

ACTIONS À MENER

Synthèse des actions envisagées, envisageables ou d'ores et déjà étudiées, pour contrer le Spam.

Axe « Technique » :	2
Améliorer la gestion des blacklists	2
Renverser le transfert de charge (Penny Black)	2
Renverser le transfert de charge (Test de Turing)	3
Adresses « gérables »	3
Une réelle traçabilité	4
Modifier les protocoles DNS et SMTP	4
Des filtres anti-spam qui mordent ! (auto-retrieving filters)	5
Montrer patte blanche (liste blanche)	5
Liste grise	6
Mise à disposition de filtres par les FAI à leurs clients	6
Taux d'équipement (quantité & qualité)	6
Prendre au sérieux les Spyware	7
Enfin, une méthodologie de benchmarking !	7
Faciliter les développements d'outils	7
Axe « Comportemental » :	8
Faciliter les analyses	8
Toujours plus d'explications et d'éducation	8
Archivage des consentements et désinscriptions (Tiers de confiance)	9
Faciliter les désinscriptions	9
Labels - Certifications	10
Valorisation des données personnelles	10
Axe « Juridique » :	11
Un « Observatoire du Spam »	11
Des contrôles de la part de la CNIL ?	11
Une loi fédérale américaine ?	11
Une réelle coopération internationale	12
L'application des lois – Affectations de moyens	12
Traitement spécifique aux « scams »	12
Assouplissement de la charge de la preuve/ Baisse des sanctions	13


A l'occasion du Spam Forum Paris 2003 qui s'est tenu le 3 novembre (www.SpamForumParis.org), nous avons voulu regrouper les actions possibles, envisagées, envisageables ou d'ores et déjà étudiées, pour contrer le fléau. Nous avons fait un choix - celui de lister en priorité celles sur lesquelles on ne sait pas encore grand chose... Il ne s'agit donc pas d'une liste de conseils pour ne pas recevoir des spams. Aucun jugement de valeur n'est associé à chaque action : quelques unes comportent cependant des + et des - qui signalent les éventuels avantages et inconvénients de chacune d'entre elles. Ces actions sont présentées sous forme de fiches. Ces fiches comporte un titre, son rattachement à un axe de lutte (technique, juridique, comportemental...), l'indication d'une nature offensive ou plutôt défensive, la description de la situation actuelle, la description de l'action envisagée, la « source » si elle est identifiée et le but recherché.

Ce document est défini perfectible et nous lançons une invitation à remarques/commentaires/propositions/corrections... Sur le site Web www.SpamForumParis.org, un formulaire sera réservé à cet usage.

Grâce à vous, ce document va donc « vivre »...

Axe « Technique » :

Améliorer la gestion des blacklists	
<i>Famille</i>	Action technique – Mesure de protection
<i>Aujourd'hui</i>	Le filtrage sur blacklist est le fait essentiellement des FAI, qui l'utilisent pour éliminer les messages douteux sans avoir besoin d'analyser leur contenu. Ses listes sont établies et gérées par des entités indépendantes, souvent inconnues. Leur efficacité est douteuse (taux de filtrage bas, mais surtout taux de faux positif élevé).
<i>Source</i>	Frédéric Aoun, Bruno Rasle www.halte-au-spam.com
<i>Projet</i>	Optimiser l'efficacité des blacklists en confiant leur gestion à des entités reconnues et dont le fonctionnement peut être contrôlé par les pouvoirs publics. Il semble légitime, compte tenu des premiers bénéficiaires de ce type de filtre, que les associations nationales de FAI soient directement concernées. + Ce type de filtrage est le moins consommateur en ressources + L'association des ISP Hollandais se penche sur cette démarche - Qui et à quel coût ? - Arrivée du « Web hosting invisible », à travers des PC proxy et DNS « variable ». Les blacklist ont-elles encore un avenir ?

Renverser le transfert de charge (Penny Black)	
<i>Famille</i>	Action technique – Mesure de protection
<i>Aujourd'hui</i>	L'envoi d'un e-mail est aujourd'hui pratiquement gratuit. La charge est répartie entre les prestataires qui assurent le transit et l'internaute qui le reçoit. L'effet auto-limitatif des mailing sur support papier ne se retrouve pas dans le domaine électronique, au plus grand bénéfice des spammeurs.
<i>Source</i>	Microsoft (1993) http://research.microsoft.com/research/sv/PennyBlack/ Projet Camram ("A practical sender-pays antispam system") www.camram.org
<i>Projet</i>	<div style="display: flex; align-items: flex-start;">  <div> <p>Le nom du projet fait référence au premier timbre de l'histoire (de couleur noire et d'une valeur d'un penny), créé en 1830 par la poste britannique. Avant cette date, c'était le destinataire qui payait les frais d'acheminement du courrier ! Par analogie, le projet Penny Black se propose de faire supporter, d'une façon ou d'une autre, la charge financière à l'émetteur de l'e-mail, et non plus au seul destinataire. La taxe peut s'appliquer soit techniquement (ajout de latence, impôt « computationnel »...) soit financièrement (micropaiements par exemple). Les spammeurs seraient ainsi gênés dans leurs envois. Pour être acceptée, elle doit cependant ne pas trop pénaliser les émetteurs lambda.</p> <p>+ S'attaque à la source du mal, et au portefeuille des spammeurs - Théorie séduisante, mais délicate à implémenter - Acceptation de la part des internautes et des professionnels du marketing direct ? - Long terme - Gêne réelle pour les spammeurs professionnels, qui disposent de gros moyens ?</p> </div> </div>

Renverser le transfert de charge (Test de Turing)	
<i>Famille</i>	Action technique – Mesure de protection
<i>Aujourd'hui</i>	Les spammeurs utilisent des robots pour ouvrir des comptes à partir desquels ils réalisent leurs envois.
<i>Source</i>	Yahoo !, Altavista, Hotmail... Spamarrest dans une utilisation « White list »
<i>Projet</i>	<p>Un tests de Turing permet de distinguer ces robots des internautes humains, et ainsi de gêner les spammeurs.</p> <p>+ Gêne aux spammeurs</p> <p>- ...mais gêne également aux humains !</p> <p>- les générations récentes de robots arriveraient à passer les tests...</p> <p>SpamArrest imposent aux émetteurs (lors du premier envoi vers l'un de leurs clients) un test de ce type – puis ajout en white list.</p>



Adresses « gérables »	
<i>Famille</i>	Action technique – Mesure de protection ...et de rétorsion ?
<i>Aujourd'hui</i>	Il est fréquent de disposer de plusieurs adresses e-mail. Il est tentant d'en utiliser certaines d'entre elles comme « jetables », notamment quand il est indispensable d'indiquer son adresse pour accéder à une information. Mais la multiplication de ces adresses en rend l'utilisation laborieuse (cf. les « 500 » adresses Yahoo).
<i>Source</i>	Lucent (projet LPWA – 1997), Dolphian, ATT...
<i>Projet</i>	<p>Dolphian : A chaque visite de site Web est associée une adresse unique dont la durée de vie est gérable. La réception d'un spam sur cette adresse permet d'identifier avec certitude l'origine de la collecte (il suffit de désactiver l'adresse pour ne plus être importuné).</p> <p>+ La seule solution technique qui respecte la définition juridique française du Spam (basée sur la collecte déloyale) – reconnue devant les tribunaux ?</p> <p>- Solution à utiliser en complément d'un filtre</p> <p>- Idéale pour les réception, mais quid de l'émission d'e-mail avec ces adresses ?</p> <p>Dans la version d'AT&T, l'adresse unique est générée avec chaque e-mail. Cette adresse cache des règles qui déterminent les correspondants autorisés à répondre au message, le nombre que réponses qui peuvent être envoyées ainsi que la date limite d'utilisation. Si cette adresse tombe entre les mains d'un spammeur, elle ne lui est d'aucune utilité.</p>

Des commentaires ? Des propositions ?.. Ce document est défini perfectible.

N'hésitez pas à nous adresser vos contributions :

www.SpamForumParis.org

Une réelle traçabilité	
<i>Famille</i>	Action technique – Mesure de rétorsion
<i>Aujourd'hui</i>	Les protocoles utilisés aujourd'hui dans le cadre de la messagerie électronique ont été conçus il y a plusieurs dizaines d'années. Ils se caractérisent par une grande facilité à modifier l'apparence des envois (les spammeurs les mettent à profit pour se masquer) et le chemin parcouru (il est techniquement très difficile de remonter jusqu'aux réels émetteurs).
<i>Source</i>	IETF/ASRG www.irtf.org/charters/asrg.html , ICANN, RIPE http://www.ripe.net/ripe/wg/anti-spam/ , projet SPF (Sender Permitted From) http://spf.pobox.com/ , ePrivacy Group – projet Trusted Email Open Standard (www.eprivacygroup.net/teos/)...
<i>Projet</i>	On peut espérer que le Spam serait fortement réduit s'il était impossible d'envoyer des e-mails avec usurpation d'adresse ou d'identité. Les contre-mesures seraient plus efficaces, les actions en justice seraient grandement facilitées (fourniture de la preuve). L'ICANN de son côté a annoncé travailler à l'amélioration de sa base WHOIS dans cette optique. + Une certaine unanimité sur la démarche + Le premier engagement de l'ASRG - A quelle échéance ? - Quels impacts sur l'environnement internet ? On pourrait également espérer l'utilisation par les prestataires techniques du protocole TLS (Transaction Layer Secure) afin de sécuriser les échanges entre les diffuseurs et les FAI.

Modifier les protocoles DNS et SMTP	
<i>Famille</i>	Action technique
<i>Aujourd'hui</i>	Peu d'informations font foi dans un courriel reçu. Tout ou presque peut-être « modifié », au plus grand bénéfice des spammeurs. De plus, les validations de domaine basées sur une vérification DNS causent plus de tort que de bénéfices (en grande partie à cause de la mauvaise configuration d'une majeure partie des DNS de la planète).
<i>Source</i>	Projet AMTP (Bill Weinman) par exemple http://amtp.bw.org
<i>Projet</i>	Modifier le protocole DNS (sans aller jusqu'à utiliser le protocole DNSSec), afin d'empêcher le spoofing de la part des spammeurs. Un draft visant l'ajout d'une nouvelle catégorie d'enregistrements dans la base de données a été déposé à l'IETF. Reste à convaincre les destinataires de faire une vérification supplémentaire à la réception d'un mail : vérifier dans le DNS chercher si l'adresse IP de l'émetteur appartient à une liste d'adresses autorisées à émettre. Cela permettrait d'arrêter à la source les envois dont le nom d'émetteur est falsifié. Modifier le protocole SMTP, pour empêcher les spammeurs de masquer leurs démarches + donnerait moins de possibilités aux spammeurs - à quelle échéance ? - nécessite que tout le monde utilise cette version

Des filtres anti-spam qui mordent ! (auto-retrieving filters)	
<i>Famille</i>	Action technique – Mesure de rétorsion
<i>Aujourd'hui</i>	Un grand nombre de spams contiennent une URL menant à un site Web (génération de trafic dans le domaine pornographique ou site marchand). Ces sites sont difficilement pris en compte par les filtres d'URL traditionnels, compte tenu de leur durée de vie très limitée.
<i>Source</i>	Paul Graham www.paulgraham.com/ffb.html
<i>Projet</i>	<p>Les filtres anti-spam iraient visiter systématiquement le site recommandé (uniquement la page d'accueil, pour éviter les webbugs). Dans le cas d'une large diffusion (un million par exemple), le site serait sans doute fortement impacté par cet afflux de visites (DoS).</p> <p>On peut imaginer de transmettre l'information au filtre d'URL associé, pour empêcher la visite du site en question par un internaute (les nouvelles générations de spams ne contiennent plus la « promesse », qui est hébergée sur un site Web associé).</p> <ul style="list-style-type: none"> + totalement automatique + contre-mesure d'amplitude directement liée à l'échelle de diffusion - attention aux faux positifs ! Notamment en tenant compte des dernières techniques dites de « Web hosting » invisible.

Montrer patte blanche (liste blanche)	
<i>Famille</i>	Action technique – Mesure de prévention
<i>Aujourd'hui</i>	Les opérations d'e-mailing légitimes sont souvent perturbées du fait du « filtrage » opéré par les FAI (en fait, la destruction pure et simple des messages, sans retour d'information) et par les outils au niveau des postes client.
<i>Source</i>	Observatoire du mail/Acsel/irepp, projet Lumos du NAI ESPC, www.networkadvertising.org/espc/project_lumos.asp , Associations des FAI européens, AOL...
<i>Projet</i>	<p>Les annonceurs/diffuseurs (professionnels reconnus du marketing direct) seraient référencés dans une liste blanche (payante ?). Tout envoi du fait d'un émetteur compris dans cette liste serait à l'abri du filtrage.</p> <ul style="list-style-type: none"> + simplicité et solution applicable à moyen terme + moins de litiges - qui gère la liste ? (dimension globale du phénomène) - comment détecter les abus ? - à quel prix ? - danger de spoofing ? <p>Le projet Lumos intègre une « valeur ajoutée », sous forme de mise à disposition de statistiques à l'usage des diffuseurs.</p> <p>Au minimum, une première étape pourrait voir s'établir une méthodologie standardisant l'interface entre les diffuseurs d'e-mailing et les FAI (gestion d'un « droit à diffusion »).</p> <p>Au niveau des internautes, la même idée générique se retrouve dans la dernière annonce de Yahoo, qui autorise les utilisateurs à n'afficher que les messages provenant des adresses contenues dans leur carnet d'adresses...</p>

Liste grise	
<i>Famille</i>	Action technique
<i>Aujourd'hui</i>	La contrefaçon d'entêtes et le détournement de serveurs est à la source de la majorité du Spam.
<i>Source</i>	Evan Harris – IETF-ASRG www.irtf.org/charters/asrg.html
<i>Projet</i>	<p>Ce projet prévoit une légère modification du comportement des relais. Avant de relayer des messages, un relais devra vérifier la connaissance du triplet @IP de la machine qui initie la connexion @e-mail source et @e-mail destination. Si le triplet est inconnu le message est rejeté avec un message d'erreur « temporary failure ». Un échéancier est alors initié pour ce triplet, une fois le temps écoulé, le triplet peut être relayé.</p> <ul style="list-style-type: none"> + possibilité d'interopérer avec protocoles existants + possibilité de faire un déploiement progressif - tests à petite échelle seulement, danger d'effets de bord non prévus - solution à long terme ?

Mise à disposition de filtres par les FAI à leurs clients	
<i>Famille</i>	Action technique – Mesure de protection
<i>Aujourd'hui</i>	Peu de FAI proposent une réelle offre dans ce domaine. Les acteurs nord-américains semblent présenter une certaine avance dans ce domaine, au point d'en faire un critère de différenciation commerciale
<i>Source</i>	AOL, MSN, Yahoo...
<i>Projet</i>	<p>L'idéal consiste à mettre à disposition de chaque internaute un outil (ou un choix d'outils) lui permettant de bénéficier d'un paramétrage personnalisé.</p> <p>+ Solution applicable à court terme</p>

Taux d'équipement (quantité & qualité)	
<i>Famille</i>	Le taux d'équipement des internautes et des entreprises en outil de filtrage de Spam est faible et sans doute de mauvaise qualité (filtres d'anciennes génération).
<i>Aujourd'hui</i>	Aucune information fiable disponible
<i>Projet</i>	Inciter les victimes potentielles à s'équiper préventivement des outils de filtrage adéquats, de les configurer correctement et de les mettre à jour régulièrement (analogie avec les pratiques dans le domaine de la sécurité).

Prendre au sérieux les Spyware	
<i>Famille</i>	Action technique
<i>Aujourd'hui</i>	Les spyware sont l'une des techniques actuellement les plus utilisées par les spammeurs pour détourner à leur profit des postes d'internautes innocents (SoBig). Un prestataire polonais (Tubul) qui propose un service de « Web Hosting » transparent aux spammeurs se targue de contrôler 450.000 machines ainsi infestées... La lecture complète des CGU (conditions générales d'utilisation), bien que rébarbative, est fortement recommandée (les CGU d'une solution de VoIP actuellement très à la mode précisent par exemple que « le logiciel permettra à des tiers de communiquer à travers le PC... »).
<i>Projet</i>	La Presse a un rôle à jouer pour attirer l'attention des utilisateurs et entreprises sur ce sujet. Trop souvent, ceux-ci s'imaginent être protégés par leur Firewall et anti-virus.

Enfin, une méthodologie de benchmarking !	
<i>Famille</i>	Action technique
<i>Aujourd'hui</i>	Les quelques comparatifs publiés sur les filtres anti-spam se sont avérés jusqu'alors assez décevants concernant les performances réelles des outils (principalement à cause de l'extrême difficulté de constituer un corpus représentatif, comprenant spams mais aussi e-mails légitimes).
<i>Source</i>	Commission Européenne http://europa.eu.int/information_society/programmes/iap/call/index_en.htm
<i>Projet</i>	Dans le cadre de son programme « Safer Internet », la Commission Européenne finance le projet « BENCH », afin de disposer d'une méthode pertinente permettant objectivement de comparer des filtres anti-spam (sur http, mais aussi sur ftp, pop3/smtp, peer-to-peer, chat, instant messaging...)

Faciliter les développements d'outils	
<i>Famille</i>	Axe technique – Mesure de protection
<i>Aujourd'hui</i>	Chaque développeur ou entité qui travaille sur le sujet a les plus grandes difficultés pour constituer un corpus de spams pour l'utiliser comme jeu de test. Ceci à cause de la difficulté à obtenir une bonne représentativité, mais aussi à cause des limitations juridiques (le corpus doit également comporter des emails légitimes, ce qui obligerait à obtenir l'accord de chaque correspondant pour les communiquer à des tiers). Ainsi les 320.000 pourriels collectés par la CNIL en 2002 à l'occasion de l'opération « Boîte à spams » ne peuvent être analysés et utilisés pour combattre le phénomène.
<i>Source</i>	Frédéric Aoun, Bruno Rasle www.halte-au-spam.com
<i>Projet</i>	Par coopération, viser à définir et à constituer un corpus de référence, pour faciliter les développements et les comparaisons. Cette « action » est à rapprocher du projet BENCH de la Commission Européenne, qui vise à mettre sur pied une méthodologie pertinente permettant de comparer des solutions techniques de filtrage de spams.

Axe « Comportemental » :

Faciliter les analyses	
<i>Famille</i>	Axe comportemental – Mesure de protection
<i>Aujourd'hui</i>	<p>Sur de multiples points, nous disposons de peu d'informations et sommes réduits à émettre des hypothèses : Le domaine d'une adresse e-mail a-t-elle un impact sur son exposition au spam ? Quel est le taux d'équipement en outils anti-spam en France ? Quelles sont les évolutions que connaît le Spam – dans la forme et dans le fond ?</p> <p>Il est quasiment impossible d'accéder à des corpus représentatifs de spams, en grande partie à cause des limitations juridiques. Ainsi les 320.000 pourriels collectés par la CNIL en 2002 à l'occasion de l'opération « Boîte à spams » ne peuvent être analysés et utilisés pour analyser le phénomène.</p>
<i>Source</i>	Frédéric Aoun, Bruno Rasle www.halte-au-spam.com
<i>Projet</i>	<p>Après que la nouvelle loi soit promulguée, la CNIL devrait se voir adresser par les internautes un nombre important de pourriels, à l'appui de leurs plaintes. Il serait intéressant d'en profiter pour « qualifier » des informations, pour en faciliter l'analyse, identifier des tendances, positionner des alertes...</p> <p>L'université d'Anvers (Département des sciences de la communication) a été chargé par la Commission de la protection de la vie privée de mener une étude sur une partie du corpus constitué lors de l'opération «boîte à spams » menée en Belgique.</p>

Toujours plus d'explications et d'éducation	
<i>Famille</i>	Action comportementale
<i>Aujourd'hui</i>	Les messages didactiques et informatifs concernant le Spam sont fractionnés (CNIL, FAI, éditeurs d'outils, associations anti-spam, presse...) et perdent ainsi de leur efficacité. D'après Yahoo (USA) qui a mené une étude sur 28.000 internautes, 48% d'entre eux restent persuadés qu'il est possible de se désinscrire en répondant aux spammeurs...
<i>Source</i>	Commission Européenne http://europa.eu.int/information_society/programmes/iap/call/index_en.htm
<i>Projet</i>	La Commission Européenne a lancé le projet AWARENOD, qui ne se limite pas à la protection des mineurs, mais qui intégrera également la manière de réagir face aux spams. Ce projet fait partie de l'enveloppe de 11,7 millions d'€ allouée dans le cadre du « Safer Internet programme ».

Archivage des consentements et désinscriptions (Tiers de confiance)	
<i>Famille</i>	Axe comportemental – Mesure préventive
<i>Aujourd'hui</i>	<p>Peu d'internautes ont pris le réflexe de conserver copie de leurs consentements, et peu de professionnels du marketing direct les archivent. Trop souvent, les internautes « sur-réagissent » auprès des annonceurs, ayant oublié leur consentement préalable. D'autres se trompent d'adresse lors d'un désabonnement – et se plaignent lors de l'envoi suivant. D'autres encore abonnent un tiers à son insu...</p> <p>Avec la nouvelle loi, on peut s'attendre à une multiplication des litiges concernant ces deux phases critiques de la relation entre l'internaute et le professionnel du marketing direct.</p>
<i>Source</i>	Frédéric Aoun, Bruno Rasle www.halte-au-spam.com / ESP (projet Lumos)
<i>Projet</i>	<p>Charger un tiers de confiance d'archiver (comme moyen de preuve ?) les consentements (début de la relation entre un internaute et un annonceur) et les désinscriptions (fin de cette relation).</p> <ul style="list-style-type: none"> + Evite au professionnel la mise en place d'un système interne + Moyen de preuve en cas de litige - Qui et à quel coût ?

Faciliter les désinscriptions	
<i>Famille</i>	Axe comportemental
<i>Aujourd'hui</i>	Entre le conseil « Ne vous désinscrivez jamais ! Vous validez en fait votre adresse auprès du spammeur » et la réticence que semblent avoir les internautes de se désinscrire aux NewsLetter légitimes, il est difficile de se tracer une ligne de conduite.
<i>Source</i>	Cloudmark - Dolphian
<i>Projet</i>	<p>Cloudmark a introduit le concept de « proxy de désinscription », qui permet de simplifier et de sécuriser les désinscriptions.</p> <p>Dolphian répond à ce même souci en attribuant une adresse spécifique et gérable à chaque NewsLetter – avec laquelle on peut se désinscrire ?</p>

Des commentaires ? Des propositions ?.. Ce document est défini perfectible.

N'hésitez pas à nous adresser vos contributions :

www.SpamForumParis.org

Labels - Certifications	
<i>Famille</i>	Axe comportemental – Mesure préventive
<i>Aujourd'hui</i>	L'essor du commerce électronique a été freiné par le passé par un manque de confiance dans les moyens de paiement. S'y ajoute désormais la crainte du spam (« Puis-je laisser en confiance mon adresse e-mail sur ce site ? Cette société respecte-t-elle - dans le fond et dans la forme – les meilleures pratiques et les obligations légales ? »). Des dérives ont été relevées aux Etats-Unis d'une utilisation abusive de certains logos et labels.
<i>Source</i>	CNIL ? (Allemagne en pointe sur ce sujet) et Commission Européenne http://europa.eu.int/information_society/programmes/iap/call/index_en.htm
<i>Projet</i>	La transposition de la directive européenne 95/46/CE prévoit que la CNIL pourra délivrer des labels à des produits tendant à la protection des données et avaliser des codes de déontologie professionnels (elle a participé activement dans celui établi par le SNCD). On pourrait donc imaginer un label « Spam free ». <ul style="list-style-type: none"> + participe de la démarche pour établir la « confiance » + encadrement ISO 9000 et P3P - quels moyens ? - risques d'utilisation abusives ? (périmètre réel ?) - moyen terme ? <p>De son côté, la Commission Européenne a ouvert un appel à candidature pour un projet dénommé QUALAB, qui se traduira par un label décerné aux FAI les plus actifs dans la lutte contre le Spam.</p> <ul style="list-style-type: none"> + implication des FAI + envergure européenne

Valorisation des données personnelles	
<i>Famille</i>	Aspects comportementaux
<i>Aujourd'hui</i>	Les données personnelles sont collectées le plus souvent sans contrepartie.
<i>Source</i>	John Deighton – Harvard Business School http://hbsworkingknowledge.hbs.edu/tools/print_item.jhtml?id=3636&t=notebook En France, l'offre www.conso-acteur.com/
<i>Projet</i>	Les fichiers de données nominatives représentent pour les entreprises de marketing direct une véritable richesse. En août 2003, John Deighton, professeur à la Harvard Business School, a lancé sur ce sujet un pavé dans la mare, en posant ouvertement la question « Si nos informations personnelles représentent une telle valeur pour ces entreprises, pourquoi ne devrions nous pas être les premiers à en bénéficier ? ». Dans son étude « Market Solutions to Privacy Problems », John Deighton suggère une contrepartie pour l'internaute, telle que des offres préférentielles ou un service spécifique. Il ajoute « Une solution serait de permettre aux consommateurs de gérer et d'affirmer la valeur de leurs données personnelles, ce qui inciterait les fournisseurs à respecter celles-ci d'avantage » ⁱ .

Axe « Juridique » :

Un « Observatoire du Spam »	
<i>Famille</i>	
<i>Aujourd'hui</i>	L'ampleur et les caractéristiques du phénomène ne sont pas mesurées de façon pertinente et indépendante. Comment combattre un fléau que l'on ne connaît pas ? Comment mesurer l'efficacité des mesures prises – dont la nouvelle loi ?
<i>Source</i>	Frédéric Aoun, Bruno Rasle www.halte-au-spam.com
<i>Projet</i>	Sans céder à la mode des « observatoires », il serait judicieux de disposer de statistiques fiables, indépendantes et pertinentes. Au minimum, il serait bon, à l'échelle européenne, de s'entendre sur des méthodologies communes.

Des contrôles de la part de la CNIL ?	
<i>Famille</i>	
<i>Aujourd'hui</i>	La CNIL travaille essentiellement en mode « réactif », à partir des plaintes des internautes.
<i>Source</i>	
<i>Projet</i>	Lors de la présentation du 23 ^{ème} rapport annuel, le président de la CNIL, M. Michel Gentot a fait part de son souhait d'augmenter sensiblement les contrôles. Mais il s'agit principalement un problème de moyens....

Une loi fédérale américaine ?	
<i>Famille</i>	Aspects juridiques
<i>Aujourd'hui</i>	Si plusieurs états américains se sont dotés de loi, aucun projet n'a jusqu'alors abouti au niveau fédéral. Les propositions actuellement à l'étude privilégient toute le principe de l'opt-out, qui autorise l'envoi de messages promotionnels sans l'accord préalable des internautes.
<i>Source</i>	
<i>Projet</i>	Le responsable de la FTC a déclaré en août 2003 que si elles étaient promulguées « qu'au mieux, ces lois seraient inefficaces, au pire, elles seraient gênantes ». Les pays étrangers auraient à craindre un « débordement » des envois hors des frontières de la part des émetteurs américains (comment éviter les envois à un internaute français qui dispose d'une adresse en .com ?). De plus, il serait très facile à un spammeur de créer une société pour 500 \$, de réaliser ses envois sans tenir aucun compte des demandes de désinscriptions, de fermer boutique pour recommencer en toute légalité dans un autre état. Fin octobre 2003, le Sénat américain a voté à une écrasante majorité (97 voix pour – 0 contre) le principe de l'opt-out et de la liste d'opposition. Pour être définitivement adopté, ce texte doit encore être approuvé par la Chambre des Représentants.

Une réelle coopération internationale	
<i>Famille</i>	Aspects juridiques
<i>Aujourd'hui</i>	Les spammeurs savent parfaitement utiliser à leur profit les manques ou les différences législatives entre les états, et n'hésitent pas à « délocaliser » leurs opérations.
<i>Source</i>	Groupe Article 29
<i>Projet</i>	 Au niveau européen, le groupe de travail « Article 29 », sorte de « super-CNIL » travaille au renforcement de la coopération au sein de l'Union et compte prochainement publier un avis sur ce sujet. http://europa.eu.int/comm/internal_market/privacy/workinggroup_fr.htm - Quid de l'efficacité réelle de la coopération avec la FTC américaine ?

L'application des lois – Affectations de moyens	
<i>Famille</i>	Aspects juridiques
<i>Aujourd'hui</i>	A ce jour, aucune condamnation n'a été obtenue en France au titre de la loi « Informatique et Liberté » sur le fondement d'une action de spam (les seuls cas d'internautes condamnés face à leur FAI respectifs l'ont été pour « non respect des Consignes Générales d'Utilisation », tandis que le groupe politique « La Droite Libre » s'est vue reprocher son action de blocage des adresses e-mail des syndicalistes au regard de la loi Godfrain) . Deux des cinq dénonciations effectuées par la CNIL a l'issue de l'opération « Boîte à spams » courant 2002 n'ont pas aboutit. La justice analyse encore les trois autres... Seule une société française a été soumise par le Tribunal de Commerce de Grenoble à une « injonction de payer », en juin 2003, suite à une initiative de l'APIPL.
<i>Source</i>	CNIL (www.cnil.fr)
<i>Projet</i>	La CNIL, par la bouche de l'un de ses Commissaires, Mme Cécile Alvergnat, a publiquement appelé de ses vœux une meilleure application des textes existants. La Commission va également bénéficier d'un nouveau pouvoir, celui d'infliger des amendes. D'une façon générale, la CNIL (discours de son Président Michel Gentot en juin 2003 lors de la présentation de son 23 ième rapport annuel) demande à disposer de moyens renforcés lui permettant de mener à bien ses missions.

Traitement spécifique aux « scams »	
<i>Famille</i>	
<i>Aujourd'hui</i>	De plus en plus de fraudeurs utilisent le spam pour réaliser leurs arnaques. Ils se présentent comme une compagnie connue, utilisent même leur logos ou le modèle de leur emails, usurpent leur nom de domaine et demandent aux personnes ciblées de confirmer leurs informations personnelles (y compris leur numéro de carte de crédit).
<i>Source</i>	Brightmail
<i>Projet</i>	« Brightmail Anti-Fraud ». Grâce a son réseau leurre, la société Brightmail se dit bénéficier d'une position unique pour alerter rapidement les entreprises victimes de ces fraudes.

Assouplissement de la charge de la preuve/ Baisse des sanctions	
<i>Famille</i>	Action juridique
<i>Aujourd'hui</i>	Les poursuites contre les spammeurs aboutissent, du fait de la difficulté à les identifier (voir « traçabilité »), mais aussi à cause de la difficulté à constituer la preuve de l'infraction. De plus, la lourdeur des sanctions maximum possibles rendent la moindre action lourde de traitement et de conséquence. L'idée générale serait de les accélérer en simplifiant les procédures (passage par un « médiateur »), en baissant les sanctions et la charge de preuve (analogie avec les procès verbaux dressés en cas d'infraction). Plus rapide et plus « perceptible », la loi serait plus efficace, car plus appliquée.
<i>Source</i>	Atelier « Spam » de la Commission Européenne, du 16 octobre 2003
<i>Projet</i>	+ Les nouvelles dispositions de la loi « pour la confiance dans l'économie numérique » seraient d'avantage prises en compte par les professionnels du marketing direct...et par les « M. Jourdain du Spam » - Les spammeurs « professionnels » ne devraient pas être gênés par ce type de démarche, qu'ils pourraient au contraire considérer comme un signe de faiblesse à leur encontre

Ce document est défini perfectible et nous lançons une invitation à remarques/commentaires/propositions/corrections... Sur le site Web www.SpamForumParis.org, un formulaire sera réservé à cet usage.

Grâce à vous, ce document va donc « vivre »...

*Frédéric Aoun
Bruno Rasle*
