurs du secteur privé contribuaient aux enquêtes sur le spam en soumettant des informations volontairement, c'est-à-dire sans avoir l'obligation de le faire. Les fournisseurs de services Internet et de services de courrier électronique étant eux-mêmes affectés par le volume des messages que le spam les obligent à traiter, l'aide apportée aux organismes d'application aux fins d'enquêtes rejoint leurs propres intérêts. Les opérateurs du secteur privé ont aussi aidé ces organismes en supprimant les serveurs créés dans le seul but d'envoyer du spam. Comme les organismes d'application lorsqu'ils souhaitent partager des informations avec des homologues étrangers, les acteurs du secteur privé se heurtent eux aussi à des conditions et des restrictions limitant le partage de l'information avec ces organismes.

Les limites auxquelles les acteurs du secteur privé sont confrontés dans le partage des informations sont de nature à la fois pratique et juridique. En Belgique, par exemple, les FAI font valoir qu'ils ne peuvent communiquer certains renseignements demandés par les organismes d'application parce qu'ils ne tiennent pas un registre de leur trafic sur une période de plus de deux semaines. De même, les fournisseurs de services de courrier électronique gratuits affirment qu'ils ne peuvent communiquer d'informations utiles parce qu'ils ne contrôlent pas l'identité ou l'emplacement géographique des utilisateurs. Les limites et restrictions juridiques au partage des informations avec le secteur privé varient d'un pays à l'autre. La plupart des entités interrogées au sein de l'Union européenne ont fait savoir que les lois sur la protection des données restreignaient le partage volontaire de l'information concernant l'identité des abonnés et que les lois sur les télécommunications exigeaient que l'on considère comme secret le contenu des messages électroniques. Toutefois, ces restrictions juridiques n'empêchent pas l'ordonnance d'un tribunal de prendre effet ni un organisme d'application d'exercer son droit d'engager une procédure contraignante. Au Portugal, par exemple, le refus d'un FAI de communiquer des informations liées à une enquête officielle peut être sanctionné par une amende ou une peine d'emprisonnement. Aux États-Unis, la loi sur le caractère privé des communications électroniques limite le droit qu'ont ces fournisseurs d'accès de divulguer volontairement les informations contenues dans les courriers électroniques de leurs abonnés aux organismes d'application. À titre d'exception, les FAI peuvent révéler des informations en vertu d'un mandat de perquisition ou d'un ordre du tribunal ou avec le consentement de l'abonné. Toutefois, le partage de renseignements en réponse à un ordre d'exécution sous peine de sanctions délivré lors d'une affaire civile instruite par un organisme d'application est limité à l'information sur les abonnés ; le contenu d'un courrier électronique n'est pas accessible en pareilles circonstances. Concernant les destinataires des informations partagées, il est précisé dans la quasi-totalité des réponses que les membres des organismes d'application ont une obligation de confidentialité vis-à-vis de l'information reçue dans le cadre d'une

enquête, que la source soit un acteur du secteur privé ou non. Cette obligation peut limiter la manière dont cette information est utilisable et les entités avec lesquelles elle peut être partagée. En général, il a été indiqué que les organismes concernés ne pouvaient partager que les informations telles que les secrets d'affaires ou les renseignements personnels obtenus dans le cadre d'une enquête en exécution de leurs fonctions officielles.

De nombreux organismes d'application ont créé des boîtes à spam permanentes ou provisoires auxquelles ceux qui ont reçu des spams peuvent les transmettre à des fins de collectes d'informations, de recherches, d'analyses et, en dernier ressort, d'introduction d'une action en justice. Du simple fait du volume considérable de spams renvoyés à ces boîtes, il est peu commode de lire et de classer manuellement tous les messages. En conséquence, pour l'essentiel, les preuves que ceux-ci pourraient contenir n'ont pas servi à engager des poursuites. En Australie, le secteur privé a mis au point, à l'intention de l'Autorité australienne des communications (ACA), un instrument utile pour résoudre cette difficulté. Les abonnés à *Pacific Internet*, un FAI australien, peuvent désormais utiliser un dispositif immédiatement connectable, inventé par Spammers, pour notifier tout spam reçu à la base de données des services de police scientifique de l'ACA, d'un seul clic de souris. La base de données fait l'économie d'un traitement manuel du spam en extrayant automatiquement les informations du message, y compris l'en-tête et le corps du texte, ce qui permet de les utiliser comme pièce à conviction devant un tribunal australien.

Lors d'une téléconférence organisée dans le cadre de la coopération menée au titre du Plan d'action de Londres, les conseillers juridiques de Microsoft ont joué un rôle précieux de mentorat auprès des représentants d'organismes d'application participant à cette activité, en leur expliquant les méthodes d'enquête particulières utiles pour dépister les spammeurs. Microsoft a intenté avec succès des actions privées contre des spammeurs en Amérique du Nord et en Europe, qu'il avait identifiés en exploitant l'information contenue dans les messages électroniques et en remontant jusqu'à chacun des liens constitutifs de la chaîne des services dont un spammeur a besoin pour accomplir ses opérations, par exemple : un fournisseur de services électroniques, un administrateur de noms de domaines, une société d'hébergement de sites Web, un fournisseur d'accès à Internet, des vendeurs de listes d'adresses électroniques, des services de traitement des paiements, etc. Il est estimé que 80 % du spam électronique sont désormais envoyés par des ordinateurs piratés, avec pour résultat que certaines des sources précitées ne peuvent servir à dépister un spammeur en tant qu'entité indépendante de la source technique du message.

En plus de la contribution qu'il a apportée aux enquêtes, le secteur privé a joué un rôle actif dans la lutte contre le spam sur plusieurs fronts qui ne sont pas liés aux mesures d'application. Les associations professionnelles ont été particulièrement dynamiques au cours des consultations destinées à élaborer une législation antispam et à établir des lignes directrices sur l'autoréglementation des pratiques de commercialisation, qui recommandent de ne pas utiliser de spam. Le Groupe de travail contre les escroqueries par hameçonnage (*Anti-Phishing Working Group* : APWG) est une association professionnelle qui cherche surtout à combattre le vol d'identités et les fraudes résultant du problème croissant des escroqueries par hameçonnage et des arnaques par voie de courrier électronique. Les attaques à coups d'hameçonnages ont recours à des courriels trafiqués et à des sites Web frauduleux pour tromper les destinataires en les incitant à divulguer des données financières personnelles telles que les numéros de cartes de crédit, les noms des titulaires de comptes bancaire, les mots de passe, etc. En piratant les marques fiables d'établissements bien connus — banques, détaillants en ligne, sociétés de cartes de crédit — les arnaqueurs parviennent à persuader jusqu'à 5 % des destinataires de répondre à leurs messages. Enfin, des organisations privées telles que Spamsquad en Belgique et le « Forum Internet convivial » (*Barátságos Internet Fórum* : BIF) en Hongrie ont activement travaillé à l'éducation des consommateurs concernant les moyens de se protéger du spam et de porter plainte auprès des organismes d'application.

Les partenariats public/privé visant à lutter contre le spam fonctionnent dans les deux sens, c'est-à-dire pas uniquement au bénéfice des organismes d'application publics ou dans l'intérêt du public. Les entités interrogées ont cité des exemples de politiques destinées à inciter le secteur privé à partager les informations avec ces organismes. En Australie, les FAI et les opérateurs qui communiquent des informations par suite de l'exercice par l'ACA de pouvoirs contraignants ne sont pas responsables des dommages pouvant résulter d'une réponse positive donnée à une demande d'information. Les organismes d'application apportent aussi une aide directe aux acteurs privés qui ont engagé des poursuites contre des spammeurs. En France, la CNIL (autorité de protection des données) a communiqué à des sociétés poursuivant des spammeurs à titre privé les plaintes d'autres utilisateurs afin qu'elles puissent renforcer leurs arguments contre les auteurs d'infractions, et a même témoigné devant les tribunaux dans le cadre d'actions judiciaires privées. Les données personnelles contenues dans les messages que les utilisateurs ont retransmis à la CNIL ont été effacées avant que les messages soient communiqués aux demandeurs privés.

VI. Conclusions

Les résultats obtenus avec le questionnaire montrent que si les responsables des orientations politiques ont reconnu dans le spam un problème crucial d'envergure mondiale qui nécessite une action internationale concertée, d'importantes mesures sont encore requises pour que l'application nationale et transfrontière des lois soit efficace. Les paragraphes suivants essaient de cerner les caractéristiques de la situation actuelle que les gouvernements souhaiteront peut-être examiner lorsqu'ils reprendront leurs travaux collectifs destinés à faciliter l'application des lois antispam de part et d'autre des frontières.

Le spam reste une activité rentable

Des chiffres récents indiquent que le volume global du courrier électronique commercial non sollicité est encore considérable. De plus, le spam revêt des formes nouvelles et plus nocives, devenant un vecteur pour la diffusion de la fraude — par exemple, les attaques par hameçonnage — et des virus. Les raisons de cette situation peuvent être diverses, mais englobent probablement les problèmes rencontrés dans l'application nationale et transfrontière des lois antispam au sens large. L'introduction d'un plus grand nombre d'actions contre les spammeurs et des décisions infligeant des amendes et des sanctions plus lourdes pour les violations les plus flagrantes contribueront à rendre le spam moins lucratif. Toutefois, la levée des obstacles à l'application nationale et transfrontière des lois antispam est indispensable pour atteindre l'objectif plus général d'une réduction du spam.

Croissance des activités d'application des lois antispam

La plupart des pays de l'OCDE se sont montrés actifs dans la lutte contre le spam et les responsables des orientations politiques reconnaissent que les mesures d'application sont une priorité. Le nombre de lois antispam a augmenté et les organismes d'application dans plusieurs pays ont engagé des actions dans ce domaine. Des initiatives auxquelles participent différents acteurs ont déjà été prises pour améliorer la coopération en matière d'application des lois. Par exemple, un réseau non officiel d'autorités a été créé dans le cadre du Plan d'action de Londres, l'Union européenne a établi un protocole d'application et plusieurs pays ont conclu des protocoles d'accord. Grâce à ces efforts, l'échange d'informations et des pratiques jugées les meilleures a déjà commencé. Le travail d'application semble toutefois fragmenté et d'autres actions coordonnées sont nécessaires pour combattre un phénomène qui se développe et revêt des formes de plus en plus dangereuses.

Problème posé par les lacunes juridictionnelles et la diversité des cadres nationaux d'application des lois

Il n'existe pas un seul ensemble de règles pour combattre le spam mais une mosaïque composée de divers éléments tels que les lois sur la protection des consommateurs, le droit pénal, les lois sur la protection des données et les lois sur les télécommunications. En ce qui concerne les procédures d'instruction des plaintes, seuls quelques organismes d'application permettent que les pourriels leur soient transmis par voie électronique ou fournissent un formulaire de plainte en ligne. Bien que les informations communiquées par les courriers électroniques envoyés aux boîtes à spam orientent de manière constructive l'action des autorités chargées de la lutte antispam et contribuent aux enquêtes concernant les spammeurs, les ressources consacrées à la création et au maintien de ces boîtes sont parfois trop modestes. Les sanctions et voies de recours actuelles ne suffisent pas toujours à décourager les spammeurs, que ce soit sur le plan national ou international. Enfin, les critères appliqués à la compétence judiciaire varient d'un pays à l'autre et les organismes d'exécution se heurtent à des restrictions lorsqu'il s'agit de tenir les spammeurs responsables de leurs activités illégales : par exemple lorsque le spammeur est physiquement présent sur leur territoire mais que le spam est envoyé à l'étranger ou, inversement, lorsque le dommage est causé à des particuliers, des entreprises ou des FAI sur leur territoire et que le spammeur est situé à l'étranger.

La coordination nationale devrait jouir de la plus haute priorité

De multiples autorités sont chargées des enquêtes et/ou de l'application des différentes lois pouvant être enfreintes par les spammeurs et, dans la plupart des cas, ne prennent pas de mesures coordonnées pour exploiter pleinement les synergies, les moyens d'action et les ressources disponibles. Certains pays ont déjà adopté un cadre de coordination. Par exemple, en Australie, quatre organismes ont convenu de coopérer sur les questions relatives au spam. Les États-Unis ont un point de contact central pour faciliter la communication entre organismes responsables de la lutte antispam au niveau fédéral et au niveau des États. D'autres pays auraient aussi besoin de prendre de nouvelles mesures pour renforcer la coopération nationale entre organismes, et la désignation d'un seul organisme comme point de contact pour les autorités étrangères faciliterait la coopération transfrontière.

L'efficacité des mesures d'application transfrontières contre le spam passe par une stratégie mondiale

Si la coordination nationale est une condition préalable à la coordination internationale, les mesures d'application au-delà des frontières tireraient profit de la mise en œuvre d'une stratégie mondiale visant à résoudre certains problèmes rencontrés dans la collecte et le partage des informations, la définition des priorités en matière d'application et la mise en place d'un cadre d'application international efficace.

Des mécanismes appropriés pour la collecte et le partage des informations sont nécessaires pour que les organismes d'application puissent mener des enquêtes, obtenir et préserver des renseignements et des preuves et les partager avec des homologues étrangers lorsque les circonstances s'y prêtent. Il se peut que la coopération transfrontière ait le plus de chances de succès lorsque les autorités du pays d'origine répondent à une demande d'une autorité dans un pays destinataire, parce que les autorités dans le pays où le spammeur est installé sont généralement mieux à même d'identifier la personne derrière un compte à partir duquel le spam a été envoyé. Si tel est le cas, les organismes d'application dans les pays où le spam est reçu devraient s'efforcer de localiser les spammeurs et fournir des preuves permettant à l'autorité dans le pays d'origine du spam d'exercer ses pouvoirs et, par exemple, d'exiger la communication d'informations.

Comme on ne peut attendre d'aucun pays qu'il mène des enquêtes et prenne des mesures en réponse à chaque demande émanant d'une autorité étrangère, il conviendrait peut-être d'établir des priorités concernant les types de plaintes qui se prêtent le mieux à une coopération internationale. Il existe

différentes manières de légiférer contre le spam, en particulier l'option d'acceptation (*opt-in*) ou l'option de refus (*opt-out*) mais, en vertu de la plupart des mécanismes juridiques actuels, un large volume de spam est considéré comme illégal. Le véritable défi à relever est de pouvoir progresser vers une stratégie commune accordant la priorité aux cas méritant le plus que soient déployés les efforts considérables exigés pour introduire une action lors d'affaires transfrontières.

Enfin, il serait utile de poursuivre l'examen des meilleures façons possibles de mettre en place des structures et des dispositifs efficaces en vue de la coopération internationale. À cet égard, la gamme des options est particulièrement large : nouveaux cadres non officiels tels que les protocoles d'accord bilatéraux, les protocoles multilatéraux ou modèles, réseaux tels que celui du Plan d'action de Londres, structures officielles telles que les Lignes directrices de l'OCDE sur la fraude transfrontière, ou instruments juridiques contraignants tels que la Convention internationale sur la cybercriminalité adoptée par le Conseil de l'Europe. Si les cadres non officiels améliorent réellement la communication et la collaboration au niveau opérationnel, un cadre officiel serait peut-être plus approprié à l'avenir pour la création d'un mécanisme d'application mondial commun stable et efficace. Ce cadre n'aurait pas besoin de couvrir tous les aspects du domaine, mais constituerait la base d'accords nouveaux ou élargis entre acteurs intéressés et une plate-forme pour les différentes initiatives actuellement prévues ou en voie d'élaboration.

Stratégie mondiale : l'objectif à retenir

L'un des principaux risques qui freinent une application efficace des lois antispam est la facilité avec laquelle les spammeurs peuvent mettre en place leurs opérations et se déplacer vers des juridictions où il n'y a pas de législation antispam, où les capacités d'application sont insuffisantes et où la coopération internationale est encombrée de conditions. Ces juridictions sont peut-être le maillon le plus faible de la chaîne. Afin d'empêcher la création de paradis pour les spammeurs, les efforts visant à renforcer la capacité de prendre des mesures à leur égard devraient s'étendre de façon à former la coalition la plus large possible réunissant les organismes d'application partout dans le monde.

ANNEXE A

QUESTIONNAIRE DE L'OCDE SUR L'APPLICATION TRANSFRONTIÈRE DES LOIS ANTISPAM

L'amélioration de la coopération transfrontière en matière d'application des lois occupe une place centrale dans le plan de travail de l'OCDE relatif au pollupostage (ou spam) [DSTI/CP/ICCP/SPAM(2004)1]. Ce plan de travail prévoit notamment la réalisation d'une enquête sur les problèmes d'application de la législation, pour approfondir l'enquête déjà effectuée par l'OCDE sur la législation antispam dans les pays membres. Le présent questionnaire constitue un instrument important pour comprendre le cadre actuel d'application de la législation dans les pays membres et pour résoudre les principales difficultés faisant obstacle à l'amélioration de la coopération transfrontière en ce domaine.

L'enquête de l'OCDE sur la législation relative au spam, qui a figuré dans le document de référence établi pour l'atelier que l'OCDE a consacré à la question, révèle un manque d'uniformité. Certains pays se sont en effet attaqués au problème en adoptant une législation antispam spécifique, tandis que d'autres ont recours aux lois en vigueur (par exemple, en matière de protection des consommateurs, de protection des données et de droit pénal) pour discipliner une activité qui, accessoirement, emploie le spam à des fins illégales.

Dans les pays qui se sont donné une législation destinée expressément à lutter contre le spam, on a en général désigné un organisme public comme responsable au premier chef de l'application de la législation. En revanche, dans les pays où plusieurs textes réglementent les activités qui sont menées à l'aide du spam, diverses instances peuvent être appelées à intervenir. Dans l'un et l'autre cas, il se peut que des organismes différents soient chargés de recevoir les plaintes de destinataires de spam, d'effectuer les enquêtes nécessaires, et de transmettre le dossier au ministère public ou d'engager des poursuites.

L'enchevêtrement complexe de cadres et d'organismes juridiques intervenant dans les enquêtes et dans l'application des lois concernant le spam pose des problèmes particuliers du point de vue transfrontière. Le questionnaire ci-après vise à résoudre ce problème en sollicitant des renseignements qui permettront de mettre en évidence les possibilités et les limites d'une application transfrontière efficace. Ce questionnaire a donc pour but :

- De recenser, parmi les dispositions juridiques nationales, celles qui se prêtent le mieux à une coopération internationale en matière d'application.
- D'identifier les points de contact nationaux pour la coopération internationale antispam.
- De solliciter des renseignements concernant les pouvoirs (et leurs limites) des organismes chargés de veiller à l'application des lois relatives au spam en ce qui concerne les enquêtes à mener à la suite de plaintes et les mesures d'exécution au niveau national aussi bien que transfrontière.

Instructions

Dans les questions qui suivent, le terme « organisme d'application des lois » désigne à la fois les organismes ou autorités publics et les organismes financés sur fonds publics qui remplissent un rôle d'application des dispositions antispam au niveau national. Ce rôle d'application peut englober l'une ou l'autre des trois fonctions suivantes : réception des plaintes, réalisation d'enquêtes, engagement de poursuites. S'il existe plus d'un organisme, veuillez répondre séparément pour chacun. Des informations supplémentaires peuvent être transmises dans une annexe si elles sont jugées utiles (par exemple, des informations relatives au contenu des plaintes). Bien que le questionnaire vise principalement les organismes d'application des lois, le secteur privé doit être consulté le cas échéant, ainsi que d'autres organisations non gouvernementales jouant un rôle dans l'application des lois antispam.

Les réponses seront analysées et constitueront la base d'un rapport qui sera présenté aux réunions de l'OCDE en octobre. Les réponses proprement dites ne seront pas rendues publiques. Une note sera envoyée aux délégations permanentes et aux délégués auprès du Comité PIIC, du Comité de la politique à l'égard des consommateurs, du GTSIVP et du GTPTSI lorsque le questionnaire sera envoyé, afin d'aider les pays membres à coordonner leurs réponses. Nous vous saurions gré de nous faire parvenir vos réponses au plus tard le **20 août 2004**, aux adresses électroniques suivantes : anne.carblanc@oecd.org et michael.donohue@oecd.org.

PAYS :

Section I : Description du cadre national d'application des lois

A. Autorité

Existe-t-il dans votre pays une loi antispam spécifique ? (Si oui, notez l'URL s.v.p.)

Dans l'affirmative, quels sont les organismes chargés de son application ? (notez l'URL s.v.p.)

Dans la négative, quels organismes d'application des lois ont engagé des poursuites contre des polluposteurs (« spammeurs ») en vertu d'autres lois, ou sont habilités à le faire ? (par exemple, organismes chargés de l'application de la loi sur la protection des consommateurs, de la loi sur la protection des données ou de la législation sur les télécommunications).

Indiquez si les organismes mentionnés dans les réponses aux questions 2 et 3 sont compétents en matière civile, pénale, administrative ou une combinaison des trois.

De quelle façon les organismes d'application reçoivent-ils les plaintes de destinataires de spam ? (par exemple, courrier électronique, formulaire en ligne, téléphone). Les organismes d'application doivent-ils lancer une enquête pour chaque plainte qu'ils reçoivent, et poursuivre en justice chaque instance portée à leur attention ?

S'il y a plus d'un organisme d'application, y a-t-il un protocole ou un système d'organisation pour échanger les dossiers des plaintes entre les organismes ?

Quels sont les principaux pouvoirs d'enquête dévolus à chaque organisme ? (par exemple, peut-il demander que la preuve soit fournie sur une base volontaire ? introduire une procédure obligatoire ? solliciter auprès d'un tribunal un mandat ou une citation à comparaître ?)

Comment chaque organisme engage-t-il la procédure contre un polluposteur ? (par exemple, peut-il engager directement une poursuite civile ou pénale ? introduire une procédure administrative ? ou référer l'affaire au ministère public ?)

B. Sanctions, moyens de recours et résultats

De quels moyens de recours ou sanctions chaque organisme d'application peut-il user ? (par exemple, ordonnances ou interdictions, sanctions civiles, amendes pénales, emprisonnement, restitution des gains mal acquis, réparation financière du préjudice causé aux destinataires de spam)

Combien de procédures liées au spam ont été engagées par chaque organisme d'application ? (Si possible, indiquer le nombre de procédures administratives, civiles et pénales). Veuillez fournir toute information aisément accessible sur l'issue des procédures qui ont été menées à leur terme.

Certaines de ces procédures ont-elles pu être réglées hors cour ? Dans l'affirmative, combien ?

Si la sanction ou la voie de droit appliquée n'est pas suivie d'effet par le polluposteur, de quels autres moyens l'organisme d'application dispose-t-il ?

C. Assistance du secteur privé

Comment le secteur privé prête-t-il son concours aux organismes chargés de l'application des lois antispam ? (par exemple, collecte de preuves, témoignage au tribunal ou déclaration écrite sous serment ?)

Quelles limites, au niveau légal ou pratique, empêchent les fournisseurs d'accès à Internet (FAI) et d'autres membres du secteur privé, de fournir aux organismes d'application de la loi des preuves concernant le spam ? Y a-t-il des lois ou des politiques pour encourager le secteur privé à partager des informations (par exemple, indemnité pour les FAI ?)

À quelles conditions, les informations que le secteur privé partage avec l'organisme d'application sont-elles traitées de manière confidentielle ? Si un tel traitement existe, comment varie-t-il selon les informations ou documents partagés par le secteur privé ?

Section II : Aspects transfrontières de l'application des lois antisпам

D. Obstacles à l'application transfrontière

Chaque organisme d'application peut-il engager des poursuites contre des polluposteurs étrangers visant des utilisateurs du courrier électronique dans le pays de l'organisme ? Dans l'affirmative, dans quelles conditions ?

Chaque organisme d'application peut-il engager des poursuites contre un polluposteur de son pays visant un utilisateur de courrier électronique étranger ? Dans l'affirmative, dans quelles conditions ?

Chaque organisme d'application peut-il notifier aux autorités d'autres pays des enquêtes liées au spam qui les concernent ?

Chaque organisme d'application peut-il partager des informations avec un organisme d'application étranger ou lui fournir une autre forme d'aide dans une enquête ? Dans l'affirmative, dans quelles circonstances ? (par exemple, le courriel concerné doit-il revêtir un caractère illégal dans les deux pays pour que l'information puisse être mise en commun ?)

Selon vos estimations ou constatations, quel est le principal obstacle à une coopération transfrontière efficace ?

E. Dispositions actuelles en matière de coopération internationale

Votre pays ou les organismes d'application de votre pays ont-ils conclu des accords bilatéraux ou multilatéraux avec d'autres pays ou organismes en vue de coopérer pour l'application des lois destinées à lutter contre les polluposteurs ? Dans l'affirmative, veuillez fournir des copies des textes pertinents (par exemple les lois, règles ou politiques).

Votre pays applique-t-il des dispositions susceptibles de faciliter la reconnaissance et l'application de jugements rendus dans des affaires de pollupostage par des tribunaux étrangers ? Dans l'affirmative, veuillez fournir des copies des textes pertinents.

F. Point de contact national pour l'application des lois antisпам

Existe-t-il dans votre pays un organisme d'application qui pourrait être désigné comme point unique de contact afin de faciliter la coopération en matière d'application de lois antisпам avec les organismes étrangers ? Dans l'affirmative, veuillez fournir le nom et les coordonnées de l'organisme.

G. Priorités en matière de coopération transfrontière

Quels types de plaintes relatives au pollupostage devraient être prioritaires pour la coopération transfrontière en matière d'application des lois ou s'y prêteraient le mieux ? (selon qu'elles concernent par exemple un spam trompeur, frauduleux ou vecteur de virus, ou un courriel commercial non sollicité ?)

Existe-t-il un organisme responsable principal pour les questions relatives aux politiques concernant le spam ? Dans l'affirmative, veuillez indiquer le nom et les coordonnées de l'organisme.

ANNEXE B

OCDE : TABLEAU DES POURSUITES ENGAGÉES

I : POURSUITES ENGAGÉES EN VERTU D'UNE LÉGISLATION ANTISPAM SPÉCIFIQUE

	Affaire	Résumé	Lois en vertu desquelles l'action a été intentée	Résultat/État actuel	Éléments transfrontières	Coopération obtenue
Danemark	Organisme national de protection des consommateurs c. Fonn Danmark www.siliconvalley.com/mlid/siliconvalley/5762085.htm	Après avoir reçu 50 plaintes, l'Ombudsman chargé de la protection des consommateurs a intenté une action contre une entreprise danoise de logiciels qui avait envoyé 156 courriels commerciaux non sollicités.	Loi sur les pratiques de commercialisation	Le Tribunal maritime et commercial de Copenhague a infligé à Fonn une amende de DKK 13 000 (environ USD 2 200)	Inconnus	
Japon	MIC c. (non divulgué) www.soumu.go.jp/joho_tsusin/eng/Releases/Telecommunications/news031113_1.html http://www.soumu.go.jp/s-news/2003/031113_2.html	Le MIC (organisme de télécommunications) a délivré à une entreprise assurant des services de rendez-vous, établie à Nakano-ku (Tokyo), qui avait envoyé des spams par téléphones mobiles, l'ordre de se conformer aux lois. L'ordre exigeait que l'entreprise fasse savoir aux destinataires que le message électronique était non sollicité et qu'elle fournisse des informations quant à l'expéditeur.	Loi réglementant la transmission de courriels spécifiques	Délivrance d'une ordonnance administrative		Néant
Japon	MIC c. SIS World www.soumu.go.jp/joho_tsusin/eng/Releases/Telecommunications/news040416_3.html www.soumu.go.jp/s-news/2004/040416_2.html	Le MIC a donné ordre de se conformer aux lois à une entreprise assurant des services de rendez-vous, établie à Shinjuku-ku, Tokyo, qui avait envoyé des spams mobiles. L'ordre exigeait que l'entreprise fasse savoir aux destinataires que le message électronique était non sollicité et qu'elle fournisse des informations quant à l'expéditeur.	Loi réglementant la transmission de courriels spécifiques	Délivrance d'une ordonnance administrative		Néant

Affaire	Résumé	Lois en vertu desquelles l'action a été intentée	Résultat/État actuel	Éléments transfrontières	Coopération obtenue
<p>FTC c. Creaghan www.ftc.gov/os/caselist/0423085/0423085.htm</p>	<p>La FTC a reçu 40 000 plaintes de consommateurs concernant des spams provenant du défendeur et de ses sites Web qui vendaient des produits factices contre le vieillissement. Le défendeur exploitait les sites Web au moyen de noms d'emprunt et d'adresses étrangères et dissimulait la source des courriels en falsifiant les adresses de retour dans le champ « Expéditeur » et en envoyant les messages par l'intermédiaire de serveurs mandataires ouverts.</p>	<p>Loi CAN-SPAM et Section 5, Loi sur la FTC</p>	<p>Un juge fédéral a émis un ordre temporaire interdisant le spam, les prétentions frauduleuses concernant les produits, et gelant les actifs du défendeur. Les faits de la cause n'ont pas encore été soumis à un tribunal.</p>	<p>Le défendeur réside en Floride et déclare que son entreprise est située au Canada, en Suède et en Suisse. Les produits sont vendus sur ses sites Web avec des noms de domaines enregistrés pour le compte d'individus en Chine. Le produit des ventes est transféré électroniquement à une banque lettone.</p>	<p>Inconnue</p>
<p>FTC c. Phoenix Avatar LLC www.ftc.gov/os/caselist/0423084/040429phoenixavatairme.no.pdf www.usdoj.gov/opa/pr/2004/April/04_cr_m_281.htm</p>	<p>Les consommateurs ont transmis plus de 490 000 courriels à la FTC concernant des produits frauduleux : patches pour perte de poids et pilules pour l'agrandissement du pénis. Les courriels donnaient de fausses adresses pour l'expéditeur, sans offrir la possibilité claire et évidente de refuser la réception de messages ultérieurs, ou sans donner une adresse physique valide.</p>	<p>Loi CAN-SPAM</p>	<p>Un juge fédéral a émis un ordre temporaire interdisant le spam, les prétentions frauduleuses concernant les produits, et gelant les actifs du défendeur. La mise en accusation est en instance.</p>	<p>Inconnus</p>	<p>Le Département de la justice — qui intente une action pénale séparée contre les défendeurs —, les FAI et les Services postaux des États-Unis ont contribué à l'enquête en suivant à la trace les documents résultant de l'enregistrement des sites Web au moyen desquels les produits étaient vendus.</p>

États-Unis

DSTI/CP/ICCP/SPAM(2004)3/FINAL

	Affaire	Résumé	Lois en vertu desquelles l'action a été intentée	Résultat/État actuel	Éléments transfrontières	Coopération obtenue
<p align="center">États-Unis</p>	<p>FTC c. Bryant and Bryant www.ftc.gov/os/caselist/0423125/041005gbacmp.pdf</p>	<p>Les défendeurs ont envoyé des spams trompeurs en prétendant dans leur message que les destinataires pouvaient gagner des sommes considérables en exerçant une activité commerciale avec une « garantie satisfait ou remboursé » ; le travail consistait à remplir des enveloppes à domicile. Les défendeurs demandaient des frais d'inscription de USD 25 et USD 25 pour un kit qui ne comprenait pas les enveloppes à remplir mais deux pages d'instructions et un CD-ROM expliquant comment commettre la même escroquerie. Les messages électroniques contenaient de faux en-têtes et adresses de retour.</p>	<p>Loi CAN-SPAM; 5 Loi sur la FTC et §45 a) du Règlement sur les ventes par telemarketing</p>	<p>Un juge fédéral a émis un ordre gelant les actifs des défendeurs et un autre ordre temporaire interdisant la poursuite des ventes et de l'expédition des produits. L'action, qui est actuellement en instance devant un tribunal civil, vise à obtenir un ordre permanent et une réparation pour les consommateurs.</p>	<p>Inconnus</p>	<p>Inconnue</p>
	<p>FTC c. Global Web Productions www.ftc.gov/os/caselist/0423086/040428globalwebmemosupporting.pdf</p>	<p>Les consommateurs ont retransmis à la FTC près de 400 000 courriels concernant des produits frauduleux : patches pour la perte de poids et pulvérisation antiviellissement.</p>	<p>Loi CAN-SPAM</p>	<p>Un juge fédéral a émis un ordre temporaire interdisant la poursuite des ventes et de l'expédition des produits.</p>	<p>Les défendeurs résident en Australie et en Nouvelle-Zélande, Global Web étant établi en Australie. Les sites Web servant normalement aux ventes changent de bureau d'enregistrement entre le Japon ; la Malaisie ; Hong-Kong, Chine et Singapour.</p>	<p>L'action a été introduite avec l'aide de la Commission australienne de la concurrence et de la Commission néo-zélandaise du commerce.</p>

	Affaire	Résumé	Lois en vertu desquelles l'action a été intentée	Résultat/État actuel	Éléments transfrontières	Coopération obtenue
États-Unis	United States c. Nicholas Tombros www.securityfocus.com/news/9606	Le défendeur circulait en voiture dans une banlieue avec un ordinateur portable et une antenne Wi-fi dépliant les points d'accès résidentiels non sécurisés, dont il se servait ensuite pour envoyer des milliers de messages concernant des sites pornographiques. Tombros a été inculpé en vertu d'une disposition de la loi CAN-SPAM qui interdit à quelqu'un de pirater l'ordinateur de quelqu'un d'autre afin d'envoyer du spam.	Loi CAN-SPAM	Le défendeur a conclu un arrangement devant le tribunal et sera condamné en décembre 2004. Un délinquant primaire risque jusqu'à un an de prison dans un établissement fédéral pour une opération de courte durée et jusqu'à trois ans en cas d'infraction à l'une des règles minimales de bonne conduite, par exemple en dirigeant une bande de spammeurs d'au moins trois personnes, en envoyant plus de 2 500 messages en une journée ou en utilisant 10 noms de domaines, ou plus, frauduleusement enregistrés.	Inconnus	Inconnue
États-Unis	United States c. Smathers and Dunaway http://newpaper.asi1.com.sg/top/story/0,4136,66784-1096646340,00.htm	Les défendeurs sont accusés d'entente délictueuse visant à voler les données de 30 millions d'abonnés d'AOL et quelque 92 millions d'adresses électroniques. Dunaway a acheté la liste des adresses à Smathers, un employé d'AOL, et l'a revendue USD 52 000 à des spammeurs. Dunaway a ensuite acheté USD 100 000 une version mise à jour de la liste qu'il a aussi revendue.	Loi CAN-SPAM	Les prévenus risquent chacun une peine maximale de cinq ans d'emprisonnement et une amende de USD 250 000 ou deux fois le gain ou la perte résultant de l'infraction.	Inconnus	Inconnue
États-Unis	United States c. Chung, Sadek, Lin and Lin (Phoenix Avatar LLC) www.usdoj.gov/opa/pr/2004/April/04_cr_m_281.htm	Quatre hommes ont été inculpés (dont deux ont été arrêtés) pour avoir envoyé des milliers de messages électroniques commerciaux faisant la publicité de patchs diététiques et autres artifices, en utilisant des en-têtes faux ou frauduleux pour dissimuler leurs identités. Ils sont soupçonnés d'avoir envoyé des centaines de milliers de messages faisant la publicité de médicaments et autres produits.	Loi CAN-SPAM et loi sur la fraude par voie postale	En instance. La loi CAN-SPAM prévoit une peine de trois à cinq ans d'emprisonnement. Les infractions à la loi sur la fraude par voie postale sont punies d'une peine allant jusqu'à 20 ans d'emprisonnement.	Inconnus	La FTC – qui a intenté une action civile séparée contre les défendeurs – les FAI et les Services postaux des États-Unis ont contribué à l'enquête en suivant à la trace les documents d'enregistrement des sites Web servant à vendre les produits.

DSTI/CP/ICCP/SPAM(2004)3/FINAL

Affaire	Résumé	Lois en vertu desquelles l'action a été intentée	Résultat/État actuel	Éléments transfrontières	Coopération obtenue
	<p>La plainte affirme aussi qu'ils avaient mis au point un système pour escroquer d'autres personnes en vendant ces artifices médicaux par la poste des États-Unis au moyen de déclarations fausses et frauduleuses.</p>				

II : POURSUITES ENGAGÉES EN VERTU DU DROIT COMMUN

	Action	Résumé	Lois en vertu desquelles l'action a été intentée	Résultat/État actuel	Éléments transfrontières	Coopération obtenue
Australie	ASIC c. Hourmouzis www.internetnews.com/bus-news/article.php/499241	La Commission australienne des valeurs mobilières et des investissements a inculpé le défendeur pour avoir interrompu l'utilisation licite d'ordinateurs serveurs de fichiers et avoir fait une déclaration fautive ou trompeuse de nature à inciter à acheter des valeurs mobilières. Le défendeur a envoyé plus de 4 millions de courriels à des conseils de discussion, prétendant que certaines valeurs atteindraient USD 3 ou plus. Par la suite, le prix a doublé avec un volume de transactions plus de 10 fois supérieur à la moyenne du mois précédent. Le défendeur aurait aussi vendu ses actions le premier jour ouvrable après les divulgations, réalisant un bénéfice de USD 17 000.	Règlements sur les valeurs mobilières	Le défendeur a plaidé coupable et a été condamné à deux ans d'emprisonnement. La Commission fédérale des opérations de bourse a engagé sa propre procédure contre le prévenu et obtenu un jugement l'obligeant à restituer des profits mal acquis pour un montant de USD 15 000.	Le résident en Australie a envoyé des courriers électroniques à des adresses aux États-Unis, en Australie et dans d'autres régions du monde, après avoir acheté 65 000 actions de Rentech par l'intermédiaire d'une maison de courtage au Canada.	Inconnue
	People c. Marinellis www.news.com.au/comm/story_page/0,4057,7726290%255E15306,00.html	Le défendeur se livrait à une escroquerie « 419 », demandant le paiement d'un montant initial en envoyant des messages électroniques pour persuader les gens qu'ils pouvaient réclamer des millions de dollars provenant de gains de loterie, d'un héritage ou d'une activité commerciale s'ils commençaient par envoyer des fonds pour « frais ». Il a recueilli ainsi un total de USD 5 millions que lui ont envoyés les victimes de son escroquerie depuis toutes les régions du monde.	17 chefs d'accusation dont cinq au pénal ont été retenus pour entente illicite avec d'autres personnes visant à tromper et à escroquer les victimes.	En instance	Le défendeur prétend servir de point de contact en Australie à une organisation comprenant 220 opérateurs à travers le monde.	Inconnue
Canada	Intitulé du procès inconnu http://p2bnet.net/story/1546	Un adolescent soupçonné d'avoir piraté des milliers d'ordinateurs a été inculpé d'actes délictueux et d'utilisation frauduleuse d'un ordinateur en contaminant d'autres ordinateurs avec le virus « Trojan » les obligeant à envoyer en même temps des milliers de messages qui avaient pour but de provoquer l'effondrement du système destinataire.	Droit pénal	En instance	Inconnus	Inconnue

	Action	Résumé	Lois en vertu desquelles l'action a été intentée	Résultat/État actuel	Éléments transfrontières	Coopération obtenue
Chine	<p>People c. Jianquan and Wenqui</p> <p>http://latelinews.com/ll/english/1311289.shtml</p>	<p>Les défendeurs avaient utilisé des messages texte transmis par téléphone pour escroquer des abonnés en leur disant qu'ils avaient gagné de l'argent à des loteries. Ils prétendaient que les destinataires pouvaient encaisser leurs gains en effectuant sur des comptes en banque désignés des versements au titre de l'impôt sur les loteries. Plus de 50 affaires analogues ont abouti à la condamnation de 65 personnes l'année dernière.</p>	<p>Droit pénal</p>	<p>Un tribunal de la province de Fujan a condamné un homme à huit ans d'emprisonnement pour avoir obtenu illicitement USD 16 000. Un deuxième a été condamné à quatre ans de prison pour gains illicites de USD 6 000.</p>	<p>Inconnus</p>	<p>Inconnue</p>
	<p>Procureur de la République (TGI de Mans) c. L</p> <p>www.legalis.net/inet/d/decisions/diffamation/tg_i_mans_071103.pdf</p>	<p>Un ancien employé d'une entreprise pharmaceutique avait falsifié l'adresse de l'expéditeur dans 700 000 messages non sollicités qu'il a envoyés pour harceler son ancien employeur. La saturation ainsi causée de la boîte d'entrée des messages a constitué une intrusion illicite dans le système d'information de l'entreprise.</p>	<p>Droit pénal [Code pénal 462-2 et 3].</p>	<p>Le Tribunal de grande instance de Mans a condamné le prévenu à 10 mois de prison avec sursis et à deux ans de mise à l'épreuve.</p>	<p>Inconnus</p>	<p>Inconnue</p>
France	<p>Procureur de la République (TGI de Paris) c. M.R.G.V.</p> <p>www.juriscor.net/ipt/visu.php?ID=533</p>	<p>Le prévenu avait acquis un CD-ROM contenant 50 000 adresses électroniques qu'il a utilisées pour envoyer du spam comportant un lien avec un site pornographique. Un destinataire a déposé plainte auprès du tribunal.</p>	<p>Droit pénal [Code pénal Article 226-16].</p>	<p>Le prévenu a été jugé coupable d'avoir traité électroniquement des données personnelles sans notification préalable à l'autorité compétente (la CNIL) et a été condamné à une amende de EUR 3 000. Le tribunal n'a toutefois pas retenu l'accusation selon laquelle il aurait recueilli illégalement des données personnelles, invoquant le fait que la simple possession d'un CD-ROM contenant ce genre de données ne constitue pas une collecte de données.</p>	<p>Inconnus</p>	<p>Inconnue</p>

	Action	Résumé	Lois en vertu desquelles l'action a été intentée	Résultat/État actuel	Éléments transfrontières	Coopération obtenue
France	TGI (Draguignan) c. Dinant Pas de lien Web connu	Un homme a été condamné pour avoir bloqué le fonctionnement d'un système d'information automatisé et recueilli illégalement des données personnelles au moyen d'un programme destiné à capter des adresses auprès d'un fournisseur d'accès. Le prévenu avait perturbé les serveurs de Wanadoo en lançant 23 millions d'attaques individuelles destinées à copier des adresses électroniques.	Code pénal 25-78-17, 226-18-1 et 226-31		Inconnus	Inconnue
France	CNIL c. Alliance Bureautique Service www.cnil.fr/fileadmin/documents/approfondir/deliberations/002-075a.pdf	La CNIL a reçu d'utilisateurs des services de courrier électronique 650 avis faisant état de messages commerciaux non sollicités reçus d'Alliance Bureautique Service accusée d'avoir utilisé un « robot-mail » dans le but de recueillir des adresses électroniques de destinataires, instrument qu'elle propose elle-même à la vente. Ce genre d'instrument est illégal selon la loi française sur la protection des données. En outre, certains des destinataires se sont plaints qu'il n'existait pas d'option de refus dans les messages reçus. Enfin, l'entreprise aurait dû notifier préalablement à la CNIL qu'elle se servirait des adresses à des fins de commercialisation directe.	Droit pénal [Code pénal article 226-16, 18].	En instance. La CNIL a adressé une plainte officielle au ministère public pour qu'il décide à sa discrétion s'il convenait d'engager des poursuites au pénal.	Inconnus	Inconnue
	CNIL c. Suniles www.cnil.fr/fileadmin/documents/approfondir/deliberations/002-078a.pdf	La CNIL a reçu d'utilisateurs de services de courrier électronique 170 avis faisant état de messages commerciaux non sollicités reçus de SUNILES. SUNILES est accusé d'avoir utilisé un « robot-mail » pour recueillir des adresses électroniques auprès des destinataires et de ne pas avoir offert l'option de refuser d'autres messages à l'avenir. En outre, l'entreprise n'a pas notifié préalablement à la CNIL qu'elle enverrait des messages à des fins de commercialisation directe.	Droit pénal [Code pénal, article 226-16, 18].	En instance. La CNIL a adressé une plainte officielle au ministère public pour qu'il décide à sa discrétion s'il convenait d'engager des poursuites au pénal.	Inconnus	Inconnue

	Action	Résumé	Lois en vertu desquelles l'action a été intentée	Résultat/État actuel	Éléments transfrontières	Coopération obtenue
France	CNIL c. (Compagnie John Doe émettrice des messages « Le Top 50 du X ») www.cnil.fr/fileadmin/documents/approfondir/deliberations/d02-079a.pdf	La CNIL a reçu d'utilisateurs de services de courrier électronique 1 000 avis faisant état de messages non sollicités reçus d'une source non identifiable promouvant des sites Web pornographiques. Les utilisateurs d'Internet ont fait valoir qu'ils n'avaient jamais eu de contact préalable avec les sites Web en question. La source non identifiée est accusée d'avoir utilisé un « robot-mail » pour recueillir des adresses électroniques auprès des destinataires et de ne pas avoir offert l'option de refuser d'autres messages à l'avenir. En outre, l'entreprise n'a pas notifié préalablement à la CNIL qu'elle enverrait des messages à des fins de commercialisation directe.	Droit pénal [Code pénal, article 226-16, 18].	En instance. La CNIL a adressé une plainte officielle au ministère public pour qu'il décide à sa discrétion s'il convenait d'engager des poursuites au pénal.	Inconnus	Inconnue
	CNIL c. BV Communication http://www.cnil.fr/fileadmin/documents/approfondir/deliberations/d02-076a.pdf	La CNIL a reçu d'utilisateurs de services de courrier électronique 260 avis faisant état de messages électroniques commerciaux non sollicités reçus de BV Communications. Les utilisateurs d'Internet ont fait valoir qu'ils n'avaient jamais eu de contact préalable avec l'entreprise en question. BV Communications est accusée d'avoir utilisé un « robot-mail » pour recueillir des adresses électroniques auprès des destinataires et de ne pas avoir offert l'option de refuser d'autres messages à l'avenir. En outre, l'entreprise n'a pas notifié préalablement à la CNIL qu'elle enverrait des messages à des fins de commercialisation directe.	Droit pénal [Code pénal, article 226-16, 18].	En instance. La CNIL a adressé une plainte officielle au ministère public pour qu'il décide à sa discrétion s'il convenait d'engager des poursuites au pénal.	Inconnus	Inconnue

	Action	Résumé	Lois en vertu desquelles l'action a été intentée	Résultat/État actuel	Éléments transfrontières	Coopération obtenue
	<p>CNIL c. GreatMeds.com</p> <p>www.cnil.fr/fileadmin/documents/approfondir/deliberations/d02-077a.pdf</p>	<p>La CNIL a reçu d'utilisateurs de services de courrier électronique environ 500 avis faisant état de messages électroniques commerciaux non sollicités reçus de GreatMeds.com. Les courriers reçus par les utilisateurs contenaient divers textes et liens permettant de naviguer jusqu'au site Web de l'entreprise, dont celle-ci se sert pour vendre divers médicaments en ligne. Les utilisateurs d'Internet ont fait valoir qu'ils n'avaient jamais eu de contact préalable avec l'entreprise en question. GreatMeds est accusée d'avoir utilisé un « robot-mail » pour recueillir des adresses électroniques auprès des destinataires et de ne pas avoir offert l'option de refuser d'autres messages à l'avenir.</p>	<p>Droit pénal [Code pénal, article 226-18].</p>	<p>En instance. La CNIL a adressé une plainte officielle au ministère public pour qu'il décide à sa discrétion s'il convenait d'engager des poursuites au pénal.</p>	<p>GreatMeds.com est apparemment une entreprise établie aux États-Unis.</p>	<p>Inconnue</p>
<p>Italie</p>	<p>Garante c. entreprise inconnue</p> <p>www.legalday.co.uk/lexnrex/levershed03/November/e80281103.htm</p>	<p>L'Autorité italienne de la protection des données (Garante) a signalé au Tribunal pénal italien qu'une entreprise d'arts graphiques continuait à envoyer du spam après que la Garante a émis un ordre « bloquant le traitement de données ». En outre, l'entreprise ne s'est pas conformée à un ordre exigeant la communication de renseignements concernant l'origine des données personnelles utilisées dans le spam, ainsi que du nom de la personne responsable de leur traitement. Certains destinataires du spam se sont plaints à la Garante, faisant valoir que l'entreprise leur avait envoyé des communications publicitaires et promotionnelles sans avoir reçu de leur part le consentement « informé » nécessaire.</p>	<p>Le nouveau Code de la protection des données adopté en juin 2003 prévoit des sanctions pénales au cas où des données personnelles seraient traitées sans respecter l'obligation d'informer les consommateurs et d'obtenir leur consentement.</p>	<p>Le représentant de l'entreprise s'est vu infliger une amende de EUR 15 000 pour n'avoir pas répondu à la demande de l'Autorité de protection des données. Une procédure pénale est en instance et pourrait aboutir à une condamnation allant jusqu'à 3 ans de prison.</p>	<p>Inconnus</p>	<p>Inconnue</p>
<p>Japon</p>	<p>METI c. Access Control</p> <p>www.meti.go.jp/policy/consumer/release/remain.pdf</p>	<p>Le Ministère de l'économie, du commerce et de l'industrie a donné ordre à Access Control de mettre fin à des violations liées au fait que l'entreprise avait omis : i) de s'identifier dans un courrier électronique non sollicité ; ii) de communiquer l'adresse électronique permettant de refuser à l'avenir d'autres messages non sollicités.</p>	<p>Loi sur les transactions commerciales spécifiées</p>	<p>Aucune autre mesure n'a été prise. À l'avenir, les violations seront signalées aux autorités pénales.</p>	<p>Néant</p>	<p>Néant</p>

	Action	Résumé	Lois en vertu desquelles l'action a été intentée	Résultat/État actuel	Éléments transfrontières	Coopération obtenue
Corée	Intitulé du procès inconnu times.hankooki.com/league/biz/200402/kt2004020919282811860.htm	La Commission des pratiques commerciales loyales a répondu à 212 plaintes concernant le spam, en donnant ordre à 25 spammeurs de modifier leurs pratiques publicitaires en ligne illégales et en leur infligeant des amendes. L'entreprise qui a été condamnée à la peine la plus lourde avait arbitrairement envoyé du spam même après que les consommateurs eurent exercé une option de refus. L'administrateur de la FTC chargé du bureau de la protection des consommateurs a fait savoir que la possibilité d'une suspension de l'activité commerciale et de plus lourdes amendes était à l'étude.	Loi sur la protection des consommateurs dans le domaine du commerce électronique	Amendes comprises entre KRW 1 et 7 millions (USD 5 800) ; deux services téléphoniques pour adultes ont dû payer une amende de KRW 5 millions chacun pour avoir envoyé du spam par SMS.	Inconnus	Inconnue
Pays-Bas	Intitulé du procès inconnu www.dmeurope.com/default.asp?ArticleID=2428	Le Ministère de la justice des Pays-Bas a accusé des spammeurs d'être responsables de la fraude électronique « escroquerie nigériane 419 », en réponse à une plainte déposée par un opérateur par câble et FAI néerlandais.	Droit pénal	Le Tribunal de district d'Amsterdam a acquitté pour manque de preuves 6 des 13 personnes soupçonnées de fraude par voie de courrier électronique, estimant que la découverte des suspects sur les lieux d'où le spam était diffusé était un motif insuffisant pour une condamnation. Le ministère public néerlandais a fait appel de la décision. L'accusation avait recueilli des preuves au moment et sur les lieux des arrestations, entre autres : des connections à Internet illégales, des logiciels permettant l'envoi de spam, des combinés téléphoniques mobiles, des modèles de lettres ayant servi pour la fraude « nigériane » et même une masse de noms et d'adresses. Le ministère public n'a pu toutefois	Les victimes de cette escroquerie par voie de courrier électronique résidaient au Japon et aux États-Unis. Les prévenus n'ont pas comparu lors du premier procès et sont soupçonnés d'avoir fui le pays, ce qui soulève la question de l'utilité pratique d'un appel. La police néerlandaise a confirmé les liens existant entre les prévenus et des trafiquants de drogue aux Antilles néerlandaises.	Inconnue

	Action	Résumé	Lois en vertu desquelles l'action a été intentée	Résultat/État actuel	Éléments transfrontières	Coopération obtenue
Russie	Intitulé du procès inconnu http://english.pravda.ru/main/18/90/361/13170_spam.htm	L'opérateur de téléphones mobiles « Uralisky GSM » s'est plaint à la police que plus de 15 000 propriétaires de téléphones mobiles recevaient des SMS non sollicités. Après enquête, la police a confisqué l'ordinateur contenant les logiciels servant à l'envoi de ces messages, que le prévenu avait lui-même créés. Il a été accusé d'avoir créé des logiciels servant à mener des attaques de déni de service, et d'avoir copié des données personnelles.	Inconnues	L'inculpé a plaidé coupable, a été mis à l'épreuve pendant un an et a dû s'acquitter d'une amende de RUB 3 000 (USD 100).	Inconnus	Inconnue
Suisse	Intitulé du procès inconnu www.edsb.ch/d/doku/empeflungen/spam_neu.pdf	Sur plaintes émanant de destinataires de courriers électroniques commerciaux non sollicités, le Préposé fédéral à la protection des données (PFPD) a signifié à un homme envoyant du spam à des entreprises et à des particuliers l'ordre de communiquer l'information en sa possession concernant les destinataires puis de l'effacer. Le PFPD lui a accordé un délai de 30 jours pour satisfaire à cette demande, sans quoi l'affaire serait soumise au ministère public.	Article 29-3 de la loi fédérale sur la protection des données	En instance	Inconnus	Inconnue
Royaume-Uni	Intitulé du procès inconnu software.silicon.com/securety/0_39024655_39122143_00.htm	Un homme qui avait été licencié pour avoir omis de remplir sa feuille de présence a riposté en lançant une attaque de déni de service contre son ancien employeur (la société d'assurances britannique Domestic & General). Cette attaque au moyen de cinq millions de courriers électroniques a provoqué la fermeture du site Web de la société et lui a coûté GBP 18 000 de contrats perdus. Le prévenu a reconnu avoir utilisé un instrument spam qu'il a téléchargé depuis Internet.	Droit pénal	Le prévenu risque six mois de prison ou une amende allant jusqu'à GBP 5 000.	Inconnus	L'unité de la fraude informatique de Scotland Yard a démasqué le suspect et l'a arrêté.

	Action	Résumé	Lois en vertu desquelles l'action a été intentée	Résultat/État actuel	Éléments transfrontières	Coopération obtenue
Royaume-Uni	<p>ICSTIS c. BW Telecom</p> <p>www.icstis.org.uk/icstis2002/default.asp?no de=74&month=2</p>	<p>Le Comité indépendant pour la supervision des standards des services d'informations téléphoniques (ICSTIS), l'organisme de réglementation financé par l'industrie pour tous les services de télécommunications à numéros surtaxés, a infligé à BW Telecom une amende de GBP 75 000 pour avoir envoyé des messages électroniques non sollicités annonçant indirectement un site Internet pour adultes à numéros surtaxés, à des adresses électroniques choisies au hasard sans tentative apparente faite pour empêcher ces messages d'être envoyés à des enfants. Le message électronique comprenait un logiciel à tarif majoré avec composeur de numéro qui déconnectait les utilisateurs de leur FAI avant de les reconnecter à un service qui leur demandait GBP 1.50 la minute pour l'accès à Internet.</p>	Code de pratique de l'ICSTIS	L'ICSTIS a interdit l'accès au service pendant 12 mois et ordonné à BW Telecom d'offrir une réparation à tous les 240 plaignants.	Société américaine établie à New-York	Inconnue
Six actions séparées	<p>ICSTIS c. Vertical Media Ltd, Fast Way Holdings Ltd, Litmus Ltd, Indiano Communications, Greenbay Ltd and Quartel Ltd</p> <p>/www.theregister.co.uk/2004/05/24/text_fine_icstis/</p>	<p>En réponse à des milliers de plaintes, l'ICSTIS, chargé de surveiller les numéros surtaxés, a condamné six entreprises à des amendes pour avoir envoyé du spam avec texte, lancé des appels téléphoniques non sollicités, utilisé du matériel d'appel automatique laissant le message « appels non aboutis » sur des téléphones mobiles, et tenté d'inciter les parieurs à répondre à des appels avec un tarif majoré coûtant jusqu'à GBP 1.50 la minute. L'organe régulateur a constaté que ces entreprises avaient délibérément tenté de tromper le public en l'incitant à appeler des numéros surtaxés pour réclamer des prix qui n'existaient pas ou qui ne correspondaient pas à ce qui avait été promis.</p>	Code de pratique de l'ICSTIS	Vertical Media Ltd, Fast Way Holdings Ltd, Litmus Ltd, Indiano Communications, Greenbay Ltd et Quartel Ltd ont reçu l'ordre de payer des amendes de GBP 75 000 chacune et de réparer les torts causés, et ont été interdites d'activité au Royaume-Uni.	Les six entreprises sont établies à l'étranger et opéraient à travers le même agent aux Royaume-Uni, Smile Telecom (Bury).	Le Département du commerce et de l'industrie, l'organe régulateur des communications Ofcom, ainsi que la police, ont été invités à enquêter sur les liens entre ces entreprises.

	Action	Résumé	Lois en vertu desquelles l'action a été intentée	Résultat/État actuel	Éléments transfrontières	Coopération obtenue
	<p>ICSTIS c. ACME Marketing</p> <p>http://www.icstis.org.uk/icsstis2002/default.asp?node=74&id=2</p>	<p>L'ICSTIS a donné suite aux plaintes émanant du public concernant la réception de spam par SMS informant les destinataires qu'ils pouvaient réclamer soit des vacances, soit GBP 5 000, et les invitant à appeler un numéro surtaxé pour s'enquérir de la manière de procéder. Le message avec texte omettait d'indiquer le coût de l'appel et les noms et coordonnées de l'entreprise et des points de contacts, alors qu'aucun des destinataires n'avait consenti à recevoir ce message. La surveillance a révélé qu'en fait les appelants ne pouvaient réclamer que les vacances et étaient inscrits à une loterie permettant de gagner un prix de GBP 5 000.</p>	<p>Code de pratique de l'ICSTIS</p>	<p>ACME Marketing a dû s'acquitter d'une amende de GBP 3 000 et l'accès au service a été interdit pendant six mois. L'entreprise a aussi reçu l'ordre d'offrir une réparation à tous les plaignants.</p>	<p>Inconnus</p>	<p>Inconnue</p>
<p>Royaume-Uni</p>	<p>Advertising Standards Authority c. C Fry</p> <p>http://www.asa.org.uk/adjudications/show_a_djudication.asp?adjudication_id=37209&form_index=by_media&dates_of_adjudications_id=546</p>	<p>L'ASA a donné suite à plusieurs plaintes concernant des messages commerciaux non sollicités annonçant la vente d'un CD-ROM fantaisiste et de services d'appels téléphoniques. Ces courriers électroniques ont été envoyés sans le consentement explicite des destinataires et prétendaient qu'ils avaient été envoyés par des entreprises associées à titre de promotions assorties d'une option d'acceptation.</p>	<p>Code de la publicité</p>	<p>L'ASA a donné ordre à l'annonceur de s'assurer à l'avenir que les messages promotionnels n'étaient envoyés qu'à des consommateurs qui avaient consenti à les recevoir et que les consommateurs consentants avaient la possibilité d'exercer une option de refus à chaque occasion. L'expéditeur prétendait qu'il n'avait pas envoyé ces messages, mais l'ASA a noté que les messages semblaient avoir été envoyés soit par lui, soit en son nom, et qu'il n'avait pas répondu à des demandes l'invitant à montrer que les destinataires avaient consenti à les recevoir.</p>	<p>Inconnus</p>	<p>Inconnue</p>

	Action	Résumé	Lois en vertu desquelles l'action a été intentée	Résultat/État actuel	Éléments transfrontières	Coopération obtenue
États-Unis	<p>FTC c. Westby and Bevelander http://www.ftc.gov/opa/2003/09/fyi0357.htm</p>	<p>La FTC a allégué que les défendeurs avaient envoyé des courriers électroniques contenant des en-têtes faux ou trompeurs, ainsi que des adresses factices, et offert des options de refus inopérantes.</p>	<p>Protection des consommateurs, §5 a) de la loi sur la FTC</p>	<p>En règlement de cette affaire, les défendeurs ont reçu l'ordre de ne plus : recourir à la fraude, utiliser des rubriques « Sujet » trompeuses, donner de faux en-têtes ou prétendre à tort qu'ils allaient retirer les consommateurs de leurs listes d'adresses électroniques. En outre, ils ont dû restituer USD 112 500 de gains mal acquis découlant des activités illégales alléguées [USD 87 500 dans le cas de Westby et USD 25 000 pour Bevelander]. Le règlement comprenait aussi des dispositions sur la tenue obligatoire de registres permettant à la FTC de s'assurer que l'ordre a été exécuté.</p>	<p>Les défendeurs, Westby et Bevelander, résident respectivement dans le Missouri et aux Pays-Bas. Les entreprises à travers lesquelles ils opéraient, Maps Holding B.V. et PB Planning & Services B.V., ont un siège social aux Pays-Bas et y sont enregistrées comme sociétés.</p>	<p>Inconnue.</p>
	<p>FTC c. Zachary Keith Hill ; United States c. Keith Hill www.ftc.gov/os/caseli/st0323102/040322cm.pdf www.ftc.gov/os/caseli/st0323102/040322pleaagree0323102.pdf</p>	<p>Le défendeur avait piraté des logos de sociétés et utilisé du spam trompeur incitant les consommateurs à communiquer 473 numéros de cartes de crédit et d'autres données financières personnelles ; il avait ensuite acheté illégalement pour USD 47 000 de marchandises.</p>	<p>Protection des consommateurs : §5 a) de la loi sur la FTC et article 521 de la loi Gramm-Leach-Bliley (GLB), droit pénal : 18 Code des États-Unis, 1029 a) 5)</p>	<p>Le défendeur a donné raison à la FTC qui l'avait accusé de fraudes violentes lois fédérales. Il a été toutefois condamné par la suite à 46 mois d'emprisonnement au terme d'une action pénale séparée engagée par le Département de la Justice des États-Unis.</p>	<p>Inconnus.</p>	<p>Assistance du Bureau local de Washington du FBI et du Procureur fédéral du District Est de la Brigade de la fraude informatique et de la propriété intellectuelle de l'État de Virginie.</p>

	Action	Résumé	Lois en vertu desquelles l'action a été intentée	Résultat/État actuel	Éléments transfrontières	Coopération obtenue
États-Unis	<p>FTC c. un mineur</p> <p>www.ftc.gov/os/2004/06/040518stipaminorb_yhisparents.pdf</p>	<p>Le défendeur mineur avait copié des logos de sociétés et utilisé du spam trompeur pour lancer une attaque classique par hameçonnage, obtenant frauduleusement de consommateurs leurs numéros de cartes de crédit et d'autres données financières.</p>	<p>§5 a) de la loi sur la FTC et article 521 de la loi Gramm-Leech-Bliley (GLB)</p>	<p>Le défendeur, qui est mineur, a donné raison à la FTC qui l'avait accusé de fraudes violant les lois fédérales. Avec l'approbation du tribunal, il lui sera interdit à vie d'envoyer du spam ; il devra aussi restituer USD 3 500 de gains mal acquis.</p>	<p>Inconnus.</p>	<p>Assistance du Bureau local de Washington du FBI et du Procureur fédéral du District Est de la Brigade de la fraude informatique et de la propriété intellectuelle de l'État de Virginie.</p>
	<p>FTC c. GM Funding</p> <p>http://www.ftc.gov/os/caselist/dojswEEP/030505gmfundstip.pdf</p> <p>http://www.ftc.gov/os/caselist/dojswEEP/030505universalsitip.pdf</p>	<p>Le défendeur avait lancé des attaques par hameçonnage au moyen de faux en-têtes de courrier électronique. Ces attaques commençaient par un message électronique prétendant provenir d'un service auquel le destinataire était abonné et auquel il pouvait effectuer des paiements électroniques, par exemple à une banque ou à un détaillant en ligne. Pour que ce service puisse continuer, le message prétendait que le destinataire devait mettre à jour ses données personnelles en remplissant un formulaire en ligne sur un site ressemblant au site Web véritable de la banque ou du détaillant mentionnés. Le formulaire en ligne comprenait généralement un espace pour les numéros de cartes de crédit et d'autres données telles que les numéros de sécurité sociale, la date de naissance et le numéro et l'adresse du compte bancaire. Une fois ces informations envoyées, le défendeur pouvait les utiliser pour transférer des fonds depuis les comptes bancaires de la victime, demander des cartes de crédit en leurs noms ou acheter des marchandises en ligne.</p>	<p>§5 a) de la loi sur la FTC et article 521 de la loi Gramm-Leech-Bliley (GLB)</p>	<p>Le règlement de l'affaire interdit au défendeur d'envoyer du spam et exige la restitution de USD 60 500 de gains mal acquis.</p>	<p>Inconnus.</p>	<p>Coordination avec les organes d'application de la loi au niveau de la juridiction fédérale, des États et des comtés.</p>

	Action	Résumé	Lois en vertu desquelles l'action a été intentée	Résultat/État actuel	Éléments transfrontières	Coopération obtenue
	<p>FTC c. Patrick Cella et al.</p> <p>www.ftc.gov/os/caselist/doisweep/031119c_ellastipjudg.pdf</p> <p>www.ftc.gov/os/caselist/doisweep/031119h_errerazulastip.pdf</p>	<p>Les défendeurs ont eu recours à du spam et à des sites Web trompeurs faisant savoir qu'avec un acompte de USD 50 les consommateurs recevraient des enveloppes et des brochures. Ils ont prétendu qu'ils leur verseraient USD 1 pièce pour le remplissage des enveloppes et que les consommateurs pouvaient ainsi gagner 500 à USD 1 500 par semaine. Certains messages promettaient que les paiements des consommateurs seraient intégralement remboursables. Au lieu de recevoir des enveloppes et des brochures, les consommateurs ont reçu un livret contenant des instructions sur la manière de vendre à d'autres consommateurs le manuel trompeur publié par les défendeurs. Aucun des consommateurs n'a encaissé les gains promis et aucun n'a reçu de remboursement.</p>	<p>§5 a) de la loi sur la FTC</p>	<p>Le règlement de l'affaire avec les défendeurs leur interdit en permanence d'envoyer du spam, de faire des déclarations trompeuses et de fournir à d'autres les moyens et instruments nécessaires pour commettre des actes de tromperie. Les défendeurs devront payer aux consommateurs USD 7 000 à titre de réparation. Si les déclarations financières se révèlent inexactes, ils devront restituer USD 536 412, soit le total de leurs gains mal acquis.</p>	<p>Inconnus.</p>	<p>Inconnue</p>
<p>États-Unis</p>	<p>FTC c. K4 Global Publishing</p> <p>http://www.ftc.gov/os/caselist/doisweep/031014k4globalstip.pdf</p>	<p>Les défendeurs avaient envoyé du spam avec comme sujet la mention « Instant Internet Empires » ; l'expéditeur prétendait ainsi vendre sur Internet le potentiel rémunérateur de cinq entreprises commerciales clés en mains. Pour un investissement de USD 47.77, les consommateurs avaient le droit de reproduire le site Web des défendeurs et de tenter d'en revendre le contenu à d'autres consommateurs. La FTC a fait valoir que, pour réaliser les gains promis, chaque consommateur serait obligé de vendre le produit à 2 400 autres consommateurs, qui devraient chacun le revendre à 2 400 autres consommateurs pour encaisser les mêmes gains, et ainsi de suite. Selon la FTC, à la troisième génération de ce système, les participants seraient obligés d'effectuer un total de 13 829 760 000 ventes, soit plus du double de la population mondiale, pour que chacun d'eux puisse réaliser les gains annoncés.</p>	<p>§5 a) de la loi sur la FTC</p>	<p>Le jugement définitif sous forme de compromis comprenait un ordre interdisant aux défendeurs de faire des déclarations fausses ou trompeuses sur d'éventuelles rémunérations, de participer à des systèmes de vente en pyramide et de fournir à d'autres les moyens et les instruments permettant de violer les lois fédérales. D'après les états financiers soumis par les défendeurs, USD 247 000 devront être versés aux consommateurs à titre de réparation. Si les déclarations financières se révèlent inexactes, le total des gains mal acquis, soit USD 634 222, devra être restitué.</p>	<p>Inconnus</p>	<p>Inconnue</p>

	Action	Résumé	Lois en vertu desquelles l'action a été intentée	Résultat/État actuel	Éléments transfrontières	Coopération obtenue
	<p>FTC c. Christopher Baith, Monarrez and Verma</p> <p>www.ftc.gov/os/caselist/0223291/040211baitcmp0223291.pdf</p>	<p>Les défendeurs avaient envoyé des spams promettant une Playstation Sony gratuite, afin d'attirer les consommateurs vers des sites Web pornographiques et de réacheminer leurs connexions Internet au moyen d'un numéro 900, avec un tarif élevé à la minute.</p>	<p>§5 a) de la loi sur la FTC</p>	<p>Le règlement de l'affaire comportait un ordre permanent interdisant aux défendeurs d'envoyer des courriers électroniques en faussant l'identité de l'expéditeur ou l'objet du message, et assorti d'une amende de USD 10 000 et de l'obligation de restituer USD 25 000 de gains mal acquis.</p>	<p>Inconnus</p>	<p>Inconnue</p>
	<p>FTC c. BTV industries</p> <p>www.ftc.gov/os/2002/04/btvcmp.pdf</p>	<p>Les défendeurs avaient envoyé des spams promettant des cadeaux aux consommateurs, qui étaient redirigés sur des services téléphoniques payants au moment où ils effectuaient les téléchargements nécessaires pour demander leurs cadeaux.</p>	<p>§5 a) de la loi sur la FTC</p>	<p>Le règlement de l'affaire comportait un ordre permanent interdisant aux défendeurs d'envoyer des courriers électroniques en faussant l'identité de l'expéditeur ou l'objet du message, et assorti d'une amende de USD 10 000 et de l'obligation de restituer USD 25 000 de gains mal acquis.</p>	<p>Un des défendeurs est une société espagnole enregistrée aux îles Canaries.</p>	<p>La FTC a travaillé avec le R.-U. et les îles Canaries.</p>
	<p>FTC c. Benoit</p> <p>www.ftc.gov/opa/1999/05/audiot10.htm</p>	<p>Des escrocs avaient dupé les consommateurs en leur faisant faire de coûteux appels téléphoniques internationaux pour annuler des factures concernant des marchandises qu'ils n'avaient jamais commandées. Les défendeurs contactaient les consommateurs en envoyant une masse de messages électroniques avec tout un ensemble de fausses adresses qui empêchaient les consommateurs de refuser les commandes par courrier électronique. Lorsque les consommateurs téléphonaient pour annuler des commandes de marchandises qu'ils n'avaient jamais passées, ils étaient automatiquement connectés à un service de paiement téléphonique pour adultes.</p>	<p>§5 a) de la loi sur la FTC</p>	<p>Les opérateurs de réseaux téléphoniques aux États-Unis facturaient généralement les consommateurs pour chacun de leurs appels et envoyaient les fonds à la compagnie téléphonique de la Dominique qui, à son tour, répartissait les recettes entre les fournisseurs du service audiotexte. En raison du décalage entre la facturation, le recouvrement et la remise des paiements, il fallait normalement 60 jours environ pour que les fonds arrivent jusqu'à</p>	<p>Consommateurs lésés par les appels en direction des Antilles.</p>	<p>Inconnue</p>

	Action	Résumé	Lois en vertu desquelles l'action a été intentée	Résultat/État actuel	Éléments transfrontières	Coopération obtenue
États-Unis	FTC c. TLD Network Ltd. et al. www.ftc.gov/opa/2003/11/fv0365.htm FTC c. 30 minute mortgage et al. www.ftc.gov/os/2003/03/30mincmp.pdf	Les défendeurs se servaient de spam pour vendre des noms de domaines inexistantes. Les défendeurs avaient envoyé des spams frauduleux annonçant des « hypothèques de 30 ans à 3.95 % » et s'étaient fait passer pour un « créancier hypothécaire national ». La société avait invité les clients éventuels à remplir des demandes détaillées de prêts en ligne comprenant des numéros de sécurité sociale, le montant des revenus et les actifs, tout en les assurant que la communication d'informations sensibles serait protégée grâce à la technologie dite <i>Secure Sockets Layer</i> (SSL).	\$5 a) de la loi sur la FTC, 108 c) de la loi TILA, et 505 a) 7) et 522 a) de la loi GLB \$5 a) de la loi sur la FTC, 108 c) de la loi TILA, et 505 a) 7) et 522 a) de la loi GLB	l'entreprise d'audiotexte. L'ordre du tribunal empêchera désormais les opérateurs de réseaux téléphoniques de verser les fonds dans les recettes et permettra d'en conserver les montants aux fins des réparations dues aux consommateurs. Inconnus Le règlement convenu interdit les pratiques illégales de façon permanente et donne ordre aux défendeurs de restituer leurs gains mal acquis. Les jugements rendus exigent le dépôt d'une caution de 1 million de dollars avant l'envoi de courriers électroniques non sollicités. Un jugement concernant le versement de USD 57 500 par le président de la société a été suspendu.	Inconnus Inconnus	La FTC travaille avec le Bureau britannique de la concurrence. Inconnue

	Action	Résumé	Lois en vertu desquelles l'action a été intentée	Résultat/État actuel	Éléments transfrontières	Coopération obtenue
Six actions séparées mais apparentées	<p>FTC c. Larsen, Va, Lutheran, Panchero, Estenson and Boivin</p> <p>www.ftc.gov/opa/2002/02/eileenspam1.htm</p>	<p>Six défendeurs ont été accusés d'avoir envoyé à des consommateurs du spam contenant des lettres en chaîne trompeuses. Les lettres promettaient « USD 46 000 ou plus au cours des 90 prochains jours » aux destinataires, qui devaient envoyer USD 5.00 en liquide à chacun des quatre participants en tête de liste. En retour d'un paiement de USD 5.00, les personnes recrutées ont reçu des « rapports » avec des instructions sur la façon de mettre en route leurs propres systèmes de lettres en chaîne et de recruter des dizaines de milliers d'autres personnes au moyen du spam.</p> <p>Les défendeurs avaient envoyé du spam avec des indications fausses ou trompeuses destinées à promouvoir des prêts à « paiements fixes » avec des taux tels que 3.5 % et 2.95 %.</p>	Inconnues	<p>Les jugements définitifs sous forme de compromis étaient assortis d'un ordre interdisant en permanence à tous les défendeurs de promouvoir, de commercialiser, d'annoncer, d'offrir à la vente, de vendre ou d'aider d'autres à organiser tout système de lettres en chaîne.</p>	L'enquête a révélé que plus de 2 000 personnes ont participé à la lettre en chaîne dans près de 60 pays à travers le monde.	Les adresses ont été extraites de la base de données de la FTC sur les courriers électroniques commerciaux non sollicités.
	<p>FTC c. Chase Financial Funding</p> <p>www.ftc.gov/os/caseli/st/0223287/040602comp0223287.pdf</p>	<p>Les défendeurs avaient envoyé des messages non sollicités faisant savoir aux consommateurs qu'ils étaient sur une liste de personnes approuvées et qu'ils étaient sûrs de recevoir des cartes de crédit majeures non sécurisées avec des plafonds de crédit de USD 5 000, en échange d'un paiement initial de USD 49.95. Les consommateurs qui ont effectué ce versement n'ont toutefois pas reçu les cartes promises. Au lieu de cela, ils disent avoir bénéficié d'un accès à un ensemble d'hyperliens avec des entreprises auxquelles ils pouvaient demander des cartes de crédit.</p>	§5 a) de la loi sur la FTC	<p>Il a été demandé au tribunal d'interdire en permanence aux défendeurs de se livrer à des pratiques de prêt trompeuses et de les contraindre à verser aux consommateurs une réparation, accompagnée d'une restitution des gains mal acquis.</p>	Inconnus	Inconnue
	<p>FTC c. Clickformail.com</p> <p>www.ftc.gov/os/2003/10/clickformailfinalord.pdf</p>	<p>Les défendeurs avaient envoyé des messages non sollicités faisant savoir aux consommateurs qu'ils étaient sur une liste de personnes approuvées et qu'ils étaient sûrs de recevoir des cartes de crédit majeures non sécurisées avec des plafonds de crédit de USD 5 000, en échange d'un paiement initial de USD 49.95. Les consommateurs qui ont effectué ce versement n'ont toutefois pas reçu les cartes promises. Au lieu de cela, ils disent avoir bénéficié d'un accès à un ensemble d'hyperliens avec des entreprises auxquelles ils pouvaient demander des cartes de crédit.</p>	§5 a) de la loi sur la FTC	<p>Les défendeurs ont convenu d'un règlement les obligeant à payer USD 815 000 à titre de réparation aux consommateurs. En dehors de ce montant à payer, le règlement leur interdit à l'avenir de faire de fausses déclarations aux consommateurs.</p>	Inconnus	Inconnue

	Action	Résumé	Lois en vertu desquelles l'action a été intentée	Résultat/État actuel	Éléments transfrontières	Coopération obtenue
États-Unis	<p>FTC c. Universal Direct et al. www.ftc.gov/os/2002/04/universaldirectmp.pdf</p>	<p>Les défendeurs s'étaient servi de spam et d'un site Web trompeurs pour inciter les consommateurs à participer à une lettre en chaîne illégale, en envoyant du spam faisant la promotion d'un « Programme cadeaux » de commercialisation à plusieurs niveaux. Le spam prétendait que les participants pouvaient gagner USD 10 000 en espèces dans les quelques mois suivant leur adhésion, et encourageait les consommateurs à recruter d'autres participants.</p>	<p>§5 a) de la loi sur la FTC</p>	<p>Le règlement de cette affaire interdit aux défendeurs de promouvoir ou de vendre des systèmes de lettres pyramidales ou en chaîne, de donner une fausse idée des gains potentiels et de la légalité de ces systèmes, d'omettre de divulguer les profits ou les gains d'autres personnes participant à un programme de commercialisation à plusieurs niveaux et de fournir à d'autres le moyen de faire des déclarations trompeuses. A la suite de cet ordre préliminaire, les défendeurs ont remboursé tout l'argent qu'ils avaient obtenu des participants à ce système.</p>	Inconnus	Inconnue
	<p>FTC c. Walker www.ftc.gov/os/2002/04/davidwalkercomp.pdf</p>	<p>Le défendeur avait utilisé un site Internet pour vendre des produits qui, disait-il, guérissaient le cancer. Le site prétendait que les traitements, qui coûtaient entre USD 2 400 et 5 200, dispensaient de recourir à la chirurgie, à la chimiothérapie et à d'autres traitements traditionnels du cancer. Une déclaration d'un célèbre oncologiste laissait entendre que ces thérapies étaient nocives pour les personnes atteintes d'un cancer.</p>	<p>§5 a) de la loi sur la FTC</p>	<p>En instance. La FTC a demandé au tribunal d'interdire en permanence toutes prétentions sans fondement et d'ordonner qu'une réparation soit versée aux consommateurs.</p>	Inconnus	Inconnue
	<p>FTC c. Cyber Data www.ftc.gov/os/2002/10/scottford.pdf</p>	<p>Le défendeur avait envoyé à des consommateurs du spam qui prétendait qu'en achetant ses listes d'adresses en masse ils pouvaient gagner de l'argent en vendant des produits et des services sur Internet. Le courrier électronique de Cyber Data prétendait aussi que les acheteurs pouvaient raisonnablement s'attendre à des gains « de plus de USD 10 000 000 » en vendant un</p>	<p>§5 a) de la loi sur la FTC</p>	<p>Le défendeur a accepté un règlement lui interdisant en permanence toute déclaration fautive ou trompeuse concernant les gains pouvant provenir de l'envoi massif de messages électroniques.</p>	Inconnus	Inconnue

	Action	Résumé	Lois en vertu desquelles l'action a été intentée	Résultat/État actuel	Éléments transfrontières	Coopération obtenue
		produit de USD 5 au moyen de l'envoi massif de messages électroniques.		de logiciels, de services, de programmes de commercialisation ou de toute autre opération commerciale. Au vu des documents financiers soumis par le défendeur, le règlement oblige Cyber Data à verser USD 20 000 aux consommateurs à titre de réparation.		
	U.S. c. Internet Specialists www.usdoj.gov/usao/pae/News/Pr/2003/oct/catson.pdf	Un amateur de baseball mécontent avait piraté des ordinateurs à partir desquels il avait lancé des attaques à coups de longs messages non sollicités pour se plaindre de la direction de son équipe préférée. Au moment où ces courriers ont été envoyés, un grand nombre d'adresses sur sa longue liste n'étaient plus valables. Lorsque les messages sont arrivés à destination, ils avaient été, a argué l'accusation, « retournés » ou « répercutés » sur les personnes qui les avaient prétendument envoyés, c'est-à-dire les personnes dont les adresses électroniques avaient été trafiquées ou piratées. Il en est résulté qu'une masse de plusieurs milliers de messages électroniques est arrivée sur ces comptes en très peu de temps, ce qui en a perturbé le fonctionnement.	§18 USC 1028, 1030	Inconnus	Le défendeur a pris le contrôle d'un ordinateur au Canada pour lancer les attaques provoquant un déni de services.	Inconnue
États-Unis	SEC c. Scott Flynn www.sec.gov/litigation/admin/34-41102.txt	Lors d'une promotion frauduleuse typique, le défendeur Flynn, un ancien agent de change condamné pour fraude boursière dans une autre affaire, avait utilisé du spam pour diffuser des informations concernant certaines entreprises, sans divulguer correctement le fait que celles-ci versaient des réparations. La Commission des opérations de bourse (SEC) a allégué que, à l'insu des investisseurs, M. Flynn avait diffusé des informations depuis son entreprise, Strategic Network Development, Inc., sans faire savoir que des indemnités d'un total d'au moins USD 183 200 en argent liquide, plus 322 500 actions, avaient été versées par au	Loi sur la SEC de 1934	La SEC a engagé une procédure de cessation d'activité contre le défendeur pour promotion frauduleuse de valeurs mobilières en violation de dispositions des lois fédérales. Affaire en instance.	Inconnus	Inconnue

	Action	Résumé	Lois en vertu desquelles l'action a été intentée	Résultat/État actuel	Éléments transfrontières	Coopération obtenue
	<p>SEC c. Smith</p> <p>www.sec.gov/litigation/litreleases/lr18130.htm</p> <p>www.sec.gov/litigation/litreleases/lr18130.htm</p>	<p>moins dix de ces entreprises.</p> <p>Le défendeur a reconnu avoir mis au point deux formules d'investissement frauduleuses au moyen de sites Web et de spam au cours de l'année 2002. La SEC l'a accusé d'avoir frauduleusement obtenu USD 102 554 en garantissant sur deux sites Web des rendements mensuels à deux chiffres et en envoyant environ neuf millions de messages non sollicités.</p>	<p>Loi de 1934 sur la SEC, Règle 10-b-5)</p>	<p>Le défendeur a accepté l'ordre du tribunal l'obligeant à payer USD 107 510 à titre de restitution et d'intérêts préalables au jugement, et lui interdisant d'enfreindre de nouveau les lois sur les valeurs mobilières.</p>	<p>Inconnus</p>	<p>Inconnue</p>
	<p>SEC c. 2DoTrade</p> <p>www.sec.gov/litigation/litreleases/lr18381.htm</p>	<p>Les défendeurs avaient mis au point un système frauduleux consistant à adjoindre artificiellement aux actions de 2DoTrade de faux communiqués de presse sous forme de spam lié à un site Web frauduleux puis à inonder illégalement un marché gonflé avec des millions d'actions.</p>	<p>Articles 5 a), 5 c) et 17 a) de la loi sur les valeurs mobilières de 1933 et articles 10 b) et 13 a) de la loi sur les places boursières de 1934</p>	<p>En instance. La SEC cherche à obtenir du tribunal un ordre permanent, la restitution des gains mal acquis avec les intérêts antérieurs au jugement et des sanctions monétaires civiles contre tous les défendeurs.</p>	<p>Inconnus</p>	<p>Inconnue</p>
	<p>SEC c. Garst</p> <p>www.sec.gov/litigation/litreleases/lr18381.htm</p>	<p>La défenderesse aurait envoyé un gros volume de messages électroniques non sollicités contenant des déclarations fausses ou trompeuses concernant le produit mis en vente, les sources de recettes et les relations commerciales d'un des émetteurs concernés par la fraude, ainsi que sur ses antécédents en matière de sélection de valeurs mobilières et les intentions commerciales des personnes responsables de l'envoi des messages. Enfin, le spam ne faisait pas savoir qu'une réparation financière avait été versée à la défenderesse par le souscripteur légal.</p>	<p>Article 10 b) 5 de la loi sur les places boursières de 1934 et infraction à l'article 17 b) de la loi sur les valeurs mobilières de 1933</p>	<p>En instance. La SEC cherche à obtenir la restitution des paiements plus un montant raisonnable d'intérêts.</p>	<p>Inconnus</p>	<p>Inconnue</p>
	<p>SEC c. Rice</p> <p>www.sec.gov/litigation/litreleases/lr17377.htm</p>	<p>Le défendeur aurait mis au point des systèmes de « <i>pump and dump</i> » (répandre de fausses informations pour gonfler les cours) dans le but de manipuler les actions de quatre sociétés, y compris la sienne. Les systèmes pour chacune des quatre entreprises consistaient à envoyer des messages électroniques non sollicités frauduleux. Ces déclarations fausses concernaient, entre autres, le produit de sa société (un prétendu moteur de recherche</p>	<p>Article 10 b) de la loi sur les places boursières de 1934 et article 17 b) de la loi sur les valeurs mobilières de 1933</p>	<p>Le défendeur a accepté un ordre l'obligeant à cesser à l'avenir toutes violations des lois sur les valeurs mobilières et à restituer ses gains mal acquis, plus les intérêts échus antérieurs au jugement.</p>	<p>Inconnus</p>	<p>Inconnue</p>

	Action	Résumé	Lois en vertu desquelles l'action a été intentée	Résultat/État actuel	Éléments transfrontières	Coopération obtenue
		perfectionné sur Internet), ses sources de recettes et ses relations commerciales avec des tiers, ainsi que ses antécédents en matière de sélection des valeurs mobilières et ses intentions en matière d'opérations boursières.				
États-Unis	FTC c. Kalvin P. Schmidt www.ftc.gov/opa/1998/07/megagnet.htm	Le défendeur avait envoyé à des consommateurs du spam qui les dirigeait sur des sites Web faisant connaître un système d'investissement pyramidal reposant sur une lettre en chaîne. Le système était fondé sur des prétentions fausses et infondées concernant les gains.	§5 a) de la loi sur la FTC	Le règlement de l'affaire par la FTC interdit à Schmidt de participer à des systèmes de lettres en chaîne ou à des systèmes de vente en pyramide et l'oblige à justifier tout gain encaissé. Il devra posséder des preuves justifiant toute déclaration concernant les recettes, les profits ou les ventes résultant de tout plan ou programme de commercialisation, ou tout fait important. Enfin, le règlement énonce certaines obligations concernant la tenue de registres.	Inconnus	Inconnue
États-Unis	FTC c. Dixie Cooley, d/b/a DWC www.ftc.gov/opa/1998/10/operasetl-3.htm	Le défendeur a utilisé du spam pour tromper les consommateurs en leur faisant croire qu'il pouvait rétablir leur solvabilité moyennant le paiement d'un certain montant. Avec des tarifs allant jusqu'à USD 1 000, il prétendait garantir aux consommateurs qu'il pouvait effacer des informations négatives à leur sujet dans les rapports d'évaluation du crédit, même si ces informations étaient exactes et à jour. Mais les entreprises ne peuvent effacer des informations négatives légitimes et, lorsqu'il y a effectivement des erreurs dans les rapports, les consommateurs ont légalement le droit de les faire corriger, dans la plupart des cas gratuitement.	Loi sur la FTC et loi sur les organisations de restructuration du crédit (loi CROA)	Le tribunal a donné ordre au défendeur de payer USD 15 451.75 à titre de réparation aux consommateurs.	Inconnus	Inconnue

	Action	Résumé	Lois en vertu desquelles l'action a été intentée	Résultat/État actuel	Éléments transfrontières	Coopération obtenue
	<p>FTC c. Epic Resorts, LLC www.ftc.gov/opa/2000/08/travelunravel.htm</p>	<p>Les défendeurs auraient vendu des voyages à forfait au moyen de spam qui trompait les consommateurs en omettant de divulguer les prix effectifs ou en cachant le fait qu'ils devaient assister à un – et peut-être plusieurs – exposés sur le temps partagé.</p>		<p>La FTC a cherché à obtenir réparation pour les consommateurs.</p>	<p>Inconnus</p>	<p>Inconnue</p>
	<p>FTC c. Associated Record Distributors, Inc www.ftc.gov/opa/2002/06/bizopswe.htm</p>	<p>Les défendeurs ont envoyé du spam faisant la promotion de faux travaux à effectuer à domicile. Les promotions exagéraient les gains potentiels et l'aide qui serait apportée à ceux répondant à l'annonce.</p>	<p>Règle sur la franchise</p>	<p>La FTC a cherché à obtenir réparation pour les consommateurs, des sanctions civiles et l'arrêt permanent des déclarations trompeuses.</p>	<p>Inconnus</p>	<p>Le Département de la police de la Floride a aidé la FTC à régler cette affaire.</p>
	<p>FTC c. NetSource One</p>	<p>Pas d'autres informations disponibles</p>		<p>Inconnus</p>	<p>Inconnus</p>	<p>Le Département de la justice a engagé trois procédures et la FTC 14</p>
	<p>United States c. A. James Black www.ftc.gov/opa/1999/02/consumerweek2.htm</p>	<p>Les défendeurs avaient fait de la publicité par courrier électronique pour des services frauduleux, avec des messages tels que « DOSSIER DE CRÉDIT ENTIÈREMENT NOUVEAU EN 30 JOURS ». Les entreprises ont vendu aux consommateurs des instructions sur la façon de substituer des numéros d'identification à neuf chiffres du personnel des administrations fédérales ou des numéros d'identification des contribuables à des numéros de sécurité sociale, et de les utiliser illégalement pour constituer un nouveau profil de crédit qui leur permettrait d'obtenir du crédit que l'on pourrait leur refuser en raison de leurs antécédents vérifiables.</p>	<p>Loi sur les organisations de restructuration du crédit et loi sur la FTC</p>	<p>Inconnus</p>	<p>Inconnus</p>	<p>Le Département de la justice et Service d'inspection des postes des É.-U.</p>
	<p>United States c. David Story www.ftc.gov/opa/1999/05/id21a4.htm</p>	<p>A peu près les mêmes faits que ci-dessus.</p>	<p>Loi sur les organisations de restructuration du crédit et loi sur la FTC</p>	<p>Inconnus</p>	<p>Inconnus</p>	<p>Département de la justice et Service d'inspection des postes des É.-U.</p>
	<p>United States c. PVI, Inc. www.ftc.gov/opa/1998/09/vendup2.htm</p>	<p>Au moyen de spam, le défendeur a fait des déclarations orales et écrites à des investisseurs potentiels concernant des machines pour la vente de photographies numériques, mais omettait de fournir soit un document d'information, soit un document justifiant leurs prétentions en matière de gains.</p>	<p>Règle relative à la franchise</p>	<p>Inconnus</p>	<p>Inconnus</p>	<p>Le Département de la justice a ouvert la procédure à la demande de la FTC.</p>

	Action	Résumé	Lois en vertu desquelles l'action a été intentée	Résultat/État actuel	Éléments transfrontières	Coopération obtenue
	FTC c. LS Enterprises www.ftc.gov/opa/1999/04/spam2.htm		\$5 a) loi sur la FTC		Inconnus	Inconnue
	FTC c. Tim Cho Investment Corporation and Timothy Cho www.ftc.gov/opa/2001/03/cho.htm		\$5(a) loi sur la FTC		Inconnus	Inconnue
	FTC c. TrendMark International, Inc. www.ftc.gov/opa/1998/06/trendmrk.htm		\$5(a) loi sur la FTC		Inconnus	Inconnue
	FTC c. Ralph Lewis Mitchell, Jr. www.ftc.gov/opa/1999/02/consumerweek2.htm					
	FTC c. Reverseauction.com, Inc www.ftc.gov/opa/2000/01/reverse4.htm					
États-Unis	FTC c. Rosalind Leahy www.ftc.gov/opa/2002/11/netforce.htm					
	FTC c. Sandra L. Rennert, et al. www.ftc.gov/opa/2000/07/iog.htm					
	FTC c. Scott d/b/a Cyber Data www.ftc.gov/opa/2000/07/iog.htm	Pas d'autres informations disponibles				
	FTC c. Seasilver USA, Inc. et al. www.ftc.gov/opa/2003/					

DSTI/CP/ICCP/SPAM(2004)3/FINAL

	Action	Résumé	Lois en vertu desquelles l'action a été intentée	Résultat/État actuel	Éléments transfrontières	Coopération obtenue
	06/seasilver.htm FTC c. StuffingforCash.com Corp www.ftc.gov/opa/2002/07/mwnefforce.htm					
	FTC c. West Coast Publications, LLC www.ftc.gov/opa/1999/9905/id21a4.htm					
	FTC c. Yad Abraham ftc.gov/os/2003/08/idpsettlemntabrahamstip.pdf					
	FTC c. Nancy H. Merrill www.ftc.gov/opa/2002/11/nefforce.htm					
États-Unis	FTC c. Nia Cano, et al. www.ftc.gov/opa/1997/11/cdi.htm					
	FTC c. One or More Unknown Parties www.ftc.gov/opa/2003/01/idpfinal.htm					
	FTC c. Para-Link International, Inc., et al. www.ftc.gov/opa/2000/10/paralink.htm					

DSTI/CP/ICCP/SPAM(2004)3/FINAL

	Action	Résumé	Lois en vertu desquelles l'action a été intentée	Résultat/État actuel	Éléments transfrontières	Coopération obtenue
	FTC c. Cliff Cross and d/b/a Build-It-Fast www.ftc.gov/opa/1999/02/consumerweek2.htm [1]					
	FTC c. D Squared Solutions www.ftc.gov/opa/2003/11/dsquared.htm					
	FTC c. David Martinelli, Jr. www.ftc.gov/opa/1999/07/dpmarket.htm					