



Chapitre de livre

2007

Published version

Open Access

This is the published version of the publication, made available in accordance with the publisher's policy.

Spam : un conflit de libertés?

Bovet, Christian

How to cite

BOVET, Christian. Spam : un conflit de libertés? In: Les droits de l'homme et la constitution : études en l'honneur du Professeur Giorgio Malinverni. Auer, Andreas ; Flückiger, Alexandre ; Hottelier, Michel (Ed.). Genève : Schulthess, 2007. p. 97–108. (Collection genevoise. Recueils de textes)

This publication URL: <https://archive-ouverte.unige.ch/unige:43249>

Spam: un conflit de libertés?

CHRISTIAN BOVET*

*Professeur à la Faculté de droit de l'Université de Genève
Vice-président de la Commission fédérale de la communication (ComCom)***

I. Introduction générale

Les courriels non sollicités envahissent notre sphère privée et constituent autant d'obstacles à notre productivité ou simplement à notre plaisir d'utiliser un ordinateur. La migration de Giorgio MALINVERNI, de Genève vers Strasbourg, ne lui a malheureusement pas permis d'échapper aux nombreux expéditeurs de spam¹ qui troublaient parfois sa réflexion dans notre Université. Malgré l'efficacité croissante des filtres informatiques, ce phénomène – qui touche aussi bien les usagers que les opérateurs, voire les fabricants de logiciels – demeure un fléau pour le monde des communications électroniques².

Les statistiques sont nombreuses et rapidement dépassées au regard de l'ampleur grandissante de l'invasion; il faut en outre, à chaque fois, s'interroger sur les motivations derrière les données présentées, leur analyse et les

* L'auteur remercie vivement Adrien ALBERINI, assistant d'enseignement et de recherche à la Faculté, pour son aide dans l'élaboration de ce texte, en particulier de l'appareil critique.

** Les avis exprimés dans cette contribution sont personnels et n'engagent d'aucune manière l'autorité précitée.

¹ Sur l'origine du terme, BOVET C., «Ni spam ni SPAM™», in: BARRELET D. (édit.), *Media Vision*, Berne (Stämpfli) 2005, p. 37.

² Sur les méthodes pour collecter des adresses électroniques, voir p. ex. la décision de la Commission fédérale de la protection des données et de la transparence (CFPDT), du 15 avril 2005 (JAAC 69.106), consid. 5.4: «E-Mail-Adressen werden auf verschiedene Arten beschafft. Einerseits können bestehende Adresssammlungen gekauft werden. Hierbei handelt es sich in der Regel um Hunderttausende von Adressen. Ein gewisser Teil ist erfahrungsgemäss unbrauchbar. Aufgrund der tiefen Kosten wird das aber in Kauf genommen. Wer keine fertige Adresssammlung kaufen will, kann Software erwerben, welche ihn beim Anlegen einer eigenen Sammlung unterstützt. Einerseits gibt es Programme, so genannte <Crawler> – oder <Spider> – Software, welche das Internet automatisiert nach veröffentlichten E-Mail-Adressen absucht und diese sammelt. Eine weitere Möglichkeit – auch für diese ist Software erhältlich – ist das Generieren von E-Mail-Adressen aus Internetadressen. Damit wird die Tatsache ausgenutzt, dass es sehr viele Adressen im Format info@domain, webmaster@domain u. Ä. gibt. Selbstverständlich können auch E-Mail-Adressverzeichnisse ausgebeutet werden.» Eg. PRÉPOSÉ FÉDÉRAL À LA PROTECTION DES DONNÉES, 10^e Rapport annuel (2002/2003), p. 69 s.

conclusions tirées³. Il convient dès lors de faire preuve de prudence lorsqu'on consulte et cite des chiffres et études relatifs au spam. On se contentera d'indiquer ici qu'en 2006 plus de 12 milliards de communications électroniques ont été échangées dans le monde quotidiennement⁴. Sur une année, la moyenne de messages publicitaires non sollicités est en moyenne de 55%, avec une pointe (*peak*) à 68% à la fin septembre-début octobre⁵. Durant une semaine, on peut même atteindre un sommet de 71% le dimanche, et pendant une journée plus de 90% à 11h. GMT⁶. 40% du spam serait envoyé depuis l'Asie (dont la moitié depuis la Chine). L'Europe et les Etats-Unis enverraient chacun environ 25% du spam, les 10% restants étant émis depuis d'autres régions⁷. Par ailleurs, dans son rapport 2006, le Service national suisse de coordination de la lutte contre la criminalité sur internet (SCOCI) constate de manière inquiétante que ces messages électroniques :

«[...] ne sont plus seulement utilisés dans le cadre de la publicité pour des produits de masse, mais sont de plus en plus souvent liés à des offres commerciales illégales. Dans ce contexte, nous pouvons citer notamment les offres de pornographie infantine, qui ont été perçues comme particulièrement choquantes par les auteurs des communications, et les spams, qui entrent directement dans la catégorie des infractions économiques. Ce dernier type de courriels est en progression croissante depuis 2003. S'ajoutent aux escroqueries et au phishing, prépondérants en 2005, d'autres branches de la criminalité économique, comme le blanchiment d'argent (recrutement des intermédiaires chargés de la livraison d'argent).»

L'ampleur du phénomène et ses conséquences économiques⁸ ont suscité des réactions de plusieurs organismes internationaux⁹, ne serait-ce que pour inciter les principaux acteurs – parlements, gouvernements, régulateurs et opérateurs – à lutter contre celui-ci.

³ Voir p. ex. les sites de MessageLabs (www.messagelabs.com/publishedcontent/publish/threat_watch_dotcom_en/threat_statistics/spam_intercepts/DA_114633.chp.html) et Viruslist (www.viruslist.com/en/analysis?pubid=204791920#res). Eg. quoique peu lisible, Union internationale des télécommunications (UIT), ITU Newslog, à l'adresse internet www.itu.int/osg/spu/newslog/CategoryView,category,SPAM.aspx. Etat des sites internet au 8 mai 2007.

⁴ Statistiques consolidées tirées du site de «Spam Filter Review». à l'adresse internet <http://spam-filter-review.toptenreviews.com/spam-statistics.html>.

⁵ Voir le lien vers le site internet de MessageLabs, supra note 3.

⁶ Ibidem. Soulignons que les usagers ne reçoivent pas tous ces pourriels, une portion significative étant déjà éliminée par les fournisseurs de services internet.

⁷ Information tirée du site de «signal spam», à l'adresse internet www.signal-spam.fr/index.php/frontend/blog/classement_des_principaux_pays_emetteurs_de_spam.

⁸ En 2004-2005, le coût pour la collectivité était estimé au niveau mondial à plus de USD 20 milliards. ABRAMS D. / BAMBAUER D. / PALFREY J., *A comparative analysis of spam laws: the quest for a model law*, Background paper for the ITU WSIS thematic meeting on cybersecurity (Document: CYB/03, prov. 10 juin 2005), p. 9, avec d'autres références.

⁹ En particulier l'Organisation de coopération et de développement économiques (OCDE), à l'adresse internet www.oecd-antispam.org. Voir ég. les travaux dans le cadre de l'UIT (note 3).

De leur côté, les législateurs ont envisagé diverses solutions, qui sont autant d'illustrations de la culture économique et politique des Etats concernés. Pour l'essentiel, on peut distinguer entre deux grandes tendances : d'une part les réglementations qui imposent aux diffuseurs de publicité ou autres annonces de masse d'avoir l'accord préalable des destinataires pour de tels envois (*opt-in*) ; d'autre part les régimes qui exigent des diffuseurs qu'ils cessent leurs envois à l'égard d'un usager dès que ce dernier le demande (*opt-out*). Dans le premier groupe, on trouve l'Union européenne et, depuis le 1^{er} avril 2007, la Suisse ; dans le second, les Etats-Unis.

Le mécanisme de l'*opt-in* privilégie la liberté de la communication dans sa forme négative, à savoir la possibilité pour toute personne de refuser de recevoir des « informations ». Par contre, l'*opt-out* tend à favoriser la liberté économique en permettant aux diffuseurs de faire connaître leurs produits ou services, sans égard au fait que ceux-ci puissent être sans intérêt, offensants voire dangereux pour les destinataires de leurs messages.

Or toutes les libertés garanties par la Constitution fédérale ont la même valeur juridique. « Le respect de l'une d'elles n'emporte donc pas en soi la conformité à toutes les autres, pas plus que la violation de l'une n'implique une violation des autres. [...] Il s'ensuit que le juge constitutionnel, appelé à évaluer un acte qui touche plusieurs libertés, doit les coordonner entre elles, et non pas en subordonner certaines à d'autres. »¹⁰ Ce travail de coordination appartient cependant en première ligne au législateur. Pour sa part, le juge doit prendre en compte les libertés qui sont restreintes pour protéger une autre et les concrétiser d'une manière conforme à la Constitution ; il « veille à ce que, dans ce processus complexe de création et de concrétisation du droit ordinaire, une liberté ne fasse pas les frais des mesures prises pour protéger les autres libertés. »¹¹

L'examen successif des options offertes au législateur pour combattre ou, à tout le moins, limiter le spam nous permet d'illustrer ces réflexions.

II. *Opt-in* et liberté de la communication

Le traitement de la publicité de masse par la réglementation communautaire (A) a en partie inspiré le nouveau régime légal suisse (B). Celui-ci a en outre été soutenu par les instances de notre pays en matière de protection des données.

¹⁰ AUER A. / MALINVERNI G. / HOTTELIER M., *Droit constitutionnel suisse, Volume II: Les droits fondamentaux*, Berne (Stämpfli), 2^e éd., 2006, p. 123 N 265.

¹¹ Idem, p. 129 N 280.

A. Situation dans l'Union européenne

L'art. 13 de la Directive 2002/58 (directive vie privée et communications électroniques)¹² exige des Etats membres de l'Union européenne qu'ils prennent un certain nombre de mesures pour lutter contre les communications non sollicitées¹³. Suivant la définition large des communications électroniques¹⁴, le Parlement et le Conseil ont opté pour un concept qui vise non seulement le courrier électronique mais aussi l'utilisation de télécopieurs ou d'automates d'appel¹⁵.

La Directive impose ainsi l'*opt-in* comme régime légal, en prévoyant que l'envoi de courrier électronique à des fins de prospection directe ne peut être autorisé qu'à l'égard de personnes *physiques* ayant donné leur consentement préalable; un nombre limité d'exceptions est prévu, pour autant que les abonnés puissent à tout moment obtenir de l'expéditeur que ces communications cessent¹⁶. Cette procédure d'opposition ou de désabonnement doit être simple et sans frais pour l'utilisateur. Quant aux personnes *morales* et autres organismes, les Etats membres doivent en particulier veiller à ce que « leurs intérêts légitimes [...] soient suffisamment protégés en ce qui concerne les communications non sollicitées. »¹⁷

En tous les cas, il est interdit de camoufler ou de dissimuler l'identité de l'émetteur de la communication ou de ne pas indiquer une adresse valable pour obtenir la cessation de ces communications¹⁸.

B. Situation en Suisse

Le Préposé¹⁹ et la Commission de la protection des données ont émis, respectivement, en 2003 et 2005, des recommandations et une décision en ma-

¹² Directive 2002/58/CE du Parlement européen et du Conseil concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques, du 12 juillet 2002, JOCE 2002 L 201, p. 37.

¹³ Pour un exemple, voir l'art. L 34-5 du Code français des postes et des communications électroniques, disponible à l'adresse internet www.legifrance.gouv.fr/WAspad/UnArticleDeCode?commun=CPOSTE&art=L34-5.

¹⁴ Directive 2002/58, art. 2(d).

¹⁵ Idem, art. 13(1).

¹⁶ Idem, art. 13(1)-(3). A titre d'illustration, voir *Regulation 22 des Privacy and Electronic Communications (EC Directive) Regulations 2003* britanniques, disponibles à l'adresse internet www.opsi.gov.uk/si/si2003/20032426.htm.

¹⁷ Directive 2002/58, art. 13(5).

¹⁸ Idem, art. 13(4).

¹⁹ Préposé fédéral à la protection des données et à la transparence (PFPDT), dont le site internet se trouve à l'adresse www.edoeb.admin.ch/index.html?lang=fr.

tière de courriels non sollicités (1), qui ont soutenu la démarche du législateur ayant abouti à la révision de la loi sur les télécommunications du 24 mars 2006²⁰ (2).

1. *Protection des données*

Comme relevé à juste titre par les deux autorités suisses précitées²¹, les adresses e-mails constituent des données personnelles au sens de l'art. 3 al. 1 lit. a de la loi fédérale sur la protection des données²²; de même, leur traitement en vue de l'envoi de publicité de masse tombe sous le coup de la lit. e de cette même norme²³. Or ce type d'opération ne doit pas porter atteinte de manière illicite à la personnalité des personnes concernées²⁴; il doit être effectué conformément aux principes de bonne foi et de proportionnalité²⁵ et doit respecter la volonté expresse des intéressés. Selon l'art. 12 al. 3 LPD, «[e]n règle générale, il n'y a pas atteinte à la personnalité lorsque la personne concernée a rendu les données accessibles à tout un chacun et ne s'est pas opposée formellement au traitement.» Enfin, «[u]ne atteinte à la personnalité est illicite à moins d'être justifiée par le consentement de la victime, par un intérêt prépondérant privé ou public, ou par la loi.»²⁶

Conformément à ces règles, la Commission de la protection des données a affirmé que :

« Von einem loyalen und vertrauenswürdigen Verhalten im Geschäftsverkehr kann jedoch keine Rede sein, wenn eine an einer Geschäftsanbahnung interessierte Partei es in Kauf nimmt, zur Gewinnung einzelner Kunden systematisch eine Vielzahl von nicht einmal ansatzweise identifizierten Adressaten wahllos mit beliebiger Streuwerbung zu bedienen. Dies gilt erst recht, wenn dieser Vielzahl von Empfängern in voraussehbarer Weise gänzlich nutzlose Auslagen und Umtriebe anfallen [...]. Insbesondere darf nicht vermutet werden, dass eine Person ihre E-Mail-Adresse bekannt gibt, damit ihr jeder beliebige Anbieter im World Wide Web seine Angebote für die Anbahnung von Geschäftsbeziehungen unterbreiten kann. Der Grundsatz von Treu und Glauben greift schon im vorvertraglichen Bereich. Daher hat die an einer Geschäftsanbahnung interessierte Partei die Privatsphäre und die Interessen des anderen zu respektieren. Dazu gehört, dass der Geschäftswilige nicht ungefragt und systematisch massenhaft nutzlose Auslagen und

²⁰ RS 784.10 (LTC).

²¹ Supra note 19.

²² RS 235.1 (LPD). Décision de la CFPDT (note 2), consid. 2.4.

²³ Décision de la CFPDT (note 2), consid. 2.5.

²⁴ Art. 12 al. 1 LPD.

²⁵ Art. 4 al. 2, 12 al. 2 lit. a et b LPD.

²⁶ Art. 13 al. 1 LPD. D'une manière générale, Décision de la CFPDT (note 2), consid. 5.2.

Umtriebe bei Dritten verursacht. Bei wahlloser Streuwerbung an nicht identifizierte Dritte ist zu beachten, dass der Anbieter nur über vage bzw. ganz und gar zufällige Aussichten auf eine Geschäftsmöglichkeit verfügt, wenn er seine Werbung an Personen und Unternehmen adressiert, von denen er nicht einmal im Ansatz weiss, um wen es sich dabei handelt und welche Interessenlage bei diesen herrscht.»²⁷

Il en résulte que la récolte systématique et automatisée de milliers d'adresses e-mail sur la toile, sans la connaissance et *a fortiori* l'accord de leurs titulaires, viole les règles de la bonne foi et va à l'encontre de la volonté des intéressés. En effet, ceux-ci n'ont à aucun moment consenti à de telles opérations destinées exclusivement à un usage commercial²⁸. Cette application de la loi sur la protection des données ne viole pas le principe de la liberté économique. Celle-ci n'étant pas absolue, elle trouve en particulier ses limites, selon les règles de la Constitution, dans la protection de la sphère privée des usagers²⁹.

Pour le surplus, l'insertion d'une possibilité d'*opting-out* – comme l'avait prévu le Préposé – ne suffit pas, selon la Commission, à rendre licite l'envoi de messages non-sollicités³⁰.

2. Révision de mars 2006

La protection des consommateurs (ou usagers) constituait l'un des objectifs de la révision de la loi sur les télécommunications. Cette modification vise, d'une part, l'introduction du *opt-in* par le biais d'un amendement de la loi contre la concurrence déloyale et, d'autre part, une responsabilisation des opérateurs en leur imposant de prendre des mesures pour lutter contre le spam, dans son acceptation la plus large³¹.

Ainsi le nouvel *art. 3 lit. o LCD*³² commence par poser le principe du consentement du destinataire, en qualifiant de déloyal et donc d'illicite le comportement de celui qui :

²⁷ Décision CFPDT (note 2), consid. 5.5.

²⁸ *Idem*, consid. 5.5 *in fine* et 5.6. Cf. é.g. arrêt du 14 mars 2006 de la Chambre criminelle de la Cour de cassation française (dernier considérant sur le fond), selon laquelle «est déloyal le fait de recueillir, à leur insu, des adresses électroniques personnelles de personnes physiques sur l'espace public d'internet, ce procédé faisant obstacle à leur droit d'opposition». Cette décision est disponible à l'adresse internet www.cnil.fr/fileadmin/documents/approfondir/dossier/internet/Cour_de_cassation_anonymise.pdf.

²⁹ Art. 13 de la Constitution fédérale (Cst; RS 101). Décision CFPDT (note 2), consid. 5.8.2.

³⁰ Décision CFPDT (note 2), consid. 6.3 et 6.5.

³¹ Voir aussi *supra* note 12, en relation avec le droit communautaire.

³² Loi fédérale contre la concurrence déloyale (LCD; RS 241).

« envoi ou fait envoyer, par voie de télécommunication, de la publicité de masse n'ayant aucun lien direct avec une information demandée et omet de requérir préalablement le consentement des clients, de mentionner correctement l'émetteur ou de les informer de leur droit à s'y opposer gratuitement et facilement ».

Selon la seconde partie de cette disposition, toutefois, le diffuseur qui a obtenu les coordonnées de ses clients lors de la vente de biens ou services n'agit pas de façon déloyale lorsqu'il leur adresse, par voie électronique, de la publicité de masse qui concerne des marchandises, œuvres et prestations propres analogues. Il doit cependant indiquer expressément aux destinataires qu'ils peuvent s'opposer à cet envoi, en particulier par une fonction de désabonnement intégrée dans ces e-mails.

Pour sa part, la *loi sur les télécommunications* impose aux opérateurs de prendre des mesures pour lutter contre la publicité de masse déloyale³³ et octroie au Conseil fédéral la compétence de définir leurs modalités et ampleur. L'ordonnance sur les services de télécommunication³⁴ rappelle – en le limitant cependant au « techniquement possible » – le principe de l'élimination de ce type de communications par ceux qui occupent la fonction d'intermédiaires entre diffuseurs de spam et usagers, à savoir les opérateurs. Ils sont en effet les mieux à même de combattre ce phénomène tant qu'il subsistera des envois émanant d'entreprises n'observant pas les prescriptions du droit suisse, intentionnellement ou par négligence, en particulier lorsque les règles de leur pays d'origine sont différentes (système du *opt-out* au lieu du *opt-in*). D'un autre côté, il faut reconnaître que c'est à eux qu'incombe principalement le coût de la série de mesures définies par le gouvernement dans son ordonnance, puisqu'ils :

- doivent bloquer immédiatement l'envoi de ces messages et empêcher l'établissement des communications y relatives³⁵ ;
- peuvent exclure de leur réseau les clients qui envoient ou transmettent de la publicité de masse déloyale³⁶ ;
- peuvent en outre librement supprimer celle-ci³⁷ ;

³³ Art. 45a LTC. Le législateur reprend ici la notion large de la loi contre la concurrence déloyale et ne limite pas aux e-mails les communications considérées comme déloyales. Celles-ci comprennent aussi les envois en masse de SMS ou de fax. A ce propos, voir le site internet de l'Office fédéral de la communication (OFCOM) : www.bakom.admin.ch/dienstleistungen/info/00542/00886/index.html?lang=fr. Cette définition tend à donner au cadre légal la souplesse nécessaire pour s'adapter à l'évolution de la technique.

³⁴ RS 784.101.1 (OST).

³⁵ Art. 83 al. 3, phr. 1, OST.

³⁶ Art. 83 al. 3, phr. 2, OST.

³⁷ Art. 83 al. 2 OST.

- doivent exploiter un service auquel peut être annoncée la publicité de masse déloyale qui provient de leur réseau ou est transmise par leur biais³⁸.

L'ordonnance met par ailleurs en place, dans la perspective de la loi contre la concurrence déloyale, un double régime de collecte et d'exploitation des données :

- Les usagers peuvent, au gré d'une procédure relativement lourde, obtenir de « leur » opérateur des informations leur permettant d'identifier le diffuseur de spam³⁹. Au moyen de ces données, ils devraient pouvoir intenter action contre les auteurs de ces actes de concurrence déloyale, conformément à l'art. 9 al. 1 LCD. Ce dernier droit devrait aussi être reconnu aux opérateurs et aux concurrents du diffuseur de publicité de masse illicite, dans la mesure où ils subissent de ce fait une atteinte dans leur clientèle, affaires ou intérêts économiques⁴⁰. Cette même qualité pour recourir est enfin accordée par la loi aux associations professionnelles, économiques ou de protection des consommateurs⁴¹.
- Le Secrétariat d'Etat à l'économie (seco) représente pour sa part la Confédération dans de telles procédures, lorsque celle-ci « le juge nécessaire pour protéger la réputation de la Suisse à l'étranger et que les personnes qui ont le droit d'intenter action résident à l'étranger »⁴². Cette double condition constitue un obstacle significatif à une action efficace du seco dans la lutte contre le pollupostage. Certes, il peut intenter les actions de l'art. 9 al. 1 et 2 LCD et déposer une plainte pénale, mais seulement lorsque la dimension internationale de l'art. 10 al. 1 lit. c LCD intervient⁴³.

³⁸ Art. 83 al. 4 OST. Pour un exemple de gestion centralisée (au niveau étatique) de ce type de service, voir le site mis en place par le régulateur hollandais (*Onafhankelijke Post en Telecommunicatie Autoriteit*; OPTA) : www.spamklacht.nl. Depuis sa création, plus de 20 000 plaintes ont été adressées à ce service.

³⁹ L'art. 82 al. 1 OST prévoit en effet que le client doit formuler sa demande par écrit et rendre vraisemblable qu'il reçoit des communications abusives ou de la publicité de masse déloyale. Ces exigences visent notamment à éviter des démarches injustifiées ou illégitimes. Celles-ci devraient cependant être rares. En outre, lorsque l'opérateur concerné ne détient pas l'information parce que le diffuseur n'est pas son client, il doit s'adresser au fournisseur de services de télécommunication dont le diffuseur est le client; il appartient alors au second opérateur de livrer les données en question au premier (art. 82 al. 3 OST).

⁴⁰ Art. 9 al. 1 LCD.

⁴¹ Art. 10 al. 2 lit. a et b LCD.

⁴² Art. 10 al. 2 lit. c LCD. La compétence du seco résulte de l'ordonnance concernant le droit de la Confédération d'intenter une action dans le cadre de la loi contre la concurrence déloyale (RS 241.3).

⁴³ Comme le relève BARMAN P., « Die Anti-Spamgesetzgebung in der Schweiz », Jusletter du 2 avril 2007, N 40 : « Richtet sich das Spam <nur> an Inländer, fehlt dem SECO die Kompetenz für eine Intervention. »

L'art. 83 al. 6 OST permet la levée de la protection des données en faveur du seco pour lui permettre d'exercer les droits précités et de mettre en œuvre la procédure d'entraide administrative internationale qui devrait être introduite par le biais d'une nouvelle révision de la loi contre la concurrence déloyale⁴⁴.

Le régulateur suisse des télécommunications devrait lui aussi intervenir pour définir les prescriptions techniques et administratives applicables à ce domaine⁴⁵ et, le cas échéant, sanctionner les opérateurs qui ne respecteraient pas ces standards⁴⁶. Dans ce sens, on signalera les travaux tendant à établir des normes internationales qui paraissent être la seule voie réaliste en la matière. On retiendra en particulier ici quatre des « 10 commandements » élaborés récemment par des représentants d'entreprises et d'opérateurs⁴⁷ :

« [...] 3. ISPs [internet service providers] and network operators block potentially infecting email file attachments. In the case of filtering email or email file attachments based on content properties, in the context of any required legislation prior agreement is to be attained from the customer ;

4. ISPs and network operators actively monitor the volume of inbound and outbound email traffic to determine unusual network activity and the source of such activity, and respond appropriately ;

[...] 8. ISPs and network operators take measures to ensure that only their account holders use their e-mail submit servers ;

9. ISPs and network operators ensure that all domain names, Domain Name System (DNS) records and applicable Internet protocol (IP) address registration records (e.g. WHOIS, Shared WHOIS Project [SWIP] or referral WHOIS [RWHOIS]) are responsibly maintained with correct, complete and current information, and that this information includes points of contact for roles responsible for resolving abuse issues including, but not limited to, postal address, phone number and email address. »

⁴⁴ DÉPARTEMENT FÉDÉRAL DE L'ENVIRONNEMENT, DES TRANSPORTS, DE L'ÉNERGIE ET DE LA COMMUNICATION (DETEC), *Rapport explicatif du 30 novembre 2006 sur la révision des dispositions d'exécution de la LTC*, p. 25 s. (ad art. 77 al. 6-8 et 78 du projet de nouvelle OST). S'agissant de l'entraide administrative internationale selon la loi sur les télécommunications, cf. art. 13b LTC.

⁴⁵ Art. 83 al. 5 OST.

⁴⁶ Art. 58 et 60 LTC.

⁴⁷ BUSINESS AND INDUSTRY ADVISORY COMMITTEE TO THE OECD (BIAC ; www.biac.org) / MESSAGING ANTI-ABUSE WORKING GROUP (MAAWG ; www.MAAWG.org), *Best practices for internet service providers and network operators*, version du 16 avril 2006, Annexe II au *OECD Anti-Spam Toolkit*, disponible à l'adresse internet : www.oecd-antispam.org/article.php3?id_article=265.

III. *Opt-out* et liberté économique

Alors que l'Union européenne et la Suisse ont adopté le régime du *opt-in*, laissant juridiquement le choix à l'internaute de recevoir des courriels publicitaires d'émetteurs qu'il a sélectionnés, les Etats-Unis ont préféré le système du *opt-out*, imposant aux expéditeurs d'indiquer clairement aux destinataires de communications non sollicitées qu'en utilisant un mécanisme intégré dans le courriel ou autrement disponible, ils peuvent exiger de ne plus recevoir de messages de ce type.

La différence de paradigme paraît significative au premier abord. Dans une perspective relativement simpliste, on pourrait considérer qu'une fois de plus « les Américains » privilégient l'économie par rapport à la sphère privée. En réalité, lorsqu'on lit attentivement le *CAN-SPAM Act* de 2003, de quelque 20 pages, on s'aperçoit que les règles mises en place sont strictes et même que certaines d'entre elles pourraient inspirer le législateur européen. Tel est par exemple le cas des dispositions relatives à des fraudes comme l'utilisation d'ordinateurs protégés ou la falsification d'identité informatique, ou encore de l'utilisation de mentions trompeuses dans les courriers électroniques (*deceptive subject headings*).

De même, les modalités du mécanisme d'*opt-out* sont décrites de manière détaillée, selon la tradition et les exigences du *common law*. Ainsi :

« INCLUSION OF IDENTIFIER, OPT-OUT, AND PHYSICAL ADDRESS IN COMMERCIAL ELECTRONIC MAIL. – (A) It is unlawful for any person to initiate the transmission of any commercial electronic mail message to a protected computer unless the message provides –

- (i) clear and conspicuous identification that the message is an advertisement or solicitation;
- (ii) clear and conspicuous notice of the opportunity under paragraph (3) to decline to receive further commercial electronic mail messages from the sender; and
- (iii) a valid physical postal address of the sender.»⁴⁸

Quant aux pénalités, elles sont significatives. En particulier :

- d'une manière générale, des amendes et des peines d'emprisonnement avec des maximums allant de un à cinq ans dans les cas de fraudes précités⁴⁹ ;
- pour les Etats, la possibilité de réclamer la réparation du préjudice causé à leurs administrés, à raison de USD 250 par message, avec un maximum

⁴⁸ 15 USC 7704, (a) para. 5.

⁴⁹ 15 USC 7703, amendant le chapitre 47 du titre 18 du US Code (§ 1037[b]).

de USD 2 000 000, voire de USD 6 000 000 (*treble damages*) dans les cas graves d'actes intentionnels ou d'utilisation de procédés prohibés⁵⁰ ;

- pour les fournisseurs de services internet, la possibilité de réclamer la réparation du préjudice qu'ils ont subi, à raison de USD 25 ou 100 par message, selon les cas, avec un maximum de USD 1 000 000, voire USD 3 000 000 dans les mêmes cas graves⁵¹.

La question cruciale n'est donc pas tant le régime qui est choisi et sa sophistication que la mise en œuvre effective des normes adoptées. Le système de l'*opt-out* est plus compliqué à contrôler et exécuter que celui de l'*opt-in*. Il requiert des moyens financiers et en ressources humaines supérieurs que les gouvernements ne sont pas toujours disposés à mobiliser. C'est donc avant tout aux personnes privées – en particulier aux opérateurs et aux producteurs de logiciels – d'intervenir par des actions privées (*private enforcement*). Or cette tâche requiert au minimum l'intervention de l'Etat en tant que coordinateur ou « animateur », et force est de constater que l'administration américaine actuelle a montré relativement peu d'entrain à assumer l'une ou l'autre de ces fonctions⁵².

IV. Conclusions

On peut certes voir les régimes de l'*opt-in* et de l'*opt-out* comme la confrontation de deux systèmes : l'un privilégiant le droit de choisir de ne pas recevoir des « informations » – une forme de la liberté de communication ; l'autre érigé pour ainsi dire en dogme sa conception de la liberté économique. En réalité, ce conflit pourrait avoir des effets limités s'il n'avait pas pour conséquence d'empêcher une harmonisation des mécanismes de lutte contre le spam et de permettre ainsi aux diffuseurs peu scrupuleux de profiter des lacunes ainsi créées. Faute d'unification des systèmes, il faut à tout le moins développer la coopération internationale, par le biais notamment d'échange

⁵⁰ 15 USC 7706(f).

⁵¹ 15 USC 7706(g).

⁵² PALFREY J., « Stemming the international tide on spam », in : INTERNATIONAL TELECOMMUNICATION UNION (édit.), *Trends in Telecommunication Reform 2006: Regulating in the broadband world*, 7^e édition, Genève (UIT) 2006, p. 111, qui indique que la US Federal Trade Commission (FTC) « with its substantial resources, has brought only approximately 70 cases against spammers. » D'un autre côté, la FTC a produit à l'attention du Congrès pas moins de trois rapports sur le sujet, à savoir : *A CAN-SPAM informant reward system* (septembre 2004), *Subject line labelling – As a weapon against spam* (juin 2005) – disponibles sur le site internet de la FTC, à l'adresse www.ftc.gov/bcp/online/edcams/spam/reports.htm – et *Effectiveness and enforcement of the CAN-SPAM Act* (décembre 2005), disponible à l'adresse www.ftc.gov/reports/canspam05/051220canspamrpt.pdf.

de données. Cela suppose évidemment que le récipiendaire de ces informations prenne à son tour des mesures...

Une part significative de la solution pourrait venir des particuliers et des entreprises privées: d'abord de chaque utilisateur, qui a appris à ne même plus ouvrir et à détruire immédiatement ces courriels qu'il peut facilement identifier comme suspects. Ensuite des fabricants de logiciels, qui doivent cependant encore améliorer des produits bloquant encore trop de messages attendus et laissant passer tout autant de courriels indésirables. Enfin des opérateurs, dont on peut attendre qu'ils intègrent dans leurs systèmes des filtres efficaces.

La nécessité d'éliminer la nuisance que constitue le *spam* tient tant à la protection de la sphère privée – l'ordinateur en fait partie –, qu'aux nombreux enjeux économiques: en particulier, la productivité des entreprises est affectée par la gestion de ces communications, que ce soit en raison du temps passé par leurs collaborateurs à éliminer ces messages ou celui de leurs informaticiens à travailler sur des mesures de prévention. Le phénomène a en outre un impact négatif sur la confiance dans internet et la croissance du *e-commerce*.

Quelle que soit l'option choisie par les législateurs, une chose est malheureusement certaine aujourd'hui: les auteurs de ces externalités négatives n'assument pas ou, dans le meilleur des cas, seulement une infime partie des coûts économiques qu'ils génèrent.