Etude parue dans *Le commerce électronique européen sur les rails ? Analyse et propositions de mise en œuvre de la directive sur le commerce électronique*, Cahiers du C.R.I.D., n° 19, Bruxelles, Bruylant, 2001, pp. 131-168.

LES AFFRES DU "*SPAMMING*", ENTRE PROTECTION DE LA VIE PRIVÉE ET LIBERTÉ DU COMMERCE

Marie DEMOULIN et Étienne MONTERO

237. Les communications commerciales constituent pour les prestataires un moyen privilégié d'assurer le développement et le financement des services de la société de l'information. Toutefois, l'envoi abusif, au moyen du courrier électronique, de communications commerciales non sollicitées est susceptible de perturber le bon fonctionnement des réseaux, et d'importuner non seulement les destinataires de ces messages, mais également les fournisseurs d'accès chargés de les acheminer (considérants n^{os} 29 et 30 de la directive sur le commerce électronique).

238. Mieux connu sous le nom de "*spamming*", le problème des communications commerciales non sollicitées est abordé par l'article 7 de la directive sur le commerce électronique. Cette disposition réserve implicitement la possibilité pour les États membres d'interdire ce genre de communications ("les États membres qui autorisent les communications commerciales non sollicitées par courrier électronique veillent (…)").

Si un État fait le choix d'autoriser pareilles communications, il doit veiller au respect de la double exigence indiquée à l'article 7. D'une part, il doit poser un principe d'identification claire et non équivoque des communications commerciales non sollicitées par courrier électronique, et ce, *dès leur réception* (art. 7, § 1er). D'autre part, il doit imposer aux prestataires qui envoient de telles communications l'obligation de consulter régulièrement les registres "*opt-out*" dans lesquels les personnes qui ne souhaitent pas recevoir ce type de communications peuvent s'inscrire, et de respecter le souhait de ces dernières (art. 7, § 2). Par cette disposition ouverte, la directive n'entend pas trancher les discussions

relatives aux moyens de lutter contre le *spamming*, se contentant de légitimer implicitement la création d'éventuels registres d'opposition.

239. Notre examen des aspects juridiques du *spamming* s'articule en trois parties. La première vise à dresser un état des lieux. De manière descriptive, nous tâchons de présenter les tenants et les aboutissants du problème du *spamming*[1] : identification des pratiques, des inconvénients suscités et des principales mesures anti-*spamming* mises en œuvre. Dans la deuxième partie, nous portons l'attention sur le terrain juridique, en faisant état des solutions légales et jurisprudentielles au problème du *spamming*, et ce, dans une perspective de droit comparé (II). Une fois dégagés les éléments de fait et de droit nécessaires à l'intelligence du problème, nous sommes mieux à même de procéder, dans la troisième partie, à une évaluation critique des solutions envisageables (III), pour conclure sur quelques recommandations en vue de la transposition de la directive.

I. LE *SPAMMING* : UN ÉTAT DES LIEUX

240. Avant tout, il convient de cerner la notion de *spamming*, telle qu'elle est envisagée par la directive sur le commerce électronique, afin de la distinguer des autres pratiques promotionnelles utilisant l'e-mail (A). Un inventaire des problèmes posés par ce type de communication commerciale (B) et des remèdes qui y sont apportés en pratique (C) achèvera de planter le décor.

A. Notion et distinctions

241. Le *spamming*, ou "publipostage électronique", consiste en la diffusion généralisée de messages non sollicités à un grand nombre d'utilisateurs de l'internet. Il est susceptible de se manifester à travers

[1] Pour un examen général des différents problèmes liés au *spamming*, voy., entre autres, l'avis n° 34/2000 de la Commission pour le protection de la vie privée, du 22 novembre 2000, relatif à la protection de la vie privée dans le cadre du commerce électronique, disponible à l'adresse http://www.privacy.fgov.be ; le rapport de la Commission Nationale de l'Informatique et des Libertés (CNIL), "Le publipostage électronique et la protection des données personnelles", rapport présenté par C. ALVERGNAT, le 14 octobre 1999, disponible à l'adresse http://www.cnil.fr ; E. DROUARD et S. GAUTHRONET, "Communications commerciales non sollicitées et protection des données", étude réalisée pour la Commission des Communautés européennes, Internal Market DG, janvier 2001, http://europa.eu.int/comm/internal_market/en/media/dataprot/studies/spamstudy.pdf ; "Report to the Federal Trade Commission of the Ad-Hoc Working Group on Unsolicited Commercial Email", July 1998, http://www.cdt.org/*spams* ; E. LABBE, "*Spamming* en Cyberespace : à la recherche du caractère obligatoire de l'autoréglementation", *Lex Electronica*, vol. 6, n° 1, 2000, p. 15, disponible à l'adresse suivante : http://www.lex-electronica.org/articles/v6-1/labbe.htm ; S. LOUVEAUX, "Le *spamming* : état de la question", document CRID, oct. 2000, disponible à l'adresse http://www.droit.fundp.ac.be/textes/louveaux9.pdf .

deux types de ressources de l'internet : soit dans les groupes de discussion *Usenet* [2] ("*newsgroups*"), soit via le courrier électronique.

Le *spamming* sur *Usenet* se présente sous la forme d'un message unique envoyé à plusieurs groupes de discussion, souvent sans rapport avec le sujet discuté. Il perturbe gravement le fonctionnement de ces *newsgroups* et complique la tâche des administrateurs de systèmes qui gèrent les thèmes qui y sont abordés.

Dans le cadre du courrier électronique, le *spamming* se caractérise par l'envoi, massif et répété, de messages non sollicités, à caractère commercial le plus souvent.

242. Quel que soit son contenu (publicité commerciale, politique, pornographie, lettre porte-bonheur…), ce qui distingue le "*spam*" d'un message électronique ordinaire est son caractère *non sollicité*. En effet, le destinataire de ce type de message n'a pas demandé à le recevoir et n'a le plus souvent jamais eu de contacts préalables avec l'expéditeur, qui s'est procuré son adresse électronique dans les espaces publics de l'internet (forums de discussion, listes de diffusion, annuaires, sites web, etc.) ou en achetant des listes d'adresses e-mail à des tiers (*infra*, n° 248).

243. L'internet étant un espace sans frontières, le recours à l'e-mail permet aux prestataires de se faire connaître à travers le monde, et de toucher ainsi un maximum de clients potentiels. Plus large est le public visé, plus grandes sont les chances d'atteindre un consommateur intéressé par le message publicitaire qui lui est adressé. C'est la raison pour laquelle le *spamming* présente également un caractère *non ciblé*.

244. De plus, le *spamming* constitue un mode de prospection simple et extrêmement peu coûteux pour les entreprises désireuses de se faire connaître auprès d'un large public. Le coût estimé de l'envoi d'un e-mail commercial sur l'internet est évalué à un centième de cent américain (soit 0,0001 $), contre 1 $ pour le même envoi par un service postal[3]. Le *spamming* revenant environ 10 000 fois moins cher que le recours à la

---

[2] "*Usenet"* : serveurs de *news* stockant les articles publiés dans les groupes de discussions (*newsgroups*) (Définition issue du Petit lexique du Net, http://pro.wanadoo.fr/nesis/index.html)
"Groupes de discussion ou *newsgroups"* : groupes ou forums sur le *Usenet* dans lesquels les utilisateurs peuvent échanger informations, idées, astuces conseils et opinions sur un thème particulier. Les groupes de discussion sont classés par rubriques (Définition issue du *Guide à destination des utilisateurs d'Internet*, Bruxelles, Ministère des Affaires économiques, oct. 2000, http://www.droit.fundp.ac.be/Textes/Guide.pdf)

[3] Voy. le document de l'IETF (*The Internet Engineering Task Force*), RFC (*Request For Comments*) n° 2635, FYI (*For Your Information*) n° 35, http://www.ietf.org/rfc/rfc2635.txt?number=2635.

Poste, il rencontre un succès retentissant auprès des annonceurs. En particulier, son faible coût le rend accessible aux petites et moyennes entreprises, qui ne disposent pas toujours des moyens financiers pour s'offrir de vastes et coûteuses campagnes publicitaires via les canaux traditionnels (presse, télévision, radio, affichage…).

245. Ceci étant, toute communication commerciale ne peut être systématiquement qualifiée de *spamming*, tel que nous l'avons décrit. Par exemple, certaines entreprises envoient des courriers électroniques à d'anciens clients, afin de les informer de la sortie d'un nouveau produit, d'une offre promotionnelle ou d'une nouvelle rubrique sur leur site web. Le destinataire de ce message peut être intéressé par ces informations, même s'il n'a pas sollicité expressément ce message, d'autant qu'il est souvent ciblé en fonction d'achats antérieurs effectués auprès de la même entreprise.

À l'inverse, nombreux sont les messages superflus ou fantaisistes qui envahissent la boîte aux lettres électronique du destinataire et qui ne sont en général même pas lus, mais directement effacés : promesse de gagner des vacances en Floride si l'on s'enregistre sur un site, recette miracle pour perdre rapidement du poids, fausses informations concernant la circulation de virus informatiques, e-mails qui portent bonheur à condition d'être transmis à quinze autres personnes, etc.

La situation peut être moins claire pour d'autres types de messages, parfois susceptibles d'intéresser certains de leurs destinataires : e-mails électoraux, pétitions, appels au boycott d'une entreprise, informations concernant des manifestations diverses, jeux, messages humoristiques… On constate ainsi qu'il existe une palette de nuances entre le message expressément sollicité et celui qui apparaît comme clairement indésirable. Le régime juridique du *spamming* et les éventuels dispositifs techniques à mettre en œuvre devront tenir compte de ces distinctions.

B. Les inconvénients liés au *spamming*

246. L'e-mail représente un outil de marketing particulièrement avantageux pour tout prestataire désireux de développer son négoce sur les réseaux. Son faible coût incite certains annonceurs à multiplier le nombre de publicités envoyées, mettant ainsi en circulation sur le réseau un volume considérable de messages électroniques[4]. Pareils abus

[4] À titre d'exemple, c'est monnaie courante pour un annonceur d'expédier deux millions d'e-mails commerciaux par semaine.

entraînent de nombreux inconvénients, tant pour les destinataires de ces messages (1) que pour les intermédiaires chargés de les acheminer, et plus spécifiquement les fournisseurs d'accès (2), sans compter les perturbations causées au réseau lui-même (3).

1. Le point de vue du destinataire du message

247. Pour le destinataire de ces publicités non sollicitées reçues au moyen du courrier électronique, le *spamming* représente avant tout une atteinte à sa vie privée (a), et génère, en outre, de nombreux désagréments (b), tels des coûts supplémentaires, l'engorgement de sa boîte aux lettres électronique, des pertes de temps.

a) L'atteinte à la vie privée

248. Le *spamming* repose essentiellement sur la *collecte d'adresses électroniques* auxquelles seront envoyés les messages publicitaires. Un véritable marché des adresses e-mail s'est ainsi développé.

Diverses sont les méthodes employées par les *spammeurs* afin de se constituer un fichier d'adresses. Tout d'abord, les données peuvent avoir été collectées directement auprès de l'internaute ou, indirectement, lors de son inscription sur une liste de diffusion ou un site web[5]. Ces types de collectes sont légaux, moyennant le respect des principes et limites établis par les législations protégeant la vie privée (loyauté de la collecte, transparence, respect des finalité…) (*infra*, n^{os} 291 à 294). Mais, il existe également des méthodes de collecte dite "sauvage", réalisée sans ou contre le consentement de la personne concernée : utilisation de *cookies*[6], collecte automatique d'adresses électroniques laissées par les internautes dans des groupes de discussion et sur leurs pages web, utilisation de logiciels permettant l'inscription à un maximum de listes de distribution afin de récupérer les adresses électroniques de leurs membres, manœuvres frauduleuses (faux concours, offres d'espaces web gratuits), etc. Il est également possible d'acheter (légalement ou illégalement) sur l'internet des listes d'adresses électroniques à télécharger, pour des sommes relativement modiques. A titre d'exemple, des offres apparaissent à 100 Euros pour 2 millions d'adresses électroniques[7].

---

[5] Par exemple, en remplissant un bon de commande lors d'un achat en ligne, en participant à un jeu, etc.

[6] Les *cookies* sont de petits fichiers d'identification envoyés par le site et stockés sur le disque dur de l'ordinateur de l'internaute lorsqu'il surfe. Les données qu'ils contiennent permettent au prestataire de profiler le client, et de l'identifier lors de son prochain passage sur le site.

[7] Ces chiffres sont issus du rapport de la CNIL, "Le publipostage électronique et la protection des données personnelles", *op. cit.*, note n° 3.

On le voit, dans certaines circonstances, le *spamming* pose un grave problème au regard de la protection des données à caractère personnel (*infra*, n^{os} 291 et s.). En Belgique, la notion de donnée à caractère personnel, telle qu'envisagée par la loi du 8 décembre 1992 relative à la protection de la vie privée[8], est très large, et recouvre toute information concernant une personne physique identifiée ou identifiable[9]. Dès lors, il ne fait aucun doute qu'une adresse de courrier électronique constitue une donnée à caractère personnel et bénéficie, à ce titre, d'une protection légale[10]. En France, un rapport de la Commission Nationale de l'Informatique et des Libertés (CNIL) confirme cette analyse : "Au regard des législations de protection des données personnelles, une adresse électronique est évidemment une information nominative : directement nominative lorsque le nom de l'internaute figure dans le libellé de l'adresse ; en tout état de cause, toujours indirectement nominative dans la mesure où toute adresse électronique est associée à un nom et à une adresse physique. De surcroît, (…) une adresse électronique fournit dans bien des cas de nombreux renseignements sur la personne : son nom, son lieu de travail, son fournisseur de messagerie ou son fournisseur d'accès, son pays d'établissement, etc."[11].

249. Enfin, l'envoi massif et répété de communications commerciales non sollicitées par e-mail peut être considéré, de manière générale, comme une *intrusion dans la vie privée du destinataire*. En effet, une boîte aux lettres électronique constitue un outil de communication personnel à son titulaire, contrairement à une boîte aux lettres classique ou une ligne téléphonique, souvent communes à plusieurs usagers. L'invasion quotidienne de messages publicitaires provenant d'expéditeurs inconnus est souvent ressentie par leur destinataire comme une forme de harcèlement.

[8] Loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel *M.B.*, 18 mars 1993, telle que modifiée par la loi du 11 déc. 1998, *M.B.*, 3 février 1999.
[9] Cf. les art. 1 et 3 de la loi citée.
[10] En ce sens, voy. l'avis n° 34/2000 de la Commission pour le protection de la vie privée, du 22 novembre 2000, relatif à la protection de la vie privée dans le cadre du commerce électronique. Voy. aussi S. LOUVEAUX, "Le *spamming :* état de la question.", *op. cit.*, p. 6.
[11] CNIL, "Le publipostage électronique et la protection des données personnelles", *op. cit.*, p. 1.

b) Désagréments divers

250. Qu'il lise ses messages ou non, le destinataire est contraint de supporter le coût de chargement de communications commerciales électroniques qu'il n'a pas sollicitées. En effet, le volume journalier de messages étant plus important, leur téléchargement nécessite davantage de temps, ce qui augmente le coût de la communication téléphonique, particulièrement pour les connexions à faible débit. Cependant, grâce aux évolutions technologiques, ce problème sera probablement bientôt résolu, à l'aide de techniques de connexion plus rapide[12]. Par ailleurs, il convient de souligner que ce problème de coût ne se pose pas lorsque l'internaute bénéficie d'une connexion à l'internet forfaitaire ou d'une connexion téléphonique locale forfaitaire (ce qui est le cas aux États-Unis, par exemple).

251. Le *spamming* peut également avoir pour conséquence la hausse des tarifs pratiqués par les fournisseurs d'accès à l'internet (FAI) vis-à-vis de leurs abonnés. En effet, pour gérer la réception massive de courrier électronique, le FAI est amené à développer des moyens importants (filtres, équipement, personnel supplémentaire…), dont le coût est souvent répercuté sur le prix de ses services (*infra*, n° 255). C'est donc l'utilisateur qui doit supporter les conséquences financières du *spamming*. Toutefois, avec la multiplication actuelle des offres d'accès "gratuit" à l'internet, un FAI qui augmenterait ses tarifs risquerait de devenir nettement moins compétitif, sur un marché où la concurrence fait rage.

252. Par ailleurs, certains fournisseurs de messagerie gratuite sur le Web limitent l'espace de stockage dont leurs abonnés disposent sur leur compte de messagerie (par exemple, maximum 2 Mo)[13]. Si cette limite est dépassée, le fournisseur se réserve le droit de supprimer certains messages, qui ne pourront plus être récupérés par la suite. Dans de telles conditions, l'affluence de courriers électroniques non sollicités pourrait rapidement provoquer la saturation de l'espace de stockage disponible,

---

[12] On pense, notamment, à la connexion par câble, par satellite ou par câble électrique, ou le LMDS (*Local Multipoint Distribution Services*) transmettant par signal radio à 500 kpbs.

[13] À titre d'exemple, Yahoo! France prévoit la clause suivante dans ses conditions d'utilisation : "Règles générales en matière d'utilisation et de stockage : Vous reconnaissez que Yahoo! peut poser des règles générales et des limites quant à l'utilisation du Service, et notamment, sans que cette énumération soit limitative, fixer un nombre de jours maximum pendant lesquels les messages e-mails, les messages affichés dans les Forums, ou tout autre contenu téléchargé seront conservés, fixer un nombre maximum de e-mails qui pourront être envoyés et reçus par un compte sur le Service, fixer une taille maximale aux e-mails qui peuvent être envoyés et reçus par un compte sur le Service, fixer un espace de mémoire maximum qui vous sera alloué sur les serveurs de Yahoo! et fixer un maximum au nombre de fois où vous pouvez accéder à un Service pendant une période donnée (ainsi que la durée maximale de chaque accès)", http://fr.docs.yahoo.com/info/utos.html.

entraînant ainsi la suppression automatique de messages importants pour l'utilisateur.

253. Un internaute victime de *spamming* peut en outre perdre un temps précieux à tenter de s'en défaire : télécharger les messages non sollicités, les effacer, tenter d'y répondre pour se faire désactiver de la liste d'adresses de l'expéditeur, installer des filtres sur son ordinateur ou encore se plaindre à son fournisseur d'accès. L'accomplissement de toutes ces démarches empêche l'utilisateur de se consacrer à d'autres tâches.

Le *spamming* consistant, par définition, en l'envoi d'e-mails publicitaires non ciblés, la majorité des destinataires de ces messages n'est pas intéressée par leur contenu, et ne les lit même pas. En conséquence, on constate non seulement un gaspillage inutile des ressources du réseau, mais encore le mécontentement général des utilisateurs face au volume croissant de communications parasitaires.

254. Enfin, lorsqu'un internaute manifeste sa volonté de ne plus recevoir de tels e-mails, non seulement sa requête est le plus souvent ignorée, mais il court de surcroît le risque de recevoir encore plus de messages non sollicités, dès lors qu'il a ainsi indiqué à l'expéditeur que son adresse e-mail est réellement utilisée[14].

2. Le point de vue du fournisseur d'accès à l'internet (FAI)

255. Pour le fournisseur d'accès à l'internet, chargé de gérer le volume de messages électroniques transitant par ses serveurs, le *spamming* génère des coûts particulièrement importants. L'augmentation du trafic sur les réseaux le contraint à élargir constamment la bande passante, à acheter davantage de mémoire pour stocker les messages, à acheter et à gérer des ordinateurs supplémentaires pour assurer la sécurité et l'intégrité de son système, ainsi qu'à engager du personnel pour faire face aux problèmes techniques et aux plaintes des utilisateurs. Tous ces investissements entraînent une diminution des profits engrangés et se traduisent souvent par une augmentation des prix des services offerts aux clients, diminuant ainsi la compétitivité du FAI sur le marché. Pour les petits fournisseurs d'accès, les conséquences peuvent être encore plus désastreuses.

[14] C'est pourquoi de nombreuses associations contre le *spamming* déconseillent formellement aux internautes de répondre aux *spams* qui leurs sont envoyés, leur recommandant au contraire de les ignorer.

256. En outre, l'arrivée massive de courrier électronique non sollicité chez le FAI provoque des encombrements qui entravent le fonctionnement de ses services. Le *spamming* est à l'origine de problèmes d'accessibilité, de fiabilité, de dysfonctionnement et de ralentissement du système. Le serveur du FAI est saturé, donc plus difficilement accessible, et les messages (qu'ils soient sollicités ou non) sont délivrés moins rapidement ou de manière moins fiable, ou pire, n'arrivent jamais à leur destinataire.

257. Pour contrer les systèmes de filtrage et être plus difficilement identifiables, certains *spammeurs* font transiter clandestinement leurs messages par des serveurs d'e-mails appartenant à d'autres personnes, notamment à des FAI. Ils utilisent ainsi les noms de domaines d'organisations sans leur consentement, ou de fausses adresses de retour. Ces pratiques frauduleuses incitent le destinataire à croire que le courrier non sollicité qu'il reçoit provient d'une personne en relation avec cette organisation, et que cette dernière n'applique pas de politique anti-*spamming*, ou qu'elle entretient des contacts avec des *spammeurs*. L'organisme victime de tels détournements de son nom de domaine se retrouve ainsi inondé sous un flot de plaintes d'utilisateurs mécontents. Les FAI subissent fréquemment ces pratiques, qui nuisent à leur réputation auprès des internautes. De plus, de nombreux abonnés victimes de *spamming* croient que leurs données personnelles ont été communiquées (ou plutôt vendues) par leur propre FAI à un tiers, à des fins de marketing. Les relations du FAI avec ses clients peuvent s'en trouver gravement perturbées.

3. Les conséquences pour l'internet

258. L'internet n'est pas une ressource inépuisable. Il existe un trafic dépendant de la structure matérielle du réseau (câbles, espaces disques…), et dont la densité peut entraver le fonctionnement. Or, le *spamming* dévore un espace considérable sur l'internet. Le volume de messages expédiés rend les transmissions moins rapides et contribue de façon significative à l'encombrement du réseau.

De plus, les désagréments causés par le *spamming* aux utilisateurs du courrier électronique (retards, pertes de messages, pannes…) nuisent à l'efficacité et au développement de cet outil de communication. De telles pratiques découragent également la participation à de nombreux autres médias de l'internet, tels que les groupes de discussion, les listes de diffusion, le *chat*, *Usenet*, etc., principales sources de collecte des adresses e-mail pour les *spammeurs*.

Ainsi, le *spamming* porte atteinte aux fondements même de l'internet, qui est par principe un espace ouvert, où tout le monde peut exprimer ses idées et échanger de l'information librement et aisément.

C. Procédés de lutte contre le *spamming*

259. Différentes solutions sont envisageables pour obvier aux inconvénients du *spamming*. Parmi celles-ci, on compte, en premier lieu, les systèmes de l'*opt-out* (1) et de l'*opt-in* (2). Nous évaluerons ultérieurement les divers avantages et inconvénients de ces deux systèmes antinomiques, ainsi que les enjeux du débat ayant cours autour de ces deux notions (*infra*, n^{os} 295 et s.). Par ailleurs, nombre de fournisseurs d'accès tentent de contrer le phénomène par l'installation de filtres sur leurs serveurs (3) et l'imposition de clauses contractuelles anti-*spamming* (4).

*1. Le système de l'*opt-out

260. Le système de l'*opt-out* repose sur une autorisation de principe d'envoyer des communications commerciales non sollicitées, à moins que le destinataire ne s'y oppose expressément[15].

Il existe différentes manières d'organiser un système d'*opt-out*. La première consiste en l'établissement de registres, dressant la liste des consommateurs qui refusent de recevoir la moindre publicité non sollicitée, ou seulement certaines d'entre elles. La seconde méthode consiste en une demande du consommateur, adressée directement à l'expéditeur du courrier électronique publicitaire, visant à faire retirer son adresse e-mail de la liste de distribution de celui-ci.

À titre d'exemple, il existe en France un service e-Robinson, mis au point par la Fédération des Entreprises de Vente à Distance (FEVAD)[16]. Il s'agit d'une liste sur laquelle les consommateurs français désireux de ne plus recevoir d'e-mails publicitaires peuvent s'inscrire, gratuitement, en enregistrant leurs nom, prénom, adresse e-mail et adresse géographique. Ces données sont chiffrées et ne transitent pas "en clair" sur le réseau. Seules les entreprises membres de la FEVAD ont accès à cette liste et sont tenues de ne pas envoyer de communications commerciales non

[15] Concernant les registres *opt-out*, voy. R. JULIÀ-BARCELÓ, E. MONTERO et A. SALAÜN, "La proposition de Directive européenne sur le commerce électronique : questions choisies", in *Commerce électronique – Le temps des certitudes*, Cahiers du CRID, n° 17, Bruxelles, Bruylant, 2000, p. 12.
[16] voy. http://www.e-robinson.com.

sollicitées à ceux qui y figurent. Les données personnelles peuvent être transmises par la FEVAD à d'autres associations étrangères ayant mis en place un service similaire d'opposition à la prospection par e-mail, afin que les internautes inscrits reçoivent également moins d'e-mails publicitaires de sociétés étrangères. Comme elle le précise elle-même, la FEVAD a mis en place un droit d'opposition général à la prospection par les courriers électroniques. Elle ne prévoit donc pas la possibilité pour celui qui le désire de sélectionner, lors de son inscription, le type de publicité qu'il souhaite (ne plus) recevoir. Malheureusement, la liste e-Robinson ne règle le problème du *spamming* que dans une faible proportion, puisqu'elle n'est contraignante que vis-à-vis des membres de la FEVAD ou des associations avec lesquelles elle est liée. Tous les autres annonceurs dans le monde peuvent donc continuer à sévir contre les internautes français inscrits sur cette liste.

2. Le consentement préalable ou opt-in

261. À l'inverse d'un système d'*opt-out*, l'*opt-in* est basé sur une interdiction de principe d'envoyer des communications commerciales non sollicitées, à moins que le destinataire n'ait préalablement marqué son consentement.

Un tel système peut fonctionner selon différentes modalités. Ainsi, les consommateurs désireux de ne recevoir qu'un certain type de publicité pourraient s'inscrire dans des registres *opt-in*. Mais l'*opt-in* peut également consister en une demande préalable et individuelle, de la part du prestataire, de l'accord exprès du destinataire à recevoir des communications commerciales. Cette demande peut intervenir soit au moment de la collecte de l'adresse e-mail auprès de la personne concernée (bon de commande d'un produit en ligne, enregistrement du visiteur du site, accès à certains services gratuits ou payants…), soit par un e-mail sollicitant le consentement du destinataire à recevoir par la suite des communications commerciales de l'annonceur.

3. Les outils de filtrage

262. Des solutions techniques existent pour lutter contre le *spamming*, les plus courantes étant les systèmes de filtrage.

Les filtres heuristiques sont chargés d'isoler les messages suspects en fonction d'un certain nombre de critères de recherche. Aucune coopération de l'expéditeur du message n'est requise pour le

fonctionnement de ces filtres. La recherche peut être basée sur l'origine du message (DNS, adresse IP, etc.) ou sur son contenu.

263. Lorsque le filtre est programmé en fonction de l'origine du message, le système le plus efficace consiste à placer ce filtre au niveau du routeur d'entrée au réseau auquel appartient le FAI, afin qu'il puisse lui-même refuser un message en provenance d'une adresse IP déterminée. Il existe, en effet, sur le réseau des listes noires, établies par des associations de lutte contre le *spamming* ou par des particuliers, pouvant être utilisées par les FAI pour programmer leurs filtres[17]. Un message provenant d'une de ces adresses sera bloqué avant même d'arriver sur le serveur de mail du FAI. Le problème des coûts de transmission et de stockage des e-mails non sollicités est ainsi résolu. De plus, le message n'arrivant pas au destinataire, celui-ci n'a plus à souffrir des inconvénients liés au *spamming*. Par contre, l'identification de l'origine réelle d'un courrier par un filtre "d'origine" n'est pas toujours aisée, étant donné que les *spammeurs* font souvent appel à des relais chargés d'acheminer le courrier à leur place, masquant ainsi l'adresse IP du véritable expéditeur. Pour tenter de remédier à ce problème, des listes d'adresses de "serveurs-relais" à usage des FAI ont également été établies[18]. Malheureusement, pour contourner de tels barrages, les *spammeurs* changent constamment d'adresse, rendant ainsi les listes noires rapidement obsolètes et inutiles.

264. De leur côté, les filtres programmés en fonction du contenu de l'e-mail interviennent *a posteriori*, après que les messages aient été reçus, pour examiner s'ils contiennent un mot ou une combinaison de mots précis (par exemple, "*sex*" ou "*make money fast*"), et les coûts liés à la transmission des messages ne peuvent être évités. Cependant, il est assez difficile de configurer ces filtres de manière parfaitement adéquate. Les FAI et les utilisateurs doivent choisir entre le risque d'éliminer par erreur des courriers électroniques sollicités et celui d'accepter certains messages non sollicités.

265. Quel que soit le type de filtre choisi, celui-ci peut être placé tant au niveau du serveur du fournisseur d'accès qu'à celui de l'ordinateur de l'utilisateur.

---

[17] Voy. par exemple la *Realtime Blackhole List* de MAPS (*Mail Abuse Preventoin System*) (http://mail-abuse.org/rbl) ou la *Blacklist of Internet Advertisers* (http://math-www.uni-paderborn.de/~axel/BL/).

[18] Voy. le *Relay Spams Stopper* de MAPS (http://mail-abuse.org/rss) ainsi que le site ORBS (*Open Relay Behaviour-modification System*) (http://www.orbs.org/), proposant des banques de données destinées à traquer les serveurs SMTP qui ont été identifiés comme servant à relayer les *spammeurs*.

Pour le destinataire, l'installation d'un filtre chez le FAI représente une solution simple et confortable. Le FAI se charge de trier et d'éliminer lui-même les messages non sollicités, ce qui constitue pour son abonné un gain de temps et d'énergie. Cependant, ce système implique que le processus de tri soit entièrement conçu et réalisé par le FAI, qui prend seul la décision de bloquer un e-mail, en fonction de certains critères. Or, certains facteurs de sélection, comme la similitude et la quantité de messages envoyés, peuvent conduire au blocage d'un message qui est, en réalité, sollicité par son destinataire. De plus, un tel système implique l'intervention, soit d'une machine, soit d'une personne qui "lise" les e-mails adressés au destinataire, afin de s'assurer de leur caractère (non) sollicité. Le message est ainsi "ouvert" avant d'avoir été lu par son destinataire, ce qui pose un problème de respect du secret de la correspondance.

À l'inverse, un filtre installé chez le destinataire n'intervient que lorsque le message lui a déjà été transmis, ou au moins son en-tête, ce qui ne résout pas le problème des coûts, pour le FAI comme pour l'utilisateur. Tout au plus ces filtres permettent-ils au FAI de diminuer indirectement certains coûts liés au traitement des plaintes et d'améliorer ainsi ses relations avec ses clients. La plupart des logiciels de filtrage installés chez le destinataire sont déjà configurés. Cependant, l'utilisateur a la possibilité de personnaliser davantage son filtre en ajoutant ou en supprimant certains critères de sélection. Le risque de perdre des messages sollicités est ici nettement moins important, le destinataire déterminant lui-même, en fonction de ses besoins, le type de messages qu'il souhaite recevoir ou non. En outre, lorsqu'il parvient à son destinataire, le message n'a pas été ouvert. Il n'y a donc aucune intrusion dans la vie privée du destinataire à ce niveau.

4. Les clauses contractuelles dans les conventions de FAI

266. Pour lutter contre le *spamming*, les FAI insèrent dans leurs conditions générales des "Principes d'Utilisation Acceptable" ("*Acceptable Use Policy*")[19]. La plupart de ces principes se réfèrent à la Nétiquette ou s'en inspirent directement. Ainsi précisent-ils qu'il est interdit d'envoyer des e-mails non sollicités qui provoquent des plaintes de leurs destinataires, mais aussi de falsifier un en-tête de message ou d'utiliser un compte du FAI comme adresse de réponse. Cependant, de

[19] Pour un aperçu de différentes conditions générales de FAI, voy. http://www.cypango.net/*spams*/aup.html et http://*spams*.ohww.norman.ok.us/tos.htm.

nombreux *spammeurs* disposent de leur propre FAI, ce qui limite les mesures pouvant être prises à leur encontre.

En cas de violation d'une de ces clauses, les sanctions varient d'un FAI à l'autre. S'il s'agit de la première infraction, le FAI envoie un avertissement ou une mise en demeure à l'abonné. S'il y a récidive, le compte de l'abonné peut être suspendu, et une enquête peut éventuellement être ouverte. D'autres fournisseurs d'accès clôturent carrément le compte ou ferment l'accès au réseau. Il est également possible de bloquer les messages envoyés de manière répétée en violation des "principes d'utilisation acceptable", ou de les effacer, sans sommation. D'autres enfin mettent à charge de l'abonné tous les frais occasionnés par l'envoi massif d'e-mails non sollicités, avec un minimum (par exemple 500 $). Certains prévoient des clauses pénales : lorsqu'un abonné du FAI fait un envoi massif d'e-mails non sollicités, le FAI peut lui réclamer, par exemple, 500 $ par jour où de tels envois ont été commis. Lorsque le FAI constate qu'un non-membre envoie des *spams* à ses abonnés, il peut lui réclamer 150 $ par abonné victime du *spamming*[20]. En pratique, face à de telles sanctions, les *spammeurs* ont souvent recours à la justice, parfois avec succès, pour les faire déclarer illégales ou disproportionnées par rapport au dommage causé (*infra*, n^{os} 281 et s.). En effet, bloquer ou effacer les messages provenant d'un *spammeur*, même notoire, peut apparaître comme une mesure radicale et contraire à la liberté d'expression. Certains juges américains ont d'ailleurs condamné de telles pratiques, ce qui donne lieu à de vifs débats aux États-Unis autour du Premier Amendement de la Constitution fédérale américaine.

267. En outre, la plupart des fournisseurs d'accès ont une adresse spéciale à laquelle les victimes de *spamming* peuvent se plaindre. Ils recommandent de joindre à leur plainte une copie du message litigieux, y compris son en-tête, afin de permettre l'identification du *spammeur* et la prise d'éventuelles sanctions.

II. TOUR D'HORIZON DES SOLUTIONS JURIDIQUES EXISTANTES

268. Après avoir exposé les inconvénients du *spamming* et divers moyens permettant de les surmonter, il s'agit à présent de jeter un regard

[20] Voy. les Principes d'Utilisation Acceptable de NETural Communications, http://www.netural.com/docs/consumer/netural-aup.html

sur les solutions consacrées à ce jour au plan juridique, tant en législation qu'en jurisprudence.

Différentes directives européennes s'intéressent au problème du *spamming*. Il s'en dégage l'impression que le législateur européen tergiverse. Manifestement, il n'a pas encore adopté une position ferme et définitive sur la question. En particulier, le débat relatif au choix entre l'*opt-in* et l'*opt-out* est loin d'être tranché (A). Ces hésitations se répercutent immanquablement au niveau du droit des États membres de l'Union européenne (B). En l'absence de critères clairs et uniformes, la jurisprudence cherche pareillement sa voie (C).

A. Les hésitations du législateur européen

269. Comme le précise le considérant n° 14 de la directive sur le commerce électronique, "la mise en œuvre et l'application de la présente directive devraient être conformes aux principes relatifs à la protection des données à caractère personnel, notamment pour ce qui est des communications commerciales non sollicitées (…)". Auparavant, ce même considérant avait pris soin de souligner que la directive 95/46/CE du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données[21] et la directive 97/66/CE du 15 décembre 1997 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications[22] sont pleinement applicables aux services de la société de l'information. L'article 1er, § 5, confirme que "la présente directive n'est pas applicable : b) aux questions relatives aux services de la société de l'information couvertes par les directives 95/46/CE et 97/66/CE".

270. Les directives 'vie privée' – et les lois qui les transposent[23] – ne traitent pas directement de la question du *spamming*. Toutefois, le respect des principes qui y figurent permet de surmonter la plupart des inconvénients posés par cette pratique irritante. Nous y reviendrons ultérieurement (*infra*, nos 291 et s.). Bornons-nous ici à relever que les

[21] *J.O.C.E.*, n° L 281 du 23 nov.1995, p. 31.
[22] *J.O.C.E.*, n° L 24 du 30 janv. 1998, p. 1.
[23] En droit belge, voy. la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, *M.B.*, 18 mars 1993, p. 5801, modifiée par la loi du 11 décembre 1998 transposant la directive 95/46/CE du 24 octobre 1995 du Parlement européen et du Conseil relative à la protection des personnes physiques à l'égard du traitement de données à caractère personnel et à la libre circulation de ces données, *M.B.*, 3 fév. 1999. Pour une analyse de cette loi, voy. Th. LEONARD et Y. POULLET, "La protection des données à caractère personnel en pleine (r)évolution - La loi du 11/12/98 transposant la Directive 95/46/CE du 24 octobre 1995", *J.T.*, 1999, pp. 377-396.

traitements des données à caractère personnel doivent respecter, notamment, les principes de loyauté, de finalité et de légitimité[24].

271. La directive 97/66/CE contient, elle, une disposition concernant plus directement notre problème. En effet, son article 12, § 1er, relatif aux "appels non sollicités", précise que "l'utilisation de systèmes automatisés d'appels sans intervention humaine (automates d'appel) ou de télécopieurs (fax) à des fins de prospection directe ne peut être autorisée que si elle vise des abonnés ayant donné leur consentement préalable". Le paragraphe 2 de cet article prévoit en outre que les appels non sollicités, effectués par d'autres moyens que ceux visés au paragraphe 1er, ne peuvent être autorisés que si les abonnés concernés ont manifesté leur consentement ou ne s'y sont pas opposés, le choix entre ces deux solutions étant régi par la législation nationale[25]. Ce texte abandonne donc aux législateurs nationaux le choix entre un système d'*opt-in* ou d'*opt-out*.

272. La directive sur le commerce électronique laisse pareillement ouvert le débat entre l'*opt-in* et l'*opt-out*. Il ressort, en effet, de la lecture de son article 7 que les États disposent d'une grande latitude dans la définition du régime des communications commerciales non sollicitées par courrier électronique : de l'autorisation pure et simple à l'interdiction absolue, en passant par toutes les solutions médianes. En cas d'autorisation, les États doivent veiller au respect des principes d'identification et de transparence déjà évoqués (*supra*, n° 238 ; voy. aussi *infra*, nos 313 et s.). Ils sont également tenus de prendre des mesures pour garantir que les *spammeurs* consultent les registres d'*opt-out* et respectent le souhait des personnes physiques qui s'y sont inscrites.

Par ailleurs, à la règle générale de l'article 3, § 1er, selon laquelle "chaque État veille à ce que les services de la société de l'information fournis par un prestataire établi sur son territoire respectent les dispositions nationales applicables dans cet État", une dérogation est prévue, précisément en ce qui concerne *l'autorisation* des communications commerciales non sollicitées par courrier électronique (cf. Annexe, dernier tiret). Cette dérogation a pour but d'empêcher un prestataire, établi dans un État membre autorisant le *spamming*, de se prévaloir de la clause "marché intérieur" de l'article 3, § 1er, pour envoyer des messages

[24] Pour une étude approfondie des principes de la directive "vie privée", voy. M.-H. BOULANGER, C. DE TERWANGNE, Th. LEONARD, S. LOUVEAUX, D. MOREAU et Y. POULLET, "La protection des données à caractère personnel en droit communautaire", *J.T.*, 1997, pp. 127 et s.

[25] Si les droits conférés par les paragraphes 1 et 2 ne s'appliquent qu'aux abonnés qui sont des personnes physiques, le paragraphe 3 demande toutefois aux États membres de garantir que les intérêts des autres abonnés soient suffisamment protégés.

non sollicités dans un État membre qui, lui, interdit le *spamming*. À l'inverse, un État membre pourrait interdire sur son territoire toute communication commerciale non sollicitée par courrier électronique, même en provenance d'un autre État. Il pourrait encore décider que l'envoi de tels messages depuis son propre territoire vers l'étranger est autorisé. Mais en réalité, dans une telle situation, il conviendra de respecter l'article 49 du Traité de Rome, qui interdit les restrictions à la libre prestation de services à l'intérieur de la Communauté à l'égard des ressortissants des États membres établis dans un pays de la Communauté autre que celui du destinataire de la prestation.

Notons que l'article 21, § 2, de la directive prévoit la possibilité d'adapter la directive, et notamment d'appliquer les principes du marché intérieur à l'envoi par courrier électronique de communications commerciales non sollicitées. L'opportunité de ce type d'adaptations devra faire l'objet d'un rapport, présenté par la Commission, avant le 17 juillet 2003, puis tous les deux ans (art. 21, § 1er).

273. Ainsi que le souligne l'exposé des motifs de la proposition de directive concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques[26], la coexistence de régimes différents en matière de *spamming* n'est pas satisfaisante du point de vue du marché intérieur. En effet, les entreprises établies sur le territoire de pays ayant opté pour un régime de consentement explicite ne peuvent plus envoyer de communications commerciales non sollicitées dans leur propre pays, mais peuvent continuer à les envoyer à des personnes résidant dans des pays qui ont adopté un système d'*opt-out*. Se pose en outre la question de l'identification du pays de résidence des destinataires de messages non sollicités dans la mesure où les adresses de courrier électronique ne donnent, souvent, aucune indication à ce sujet.

L'article 13 de la proposition de directive – intitulé "Communications non sollicitées" – dispose que "l'utilisation de systèmes automatisés d'appel sans intervention humaine (automates d'appel), de télécopieurs ou de courrier électronique à des fins de prospection directe ne peut être autorisée que si elle vise des abonnés ayant donné leur consentement préalable".

La proposition de directive reprend, en son article 13, le contenu de l'article 12 de la directive 97/66/CE, en ajoutant le courrier électronique

[26] COM (2000) 385 final, *J.O.C.E.*, n° C 365 E du 19 décembre 2000, p. 223.

au nombre des moyens de communication nécessitant le consentement préalable du destinataire lorsqu'ils sont utilisés à des fins commerciales. Notons que le terme "appels" de la directive sur les contrats à distance[27] a été remplacé par celui de "communications" que la Commission européenne estime plus neutre sur le plan technologique.

274. Ainsi, alors que la directive sur le commerce électronique laisse aux États membres le choix entre l'*opt-in* et l'*opt-out*, la proposition de directive "communications commerciales" se prononce explicitement en faveur de l'*opt-in* pour résoudre le problème du *spamming* [28].

Ces divergences d'opinions au sein même de la Commission européenne ont semé la confusion parmi les États membres, qui, dans ces circonstances, ont opéré des choix en sens divers.

B. Aperçu de droit comparé

275. Certains États ont d'ores et déjà adopté des mesures, plus ou moins contraignantes, concernant les communications commerciales non sollicitées.

1. L'autorisation des communications commerciales à certaines conditions

276. Parmi les différents types de mesures pouvant être adoptées, la moins stricte consiste à autoriser l'envoi de communications commerciales non sollicitées moyennant le respect de certaines conditions. Ainsi, aux États-Unis, de nombreux projets de loi sont en

[27] Directive 97/7/CE du Parlement européen et du Conseil du 24 octobre 1995 concernant la protection des consommateurs en matière de contrats à distance, *J.O.C.E.*, n° L 144 du 4 juin 1997, p. 19. L'article 10, § 1er, de cette directive, relatif aux "limites à l'utilisation de certaines techniques de communication à distance", prévoit, que l'utilisation par un fournisseur de systèmes automatisés d'appel sans intervention humaine (automates d'appel) ainsi que de télécopieurs est soumise au consentement préalable du consommateur. Les autres techniques de communication à distance (dont une liste indicative figure à l'annexe I), ne peuvent être utilisées qu'en l'absence d'opposition manifeste du consommateur.
L'article 14 de la directive, qualifié de "clause minimale", précise toutefois que les États membres peuvent adopter ou maintenir, dans le domaine régi par la directive, "des dispositions plus strictes compatibles avec le traité, pour assurer un niveau de protection plus élevé au consommateur".

[28] Concernant le traitement de données, il convient de souligner que l'article 12 de cette proposition de directive donne aux abonnés le droit de décider si les données les concernant doivent ou non figurer dans un annuaire public et, dans l'affirmative, de déterminer lesquelles de ces données doivent être rendues publiques. Les abonnés doivent en outre être informés de toute autre possibilité d'utilisation de l'annuaire.

préparation, afin d'autoriser le marketing par e-mail, tout en prévoyant des mesures de lutte contre le *spamming*[29].

La plupart de ces projets imposent des obligations aux expéditeurs de tels e-mails. Ceux-ci devraient, par exemple, indiquer dans le message qu'il s'agit d'un courrier électronique non sollicité à caractère commercial et que le destinataire a le droit de notifier sa décision de ne plus recevoir pareil message. Ils devraient également fournir une adresse électronique à laquelle le destinataire pourra signifier un tel souhait. Enfin, ils seraient tenus de retirer de leurs listes de diffusion l'adresse e-mail de tout destinataire qui en fait la demande. Il s'agit là d'une forme d'*opt-out*, sans registre centralisé, offrant la possibilité de demander individuellement à chaque *spammeur* de ne plus recevoir d'e-mails publicitaires de sa part. Sachant qu'il est fréquent, aux États-Unis, de recevoir des dizaines de *spams* tous les jours, un tel système ne devrait pas être d'un grand secours aux victimes de *spamming*. Par ailleurs, de nombreux textes interdisent la falsification des en-têtes de message, ainsi que l'utilisation de l'adresse électronique ou de l'identité d'un tiers sans son autorisation.

Certains projets prévoient en outre que les fournisseurs d'accès ont le droit d'agir en justice à l'encontre de toute personne qui ne se conformerait pas à leur politique en matière de *spamming*, telle qu'elle doit être affichée sur leur site web. C'est donc au juge américain que reviendrait la tâche délicate de régler les conflits liés au *spamming*. D'autres projets confient à la *Federal Trade Commission* le soin de veiller au respect de la réglementation anti-*spamming*. Ceci dit, la menace d'une action en justice peut constituer une arme efficace contre les *spammeurs*, et nombreux sont les FAI qui en usaient déjà auparavant, souvent avec succès (voy. *infra*, n^{os} 281 et s.). Des peines d'amendes sont également envisagées, parfois en fonction du nombre d'e-mails envoyés.

2. L'interdiction des communications commerciales non sollicitées sans l'accord préalable du destinataire

277. L'Autriche[30] et l'Italie[31] ont choisi d'appliquer un système d'*opt-in*. En Autriche, les appels (y compris les fax) réalisés dans un but commercial ne sont pas autorisés sans l'accord préalable de la personne concernée. La loi précise que l'envoi d'e-mails commerciaux ou de

[29] Ces projets de loi sont accessibles à partir du site de CAUCE (*Coalition Against Unsolicited Commercial Email*), à l'adresse http://www.cauce.org/legislation/index.shtml.
[30] Loi du 9 juillet 1997 sur les télécommunications, modifiée par la loi du 19 août 1999.
[31] Décret législatif du 22 mai 1999 transposant la Directive 97/7/CE du Parlement européen et du Conseil du 22 mai 1997 concernant la protection des consommateurs en matière de contrats à distance.

spamming requiert l'accord préalable du destinataire. Un tel consentement peut être révoqué à tout moment. Toute personne qui enverra des communications commerciales non sollicitées, des e-mails publicitaires ou du *spamming* en violation de cette disposition est passible d'une amende de 500.000 Schilling (soit environ 36.000 Euros !).

En transposant la directive sur les contrats à distance, l'Italie a ajouté le courrier électronique à la liste des moyens de communication (fax, automate d'appel) qui requièrent le consentement préalable du destinataire, lorsqu'ils sont utilisés dans un but commercial. Une peine d'amende de 500 à 5.000 Euros est également prévue en cas de violation de la loi, cette peine pouvant être doublée en cas de récidive grave.

278. Au Danemark[32], il est également interdit de contacter quelqu'un par e-mail, par un automate d'appel ou par fax, dans le but de lui vendre des biens ou des services, à moins que la personne ait donné son consentement préalable à recevoir de telles communications. En revanche, il est permis de contacter une personne par un autre moyen de communication, à moins qu'elle n'ait exprimé son désir de ne pas recevoir de tels appels en s'inscrivant dans une liste *opt-out* établie par le "*Civil Registration System*".

3. Les systèmes hybrides

279. La Finlande[33] établit des distinctions en fonction de la personne qui est destinataire du message. Il est interdit d'envoyer des communications commerciales non sollicitées à des particuliers ou à des groupes de discussion. Il est précisé que l'envoi de *spamming* d'un autre pays vers la Finlande est également illégal. Par contre, lorsque le destinataire est un professionnel, les communications commerciales sont autorisées, à moins qu'il n'ait signifié son souhait de ne plus en recevoir. La Finlande a donc opté pour une interdiction absolue du *spamming* en ce qui concerne les particuliers et pour un système d'*opt-out* en ce qui concerne les professionnels. Il n'est cependant pas certain qu'une telle interdiction, radicale et inconditionnelle, convienne parfaitement aux attentes des consommateurs. De plus, elle prive les entreprises d'un outil de marketing simple et peu coûteux.

[32] *Consolidated Act* No. 699 of 17 July, 2000, *The Danish Marketing Practices Act*.
[33] Pour plus de détails, voy. le site d'Euro CAUCE, http://www.euro.cauce.org/fr/countries/c_fi.html .

4. L'interdiction de certains types de communications commerciales

280. La loi "anti-*spamming*" adoptée par l'État de Washington est considérée, aux États-Unis, comme l'une des plus contraignantes en la matière. Cette loi prohibe les courriers électroniques commerciaux qui affichent, dans l'espace réservé à l'objet du message, une information trompeuse, mais aussi les e-mails contenant une adresse de retour incorrecte ou dont le chemin de transmission sur l'internet, indiqué dans l'en-tête du message, a été falsifié. En outre, il est permis aux personnes physiques ou morales de l'État de Washington, ainsi qu'au Procureur général de cet État, d'intenter une action civile contre les *spammeurs*. Depuis l'adoption de la loi en 1998, cette possibilité a fréquemment été utilisée, et de nombreuses actions judiciaires ont été intentées[34].

C. La diversité des approches jurisprudentielles

281. On épingle ici quelques décision jurisprudentielles, américaines et européennes, traitant du problème du *spamming*.

1. La jurisprudence nord-américaine

282. Ces dernières années, les juges nord-américains ont souvent été amenés à trancher des litiges opposant des fournisseurs d'accès à des *spammeurs*. Bien qu'il soit encore trop tôt pour qu'une jurisprudence constante se dégage de ces arrêts, certains d'entre eux ont fait sensation en appliquant pour la première fois certains principes ou législations américains à l'envoi de courrier électronique non sollicité.

283. Aux États-Unis, le débat fait rage autour de la question de savoir si le *spamming* est protégé ou non par le Premier amendement de la Constitution américaine, qui assure de manière très large la liberté d'expression. Des arrêts divergents ont été rendus à ce sujet, mais certains commentateurs affirment que la jurisprudence s'oriente vers une réponse négative. Si elle venait à se confirmer, une telle jurisprudence priverait les *spammeurs* d'un de leurs principaux moyens de défense. Dans le même ordre d'idées, la jurisprudence est divisée quant au droit qu'aurait le FAI de bloquer l'accès à son serveur à tout message provenant d'un nom de domaine particulier qui pratiquerait le *spamming* en violation de la

[34] Pour une application récente de cette loi, voy. l'article de D. ASSOR, "La loi 'anti-*spams*' de Washington, inconstitutionnelle", sur le site Juriscom, http://www.juriscom.net/elaw/e-law15-16.htm#11.

politique du FAI. Ainsi, une décision *Cyberpromotions v. AOL* [35] interdit à AOL de bloquer le nom de domaine de Cyberpromotions, mais l'autorise à fournir à ses usagers un logiciel pour filtrer tous les messages provenant du FAI de Cyberpromotions. À l'inverse, dans l'affaire *Compuserve v. Cyberpromotions* [36], le juge autorise le FAI Compuserve à bloquer le nom de domaine de Cyberpromotion si ce dernier ne respectait pas certaines conventions de Compuserve.

284. En revanche, il est extrêmement fréquent que les juges accordent aux fournisseurs d'accès un droit au remboursement, par le *spammeur*, des frais occasionnés par la gestion d'un volume important de courrier électronique sur le serveur du FAI. En outre, le montant de ces frais est souvent multiplié par deux ou trois, à titre de dommages et intérêts, pour sanctionner le comportement dolosif du *spammeur*. Ces mesures sont en général accompagnées d'une injonction permanente faite au *spammeur* de ne plus envoyer de courrier électronique aux clients du FAI concerné. Ainsi, un arrêt *Concentric v. Cyberpromotion* [37] interdit à Cyberpromotion d'envoyer des e-mails aux clients de Concentric, d'utiliser le réseau de Concentric ou d'effectuer une contrefaçon du nom de Concentric dans ses e-mails.

285. Les clauses contractuelles insérées dans les conventions de fourniture d'accès au réseau constituent un procédé efficace de lutte contre le *spamming*. Nombreux sont les FAI qui imposent à leur cocontractant le respect de la Nétiquette lors de l'envoi de courrier électronique ou lors de la participation à un groupe de discussion. En cas de violation de semblables clauses, le FAI se réserve le droit de rompre le contrat et de suspendre ou de fermer l'accès au réseau pour le client. Dans l'affaire *1267623 Ontario Inc. V. Nexx Online*[38], la Cour supérieure de l'Ontario a légitimé de telles sanctions. Le juge conclut qu'au vu de la jurisprudence américaine (le Canada ne disposant pas de jurisprudence en la matière), des extraits de rapports fournis sur le *spamming* et de la réaction des internautes, il semble clair que l'envoi massif de courrier électronique non sollicité à des fins commerciales est contraire aux principes de la Nétiquette, sauf si un fournisseur d'accès le permet spécifiquement par contrat. Ainsi, le FAI Nexx Online avait le droit de

[35] *Cyber Promotions, Inc. v. America Online, Inc*., C.A. No. 96-2486 (E.D. Pa. Feb. 4, 1997), voy. le compte rendu de ce jugement à http://news.cnet.com/news/0-1005-200-316333.html?tag=/ .
[36] *CompuServe Inc. v. Cyber Promotions, Inc*., No. C2-96-1070 (E.D. Pa. May 9, 1997), http://www.jmls.edu/cyber/cases/cs-cp3.html.
[37] *Concentric Network Corp. v. Wallace,* No. C-96 20829-RMW (EAI) (N.D. Cal. Nov. 5, 1996), http://www.jmls.edu/cyber/cases/concent1.html.
[38] *1267623 Ontario Inc. v. Nexx Online Inc.,* [1999] O.J. No. 2246 Court File No. C20546/99 (Ontario Superior Court of Justice, June 14, 1999)(CANADA), http://www.ncf.carleton.ca/~ag221/ruling.txt.

fermer le site de la compagnie Ontario et de rompre leur contrat, après un avertissement, au motif qu'il avait reçu de nombreuses plaintes d'internautes concernant l'envoi d'e-mails non sollicités en provenance d'Ontario Inc[39].

286. La violation du droit des marques est désormais invoquée avec succès par les FAI, dont le nom de domaine est utilisé frauduleusement dans le contenu du message, ou figure à tort dans un en-tête falsifié[40]. Les fournisseurs d'accès sont en effet très sensibles à ces usages illégitimes de leur nom de domaine, qui nuisent à leur réputation en donnant à croire aux victimes du *spamming* que le FAI cautionne ce genre de pratiques.

287. Enfin, de plus en plus de FAI installent, sur leur serveur ou sur le routeur d'entrée de leur réseau, des logiciels et des systèmes de filtrage, destinés à détecter et à bloquer les *spams*. Face à ces mesures défensives, de nombreux *spammeurs* emploient de nouvelles techniques et développent des logiciels pour forcer les barrages et continuer ainsi à inonder le réseau de *spamming*. Depuis 1998, ces méthodes sont considérées par certains juges comme contraires aux lois sur la fraude informatique[41]. Les fournisseurs d'accès disposent ainsi d'une nouvelle arme juridique contre les *spammeurs*.

2. La jurisprudence en Europe

288. En Espagne, dans une décision inédite, l'Agence de Protection des Données (*Agencia de Protección de Datos*) a sanctionné, sur la base de l'article 43, § 3, d, de la loi espagnole sur la protection des données (LORTAD[42]), une société établie en Espagne qui avait répondu par un e-mail publicitaire au message d'un internaute manifestant sa volonté de ne plus recevoir de la publicité de sa part. Selon l'Agence, il s'agissait en l'occurrence d'une atteinte caractérisée à l'intimité de la vie privée.

289. En Allemagne, diverses décisions concernant le *spamming* ont déjà été rendues en sens divers. Plusieurs juges ont considéré que le *spamming*

---

[39] Voy. un commentaire de cet arrêt par M.-H. DESCHAMPRS-MARQUIS, "Courriels indésirables s'abstenir !", http://www.juriscom.net/espace1/art8.htm .

[40] Voy. sur ce point un article paru sur CNET news.com (http://news.cnet.com/news/0-1005-202-336642.html) concernant trois affaires de ce genre, impliquant le fournisseur d'accès AOL, rendues en décembre 1998 : *AOL Inc. v. LCGM, Inc*. (http://legal.web.aol.com/decisions/dljunk/lcgmopin.html), *AOL, Inc. v. Prime Data Systems, Inc.* (http://zeus.bna.com/e-law/cases/prim01.html) et *AOL, Inc. v. IMS, Inc.*
(http://legal.web.aol.com/decisions/dljunk/imsopin.html).

[41] Voy. l'arrêt *AOL v. LCGM, op. cit*.

[42] *Ley Orgánica del Tratamiento Automatizado de Datos* (LORTAD) Loi organique 5/1992, du 29 octobre 1992.

entraînait des pertes économiques pour les internautes du fait de l'augmentation des coûts de connexion dus au téléchargement des messages[43]. Un tribunal a condamné le *spamming* au motif qu'il porte atteinte à la vie privée[44]. À l'inverse, un tribunal de Kiel a admis la licéité du *spamming* au motif que la directive 97/7 sur les contrats à distance ne prohibait pas ce genre de pratiques[45]. Il semble cependant qu'il s'agisse d'une jurisprudence isolée[46].

III. APPRÉCIATIONS CRITIQUES

290. En substance, les inconvénients majeurs posés par le *spamming* se déclinent comme suit : 1° la captation d'adresses e-mail sur les espaces publics de l'internet, sans le consentement des personnes concernées – en vue de leur utilisation à des fins de *marketing* direct, ou *one to one* – pose question au regard des exigences légales en matière de protection de la vie privée ; 2° l'obstruction du réseau, des serveurs et des boîtes aux lettres électroniques est source de préjudices tant pour les destinataires des *spams* que pour l'ensemble de la communauté des usagers de l'internet ; 3° le comportement frauduleux de certains *spammeurs*, à défaut de pouvoir les identifier, rend malaisée l'application d'éventuelles sanctions.

Nous avons exposé diverses solutions apportées aux problèmes épinglés, soit par le législateur européen et, à sa suite, par les législateurs nationaux, soit sous l'action des cours et tribunaux.

Il s'agit à présent d'évaluer ces solutions, de manière critique, afin de pouvoir suggérer une politique juridique efficace et cohérente en la matière. A cet effet, nous procéderons en trois temps. Après un rappel des incontournables exigences légales relatives à la protection de la vie privée (A), nous tâcherons de faire le point sur le débat *opt-in/opt-out* (B), avant de conclure par un essai de synthèse (C).

---

[43] LG Traunstein 18/12/97, 2 HKO 3755/97, voy. http://www.jmls.edu/cyber/cases/traun.html et LG Berlin, 14/05/98, 16 O 301/98 et 02/04/98 16 O 201/98,. voir http://www-domino.crpgl.lu/HomePage/lde.nsf.

[44] AG Brakel, 11/02/98, 7 C 748/97, voy. http://www-domino.crpgl.lu/HomePage/lde.nsf.

[45] AG Kiel, 30/09/99, 110 C 243/99, voir http://www-domino.crpgl.lu/HomePage/lde.nsf

[46] Ces informations sont issues de la chronique du 17 février 2000 du Laboratoire de Droit Economique du Centre de Recherche Public Gabriel Lippmann Luxembourg, http://www-domino.crpgl.lu/HomePage/lde.nsf.

A. Le nécessaire respect de la législation relative à la protection de la vie privée

291. On l'a vu, en amont du phénomène du *spamming*, la collecte et l'utilisation des adresses de courrier électronique posent question au regard de la protection des données à caractère personnel (*supra*, n° 248). En droit belge, tout traitement de données à caractère personnel doit être conforme à la loi relative à la protection de la vie privée[47] (ci-après : "la loi"), qui pose une série de principes.

292. En premier lieu, la finalité poursuivie par le responsable du traitement doit être légitime (principes de finalité et de légitimité, inscrits à l'art. 4, § 1er, 2°, de la loi). Cette légitimité s'apprécie en mettant en balance, d'une part, les intérêts légitimes du responsable du traitement, d'autre part, le droit à la protection de la vie privée de la personne concernée (principe de proportionnalité, inscrit à l'art. 5, f, de la loi). Dans un avis relatif à la protection de la vie privée dans le cadre du commerce électronique, la Commission de la protection de la vie privée précise : "lorsque des données sont collectées et utilisées à des fins de marketing ciblé (*marketing one to one*), il ne paraît pas qu'un équilibre entre les droits et intérêts des parties en présence soit atteint. Il faudra dans ce cas obtenir le consentement de la personne concernée, tel que le prévoit l'article 5a [de la loi]"[48].

Selon cette interprétation, la légalité du traitement des données serait subordonnée au consentement *préalable* de la personne, même si la loi ne le dit pas de manière explicite. Il s'agit bien, de la part de la Commission de la protection de la vie privée, d'une prise de position ferme en faveur de l'*opt-in* (*infra*, n° 310). La loi, quant à elle, stipule clairement que, lorsque les données sont collectées à des fins de *marketing* direct, la personne concernée a le droit de s'opposer, gratuitement et sans aucune justification, au traitement de ses données (art. 12, § 1er, al. 3, de la loi). La Commission ajoute que "la faculté qui serait laissée au particulier de s'opposer *a posteriori* (*opt-out*) à ce traitement est insuffisante"[49].

---

[47] Loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, *M.B.*, 18 mars 1993, p. 5801, modifiée par la loi du 11 décembre 1998 transposant la directive 95/46/CE, *M.B.*, 3 février 1999.

[48] Avis n° 34/2000 de la Commission pour le protection de la vie privée, du 22 novembre 2000, relatif à la protection de la vie privée dans le cadre du commerce électronique, pp. 5 et 9. L'avis est disponible en ligne à l'adresse : http://www.privacy.fgov.be.

[49] Voy. l'avis n° 34/2000, *op. cit.*, p. 9.

293. En tout état de cause, préalable ou non, le consentement doit être libre, spécifique et informé (art. 1er, § 8, de la loi)[50].

Le consentement doit être libre, c'est-à-dire donné sans qu'aucune pression n'ait été exercée sur la personne concernée. Ainsi, aucune discrimination ne pourra être établie dans le cadre de la fourniture d'un service ou d'un produit demandé, vis-à-vis de ceux qui auront refusé de divulguer, par exemple, leur adresse e-mail à des fins de *marketing* [51].

Le consentement doit porter sur des traitements spécifiques et précisément définis. Il ne peut avoir un objet général ou indéterminé. En outre, les données traitées ne peuvent être utilisées d'une manière incompatible avec la finalité déclarée (principe de compatibilité, inscrit à l'art. 4, § 1er, 2°, de la loi). Ainsi, les adresses de courrier électronique disponibles sur des sites publics (groupe de discussion, forum, *chat*…) sont diffusées dans un contexte spécifique, par exemple l'échange de vues sur un sujet déterminé, et ne peuvent être utilisées à des fins de prospection commerciale[52].

Enfin, le consentement doit être informé. A cet égard, dans un souci de transparence, une série d'informations doivent être communiquées à la personne dont les données sont traitées (art. 9 de la loi). La loi distingue selon que les données sont obtenues directement auprès de la personne concernée (art. 9, § 1er) ou auprès d'un tiers (art. 9, § 2). Dans les deux cas, elle impose une information minimale, concernant le nom et l'adresse du responsable du traitement, les finalités du traitement, les destinataires des données, l'existence d'un droit d'accès et de rectification des données, le cas échéant, et du droit de s'opposer, gratuitement et sans aucune justification, au traitement de ses données à des fins de *marketing*.

Lorsque les données sont obtenues directement auprès de la personne concernée, le caractère obligatoire ou non des réponses aux demandes de

---

[50] Concernant les conditions du consentement comme source de la légitimité des finalités de marketing "*one to one*", voy. Th. LÉONARD, "E-commerce et protection des données à caractère personnel. Quelques considérations sur la licéité des pratiques nouvelles de marketing sur internet", pp. 11 et s., disponible en ligne à l'adresse suivante : http://www.droit.fundp.ac.be/Textes/Leonard1.pdf ; Th. LEONARD et Y. POULLET, "La protection des données à caractère personnel en pleine (r)évolution. - La loi du 11/12/98 transposant la Directive 95/46/CE du 24 octobre 1995", *J.T.*, 1999, p. 380, n° 7.

[51] Avis n° 34/2000 précité, *op. cit.*, p. 8. Selon Th. LEONARD et Y. POULLET ("La protection des données à caractère personnel en pleine (r)évolution…", *op. cit.*, p. 380, n° 7), cette condition paraît bien illusoire en pratique : "La pression économique consistant dans le risque de se voir refuser un produit ou un service considérés à tort ou à raison comme essentiels par la personne concernée l'amènera bien souvent à donner son consentement sans aucun esprit critique".

[52] Voy. l'avis n° 34/2000, *op. cit.*, p. 6.

renseignements doit apparaître clairement[53]. Les informations mentionnées ci-dessus doivent être communiquées au moment de la collecte. Mais il arrive également que les données soient collectées auprès d'un tiers (*supra* , n° 248). Dans ce cas, la loi prévoit que la personne a le droit d'être informée dès l'enregistrement des données ou, au plus tard, au moment de la première communication des données à un tiers, le cas échéant. Concernant le *marketing* direct, la personne est souvent informée de l'existence d'un traitement de ses données lorsqu'elle reçoit une publicité non sollicitée par courrier électronique. Selon la Commission de la protection de la vie privée, les informations requises devraient figurer de manière complète et précise dans le corps du message de courrier électronique, et un moyen simple et direct d'exercer le droit d'opposition devrait être fourni à la personne concernée, par exemple en cliquant sur un hyperlien ou en répondant au message. Semblable e-mail publicitaire devrait en outre préciser que la personne peut exercer ce droit de refus à tout moment[54].

294. Assurément, une correcte application de la législation relative à la protection de la vie privée permettrait de régler nombre de problèmes liés au *spamming*, en assurant une collecte licite et un usage loyal des adresses de courrier électronique à des fins publicitaires. A cet égard, on note qu'un nombre croissant de prestataires affichent sur leur site une politique de protection de la vie privée (*Privacy Policy*). Ils ont d'ailleurs tout à y gagner, à commencer par la confiance de leur clientèle, élément indispensable au développement de leur négoce sur les réseaux. Malgré tout, l'expérience montre que certains prestataires recourent à des manœuvres peu transparentes, voire illicites, pour se procurer des fichiers d'adresses (*supra*, n° 248). Outre un problème de contrôle de l'application de la loi, ce constat révèle la nécessité de prendre à l'encontre du *spamming* des mesures supplémentaires, ce qui nous amène à nous pencher sur le débat que suscitent les solutions de l'*opt-in* et de l'*opt-out.*

B. Le débat opt-in/opt-out

295. Deux solutions sont généralement avancées face au problème du *spamming* : d'un côté, l'autorisation de principe des communications commerciales non sollicitées par courrier électronique, à moins que leur destinataire ne s'y soit opposé (*opt-out*) ; de l'autre, l'interdiction de

[53] En pratique, le caractère obligatoire des informations à communiquer par la personne concernée est généralement indiqué à l'aide d'une astérisque, placée à côté des champs concernés du formulaire à remplir.
[54] Voy. l'avis n° 34/2000, *op. cit.*, p. 9.

telles communications, à moins d'avoir obtenu le consentement préalable de leur destinataire (*opt-in*). Loin du débat politique mené actuellement autour de ces deux systèmes, nous tenterons de faire la lumière sur les différents avantages et inconvénients de l'un et l'autre.

*1. L'***opt-out** *: la liberté du commerce*

296. Fondé sur le principe de liberté du commerce, le système de l'*opt-out* permet aux annonceurs d'envoyer des communications commerciales non sollicitées par e-mail, sous certaines conditions. L'avantage est de taille pour les prestataires, et singulièrement les PME, étant donné que le courrier électronique publicitaire représente un outil particulièrement précieux pour le développement de leurs activités en ligne (*supra*, n° 244).

En termes de lutte contre le *spamming*, l'*opt-out* intervient *a posteriori*, par l'exercice du droit de s'opposer à recevoir des courriers électroniques non sollicités à l'avenir. D'évidence, une opposition exprimée au cas par cas, adressée individuellement à l'annonceur en réponse à son e-mail, s'avère totalement impuissante à diminuer le volume de *spams* en circulation sur les réseaux. Dès lors, l'adoption d'un système d'*opt-out* efficace nécessite la mise en place de registres d'opposition, dressant la liste des personnes qui ne désirent plus recevoir de publicités non sollicitées par courrier électronique.

L'*opt-out* n'a pas pour effet d'assainir la collecte d'adresses e-mail, mais l'utilisation de ces dernières. Les annonceurs ont l'obligation de consulter régulièrement ces registres, et de respecter la volonté des personnes qui y sont inscrites (art. 7, § 2, de la directive sur le commerce électronique). En pratique, cela signifie que les annonceurs, avant de lancer une campagne de *spamming*, doivent rayer de leurs listes d'adresses tous les noms des personnes figurant sur ces registres. Peu importe, dès lors, la méthode employée pour se constituer de telles listes. Le problème de la collecte 'sauvage' d'adresses est donc renvoyé à l'application et au contrôle strict de la législation relative à la protection de la vie privée.

297. La figure du registre *opt-out* est loin d'être une nouveauté. Elle existe déjà dans de nombreux pays pour les modes traditionnels de marketing direct (courrier postal, téléphone, fax) et relève le plus souvent d'initiatives privées. Toutefois, il convient de souligner une différence de taille entre ces modes traditionnels de publicité *one to one* et le courrier électronique non sollicité. Le coût élevé des premiers contraint pratiquement les annonceurs à se cantonner au territoire d'un État, alors

que le phénomène du *spamming*, lui, est d'ampleur internationale, vu son faible coût et les facilités de communication en réseau ouvert. Dans ces circonstances, il est peu probable que l'inscription d'une poignée d'internautes belges sur un registre d'opposition national ait pour effet de diminuer considérablement le volume de courriers électroniques non sollicités qui atteignent leur boîte aux lettres électroniques. Par ailleurs, il serait excessif et impraticable d'imposer aux prestataires de consulter régulièrement toutes les listes d'opposition nationales (voire régionales ou sectorielles) existantes. Dès lors, il convient de veiller à la centralisation ou à l'interconnexion des registres *opt-out* à un niveau européen, ou mieux, international[55].

298. La mise en place d'un réseau de registres d'opposition au niveau international nécessite un investissement important. Pour que le jeu en vaille la chandelle, il faut qu'une telle opération rencontre un certain succès auprès du public, faute de quoi, l'impact sur le *spamming* sera quasiment nul. En conséquence, il convient d'accorder une attention particulière à la 'publicité' de ces registres. A cet égard, l'on pourrait imposer aux annonceurs une obligation d'information concernant l'existence de ces registres et leurs modalités de fonctionnement, lors de l'envoi d'e-mails publicitaires non sollicités. Par ailleurs, les associations de consommateurs, mais aussi les fournisseurs d'accès, pourraient communiquer une information complète sur ces registres, ainsi que sur les droits des internautes face au *spamming* et les recours dont ils disposent en cas de violation par les prestataires des obligations qui leur sont imposées. En outre, le fonctionnement de tels registres doit revêtir une grande simplicité. L'inscription doit être possible en ligne, gratuite, et effective dans un délai raisonnable.

299. S'agissant de listes de données personnelles, il est indispensable d'assurer une protection efficace contre toute intrusion frauduleuse dans le système, tout en maintenant un accès suffisamment aisé pour permettre aux annonceurs de consulter régulièrement les registres. A cet égard, un équilibre doit être trouvé entre sécurité et simplicité du système.

300. Quant à la gestion de tels registres, elle devrait être confiée à un organisme de confiance, public ou privé, dont l'activité serait réglementée.

---

[55] Cf. R. JULIÀ-BARCELÓ, E. MONTERO et A. SALAÜN, "La proposition de directive européenne sur le commerce électronique : questions choisies", *op. cit*., pp. 12-13.

Dans ces conditions, l'instauration de registres *opt-out*, si elle permet de préserver la liberté du commerce, s'avère donc complexe et coûteuse.

*2. L'***opt-in** *: la protection de la vie privée*

301. L'interdiction de l'envoi de communications commerciales non sollicitées, traite le problème à sa source : le volume de messages en circulation sur les réseaux est considérablement réduit, supprimant ainsi la plupart des inconvénients liés au *spamming*. En outre, dans un tel système, toute publicité par e-mail doit, par définition, être sollicitée. Ainsi, l'*opt-in* privilégie avant tout la protection de la vie privée : la collecte d'adresses de courrier électronique et leur utilisation à des fins de marketing sont subordonnées au consentement préalable de la personne concernée.

302. Pour l'annonceur, la tâche se complique sérieusement, dans un tel système, lorsqu'il s'agit d'obtenir ce consentement. Rappelons que la loi relative à la protection de la vie privée exige que le consentement soit libre, spécifique et informé (*supra*, n° 293). En outre, vu la philosophie et les objectifs qui sous-tendent l'*opt-in*, il ne serait guère admissible que le consentement à recevoir des publicités par e-mail soit demandé… par e-mail ! Une telle pratique s'apparenterait à du *spamming*. L'accord devra donc être obtenu par d'autres moyens, moins intrusifs et suscitant davantage la confiance. A cet égard, il est possible d'envisager un *opt-in* individuel, intervenant dans le cadre d'une relation entre un prestataire et son client, ou un *opt-in* général, par la création de registres, dans lesquels les internautes s'inscriraient pour recevoir les publicités qui les intéressent.

303. L'intérêt de l'*opt-in*, du point de vue commercial, est de permettre l'obtention de profils ciblés de clients potentiels. En effet, le consentement à recevoir des e-mails publicitaires porte le plus souvent sur des catégories précises de produits ou de services. Dès lors, le marché des profils détaillés de consommateur est nettement plus juteux que celui des simples listes d'adresses e-mail, et les risques de détournement sont bien réels à cet égard. Alors que le problème de l'atteinte à la vie privée est supprimé au niveau de la collecte des adresses, il menace de resurgir sur le plan de l'usage abusif qui pourrait en être fait.

En outre, les publicités sollicitées par e-mail ont de grandes chances d'être accueillies favorablement par leur destinataire, alors que le *spamming* est le plus souvent 'mis à la corbeille' sans avoir été lu. Cependant, en pratique, les listes d'*opt-in* développées sur le marché

rencontrent actuellement un faible succès auprès des internautes, ce qui diminue considérablement leur valeur commerciale. En effet, l'aversion des internautes à l'égard des e-mails publicitaires ainsi que la crainte d'un détournement de leurs données personnelles constituent autant d'obstacles au développement de telles listes.

304. Par ailleurs, l'interdiction des publicités non sollicitées par e-mail pourrait se révéler néfaste pour les petites et moyennes entreprises, qui se voient privées d'un moyen de promotion commode et peu coûteux. En effet, le recours aux autres modes de publicité (bannières, marketing par courrier postal, télévision, affichage…) s'avère nettement plus onéreux. Le choix de l'*opt-in*, risque de mettre à mal la liberté du commerce et les intérêts économiques de certains prestataires. Pareille solution semble favoriser les grandes entreprises qui peuvent se payer le luxe de campagnes publicitaires coûteuses, notamment sur les chaînes de télévision européennes.

305. On peut également s'interroger sur la conformité de ce système avec l'article 10 de la Convention européenne des droits de l'homme, protégeant la liberté d'expression (qui comprend la liberté d'opinion et la liberté de recevoir ou de communiquer des informations…). Un débat similaire a lieu aux États-Unis au regard du Premier Amendement de la Constitution. L'interdiction, par voie légale, de l'utilisation d'un moyen de communication pour l'expression d'un message d'un type spécifique (la communication commerciale) pourrait-elle s'autoriser de l'un des motifs énumérés à l'alinéa second de l'article 10 ? Il faudrait réaliser le test de proportionnalité consistant à pondérer les droits, libertés et intérêts en concours de manière à vérifier si l'éventuelle restriction apportée à la liberté de communication n'excède pas ce qui est nécessaire à la protection des valeurs et intérêts prétendument lésés par la pratique du *spamming*.

C. Essai de synthèse et recommandations

306. La solution au problème du *spamming* nécessite avant tout de trancher entre autorisation ou interdiction des courriers électroniques publicitaires non sollicités (1). Toutefois, quelle que soit l'orientation retenue, elle s'avérera inopérante sans l'adoption d'une série de mesures qui nous paraissent, dans tous les cas, incontournables (2). Enfin, des mesures complémentaires, sous forme d'initiatives privées, peuvent être envisagées (3).

1. Opt-in *ou* opt-out *: quelle politique juridique ?*

307. On l'a vu, dans le débat qui oppose partisans de l'*opt-in* et défenseurs de l'*opt-out*, il existe des arguments forts de part et d'autre : protection de la vie privée, liberté du commerce, liberté d'expression… A la vérité, la décision de privilégier l'une ou l'autre solution relève avant tout d'un choix de politique juridique.

308. Selon une volumineuse étude réalisée pour le compte de la Commission européenne[56], il apparaît que les annonceurs sont de plus en plus nombreux à demander le consentement préalable de la personne concernée à recevoir de la publicité par e-mail. Les piètres résultats du *spamming* comme outil de promotion et les abus auxquels il a donné lieu ont fait réfléchir les annonceurs, qui arborent désormais l'étendard de la confiance afin d'assurer le développement de leurs activités. Toutefois, certaines sociétés de marketing estiment que l'*opt-in* n'est pas suffisant pour se faire connaître du public. Nombre d'entre elles défendent l'idée d'un système mixte, où l'*opt-out* serait la règle et où l'*opt-in* ne serait qu'une modalité de publicité supplémentaire, laissée au libre choix des acteurs concernés.

309. Les prestataires intermédiaires – fournisseurs d'accès et opérateurs de télécommunication – semblent favorables à l'idée d'un système d'*opt-in*. En effet, l'interdiction des communications commerciales non sollicitées par courrier électronique réduirait fortement le trafic sur les réseaux, les coûts d'acheminement et de gestion des messages, ainsi que les risques de dysfonctionnement (*supra*, n^{os} 255 et s.).

310. La Commission belge de la protection de la vie privée, quant à elle, prend résolument position en faveur de l'*opt-in* : "La Commission est d'avis que la collecte d'adresses électroniques et leur utilisation à des fins de marketing à l'insu de l'individu est un exemple d'utilisation de données à caractère personnel (…) contraire aux intérêts et aux droits fondamentaux de l'individu. La collecte ne devrait pouvoir être effectuée que si l'individu a donné son consentement préalable (*opt-in*) au traitement de ses données à caractère personnel. (…) Elle insiste, dès lors, pour que [le courrier électronique non sollicité] se voie appliqué le régime dont bénéficie aujourd'hui la publicité par fax et par automate d'appel, tel que visé par l'article 82 de la loi du 14 juillet 1991 [sur les pratiques du commerce et sur l'information et la protection du consommateur]"[57].

---

[56] E. DROUARD et S. GAUTHRONET, "Communications commerciales non sollicitées et protection des données", *op. cit.*, *passim*.
[57] Voy. l'avis n° 34/2000, *op. cit.*, p. 9.

Signalons que l'article 82, § 2, de la LPC – qui assure la transposition de l'article 10 de la directive du 20 mai 1997 concernant la protection des consommateurs en matière de contrats à distance – prévoit que, dans le cas de contrats à distance, l'utilisation, par un vendeur, d'un système automatisé d'appel sans intervention humaine (automate d'appel) ou d'un télécopieur nécessite le consentement préalable du consommateur (*opt-in*). Les autres techniques de communication ne peuvent, quant à elles, être utilisées qu'en l'absence d'opposition manifeste du consommateur (*opt-out*). Les modalités d'exercice de ce droit d'opposition doivent être déterminées par le Roi. Mais, il est à noter que ce dernier peut étendre la liste des techniques de communication soumises au consentement préalable du consommateur. De la sorte, certaines techniques de communication soumises au régime de l'*opt-out* peuvent passer sous le régime de l'*opt-in*.

311. Au niveau européen, l'examen de quelques textes révèle que la Commission européenne ne parlait pas d'une seule voix (*supra*, n^{os} 269 et s.). Jusqu'ici, elle laissait les États membres libres de choisir l'une ou l'autre solution (cf. les directives 97/7 et 97/66). Cette liberté est maintenue dans la directive sur le commerce électronique, qui se contente de préciser que les États membres ayant tranché en faveur de l'*opt-out* doivent veiller à ce que les prestataires consultent régulièrement les registres d'opposition et respectent la volonté des personnes qui y sont inscrites (art. 7, § 2). Toutefois, la dernière proposition de directive concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques impose l'*opt-in* en ce qui concerne les communication commerciales non sollicitées par courrier électronique.

312. Quoiqu'il en soit, autorisation réglementée ou interdiction stricte, une solution uniforme devra être adoptée par les États membres de l'Union européenne, sous peine de générer des entraves à la libre circulation des services de communications commerciales dans le marché intérieur.

2. De quelques certitudes

313. Quelle que soit l'orientation choisie, un certain nombre de mesures s'imposent pour régler le problème du *spamming*. A cet égard, afin d'assurer un usage loyal du courrier électronique à des fins de *marketing*, nous prônons une réglementation de *toutes* les communications commerciales par courrier électronique, qu'elles soient sollicitées ou non.

Une telle solution ne va pas à l'encontre de la directive électronique : elle dépasse son champ d'application, en réglant une question non traitée spécifiquement par la directive.

314. Selon nous, toute communication commerciale par courrier électronique doit être clairement identifiable comme telle (art. 6, a), et ce, *dès sa réception par le destinataire*. Pareille exigence va au-delà de l'article 7, § 1er, qui ne traite que des e-mails publicitaires non sollicités[58]. Nous sommes d'avis qu'une identification immédiate de toute publicité favorisera la transparence dans les pratiques de *marketing* (voy. *supra*, nos 199 et 200, notre proposition de transposition de l'article 6). En ce qui concerne le courrier électronique, cette obligation d'identification *dès la réception* a pour objectif de faciliter le fonctionnement des éventuels dispositifs de filtrage mis en place par les entreprises (cf. le considérant n° 30). Concrètement, il s'agit de faire figurer dans la rubrique "Objet" du message une mention spécifique permettant aux filtres de détecter, puis de bloquer, les messages publicitaires.

315. En outre, la personne physique ou morale, pour le compte de laquelle la communication commerciale est faite, doit être clairement identifiable (art. 6, b). Rappelons que l'article 5 de la directive impose à tout prestataire d'un service de la société de l'information de fournir un certain nombre de renseignements concernant son identité et son activité (*supra* , nos 181 et s.). Une combinaison des articles 5 et 6 de la directive nous amène à conclure qu'une publicité par courrier électronique effectuée pour le compte d'un prestataire doit permettre d'accéder facilement et directement aux informations mentionnées à l'article 5. Ces dernières pourraient apparaître dans le corps du message, ou en cliquant sur un hyperlien renvoyant directement à une page web contenant les informations requises[59].

316. Par ailleurs, il devrait être formellement interdit : *primo*, d'utiliser l'adresse de courrier électronique ou l'identité d'un tiers pour envoyer des publicités par e-mail ; *secundo*, de falsifier ou de masquer, dans l'en-tête du message, toute information permettant d'identifier son origine ou son chemin de transmission.

---

[58] L'article 23, 5°, alinéa 2, de la loi sur les pratiques du commerce dispose déjà que "La publicité par courrier électronique, non sollicitée, doit être identifiable comme telle d'une manière claire et non équivoque dès sa réception par le destinataire" (l'article 23, 5°, a été introduit dans la LPC par l'article 5, 3°, la loi du 25 mai 1999, *M.B.*, 23 juin 1999).

[59] Concernant la deuxième solution, il serait inadmissible que l'hyperlien renvoie simplement aux pages commerciales du site web du prestataire, en laissant le destinataire chercher lui-même la page contenant les renseignements sur l'identification du prestataire.

317. En outre, il convient de souligner que le destinataire d'un courrier électronique publicitaire dispose, à tout moment, d'un droit d'opposition, même si l'annonceur avait auparavant obtenu son consentement. Dès lors, il devrait être exigé que tout e-mail à caractère commercial, sollicité ou non, contienne une information claire et compréhensible concernant le droit de s'opposer à recevoir ces messages à l'avenir, et indique et mette à disposition un moyen approprié d'exercer efficacement ce droit par voie électronique. Ce moyen pourra consister, en l'indication, dans le corps du message publicitaire, d'une adresse e-mail de réponse ou d'un hyperlien renvoyant à une page web du prestataire, sur laquelle le droit d'opposition peut être exercé. Dans un système d'*opt-out*, le message devrait contenir un hyperlien renvoyant au site d'un registre d'opposition.

318. Dans l'hypothèse où un destinataire se plaindrait d'avoir reçu des publicités par e-mail alors qu'il s'y était expressément opposé, la charge de la preuve du caractère sollicité du message devrait peser sur le prestataire[60].

319. Enfin, la lutte contre le *spamming* passe inévitablement par l'instauration de mesures coercitives. A cet égard, la directive sur le commerce électronique prévoit que "les États membres déterminent le régime des sanctions applicables aux violations des dispositions nationales adoptées en application de la présente directive et prennent toutes mesures nécessaires pour assurer leur mise en œuvre. Les sanctions ainsi prévues doivent être effectives, proportionnées et dissuasives" (art. 20). Ainsi, en cas de violation des obligations et interdictions prévues par la loi en matière de *spamming*, des peines d'amende pourraient être infligées. Le *spamming* consistant souvent en des comportements répétés, toute récidive entraînerait le double de la peine prévue. L'affichage de la condamnation sur le site du prestataire pourrait être ordonnée par le juge. Notons enfin qu'une action en cessation, une procédure d'avertissement ou de transaction pourraient en outre être mises sur pied pour mettre fin aux comportements illicites des annonceurs (sur ces questions, voy. *infra*, n^{os} 733 et s.)

Soulignons toutefois la difficulté d'appliquer des sanctions à un prestataire dont le comportement illicite consiste justement à masquer soigneusement son identité par une série de procédés technologiques. Pour remédier à ce problème, une cellule technique pourrait être mise en place, dont le rôle serait de rechercher et d'identifier les *spammeurs* qui

[60] Pour un précédent de ce genre en ce qui concerne les publicités envoyées à un consommateur par fax ou par automate d'appel, voy. l'art. 82, § 1er, de la LPC, qui énonce que la preuve du consentement du consommateur incombe au vendeur.

ne se soumettent pas à la réglementation, afin de pouvoir leur appliquer les sanctions prévues.

3. Les mesures complémentaires proposées

320. Afin de résorber le problème du *spamming*, il semble indispensable de s'assurer le concours des acteurs privés du réseaux.

a) Le recours à la labellisation et aux codes de conduite

321. L'article 16 de la directive sur le commerce électronique recommande aux États membres d'encourager l'élaboration, par les associations ou organisations d'entreprises, professionnelles ou de consommateurs, de codes de conduite au niveau communautaire, destinés à contribuer à la bonne application des articles 5 à 15 de la directive (*infra*, n^{os} 551 et s.).

Le recours à des codes de conduite pourrait s'avérer précieux pour lutter contre le problème du *spamming*. La technique de la labellisation pourrait également être utilisée. En effet, l'affichage d'un label de qualité a pour but d'offrir une garantie du sérieux du prestataire, et de renforcer la confiance du consommateur, qui est une des clés du développement du commerce électronique.

322. Ainsi, les autorités de labellisation existantes pourraient se voir confier la gestion des registres *opt-out* et le soin de veiller à leur respect. Un label de qualité serait octroyé moyennant le respect d'un code de conduite. Celui-ci imposerait aux prestataires de consulter régulièrement ces registres et de se conformer à la volonté de ceux qui y sont inscrits. Il prévoirait en outre l'obligation pour le prestataire, lors de la collecte d'adresses électroniques, d'informer la personne concernée, de manière claire et complète, des finalités du traitement et de son droit d'opposition.

323. La résolution des conflits survenant suite à l'envoi de *spamming*, entre un prestataire labellisé et un internaute inscrit dans le registre *opt-out*, pourrait être facilitée par l'établissement d'un système de règlement extra-judiciaire des litiges (art. 17 de la directive, commenté *infra*, n^{os} 610 et s.). L'établissement de sanctions adéquates (retrait du label, par exemple) assurerait le respect des règles ainsi établies.

b) L'implication des prestataires intermédiaires

324. Il serait vain de vouloir réglementer le *spamming* sans le concours des acteurs du réseau. En effet, l'internet n'étant soumis à aucune autorité, la coopération active de ceux qui en constituent les rouages essentiels est indispensable au respect et à l'effectivité de la loi en la matière. Intéressés au premier chef par la problématique du *spamming*, les fournisseurs d'accès à l'internet pourraient sans doute apporter leur soutien technique à la loi. En tout état de cause, quelles que soient les solutions retenues, il est impérieux de pouvoir compter sur leur collaboration pour la mise en œuvre de celles-ci.

325. Une solution technique envisageable, parmi d'autres, serait que le FAI mette à la disposition de ses abonnés deux types d'adresses e-mail, l'une refusant toute communication commerciale non sollicitée, l'autre les acceptant[61]. Les internautes disposant du premier type d'adresse seraient ainsi à l'abri de tout courrier électronique non sollicité. Tout prestataire envoyant de tels e-mails à une adresse refusant le *spamming* devrait verser au FAI des dommages et intérêts. Inversement, en optant pour le second type d'adresse, les utilisateurs manifesteraient leur consentement à recevoir des e-mails publicitaires. Il serait évidemment possible pour un même utilisateur de disposer des deux catégories d'adresses : l'une réservée, par exemple, à sa correspondance privée, l'autre aux transactions commerciales.

Chaque adresse dépendrait de serveurs SMTP différents et indépendants, l'un bloquant systématiquement les *spams*, l'autre ne les bloquant pas, ou se contentant d'un filtrage. Hormis les difficultés habituelles liées à l'utilisation de filtres, un tel dédoublement de serveurs SMTP ne poserait pas de problème technique particulier, s'agissant simplement de deux serveurs autonomes, administrés séparément.

326. La généralisation de tels dispositifs techniques permettrait de mieux contrôler le flux des e-mails non sollicités en circulation sur le réseau. À cet égard, des accords d'interconnexion pourraient être conclus entre les plus gros fournisseurs d'accès pour empêcher le transit de tels messages par les serveurs "anti-*spams*". Ainsi, les *spammeurs* n'auraient d'autre choix que d'adresser leur publicités électroniques uniquement aux serveurs qui les acceptent.

[61] Dans cette optique, on pourrait ainsi concevoir une adresse du type "nom.prénom@isp_nospams.toplevel" et une autre du type "nom.prénom@isp_spams.toplevel".

Certes, la mise en place de deux serveurs distincts entraînerait un surcoût pour le FAI. Néanmoins, par cet investissement, le FAI fournirait à ses abonnés la possibilité de choisir le type d'adresse e-mail qui leur convient le mieux, ainsi qu'un accès au réseau en toute sécurité, sans que leur adresse "*no spams*" ne soit détournée à des fins de *spamming*. À l'heure de "l'internet gratuit", les FAI qui décideront de mettre l'accent sur la qualité du service offert à leur abonnés et sur une politique rigoureuse en matière de vie privée gagneront la confiance d'un plus grand nombre d'utilisateurs.