

**INSTITUT D'ÉTUDES ET DE RECHERCHE
EN DROIT DE L'INFORMATION ET DE LA COMMUNICATION**
Université d'Aix-Marseille III, Faculté de droit et de science politique

**Publicité non sollicitée sur Internet
et droit de la concurrence**

Par Michelle CRISTOFARI et Rubin SFADJ,

Sous la direction de M. Le Professeur Xavier PHILIPPE,

Dans le cadre du séminaire « Concurrence et concentration des médias ».

Sommaire.

Introduction	Page 3
Première partie : le <i>spamming</i>, par Michelle CRISTOFARI	Page 6
I. <i>L'encadrement juridique du spamming par les règles du droit de la concurrence</i>	Page 8
II. <i>Le cadre juridique flou du spamming</i>	Page 16
Seconde partie : <i>pop-up ads</i> et <i>spywares</i>, par Rubin SFADJ	Page 25
I. <i>La publicité en ligne et le consommateur</i>	Page 26
II. <i>La publicité en ligne et la concurrence</i>	Page 38
Conclusion générale	Page 48

Introduction.

Le développement du commerce électronique va de pair avec celui de la publicité et du marketing sur Internet. Le profil des annonceurs se diversifie, et la publicité en ligne n'est plus l'apanage de l'industrie informatique et du secteur des médias. Les secteurs de l'automobile, de la banque, des produits de luxe, pour ne citer qu'eux, se lancent également dans des campagnes publicitaires en ligne, avec la volonté de conquérir ce nouveau support publicitaire. Or, l'essor de l'« e-pub » a permis celui de la publicité illicite, à savoir, la publicité non sollicitée qui porte directement atteinte à l'internaute, consommateur potentiel qui n'a pas demandé à être démarché. Cet usage de la publicité peut également porter atteinte à la libre concurrence, très présente sur le média Internet.

En effet, le flux incessant de ces publicités en ligne entraîne des inconvénients pour les internautes qui doivent subir, soit l'envoi de messages électroniques non sollicités, le *spamming*, soit l'apparition de fenêtres publicitaires sur leur écran, et gênant leur navigation sur la toile, appelées *pop-up ads*. Ces pratiques illicites ne sont pourtant pas évidentes, et sont utilisées par certaines entreprises dans le but de toucher un maximum de clients avec un minimum de coût, mais sans se soucier de la réglementation sur la publicité loyale. Or, si l'application des règles de la publicité à Internet a pu poser problème, le Bureau de Vérification de la Publicité, après avoir privilégié l'autorégulation sur le média Internet, vient de créer une nouvelle entité qui contrôle toutes les publicités, quel que soit le média concerné.

Cette structure, opérationnelle dès le 1^{er} juin 2003, regroupe le traitement des avis et conseils des campagnes publicitaires qui sont soumises au BVP. Mais, en dehors du média télévision où la soumission est obligatoire, elle est laissée au libre choix des adhérents au BVP pour le reste des supports. Ainsi, même si le BVP peut se saisir d'office pour donner son avis sur une publicité qui serait illicite, concernant le support Internet, seulement une centaine de soumissions a été enregistrée. En effet, Internet est un média jeune qui n'a pas l'habitude de faire appel au BVP. Le contrôle des publicités sur Internet est soumis aux mêmes règles que celles édictées pour les autres supports, et les recommandations du BVP s'appliquent donc pour Internet.

Cependant, ces recommandations ne sont pas suffisantes pour mettre un terme aux pratiques, telles que le *spamming* ou l'usage des *pop-up ads*, qui polluent les écrans des internautes, ainsi que leur boîte aux lettres. Il apparaît, donc indispensable de se diriger vers

des dispositions plus répressives afin de qualifier l'infraction commise par ce type de publicité. Or, pour l'instant, aucune disposition française ne sanctionne expressément ces pratiques sur Internet. Seul le droit communautaire tente de faire adopter par les pays membres, une législation commune sur les communications non sollicitées. En matière de prospection par télécopies et automates d'appel, les directives 97/7/CE sur la vente à distance, retiennent le système de l'*opt-in*, ou le consentement préalable du destinataire pour l'envoi de communications non sollicitées. Ces dispositions sont insérées à l'article L. 33-4-1 du Code des postes et télécommunications par une ordonnance n° 2001-670 du 25 juillet 2001, sans qu'une sanction spécifique à cette interdiction ne soit prévue.

Pour les autres moyens de prospection, notamment, les prospections par voie électronique, l'ancienne directive laissait le choix aux États membres entre les systèmes de l'*opt-in* et celui de l'*opt-out*, c'est-à-dire, soit une protection du destinataire des messages, soit une libre prospection de ces messages, avec la possibilité pour l'internaute de demander son retrait du fichier de l'émetteur afin de ne plus être démarché. Si la plupart des pays européens ont fait le choix du consentement préalable en matière de prospection par courrier électronique, la France a préféré le système de l'*opt-out*, et un nouvel article a été inséré dans le code de la consommation. Par conséquent, selon le mode de communication, la législation change, et semble plus sévère pour les prospections par télécopie et par automates d'appel que pour les prospections par courrier électronique.

Le constat d'une réglementation floue peut donc être fait, d'autant qu'une nouvelle directive « vie privée et communications électroniques » du 12 juillet 2002, vient la perturber, prévoyant le système de l'*opt-in*, contre le *spamming*. La transposition de cette directive est fixée au 31 octobre 2003.

La publicité non sollicitée sur Internet semble, ainsi, trouver ses propres règles, certes encore imprécises. Pourtant, elle pose non seulement des problèmes quant à la protection des internautes consommateurs, mais également, en matière d'atteinte à la concurrence. En effet, les pratiques utilisées pour la publicité non sollicitée sont des pratiques déloyales, et constituent une atteinte aux règles de bonne conduite de la Netiquette.

Si le *spamming* semble faire l'objet d'une réglementation aussi bien hors Union européenne, qu'au sein du territoire communautaire, l'usage des *pop-up ads*, quant à

lui, ne dispose pas de règles précises. Pourtant ces deux pratiques sont utilisées par la voie électronique et semblent parfois illicites. Elles sont donc visées par les directives européennes, mais le spamming concerne particulièrement la protection des consommateurs et le comportement loyal (I), tandis que les *pop-up ads* portent atteinte plus directement aux règles de concurrence (II).

Première partie : Le *spamming*, par Michelle CRISTOFARI.

Introduction.

Du 30 avril au 2 mai 2003, s'est déroulé aux États-Unis le « *FTC Spam Forum* ». Cet évènement, organisé par la Commission fédérale du commerce américaine, visait à définir les moyens de lutte contre le développement exponentiel du « *spam* »¹. Des propositions de loi *antispam* incluant des peines civiles et des poursuites pénales pour les récidivistes ont été faites. Mais l'obligation de porter un label indiquant que le *spam* commercial revêt un caractère publicitaire est sans doute la disposition la plus intéressante en ce qui concerne la réglementation du *spamming* pour l'internaute.

Le *spamming*, ou l'envoi d'e-mails non sollicités, à caractère publicitaire, est une pratique qui s'est généralisée très rapidement. Cette nouvelle forme de publicité sur Internet offre, il est vrai, un avantage considérable aux entreprises qui, pour un budget limité, peuvent prospecter sur Internet un marché de plusieurs milliers, voire plusieurs millions de personnes. Mais les destinataires de ces messages dénoncent de plus en plus violemment les abus et la gêne qui en résultent : engorgement des boîtes aux lettres, ralentissement du temps de connexion, saturation du système informatique. Pourtant, et ce afin de déterminer l'abus occasionné par le *spamming*, il convient d'établir un lien entre cette pratique et la notion de publicité. En ce sens, l'article L. 121-1 du Code de la consommation prévoit un délit relatif à la publicité trompeuse ou de nature à induire en erreur. Ce texte a vocation à s'étendre à la publicité sur Internet grâce à l'interprétation large dont bénéficie la notion de publicité inscrite dans l'article. En effet, la jurisprudence a élargi le champ d'application du texte de sorte que l'incrimination s'applique à toutes les publicités, quel que soit leur forme et le support publicitaire sur lequel elles prennent place².

Une telle utilisation de la publicité est contraire à l'article L 121-1 du Code de la consommation, puisque le message reçu par l'internaute n'est pas désiré et qu'il ne présente

¹ Florence SANTROT, Trois jours contre le *spam*, *le Journal du Net*, <http://www.journaldunet.com>.

² Lamy *Droit des médias et de la communication*, n° 615-18, tome 2 ; février 2000.

pas de signe le distinguant d'un autre courrier électronique, induisant ainsi le consommateur en erreur. D'ailleurs, l'article 7, alinéa 1 de la directive relative au commerce électronique du 8 juin 2000, prévoit que les communications commerciales non sollicitées par courrier électronique doivent pouvoir être identifiées de manière claire et non équivoque dès réception par le destinataire. Ainsi, le *spamming* peut s'apparenter à de la publicité clandestine ou mensongère, mais l'atteinte ne concerne pas directement les règles du droit de la concurrence.

Si cette pratique porte atteinte aux internautes, elle est utilisée à des fins commerciales et c'est en ce sens qu'elle peut être une pratique déloyale et abusive. Pour qu'une pratique sur un marché donné, en l'occurrence la publicité, puisse porter une quelconque atteinte aux règles de concurrence, il faut qu'elle constitue soit une pratique restrictive de concurrence, soit une pratique anticoncurrentielle. La question se pose alors de savoir si le *spamming* peut constituer l'une ou l'autre des deux pratiques préjudiciables envers le jeu de la concurrence.

En d'autres termes, le *spamming* peut-il dépendre des règles encadrant le droit de la concurrence ? Jusqu'à présent, aucun texte juridique n'a évoqué expressément les règles du droit de la concurrence pour encadrer le *spamming*. Le droit communautaire a tenté de réglementer le *spamming* par l'intermédiaire de plusieurs directives, sans véritablement trancher sur le mécanisme à adopter afin de lutter efficacement contre cette pratique. Et la France, comme tous les autres pays membres de l'Union européenne, doit transposer ces directives. Ainsi, le projet de loi sur la confiance dans l'économie numérique tente, lui aussi, de clarifier le problème des publicités non sollicitées sur Internet, mais l'on constate une difficulté de définition de la pratique illicite et par conséquent, une difficulté pour mettre en place un système capable de lutter contre cette pratique.

En effet, si le *spamming* peut s'apparenter à une pratique portant atteinte indirectement au droit de la concurrence (I), il n'en reste pas moins que son cadre juridique reste flou aussi bien au niveau européen, qu'au niveau national. Ainsi, selon que le pays décide de protéger le consommateur ou bien la liberté du commerce, le système diffère et n'entraîne pas les mêmes conséquences (II).

I. L'encadrement juridique du spamming par les règles du droit de la concurrence.

Si l'objectif du « spammeur » est de promouvoir un produit ou un service, ce but à atteindre pourrait ne pas être répréhensible mais les moyens utilisés pour y parvenir constituent un comportement abusif. Or, pour les partisans de cette pratique, le *spamming* permettraient aux petites entreprises de faire de la publicité de masse à un prix minimum. Ainsi, elles auraient la capacité de concurrencer les grandes entreprises en visant le maximum de clients. De plus, le *spamming* permettrait aux consommateurs de faire de meilleurs choix entre les produits et services qu'ils leur sont proposés. Pourtant, ces arguments ont un poids faible face aux nombreuses plaintes des internautes et à la mobilisation juridique pour la lutte contre cette pratique.

Si le *spamming* ne semble pas s'apparenter à une entrave à la concurrence (A), il constitue, néanmoins, une concurrence déloyale sur la toile, ne respectant pas la Netiquette (B).

A. La difficile application des entraves à la concurrence à la pratique du *spamming*.

Selon la définition choisie de cette pratique, il est possible de la considérer en tant qu'activité commerciale. En effet, le *spamming* consiste à récolter, généralement, dans les espaces publicitaires d'Internet, des adresses e-mail à l'insu de leurs titulaires pour leur envoyer des messages publicitaires en grand nombre, vantant les mérites d'un produit ou d'un service. Les éléments caractérisant une activité commerciale sont présents, à savoir dans ce cas précis, la prestation de bien ou de service pour le consommateur. Mais la notion d'abus du consommateur apparaît, l'activité se faisant à son insu, traduisant ainsi, le caractère illicite de cette activité. Toutefois, le *spamming* constitue-t-il pour autant, une pratique portant directement atteinte à la concurrence ?

1. Le *spamming*, une pratique anticoncurrentielle ?

Les pratiques anticoncurrentielles sont représentées par les abus de position dominante et les ententes. L'article 41-4 de la loi du 30 septembre 1986 modifiée soumet les entreprises de communication audiovisuelle au contrôle des règles de concurrence en ce secteur telles qu'elles résultent de l'ordonnance du 1^{er} décembre 1986. L'organe régulateur est le Conseil de la concurrence qui veille au respect du principe de la liberté de la concurrence dans le secteur des médias. Ces pratiques anticoncurrentielles sont également susceptibles d'être contrôlées par la Commission européenne au titre des pouvoirs de contrôle qu'elle détient selon les articles 86 et 87 (anciens articles 90 et 92) du Traité CE.

Or, il apparaît que le fait d'envoyer des messages commerciaux à caractère publicitaire, dans le but de promouvoir un produit ou un service, ne constitue ni une quelconque position dominante, ni une entente. Une entreprise, qui veut promouvoir son produit, et pratique pour cela le *spamming*, profite ainsi du faible coût de la campagne publicitaire engagée, pour toucher un maximum de clients. En effet, l'envoi de messages électroniques constitue un outil extrêmement intéressant pour les sociétés de marketing direct : les coûts sont beaucoup plus faibles que ceux d'une campagne de publipostage classique et le taux de « concrétisation » nettement plus élevé.

En outre, cette pratique peut certes entraver le jeu de la concurrence du fait qu'elle fait profiter de la situation qu'un certain nombre d'entreprises, mais elle n'empêche pas la concurrence de s'exercer sur le marché considéré.

D'ailleurs, pour évaluer si l'abus de position dominante a eu lieu, le Conseil de la concurrence doit identifier un marché de référence, afin d'évaluer ensuite, si l'abus est constitué sur ce marché. Or, concernant le *spamming*, si le marché de référence semble être la publicité sur Internet, le Conseil de la concurrence n'a jamais eu à se pencher sur la question.

2. Le *spamming*, une pratique restrictive de concurrence ?

Le *spamming* ne semble pas non plus constituer une pratique restrictive de concurrence. En effet, cette pratique se définit comme une atteinte à la concurrence qui n'empêche pas celle-ci de fonctionner mais la fausse au point que le jeu normal du marché en soit affecté. Elle est représentée par les différentes pratiques contraires au droit commercial, telles que le refus de vente, les pratiques discriminatoires, les prix imposés³.

Or, le *spamming* concerne la publicité non sollicitée sur Internet, et ne pose pas directement le problème de concurrence déloyale entre entreprises. Mais il peut être constitutif d'un dénigrement, c'est-à-dire une action dirigée contre une entreprise concurrente dans le but de détourner sa clientèle, notamment en discréditant ses produits, son travail ou la personne de celle-ci. En effet l'envoi massif de messages publicitaires permet de viser un nombre non négligeable de clients sans se préoccuper d'autres annonceurs, qui eux, utilisent des campagnes publicitaires licites et loyales. Ainsi, les moyens utilisés par ces entreprises et les effets produits sont susceptibles de porter atteinte aux autres entreprises concurrentes. Cependant, la jurisprudence n'a toujours pas qualifié le *spamming* comme étant constitutif d'un tel acte.

Dans la pratique, les messages envoyés par les spammeurs continuent d'impliquer, du côté du fournisseur, des coûts additionnels pour l'achat et la gestion d'ordinateurs supplémentaires afin d'assurer la sécurité et l'intégrité des fournisseurs d'accès, des coûts

³ Sous la direction de Charles DEBBASCH, *Droit des médias*, Dalloz référence, 2002, Paris, p. 528.

additionnels pour l'achat de mémoire afin d'entreposer les *spams*. Du côté de l'utilisateur, des coûts additionnels pour le temps de chargement, pour les usagers qui utilisent une communication interurbaine et une baisse de productivité liée au temps à passer à filtrer les *spams*.

De plus, la pratique du *spamming* entraîne une atteinte à la vie privée car les spammeurs collectent les adresses des internautes dans des groupes de discussion à l'insu des internautes. Or, l'adresse e-mail d'une personne est une donnée personnelle protégée et le fait de la collecter et de l'utiliser pour promouvoir un produit ou un service sans que la personne ne soit avertie constitue une atteinte à sa vie privée.

Ce n'est donc pas uniquement sur le terrain de la concurrence que le *spamming* peut être attaqué, mais aussi sur celui de la vie privée. Pour l'instant, le *spamming* n'a pas été condamné sur le fondement de la vie privée, même si pour la jurisprudence, cette pratique cause des désagréments pour les internautes, destinataires de ces messages. Par contre, cette pratique a été rendue illicite sur le fondement d'un usage, plus précisément sur celui des règles de bonne conduite à suivre sur le net.

B. Le *spamming*, une pratique déloyale, attentatoire à la Netiquette.

Le *spamming* consiste à faire de la publicité non sollicitée sur Internet. En France, le Bureau de vérification de la publicité (BVP) a adopté des recommandations sur la publicité sur Internet. Ainsi, il préconise le respect d'une publicité loyale, véridique, honnête et décente, « *qui doit être conforme aux principes de concurrence loyale, tels qui sont généralement admis dans les relations commerciales* ». Plus, précisément, concernant les messages non sollicités, « *toute publicité doit être identifiée comme telle d'une manière claire et non équivoque, dès sa réception par le destinataire* ». Pourtant, ce n'est pas le cas pour l'internaute qui reçoit des *spams* sans l'avoir souhaité. Le BVP n'a pas encore pu contrôler ce type de message publicitaire, et la jurisprudence a préféré se fonder sur l'atteinte à un usage, celui de la Netiquette regroupant, elle aussi, des règles déontologiques, mais ayant une vocation universelle.

1. L'engagement de la responsabilité des « spammeurs » face aux atteintes à la Netiquette.

À l'instar des us et coutumes qui régissent la vie courante, les pionniers du web ont édicté des règles de courtoisie et de bonne conduite applicables à l'Internet. Ainsi, les correspondances sur le net doivent suivre des règles déontologiques, puisque les internautes sont des être humains qui communiquent entre eux et que la politesse s'applique aussi pour Internet. Il s'agit moins de règles absolues que de recommandations destinées à pacifier les échanges entre internautes. La Netiquette, contraction de « *Networking Etiquette* », se présente comme un code déontologique à respecter mais qui n'a pas de valeur juridique et qui ne peut donc pas sanctionné. Cependant, certains sites, notamment les newsgroups, n'hésitent pas à menacer d'exclusion, ceux qui ne suivraient pas ces règles.

En octobre 1995, le groupe de travail RUN⁴, de l'IETF⁵, l'organisme de normalisation du réseau a édicté un code de bonne conduite appelé « *les règles de la Netiquette* », aussi connu sous le nom de code RFC*⁶ 1855, et traduit en français par Jean-Pierre Kuypers. Ces règles sont aujourd'hui des références sur la toile, que les institutions peuvent utiliser et adapter pour leur propre usage, et que la jurisprudence a également utilisé pour condamner des pratiques, telles que le *spamming*.

En effet, cette charte de bonne conduite a pu constituer un usage sur lequel les juridictions peuvent se fonder afin d'engager la responsabilité de personnes ayant eu des comportements contraires à cette charte. En droit interne, il s'agit donc de l'article 1135 du Code civil qui dispose que « *les conventions obligent non seulement à ce qui y est exprimé, mais encore à toutes les suites que l'équité, l'usage ou la loi donnent à l'obligation d'après sa nature* ». Ainsi, la Netiquette fait parti de cet « *usage* » qui entraîne pour les internautes et leurs prestataires de service des obligations à respecter et des manquements susceptibles d'être sanctionnés.

De plus, l'auteur d'un *spam* peut être poursuivi sur le fondement des articles 226-16 et 226-24 du Nouveau Code pénal, issus de la loi « Informatique, fichiers et libertés » de 1978, car sa liste d'adresses électroniques constitue un traitement automatisé d'informations nominatives, dont la collecte doit être loyale et non frauduleuse et faire l'objet d'un renseignement de la personne fichée. De même l'article 323-2 du NCP, tiré de la loi sur les atteintes aux traitements automatisés de données, peut permettre de sanctionner les pratiques des spammeurs ayant pour résultat de perturber le fonctionnement de l'un des systèmes visés par la manœuvre. Ce délit d'entrave au fonctionnement des traitements automatisés de données a d'ailleurs été utilisé récemment par la jurisprudence pour condamner le *spamming*, de même que l'article 1135 du Code civil.

⁴ *Responsible Use of the Network.*

⁵ *Internet Engineering Task Force.*

⁶ *Request For Comments.*

2. Applications jurisprudentielles.

Selon deux arrêts rendus, l'un le 28 février 2001, l'autre le 15 janvier 2002, l'utilisation du *spamming* est contraire aux usages de l'Internet et justifie la résiliation du contrat d'accès au réseau⁷. Si cette jurisprudence place le *spamming* sur le terrain du droit des contrats et la considère comme une pratique pouvant porter atteinte aux droits des contractants, elle justifie la condamnation de l'auteur du *spamming* par le fait qu'elle est contraire aux usages de l'Internet. Il est vrai qu'aux termes de l'article 1135 du Code civil, la convention peut être interprétée par le juge à la lumière d'un usage. D'ailleurs, dans les deux décisions, les juridictions emploient les termes suivants : « *Il existe un usage proscrivant le spamming dans les groupes de discussion* » ; « *La pratique du spamming considérée dans le milieu de l'Internet comme une pratique déloyale et gravement perturbatrice, est contraire aux dispositions de la charte de bonne conduite* ».

La référence à une pratique contraire à la charte de bonne conduite permet de punir le *spamming* sur le terrain de la déontologie dans le milieu de l'Internet, mais aussi, elle permet de déterminer le caractère abusif de cette pratique, et de condamner le spammer s'il ne donne pas suite aux mises en demeure du fournisseur d'accès. En effet, dès lors qu'en dépit de très nombreux rappels aux conditions d'utilisation des accès à Internet, l'émetteur a persévéré dans sa démarche, le fournisseur d'accès était fondé à lui couper les accès à Internet, simple conséquence du non respect de ses obligations contractuelles⁸.

La charte de bonne conduite n'a qu'une valeur d'interprétation et non une valeur juridique. Cependant, elle acquiert une valeur déterminante dans l'engagement de la responsabilité, et il est donc recommandé aux professionnels qui mettent à disposition des outils ou des espaces électroniques de faire référence à cette Netiquette, afin de tenter de se dégager de leur responsabilité.

Le 24 mai 2002, le Tribunal correctionnel de Paris a condamné un spammeur à quatre mois de prison avec sursis et 20 000 euros de dommages et intérêts au profit de l'opérateur Noos sur le fondement de l'article 323-2 du Code pénal, réprimant toute entrave au

⁷ Note de jurisprudence, Luc GRYNBAUM, revue *Communication Commerce Électronique*, Avril 2002, éd. Juris Classeur, pp. 24-25. TGI Rochefort-sur Mer, 28 février 2001, Ch. G. c/ Sté France Télécom Interactive SA, TGI Paris, référé, 15 janvier 2002 : P. V. c/ Sté Liberty Surf et a.

⁸ Charles MARNA, Courriers électroniques publicitaires et responsabilités, Actualité jurisprudentielle, *Dalloz* 2002, n° 13, p. 1138.

fonctionnement d'un système de traitement automatisé. Cette sanction montre combien la volonté de dissuader d'autres spammeurs est grande. Mais, surtout, le fondement de la sanction prouve que le *spamming* est une pratique répréhensible et pénalement condamnable.

Or, il est possible d'établir un parallèle entre l'article 323-2 du Code pénal et l'article 1135 du Code civil, dans la mesure où ces deux articles font référence à la Netiquette, l'un directement par l'intégration de la charte de conduite dans les usages, et l'autre par le renvoi à la protection d'un système de traitement automatisé.

Ainsi, les atteintes faites aux usagers d'Internet, et susceptibles de brimer l'utilisation de cet outil de communication sont sanctionnées par la voie civile ou pénale.

Il ressort de ces jurisprudences une volonté de condamner la pratique du *spamming*, mais pas directement sur le terrain de la concurrence. En effet, le *spamming* est plutôt considéré comme une atteinte aux usages d'Internet. Même si elle constitue une pratique déloyale, il s'agit plus d'acte commis contre une règle déontologique, la loyauté, l'éthique, que d'une action en concurrence déloyale.

Afin d'éviter que cette pratique ne devienne un véritable fléau, les autorités nationales et européennes ont constitué un arsenal juridique pour la lutte *antispam*. Certes, cet ensemble de textes ne semble pas encore très précis quant aux moyens à mettre en œuvre pour condamner cette pratique, mais il a le mérite d'exister et de vouloir protéger le consommateur internaute, qui subit l'envoi de messages non sollicités.

II. *Le cadre juridique flou du spamming.*

Nouvel et indispensable outil de promotion pour les uns, qui développent leur commerce sur Internet ou par son intermédiaire, il est le plus souvent subi par les autres, les consommateurs. Selon une étude réalisée par Netvalue France auprès d'internautes allemands, anglais, espagnols et français, le nombre moyen de messages publicitaires serait en augmentation, tout comme le pourcentage de messages publicitaires reçus par un internaute au regard du nombre total de messages dont il est destinataire. C'est d'ailleurs en France que cette pression promotionnelle est la plus forte⁹.

Aux États-Unis, les sociétés de marketing direct se sont tournées vers le « *permission marketing* » qui suppose le consentement préalable de l'internaute. On peut alors se demander si le cadre juridique européen et français reflète cette nouvelle tendance, prônée par certains acteurs économiques. Au plan juridique, on oppose schématiquement deux réponses au *spam* :

– L'*opt-in*, qui consiste à poser un principe d'interdiction de l'envoi de courriers promotionnels non sollicités. Cet envoi est possible par exception si l'internaute y a consenti au préalable. Cette solution est la plus protectrice pour le consommateur, dont a pu dire face aux sollicitations publicitaires croissantes qu'il avait « *un droit à la tranquillité* »¹⁰.

– L'*opt-out*, qui consiste à admettre en principe la liberté de diffusion de messages promotionnels non sollicités. C'est uniquement si l'internaute a manifesté son opposition à la réception de tels messages que leur envoi est illicite.

Si au niveau européen la multiplicité des textes crée une impression de confusion (A), en France, le projet de loi en cours d'adoption, bien qu'il semble consacré le système de l'*opt-in*, manque également de clarté sur le sujet épineux du *spamming* (B).

⁹ Vincent VARET., Le cadre juridique du *spam* : état des lieux, *Revue Communication Commerce Électronique*, éd. Juris-Classeur, septembre 2002, p. 14.

¹⁰ Jean FRAYSSINET, Nouvelles technologies de l'information et de la communication et protection des libertés des consommateurs, *Cahiers Lamy droit d'informatique et des réseaux*, n° 127, juillet 2000, p. 7.

A. Les tentatives d'éclaircissement des directives européennes sur le *spamming*.

Si la solution de l'*opt-in* favorise le droit à la tranquillité, le droit à la protection des données personnelles et le droit à la vie privée, le choix de l'*opt-out*, favorise la liberté de prospection des annonceurs.

Actuellement, au gré des différentes directives adoptées et des législations nationales, les différents types de prospection ne suivent pas le même régime. Pourtant, la réflexion sur l'envoi de courriers non sollicités a largement évolué dans le cadre des débats sur la modification de la directive concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques. Ainsi, avec le projet de loi français sur la confiance dans l'économie numérique, on peut espérer une transposition de la directive « Vie privée et communications électroniques », et, enfin, un choix non équivoque sur le système de protection à appliquer contre le *spamming*.

1. Le choix de l'*opt-out* par la première directive relative à la protection des consommateurs en matière de contrats à distance.

La directive 97/7/C du 20 mai 1997 distingue dans son article 10, les automates d'appel et les télécopieurs, pour lesquels elle retient le système de l'*opt-in*. Or, implicitement, le texte prévoit pour les moyens de communication autres que les automates d'appel et les télécopieurs, un principe de licéité de la prospection ; ce n'est que si l'utilisateur a marqué son opposition « *manifeste* » que cette pratique est interdite.

Selon, ce premier texte, la pratique du *spam* est donc régie par le système de l'*opt-out*. On pourrait reprocher la distinction faite entre les automates d'appel, les télécopieurs, et les autres moyens de communication, qui exclut une catégorie pourtant susceptible d'utiliser de façon abusive le *spamming*. Mais cette solution a été transposée en droit français à travers l'ordonnance n° 2000-741 du 23 août 2001. Dans son article 12, cette ordonnance insère dans le code de la consommation un article L. 121-20-5 qui reprend l'article 10 de la directive. Ainsi, le principe de licéité du *spamming* prévaudrait en droit français.

2. La liberté de choix laissée aux États membres : les directives 97/66/CE et 2000/31/CE.

La directive relative au traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications, du 15 décembre 1997, reprend la solution de l'*opt-in*, mais laisse le choix aux États membres entre un principe d'autorisation préalable et un droit d'opposition pour les autres modes de communication.

Si une telle liberté peut permettre aux États de mieux protéger l'internaute, elle peut aussi revenir à une absence d'harmonisation, génératrice d'une grande insécurité juridique pour les entreprises qui utilisent le courrier électronique comme moyen de promotion.

Ainsi, cette directive semble être en contradiction avec la première puisqu'elle préconise le système inverse contre le *spamming*. Cependant, les États sont en droit d'aller au-delà de ce que leur propose la première directive, à savoir l'*opt-in*. En réalité, cinq États ont choisi la voie la plus protectrice des internautes, l'interdiction des communications commerciales non sollicitées, sauf accord préalable du destinataire. Et d'autres, comme la France, ont préféré un principe de licéité.

La troisième directive relative à certains aspects du commerce électronique du 8 juin 2000, comporte deux règles relatives aux courriers commerciaux non sollicités. L'article 7.1 pose à la charge des spammeurs, une obligation d'identification du caractère commercial ou promotionnel des messages qu'ils envoient, tout en laissant par ailleurs, clairement aux États membres le choix de décider de la licéité du *spam*.

À ces textes, traitant spécifiquement du *spamming*, s'ajoute le cadre relatif à la protection des données personnelles, qui conduit à s'interroger sur la licéité de la collecte et de l'utilisation des adresses électroniques. Ces adresses, étant des données personnelles, les principes de loyauté et de légitimité de la collecte des données personnelles, posés par la loi française « Informatique et libertés » du 6 janvier 1978, permettent de faire obstacle au spam, lorsque ces adresses ont été collectées sauvagement, notamment sur des forums de discussion, des annuaires, etc. De plus, ce texte confère aux individus un droit d'opposition au traitement de leurs données personnelles, à la condition de faire valoir un intérêt légitime.

Dans l'absolu, les règles relatives aux données personnelles semblaient fournir un dispositif juridique suffisant pour régir l'envoi de messages commerciaux non sollicités. Cependant, l'adoption postérieure des directives précitées comportant des dispositions spécifiques au *spam* vient perturber cette cohérence, entraîne l'insécurité juridique pour les commerçants qui utilisent Internet et nuit à la protection des internautes.

C'est certainement afin de pallier à ce flou juridique, qu'une nouvelle directive « Vie privée et communications électroniques » est entrée en vigueur le 31 juillet 2002.

3. La consécration de l'*opt-in* par la directive « Vie privée et communications électroniques ».

Ce nouveau texte abroge la directive 97/66/CE relative au traitement des données à caractère personnel et la protection de la vie privée dans le secteur des télécommunications. Il vise à adapter la réglementation à l'évolution des marchés et service de communication électroniques. Il s'agit d'accorder le même niveau de protection des données à caractère personnel, indépendamment des technologies utilisées.¹¹ Le 21 janvier 2002 le Conseil européen a adopté une position en faveur de l'*opt-in* dans son article 13.

La directive clarifie et unifie le régime applicable en matière de prospection par des communications non sollicitées. L'article 13 prévoit que « *L'utilisation de systèmes automatisés d'appel, sans intervention humaine (automates d'appel), de télécopieurs ou de courriers électroniques à des fins de prospection directe ne peut être autorisée que si elle vise des abonnés ayant donné leur consentement préalable* ». La clarification opérée par cette directive n'est toutefois pas complète, même si elle opte pour une protection maximale de l'internaute.

En premier lieu, la directive laisse aux États membres le choix du régime concernant la prospection des personnes morales. En second lieu, la directive prévoit un régime dérogatoire pour les relations post-contractuelles. Lorsqu'une société a obtenu directement de ses clients, dans le cadre d'une vente d'un produit ou de la fourniture d'un service, leurs

¹¹ Considérants 4 à 7 de la directive n° 2002/58/CE, 12 juillet 2002, JOCE 31 juillet n° L 201, p. 37.

coordonnées électroniques, elle peut les exploiter à des fins de prospection directe pour des produits ou services analogues. Les clients conservent, de manière classique, un droit d'opposition.

La CNIL émet une réserve sur ce régime dérogatoire qui découle de la vente et de la fourniture de services. En effet, elle considère qu'outre les difficultés d'interprétation qui peuvent être soulevées par cette dérogation, rien ne justifie une distinction entre les services marchands et non-marchands.

En tout état de cause, ces dispositions ne connaîtront leur effectivité que lors de leur transposition en droit positif interne. En attendant, les principes généraux régissant le traitement des données personnelles et notamment, celui de la loyauté de la collecte, restent applicables aux communications électroniques non sollicitées. La directive doit être transposée en droit français avant le 31 octobre 2003.

Déjà, le projet de loi sur la confiance dans l'économie numérique semble se rapprocher du choix fait par cette directive. Pourtant, il est postérieur à celle-ci et se base plutôt sur la directive « Commerce électronique » du 8 juin 2000 qui a donc précédé la directive « Vie privée et communications électroniques ».

B. L'interdiction ambiguë du *spamming* par le projet de loi LEN.

La directive « Commerce électronique » du 8 juin 2000 a déjà fait l'objet d'une transposition à travers le projet de loi « Société de l'information » du 14 juin 2001. Ce dernier étant devenu caduc par le changement de législature, le gouvernement a déposé un nouveau projet de loi le 15 janvier 2003 « Pour la confiance dans l'économie numérique ». Le texte vient d'être adopté en première lecture à l'Assemblée nationale, le 26 février dernier.

1. La protection de l'internaute.

Cette protection, dont il convient de susciter la confiance, passe par son information et l'encadrement de la publicité. L'article 9 du projet oblige le prestataire à décliner son identité ou raison sociale sur la page d'accueil du service et « *des pages visionnées par le client lors de la transaction* », le tout « *sans préjudice des autres obligations d'information prévues par les textes législatifs et réglementaires en vigueur* ». Cette disposition existe déjà dans l'article L. 121-18 du Code de la consommation qui prévoit une obligation renforcée portant sur l'identité du vendeur ou du prestataire et sur les caractéristiques de ces produits ou de ses services dans les contrats à distance. Mais sa réaffirmation dans un texte général aura le mérite de bénéficier également à tout internaute, professionnel ou non¹².

En effet, jusque là, l'obligation d'identification ne s'appliquait pas aux services en ligne et par conséquent, ne visait pas non plus les publicités non sollicitées. C'est donc, par la création d'un article 43-15 qui devra être inséré dans la loi du 30 septembre 1986, que cette obligation concernera « *toute publicité, sous quelque forme que ce soit, accessible par un service de communication publique en ligne* ». De même, le projet de loi prévoit dans son article 11 que les publicités non sollicitées devront suivre cette obligation d'identification « de manière claire et non équivoque ».

¹² Luc GRYNBAUM, « Projet de loi pour la confiance dans l'économie numérique » : encore un petit effort de rigueur juridique pour un « contrat électronique » fiable, *Le Dalloz*, 2003, n° 11, p. 746.

L'internaute, personne physique ou morale, non inscrite au registre du commerce et des sociétés, devrait être prémuni contre la prospection directe. C'est donc, l'article 12 du projet qui prévoit l'interdiction de cette pratique, le *spamming*, traduit par « *prospection directe* » qui consiste en un harcèlement publicitaire par automate d'appel, télécopieur ou courrier électronique. De plus, le consentement préalable du destinataire est indispensable. Le système de l'*opt-in* est donc préconisé, comme le prévoit la directive « Commerce électronique ». Cependant, le prestataire qui aura déjà vendu un bien ou un service à l'internaute pourra ensuite lui adresser des messages publicitaires en prévoyant la faculté de s'opposer à de tels envois. Cette disposition est inspirée de l'interdiction du *spamming* sans consentement préalable instaurée par la directive dite « Vie privée et communications électroniques » du 12 juillet 2002.

Mais l'article 11 du projet qui prévoit une disposition autorisant les publicités dès lors qu'elles sont identifiées de « *manière claire et non équivoque* », ne coïncide pas avec l'article 12 qui interdit les publicités non sollicitées. En effet, quelle différence fait-on entre la « *prospection directe* » qui serait interdite à l'article 12 et les « *publicités* » autorisées par l'article 11 ? Ces dernières sont présentées comme étant « *notamment les offres promotionnelles, telles que les rabais, les primes, les cadeaux, adressés par courrier électronique* ».

Ainsi, il suffirait que « *la communication commerciale non sollicitée* », pour employer les termes de la directive commerce électronique, présente un service ou un produit sous forme d'offre promotionnelle ou de rabais pour qu'elle soit licite. L'interdiction ne vaudrait que pour une « *prospection directe* » sans offre promotionnelle ou rabais. Or, les *spams* se présentent très souvent comme des offres promotionnelles, et ces deux articles combinés viennent restreindre la protection de l'internaute.

2. Une protection difficilement applicable.

Si l'interdiction du *spamming* semble être limitée par l'article 11 du projet, il n'est pas prévu de faculté de refuser l'envoi de « *publicités* » telles que définies par le futur article L. 122-15-1 du Code de la consommation. En outre, ce nouveau texte serait également applicable aux publicités, offres, concours, ou jeux à destination des professionnels, aux

termes d'un nouvel article L. 121-15-3, c'est-à-dire à tout internaute. Ce projet de loi crée un étonnant paradoxe par lequel il autorise partiellement dans le Code de la consommation, ce qu'il interdit dans le Code des postes et télécommunications¹³.

In fine, même la transposition en droit interne semble se perdre dans le choix entre le système de l'*opt-in* et celui de l'*opt-out*, le premier étant protecteur de l'internaute consommateur, et le second défendant la liberté du commerce.

Or, il s'agissait de s'aligner avec la directive européenne qui a tranché pour le système de l'*opt-in*. Actuellement, et sous réserve du respect de loi informatique et libertés, le droit français connaît le système de l'*opt-out*, à savoir qu'il appartient au consommateur d'effectuer la démarche pour s'opposer aux communications non sollicitées par courriers électroniques.

Pour ajouter à la confusion, le projet de loi prévoit que « *Dans tous les cas, il est interdit d'émettre des courriers électroniques à des fins de prospection directe sans indiquer d'adresse valable à laquelle le destinataire peut transmettre une demande tendant à obtenir que ces communications cessent. Il est également interdit de dissimuler l'identité de la personne pour le compte de laquelle la communication est émise, notamment en mentionnant un objet sans rapport avec la prestation ou le service proposé* ».

La notion d' « *adresse* » n'est pas claire : se réfère-t-elle exclusivement à une adresse de courrier électronique à laquelle le destinataire peut notifier son droit d'opposition ? Son droit à s'opposer à de tels courriers n'est pas expressément indiqué.

Ce projet présente donc des incertitudes quant à la bonne volonté de protection de l'internaute face à la prospection directe. Peut être que le texte définitif sera plus précis quant au système à utiliser contre le *spamming*, sachant que le consentement préalable du destinataire du message est le système le plus protecteur.

¹³ Luc GRYNBAUM, *op. cit.*, p. 747.

Conclusion.

Le 23 mai 2003, un projet de loi très attendu, interdisant le *spam*, a été présenté aux États-Unis et devrait être rapidement adopté par le Congrès, en dépit des contestations exprimées par les associations de consommateurs qui estiment que son impact sera négligeable. La proposition de loi défendue par le représentant de l'État de la Caroline du Nord, Richard Burr, est le résultat de nombreux mois de discussions entre les Républicains de la Chambre qui espèrent réduire le *spam* tout en permettant aux entreprises de faire de la publicité sur Internet.

La loi connue sous le nom de *Reduction in Distribution of Spam Act (RID)*, établira des amendes pour les sociétés qui masquent leur identité ou utilisent des techniques de marketing mensongères mais n'interdira pas aux entreprises de contacter les internautes en utilisant leur courrier électronique. Ainsi, ce projet se rapproche du projet de loi français dans la mesure où il prévoit une obligation d'identification et où il n'interdit pas véritablement l'usage des adresses des internautes par les entreprises qui ont déjà été en relation avec eux.

La future loi américaine espère diminuer le *spam* en obligeant les entreprises à donner leur véritable adresse Internet et physique et en les forçant à retirer les internautes qui le souhaitent de leurs fichiers. Il ne semble pas qu'il soit prévu un système d'*opt-in* pour l'internaute dans ce projet, et l'absence d'un tel mécanisme a pu heurter les associations de consommateurs.

Ainsi, selon les groupes de lutte contre le *spam*, cette loi ne devrait pas améliorer le sort des internautes dans la mesure où les entreprises pourront envoyer autant d'emails qu'elles le souhaitent. Toujours selon ces groupes, et plus particulièrement, la *Coalition Against Unsolicited E-mails* qui rassemble 40 000 internautes, il semble incompréhensible que « *la réponse du Congrès soit de protéger les entreprises et de priver les consommateurs de leur droit à être laissé tranquille* ».

Comment obtenir une législation protectrice des consommateurs en Europe, si au niveau international, les projets penchent vers la protection des entreprises avec comme solution, des amendes importantes (jusqu'à 1,5 millions de dollars), mais l'impossibilité pour un particulier de saisir la justice ! La guerre contre le *spam* n'est donc pas terminée, il reste à savoir si l'internaute sera en mesure de se défendre correctement contre la prospection directe.

Deuxième partie : *Pop-up ads* et *spywares*, par Rubin SFADJ.

Introduction.

En matière de publicité non sollicitée sur Internet, si le *spamming* attire actuellement toute l'attention du législateur, outre-atlantique comme en Europe, un autre phénomène est apparu plus récemment, qui se manifeste directement durant le temps passé à naviguer sur Internet : les *pop-up ads*.

Par ce terme anglo-saxon, on désigne les petites fenêtres à contenu publicitaire qui apparaissent par-dessus la fenêtre du site web visité par l'internaute, rendant la navigation moins agréable, et à terme souvent impraticable.

Aujourd'hui largement répandues sur Internet, envoyées par le site visité par l'utilisateur ou par un petit programme espion installé sur son disque dur (*spyware*), les *pop-up ads* sont techniquement bien plus faciles à réaliser que l'envoi d'un courrier électronique à un large panel de personnes. Elles constituent une forme de publicité non sollicitée dite *en ligne*, par opposition au *spamming*, dont l'envoi ne s'effectue pas en temps réel.

Or, tandis que le *spamming* est aujourd'hui bien connu des juristes spécialisés en droit des nouvelles technologies ou en droit de la consommation, les *pop-up ads* semblent, en raison de leur (relative) nouveauté, échapper à la fois à l'attention de la doctrine et à celle du législateur. Comme nous allons le voir, cette pratique soulève néanmoins de nombreuses interrogations juridiques.

Le phénomène des *pop-up ads* intéresse en effet spécialement deux branches du droit étroitement liées à la sauvegarde d'une concurrence saine : la protection du consommateur, qui garantit un minimum de loyauté dans le jeu de la concurrence (I), et les règles du droit de la concurrence *stricto sensu* (II).

I. La publicité en ligne et le consommateur.

C'est le consommateur que le législateur, aux États-Unis comme en Europe, a entendu protéger prioritairement contre les causes et les effets de la publicité non sollicitée affichée lors de la navigation sur Internet.

En effet, pour diffuser une publicité non sollicitée de façon ciblée, il est nécessaire au préalable de recueillir un ensemble de *données personnelles* au sujet de l'internaute. Ce sont donc la collecte, le traitement et le transfert de ces données personnelles que les autorités ont entendu encadrer en tout premier lieu.

Avant d'étudier la mise en œuvre en droit français, par le biais des droits communautaire et interne, de la protection du consommateur face à ces publicités en ligne (B), nous verrons comment le droit américain, tant par les normes édictées que par la jurisprudence, s'est positionné en avant-garde dans ce domaine et peut constituer une forme de modèle (A).

A. L'avant-garde : le droit américain.

Le droit américain, très avancé en matière de droits du consommateur comme des nouvelles technologies, encadre la publicité non sollicitée sur Internet à la fois par l'action de la *Federal Trade Commission*, dont nous examinerons le rôle et les attributions dans un premier temps, mais aussi par l'action d'une jurisprudence donc la souplesse et l'autorité sont caractéristiques des pays de *Common law*.

1. Les normes adoptées.

Nous examinerons ici d'une part le rôle et les fonctions de la *Federal Trade Commission*, et d'autre part la nature des règles qu'elle a édictées qu'elle fait appliquer en matière de protection des données personnelles en ligne.

a. La *Federal Trade Commission*.

La *Federal Trade Commission* (Commission fédérale pour le commerce, FTC) a pour mission d'assurer la bonne application de nombreuses dispositions fédérales dans les domaines du droit de la concurrence et du droit de la consommation. La FTC s'assure que le marché national fonctionne de façon concurrentielle. D'autre part, la FTC donne des avis auprès du Congrès et du pouvoir exécutif en matière de droit public économique.

Une enquête de la FTC peut être actionnée par une lettre (de consommateur comme de professionnel), une requête émanant du Congrès ou même sur sa propre initiative. Ces enquêtes peuvent être publiques ou non publiques, la mise au contentieux est toujours précédée d'une tentative de conciliation (*consent order*). La procédure devant la FTC est de type administratif, et l'entreprise condamnée peut interjeter appel devant la Cour d'Appel puis la Cour Suprême des États-Unis.

Enfin, la commission peut édicter des « règles de régulation commerciale » (*Trade Regulation Rules*) lorsqu'elle constate l'existence de pratiques anticoncurrentielles sur un

marché entier. Ces normes ont force de loi, et peuvent être contestées devant les Cours d'Appel du pays.

Dans le domaine du droit des consommateurs face à la publicité intrusive sur Internet, la FTC connaît depuis quelques années une forte activité.

b. *Les Fair Information Practices.*

La FTC a identifié cinq principes dits « de bonne information » (*Fair Information Practices*). Il s'agit des principes de notification (*notice*), choix (*choice*), accès (*access*), sécurité (*security*) et de respect des normes (*enforcement*).

Le principe de notification impose de porter à la connaissance du consommateur la collecte, l'utilisation et la divulgation des informations personnelles obtenues. Un rapport de la FTC¹⁴ recommande aux sites web de fournir une notification « mise en évidence et claire » de la mise en œuvre de telles pratiques. La plupart des sites ont par conséquent ajouté une déclaration sur les données personnelles afin de respecter ce principe.

Le principe de choix nécessite que les consommateurs conservent un choix quant à l'utilisation des données recueillies au-delà de leur utilisation immédiate (commande d'article ou prise d'informations, par exemple). Ce choix doit inclure à la fois l'utilisation dite secondaire des données (*back marketing*) et les utilisations dites externes, telles que la cession ou la divulgation des informations personnelles à d'autres entreprises.

Dans de nombreux sites, l'application du principe de choix se fait par la mise en œuvre de l'*opt-in* ou de l'*opt-out*¹⁵. Dans le premier cas, le consommateur accepte par défaut l'utilisation des informations personnelles : dans les plupart des sites, il n'est cependant pas clair qu'appuyer sur le bouton « Continuer » ou « Suivant », revient à donner son consentement. Quant à l'*opt-out*, il s'agit de permettre au consommateur de jouir d'un droit d'opposition quant à l'utilisation de ses données personnelles.

¹⁴ *Federal Trade Commission Report "Privacy Online: Fair Information Practices in the Electronic Marketplace. A report to the Congress"* (Mai 2000).

¹⁵ À ce sujet, *cf. supra*, Première partie.

Le principe d'accès implique que le consommateur ait accès à l'information collectée, et ainsi la possibilité de corriger ou de supprimer cette information.

Le principe de sécurité impose au site des « efforts raisonnables » afin de maintenir la sécurité de l'information collectée. La plupart des sites de vente en ligne utilisent à cette fin le logiciel *Secure Sockets Layer* (SSL), véritable standard de l'industrie.

Le principe de respect des normes impose à la fois une forme d'autorégulation et la prise par les États de lois visant à assurer le respect des principes précédemment cités. S'il est permis de douter de l'efficacité de l'autorégulation, de nombreuses entreprises considèrent que sans la confiance accordée par les consommateurs, le commerce électronique ne saurait survivre. Il a donc été créé une organisation à but non lucratif, dénommée *TRUSTe*, d'une part afin de vérifier l'application des principes de la FTC, et d'autre part pour délivrer un certificat de conformité à ces principes aux acteurs du marché (*FTC Compliance Certificate*).

Comme il est courant en droit anglo-saxon, à côté des règles générales, une grande importance est donnée à la jurisprudence. Dans le domaine qui nous intéresse, deux affaires font figure de pierres angulaires : les affaires « AOL » et « Double Click ».

2. Les affaires AOL et Double Click.

En effet, en matière de protection du consommateur face à la publicité non sollicitée sur le web, la justice américaine a pu, à l'occasion des affaires AOL et Double Click, clarifier certains points de questionnement juridique.

a. L'affaire AOL : *Class action* et *pop-up ads*.

Dans un arrêt du 20 juin 2000, un juge de Floride a accepté de qualifier en *Class action* une plainte à hauteur de plusieurs millions de dollars contre le plus grand fournisseur d'accès à Internet du monde, America Online, sur la base de l'affichage de publicités « *pop-up* ».

En effet, AOL bloquait l'accès du consommateur à ses services pendant que les *pop-up ads* apparaissaient à l'écran. Selon les demandeurs, les 2,5 millions d'abonnés à AOL ne devraient pas être facturés pour ce temps « *perdu* ». En effet, AOL facture à ses abonnés chaque heure d'utilisation une fois dépassé leur forfait, à l'époque de trois ou cinq heures.

La Juge Fredericka Smith, du Tribunal du Comté de Miami-Dade, constatait le 20 juin 2000 que « *Les demandeurs ont établi que la mise en œuvre de cette espèce comme Class action est plus opportun que de demander à chaque intéressé de poursuivre AOL de façon individuelle.* »

Selon les demandeurs, le système revient à faire payer deux fois l'abonné pour le même produit : une fois par le biais de l'abonnement et du dépassement de forfait, et une fois par la publicité.

Si le jugement n'a pas encore été rendu dans cette affaire (le juge s'étant pour l'instant contenté d'accepter la qualification de *Class action*), il est demandé vingt millions de dollars en dommages et intérêts, et évidemment l'arrêt des pratiques reprochées à AOL.

Le 12 mars 2003¹⁶, le fournisseur d'accès prenait les devants en annonçant la mise au point d'un logiciel qui offrirait aux abonnés la possibilité d'interdire l'affichage des fenêtres de publicité non sollicitée apparaissant au-dessus et au-dessous (*pop-under*) ses pages web. Ce logiciel sera également intégré aux nouvelles versions du kit de connexion d'AOL.

Si cette initiative peut paraître judicieuse compte tenu des poursuites engagées, on peut considérer que le fournisseur d'accès s'expose à présent à des actions sur le terrain du droit de la concurrence : en effet, ce logiciel « *anti-pop-up* » ne bloque pas, par défaut, les publicités émises par AOL et les autres entreprises du groupe AOL Time Warner...

b. L'affaire Double Click.

Double Click, entreprise de premier plan sur le marché des fournisseurs de contenu publicitaire en ligne, a racheté en 2000 pour 1,7 milliard de dollars Abacus Direct, fournisseur de bases de données d'informations personnelles. Ce faisant, Double Click comptait intégrer à

¹⁶ *Associated Press*, Mars 2003.

sa propre base de données le catalogue d'informations d'Abacus, afin de disposer d'un profil utilisateur complet pour chacun des individus fichés. Une telle banque de données serait utilisée dans le cadre d'envoi de publicités dans les boîtes aux lettres électroniques, mais surtout directement sur les écrans des utilisateurs. Selon l'entreprise¹⁷, « *Il s'agit de délivrer la bonne publicité à la bonne personne, au bon moment.* »

La fusion des bases d'information sur les habitudes de navigation et des informations à caractère personnel a déclenché une véritable levée de boucliers. Une telle opération a même été qualifiée « *D'attaque de plein fouet, financée par Wall Street, contre l'anonymat sur Internet.* »¹⁸

En effet, la fusion avec Abacus Direct permettait à Double Click de suivre les habitudes d'un consommateur de « magasin » en « magasin », d'identifier ses achats, mais également de revisiter chaque page consultée. L'opération permettait ainsi de faire fusionner une série d'informations à caractère personnel et nominatif avec des données auparavant anonymes sur les habitudes du consommateur, sans le moindre consentement des intéressés.

Une poursuite de type *Class action* a donc été engagée¹⁹ devant la FTC pour le compte de tous les utilisateurs ayant sur leur disque dur des *cookies* installés par Double Click, et donc leur navigation « espionnée ». Les demandeurs fondaient leur action sur la violation de trois lois fédérales : le titre II de l'*Electronic Communications Privacy Act*, le *Federal Wiretap Act*, et le *Computer Fraud and Abuse Act*. L'affaire fut résolue en faveur de Double Click, les demandeurs n'étant pas parvenus à établir l'existence d'un préjudice nécessitant réparation.

Il a en effet été considéré dans un premier temps que l'*Electronic Communications Privacy Act (ECPA)* avait pour but d'empêcher le piratage. Selon les demandeurs, l'activité de Double Click (réunion d'informations, installation de *cookies*) constituait une forme de piratage. Mais il a été retenu par le juge que les activités de Double Click n'entraient pas dans le champ de l'*ECPA*.

¹⁷ *USA Today*, Février 2000.

¹⁸ Jason Catlett, *JunkBusters* (association pour l'anonymat du consommateur).

¹⁹ *In Re Double Click Inc. Privacy Litigation*, 154 F. Supp. 2nd 497 (2001).

Concernant le *Federal Wiretap Act* (loi fédérale sur les écoutes), qui organise le régime pénal et civil des écoutes vocales, câblées ou électroniques, il a été rappelé par le juge qu'il ne s'appliquait pas lorsque le consentement des parties avait été recueilli.

Enfin, le *Computer Fraud and Abuse Act (CFAA)* permet aux victimes d'accès non autorisé à leur ordinateur d'obtenir dommages et intérêts. Double Click, sans chercher à prouver que les *cookies* ne constituaient pas un accès non autorisé à l'ordinateur de l'utilisateur selon les termes de la loi, a soutenu à bon droit qu'aucun préjudice n'avait été causé. En effet, le *CFAA* nécessite pour être appliqué que soit prouvée l'existence d'un préjudice d'au moins cinq mille dollars par an et par personne.

Il fut enfin rappelé par le juge que les utilisateurs, par un paramétrage adéquat de leur navigateur Internet, pouvaient bloquer les *cookies* de Double Click, et qu'ils pouvaient également, sur le site de Double Click, mettre un terme à l'envoi des *cookies*.

Si cette victoire est d'une très grande importance pour Double Click (tant en terme d'image qu'au point de vue financier), l'entreprise reste dans le collimateur de la justice américaine, avec pas moins d'une douzaine de plaintes déposées contre elle.

En droit américain, comme nous l'avons vu, la protection du consommateur face à la publicité non sollicitée sur Internet est donc à la fois assurée par un corps de règles assez largement respectées, et par une jurisprudence peu ambiguë et raisonnable.

B. Le droit français, en gestation.

Si le droit américain, nous l'avons vu, organise une protection efficace du consommateur contre la publicité intrusive et les usages dangereux de ses données personnelles, le droit français reste adapté en partie seulement à ces deux combats.

Nous étudierons dans un premier temps l'apport communautaire en la matière (1), puis la difficile évolution du droit interne (2).

1. L'apport communautaire.

En matière de publicité en ligne, trois grands textes communautaires, assez récents, ont vocation à s'appliquer : il s'agit des directives européennes « Commerce électronique » (2000/31/CE du 8 juin 2000) « Protection des données personnelles » (95/46/CE du 24 octobre 1995) et « Traitement des données à caractère personnel et protection de la vie privée » (2002/58/CE du 12 juillet 2002). Nous examinerons en quoi la publicité intrusive sur Internet peut entrer dans le champ de chacun de ces textes.

a. La directive européenne du 8 juin 2000, dite « Commerce électronique ».

La directive couvre tous les services de la société de l'information, qu'ils soient fournis entre entreprises (*B to B*) ou entre entreprises en consommateurs (*B to C*). La partie de la directive qui nous intéresse, dans le cadre de la présente étude, est la Section 2 du Chapitre II : *Communications commerciales*.

La directive soumet les communications commerciales à certaines conditions de transparence pour renforcer la confiance du consommateur et garantir des pratiques commerciales loyales. Ainsi, il est imposé que ces communications soient clairement identifiées comme telles, et que la personne physique ou morale pour le compte de laquelle la communication commerciale est faite soit clairement identifiable (article 6).

L'article 7, qui concerne les communications commerciales non sollicitées, ne s'applique qu'aux messages publicitaires de cette nature transmis par courrier électronique

(*spamming*). A ce titre, on peut regretter que son champ d'application ait été restreint, tandis que le législateur américain n'a lui pas considéré comme utile de faire la distinction entre la publicité non sollicitée envoyée par courrier électronique et celle affichée directement à l'écran.

b. La directive européenne du 24 octobre 1995 et la directive du 12 juillet 2002.

La directive du 24 octobre 1995, entrée en vigueur en 1998, accorde certains droits aux individus dont les données font l'objet d'une collecte, d'un traitement ou d'un échange. La personne a le droit d'accéder, de rectifier ses données à intervalles raisonnables et sans qu'il y ait entrave à ce droit, c'est-à-dire sans que la procédure d'accès soit trop lourde ou fastidieuse. De la même façon, il est prévu un droit de s'opposer au traitement des données à caractère personnel, notamment lorsque celles-ci sont utilisées à des fins de prospection.

L'article 6 *a* de la directive dispose que les données à caractère personnel doivent être traitées loyalement et licitement. La référence à la loyauté est particulièrement adaptée tant le manquement à ce principe est devenu fréquent en matière de publicité sur Internet : c'est le cas avec les identifiants cachés, les *proxies*, les *cookies* et autres dispositifs logiciels (*spyware*, *adware*). La finalité annoncée n'est pas la même que la finalité réelle du traitement, et la loyauté incite le responsable du traitement à la transparence et à la fluidité, au respect du droit d'opposition.

Quant à la toute récente directive du 12 juillet 2002, si elle s'adresse principalement aux fournisseurs d'accès, son article 13, « Communications non sollicitées », présente un champ d'application *a priori* plus large que celui des dispositions contenues dans la directive du 8 juin 2000.

En effet, l'article 13 § 3 concerne selon la directive « *les cas autres que ceux visés aux paragraphes 1 et 2* » ; autrement dit, les communications non sollicitées autre que télécopies, audiotel et messages électroniques. Concernant cette catégorie, à laquelle on rattachera les pop-up ads, il est laissé aux États membres le choix entre *opt-in* et *opt-out*, non sans les contraindre à choisir l'une ou l'autre de ces solutions. C'est dire que les États membres de l'Union européenne vont avoir à légiférer sur la publicité non sollicitée sur Internet, en dehors du cas du *spamming* déjà en cours de règlement. Le paragraphe 4 du même article, pour sa part, impose aux émetteurs de tous « *messages électroniques à des fins de prospection*

directe » de « *camoufler* » leur identité. Le terme « *message électronique* », on le conçoit aisément, est plus large que celui de « *courrier électronique* » : il peut tout à fait désigner une communication publicitaire par affichage direct à l'écran.

2. Le droit interne.

Si le droit interne organise, depuis la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, une protection assez avancée des données personnelles en ligne comme hors ligne, sa gestion des publicités non sollicitées sur Internet reste encore suspendue à la transposition des directives européennes mentionnées plus haut, et donc au fameux projet de loi pour la confiance en l'économie numérique (projet dit « LEN »).

a. La loi du 6 janvier 1978, « Informatique, fichiers et libertés ».

La loi de 1978 a imposé au gestionnaire des données personnelles de multiples obligations : réglementation du mode de collecte des données, obligation de donner des renseignements, protection de la sécurité des données, obligation de veiller à la qualité de l'information. Lorsque les données personnelles font l'objet d'un « traitement automatisé », de nouvelles obligations viennent s'ajouter : déclaration préalable à la CNIL (Commission nationale informatique et libertés), respect de la finalité du traitement, conservation limitée...

Quant à la personne concernée par les données, elle jouit des droits suivants : droit à la curiosité, droit d'accès et de communication des données, droit de contestation et de rectification, opposition à certains traitements automatisés. A fin de veiller au respect de ces dispositions, il a été créé une autorité administrative indépendante, la Commission nationale informatique et libertés, qui a su bâtir au fil des années une véritable doctrine d'interprétation de la loi.

Même si le phénomène des *pop-up ads* et autres *spyware* est assez récente, les dispositions de la loi de 1978, telles qu'interprétées par la CNIL, trouveraient vocation à s'appliquer si, d'aventure, une affaire du type « Double Click » venait à naître en France. En effet, la Commission a par exemple estimé que les garanties suffisantes d'exercice du droit d'opposition n'existaient pas lorsque la suppression de la « case à cocher », sur un

questionnaire alimentant une base de données de consommateurs, pour refuser la cession des données à un tiers, avait en fait pour objet et effet de réduire le nombre de personnes interrogées pouvant manifester leur opposition. L'arrêt Société Consodata du Conseil d'État²⁰ précise que la CNIL ne commet en la matière ni erreur de droit, ni erreur d'appréciation.

Toutefois, selon Jean Frayssinet²¹, « *La loi du 6 janvier 1978 est arrivée à la fin de sa première vie. [...] La nécessité d'opérer la transposition de la directive communautaire du 24 octobre 1995 ouvre la voie à une loi Informatique, fichiers et libertés de deuxième génération, plutôt qu'à un changement complet du paysage législatif français.* »

b. La transposition du droit communautaire et le projet « LEN ».

En effet, si la loi de 1978 organisait jusque récemment une protection satisfaisante des données personnelles, le phénomène de la publicité non sollicitée sur Internet et le besoin de réglementer les pratiques qu'il recoupe entraînent la nécessité d'une nouvelle loi sur les données personnelles, sur le modèle des directives européennes et, pourquoi pas, des règles édictées par la FTC américaine.

La transposition en droit interne des dispositions de la directive du 24 octobre 1995 (entrée en vigueur en 1998) semblait donc, dans cette optique, indispensable. Alors qu'a été promulguée la nouvelle directive du 12 juillet 2002, cette tâche n'avait toujours pas été accomplie.

Le gouvernement a récemment annoncé²² que ce travail de transposition serait accompli par trois lois : la loi sur la confiance dans l'économie numérique, la loi sur les communications électroniques et la loi sur le droit d'auteur. A l'heure où nous écrivons ces lignes, n'est disponible qu'un *projet de loi* sur la confiance dans l'économie numérique.

Concernant le régime des communications publicitaires non sollicitées sur Internet, force est de constater que la transposition est incomplète : alors que la directive du 12 juillet 2002 couvre pour certaines de ses dispositions les techniques autres que le *spamming*, ce n'est

²⁰ CE 30 juillet 1997, Société Consodata ; *JCP*, 1997, II, 22950, note J. FRAYSSINET.

²¹ André LUCAS, Jean DEVÈZE, Jean FRAYSSINET, *Droit de l'informatique et de l'Internet*, Thémis droit privé, P.U.F. Titre I, *La protection des données personnelles*.

²² <http://www.telecom.gouv.fr/internet/plen.html>.

pas le cas du projet dit « LEN » dans son état actuel. En effet, ce texte prend soin de ne couvrir dans le domaine qui nous intéresse que les communications effectuées par automate d'appel, télécopieur et courrier électronique, à l'exception – par simple oubli ? – de ce que la directive « vie privée » rangeait dans la catégorie plus large des « *messages électroniques* »²³.

Cette différence entre la directive et le projet de loi est d'autant plus regrettable que, compte tenu des nombreuses contestations contre des dispositions plus sensibles et plus polémiques du projet de loi, il y a fort à parier que personne ne jugera nécessaire d'y remédier.

Il en reste ainsi qu'à espérer que la future loi sur les communications électroniques, dont c'est peut-être plus la vocation, inclura des dispositions relatives aux publicités non sollicitées en lignes autres que le *spamming* – au moins dans un souci de transposition fidèle des termes de la directive du 12 juillet 2002.

²³ *cf. supra.*

II. La publicité en ligne et la concurrence.

S'il est totalement compréhensible que la protection du consommateur requière toute l'attention du législateur, la publicité non sollicitée sur Internet reste néanmoins la source d'un nombre de plus en plus important d'atteintes à la concurrence.

En matière de droit de la concurrence toutefois, l'intervention législative est moins nécessaire, et les principes traditionnels restent applicables aux situations créées par les nouvelles technologies.

La principale affaire impliquant des *pop-up ads* en droit de la concurrence est l'affaire Gator ; elle concerne le droit américain (A). Son indispensable analyse, tant technique que juridique, sera suivie d'une étude des règles de concurrence françaises applicables aux *pop-up ads*, qu'il s'agisse de concurrence déloyale ou de propriété intellectuelle (B).

A. Le droit américain : l'affaire Gator.

Si l'affaire Gator ne peut être étudiée sans un rappel minutieux de ses aspects techniques (1), nous nous pencherons ensuite sur ses implications juridiques (2).

1. L'aspect technique.

D'un point de vue technique, il convient de rappeler comment de nombreux logiciels ont recours à la publicité comme mode de financement, puis d'analyser la plus récente et la plus dangereuse de ces techniques, le *spyware*.

a. Le financement des logiciels par la publicité.

Jusqu'à la fin des années 1990, les logiciels informatiques distribués par Internet pouvaient être regroupés en trois catégories : ils étaient soit *payants*, comme la plupart des

logiciels sur le marché, soit de type *shareware*, c'est-à-dire gratuit pendant une certaine période d'utilisation ou jusqu'à un certain niveau de fonctionnalité, puis ensuite payants, soit complètement *gratuits*.

Le premier cas se trouve assez rarement sur Internet : on peut certes acheter en ligne un logiciel, comme on achèterait un disque ou un livre, mais ce dernier sera livré par colis, non par téléchargement. Le cas où le client donne son numéro de carte bancaire afin de pouvoir simplement *télécharger* le logiciel est somme toute assez rare.

La technique la plus répandue pour faire des bénéfices avec un logiciel spécialement distribué par Internet – donc téléchargé par les clients potentiels – restait donc, jusque récemment, celle du *shareware*. Le principal inconvénient de cette dernière étant évidemment que très peu d'utilisateurs jugeaient nécessaire de rémunérer l'éditeur de leur logiciel.

Avec le développement de la publicité en ligne, une nouvelle technique de financement des logiciels, bien plus pratique est efficace, fut mise au point : à l'instar d'un magazine ou d'une chaîne de télévision, certains éditeurs commencèrent à avoir recours à la publicité pour financer leurs logiciels distribués en ligne. On peut citer l'un des premiers logiciels de *peer-to-peer*, Napster (aujourd'hui mis hors service), qui affichait des bandeaux publicitaires dans un cadre de sa fenêtre : on parle alors d'*adware* (contraction de *advertisement*, publicité, et *software*, logiciel).

b. Le phénomène du *spyware*.

Aujourd'hui, les logiciels dits gratuits continuent de recourir massivement aux bandeaux publicitaires, cette technique ne posant juridiquement pas de réel problème. Dans la grande majorité des cas, l'utilisateur est averti avant le téléchargement du logiciel que la version gratuite qu'il s'apprête à installer est financée par la publicité.

Les logiciels qui posent de sérieux problèmes juridiques sont eux encore plus « évolués » : un module fonctionnant en tâche de fond, donc de manière invisible pour l'utilisateur lambda, appelé *spyware*, recueille diverses informations au sujet de l'internaute et les envoie directement à l'éditeur du logiciel, qui acquiert ainsi une base de données de très forte valeur commerciale.

La société américaine Gator Corporation a mis au point en 2001 un logiciel, *Gator*, intégrant un module *spyware*. En effet, alors que le logiciel Gator a pour principale fonction de faciliter la gestion des mots de passe et autres informations personnelles de l'internaute (en lui évitant de retaper à chaque fois ses nom, prénom, adresse, etc. sur les questionnaires en ligne), sa principale activité est en réalité de recueillir des données personnelles sur l'utilisateur, données qui seront utilisées pour afficher des publicités de type *pop-up*. Cette technologie est baptisée par Gator Corporation : *Gator Advertising and Information Network (GAIN)*.

Grâce aux données recueillies, les publicités sont ciblées ; lorsque l'internaute visite un site, les publicités envoyées émanent d'annonceurs évoluant dans la même branche commerciale que le site visité.

2. L'application des règles de concurrence.

Après avoir analysé le fondement juridique des thèses concurrentes en l'espèce, nous relaterons l'issue de l'affaire Gator et ses différentes implications.

a. Le fondement juridique.

C'est ici que naît le problème juridique de l'affaire Gator (*Washingtonpost.newsweek Interactive Company, LLC, et al. v. The Gator Corporation*)²⁴ : les sociétés propriétaires de douze sites web d'information ont mis en œuvre en juin 2002 des procédures judiciaires contre Gator devant le Tribunal d'Alexandrie, en Virginie. Selon les demandeurs, les activités du logiciel Gator empêchaient l'affichage régulier de leurs pages, et les fenêtres *pop-up* de Gator couvraient notamment les bandeaux publicitaires payés par les annonceurs des sites requérants.

Le fondement juridique de la demande consistait en une violation de *copyright* et du droit des marques, privant les sociétés propriétaires des sites de revenus publicitaires. Il a également été avancé par les demandeurs qu'un préjudice serait causé par le fait que

²⁴ C.A. No. 02-909-A (E.D. Va., 16 juillet 2002).

l'affichage ininterrompu de publicités non sollicitées sur leurs sites ferait penser aux visiteurs que les propriétaires des sites en question manquaient à leurs obligations déontologiques. Dans le même sens, les demandeurs accusaient également Gator Corporation de compétition déloyale et d'enrichissement sans cause.

Dans un premier temps, le 16 juillet 2002, le tribunal obligea Gator Corporation, par une « injonction préliminaire » (*preliminary injunction*) de bloquer l'affichage de *pop-ups* sur les sites Internet des demandeurs. En effet, l'arrêt avant dire droit à l'origine de cette injonction reconnaît clairement la violation de *copyright* et de *trademark* ; il est intéressant de citer le juge Claude Hilton :

« Je considère qu'il est suffisamment clair qu'il y a violation du droit des marques dans cette technique de publicité. Un préjudice irréparable est à présumer en l'espèce. Et je considère que les demandeurs sont fondés à bénéficier d'une injonction préliminaire, garantissant pendant ce procès l'absence de violation du droit des marques. »

La société Gator Corporation, quant à elle, soutenait que son réseau réunissait « 25 millions de consommateurs, ayant tous donné leur autorisation » à l'envoi de publicités suite au téléchargement de ses logiciels *eWallet* et *Precision Time*. Mais en délivrant des *pop-up ads* aux visiteurs des sites des demandeurs, Gator diminue la possibilité pour ces derniers de vendre de la publicité.

Dans le cas où les thèses des demandeurs, selon lesquelles les *pop-up ads* violent le droit des marques, étaient reprises *in fine* par le juge, quel avenir pour tous les logiciels utilisant des systèmes similaires, et surtout, par ricochet, quel avenir pour les programmes bloquant la publicité sur les sites visités ? On pourrait même penser que les internautes qui configurent leur navigateur afin qu'il n'affiche aucune image sur les pages web – ce qui accélère leur chargement – violent le droit exclusif de l'éditeur du site sur la façon dont ses pages s'affichent !

b. L'issue des débats.

L'arrêt du tribunal fédéral d'Alexandrie était très attendu : en effet, il semble que les logiciels de Gator Corporation portent atteinte simultanément aux droits des consommateurs – par la collecte des données personnelles gérées par le logiciel *eWallet* –, à ceux des

concurrents des annonceurs partenaires de Gator Corporation, et au final aux éditeurs des sites visités par l'utilisateur des logiciels *eWallet* et *Precision Time*.

Le juge Hilton avait donc l'occasion de rendre le 27 janvier 2003 une décision fondatrice en matière de *pop-up ads* et de droit de la concurrence en ligne. Les questions posées par l'affichage, par-dessus la fenêtre d'un site Internet, de publicités concurrentes tantôt de l'éditeur du site, tantôt des annonceurs de ce dernier, étaient à rapprocher du débat né autour de la technique du *framing*, qui consiste pour un créateur de site web à afficher un autre site dans un cadre (*frame*) sur son propre site.²⁵

Mais le 5 février 2003, les parties sont arrivées à trouver un terrain d'entente, par la signature d'un compromis dont les termes restent strictement confidentiels. Cette affaire ne fournira donc pas aux publicitaires, aux responsables de sites et aux juristes la prise de position qu'ils appelaient de leurs vœux. Dans une affaire précédente, Gator Corporation avait déjà réussi à « décrocher » un compromis extrajudiciaire, avec l'*Interactive Advertising Bureau* en novembre 2001. Et la publicité sur les sites des demandeurs ne représente qu'environ 0,33 % des recettes publicitaires totales de la société.

La conséquence la plus probable de cette affaire, selon un avocat spécialisé²⁶, sera un changement dans la technologie utilisée par Gator : les publicités pourraient à l'avenir apparaître « sous » les sites web plutôt que par-dessus – on parle alors de *pop-under*. Un changement qui réduirait certes les risques juridiques pour la société, mais n'étendrait pas la polémique née de la manipulation et de l'utilisation déloyale de données personnelles massivement collectées.

²⁵ Anne GIRAUDEL, Les liens hypertextes face au droit, *Juriscom.net*, juin 1998.

²⁶ Doug ISENBERG, Are Pop-up Advertisements On The Web Illegal? *Gigalaw*, novembre 2002.

B. L'applicabilité des règles de concurrence en France.

Aucun litige n'a encore été porté à la compétence des tribunaux français en matière de *pop-up ads* ; les seules espèces en matière de publicité non sollicitée sur Internet relèvent en effet du *spamming*. On peut toutefois se demander, si une affaire du type Gator venait à voir le jour en France, quelles seraient les règles susceptibles de s'appliquer en droit de la concurrence.

Il apparaît que celles-ci sont à ranger dans deux catégories : la concurrence déloyale d'une part (1), et d'autre part un domaine ne relevant pas *directement* du droit de la concurrence, mais s'y rattachant souvent, la propriété intellectuelle (2).

1. La concurrence déloyale.

Les comportements susceptibles de caractériser une concurrence déloyale en matière de publicité non sollicitée en ligne peuvent varier. Il peut s'agir d'actes de dénigrement, d'imitations des signes de l'entreprise concurrente, de désorganisation de celle-ci ou enfin de parasitisme commercial.

a. L'acte de dénigrement.

Le dénigrement est défini par la jurisprudence comme une affirmation malicieuse, dirigée contre un concurrent dans le but de détourner sa clientèle, notamment en discréditant ses produits, le travail ou la personne de celle-ci.

Selon un arrêt du Tribunal de commerce de Paris du 16 novembre 1983, le dénigrement peut être réalisé par l'envoi de lettres missives adressées à plusieurs clients de sociétés concurrentes. Outre sa possible application au phénomène du *spamming*, on comprend que cette jurisprudence pourrait tout à fait être reprise dans un cas similaire à

l'affaire Gator, les publicités non sollicitées étant affichées sur l'écran de l'internaute spécifiquement en fonction des sites visités.²⁷

Le dénigrement ouvre droit à réparation lorsque l'entreprise visée est désignée, expressément ou implicitement, ou identifiable par sa clientèle.

b. L'imitation des signes de l'entreprise concurrente.

Un des procédés couramment utilisés et sanctionnés par les tribunaux consiste à utiliser les méthodes d'un concurrent en vue de créer une confusion susceptible d'attirer la clientèle de ce dernier au profit de l'imitateur.

Parmi les moyens utilisés, on peut noter l'imitation de publicité, elle aussi parfaitement constituée dans l'affaire Gator, encore une fois en raison du caractère ciblé des publicités diffusées lors de la navigation.

c. La désorganisation de l'entreprise concurrente.

La désorganisation de l'entreprise concurrente peut être constatée par le juge et constituer un acte de concurrence déloyale en cas de détournement de clientèle. Or, dans l'affaire Gator, la collecte par le logiciel *eWallet* des données rentrées par l'utilisateur sur le site visité, et la réutilisation de ces données afin d'envoyer des publicités concurrentes, semble pouvoir caractériser un tel détournement de clientèle, et un détournement de listes de clients.

d. Le parasitisme commercial.

Le parasitisme est l'ensemble des comportements par lesquels un agent économique s'immisce dans le sillage d'un autre afin de tirer profit sans rien dépenser de ses efforts et de son savoir-faire.

²⁷ En ce sens, Gérard PICOVSKI, Concurrence déloyale et site web, *Legalbiznext.com*.

L'agissement parasitaire est le fait, pour une entreprise, de vivre aux crochets d'une autre, de tirer profit de l'activité d'autrui sans bourse délier, et permet de condamner quiconque usurpe une valeur économique d'autrui, même non concurrent.

L'affichage de *pop-up ads* publicitaires par-dessus les pages de sites commerciaux concurrents semble, quelles que soient les conditions, constitutif de parasitisme commercial. En effet, le principe même de profiter du fait que l'internaute accède à un site Internet pour lui envoyer des publicités dont l'annonceur n'est ni l'éditeur du site visité, ni un de ses partenaires, revient bien à tirer profit du travail de conception et de référencement du site « parasité ». Il est d'ailleurs révélateur que dans le cadre de l'affaire Gator, les demandeurs aient qualifié Gator Corporation de « *parasite du web, passager clandestin qui profite du travail et des investissements des éditeurs de sites.* »

L'action en concurrence déloyale, basée sur la responsabilité civile délictuelle, peut donc être menée sur plusieurs fondements juridiques. Mais le phénomène des *pop-up ads* peut aussi contrevenir au droit de la propriété intellectuelle.

2. La propriété intellectuelle.

Avant d'expliquer comment une publicité de type *pop-up* peut porter atteinte à la propriété intellectuelle d'un éditeur de site sur ses créations, il convient de rappeler dans quelles conditions le site Internet est protégé par le droit d'auteur.

a. La protection du site visité.

Les droits d'auteur s'appliquent à toute œuvre de l'esprit, quels qu'en soient le genre, la forme d'expression, le mérite ou la destination, selon la formule de l'article L. 112-1 du Code de la propriété intellectuelle. Pour qu'une œuvre de l'esprit soit protégée par le droit d'auteur, il faut qu'elle soit originale, c'est-à-dire qu'elle soit le reflet de la personnalité de l'auteur, d'une activité créatrice propre.

A ce titre, un site web peut être protégé par le droit d'auteur lorsqu'il constitue un ensemble original ; ses différents éléments peuvent également être protégés individuellement : photographies, extraits musicaux, graphismes, logos, articles... et publicités.

On peut donc ainsi considérer que l'affichage de fenêtres *pop-up* sur un site Internet porte atteinte non seulement au site lui-même, mais également aux publicités qu'il contient.

b. L'atteinte au droit au respect de l'œuvre.

En effet, l'auteur dispose de droits moraux, qui présentent la particularité d'être perpétuels et inaliénables, parmi lesquels l'un peut s'appliquer à la publicité par *pop-up* : le droit au respect de l'œuvre. Ce droit vise à protéger l'œuvre de toute dénaturation, modification, altération, ou mutilation. Le fait de superposer un logo lors de la télédiffusion d'un film a été notamment considéré comme une atteinte à l'intégrité de l'œuvre.

Par analogie, dès lors que la publicité émise par un site Internet peut être regardée au sens du Code de la propriété intellectuelle comme une œuvre, le procédé qui établit une confusion graphique par superposition entre celle-ci et une autre publicité, envoyée par un tiers, constitue donc une atteinte au droit au respect de l'œuvre par dénaturation (la première publicité étant privée d'effet).

Plus directement encore, on peut considérer que l'affichage systématique par un tiers d'une fenêtre de publicité au-dessus d'un site Internet est constitutive d'une atteinte au respect de l'œuvre, puisque l'affichage de celle-ci à l'écran s'en trouve totalement obstrué, et donc altéré, voire mutilé.

Même si le droit américain ne connaît pas la notion de « droit moral de l'auteur », lorsque les demandeurs dans l'affaire Gator soulèvent une « violation de copyright »²⁸, c'est bien de la même protection de l'œuvre qu'il s'agit.

²⁸ *cf. supra.*

Conclusion.

Comme on peut le constater, l'utilisation abusive des *pop-up ads* entre, à de nombreux égards, dans le champ d'application du droit de la concurrence. Le droit américain, grâce à la formidable souplesse des systèmes de *Common law*, semble parfaitement en mesure de réprimander de telles pratiques.

Qu'en est-il de l'autre côté de l'Atlantique ? Au niveau communautaire, on peut évidemment regretter le manque de fermeté et le caractère étroit des dispositions relatives à la publicité non sollicitée sur Internet contenues dans les différentes directives étudiées.

Toutefois, en droit interne, de nombreuses solutions restent à la portée du législateur, à commencer par une application extensive des dispositions de la loi Informatique, fichiers et libertés. Ensuite, la transposition de la directive « Vie privée et communications électroniques » pourrait aller plus loin que le texte original, réprimant également les publicités envoyées *directement en ligne*. La loi du 1^{er} août 2000, modifiant la loi de 1986 sur la liberté de communication, impose aux fournisseurs d'accès à Internet de fournir à leurs clients un logiciel de contrôle parental (article 43-7) ; pourquoi ne pas ajouter à cette disposition l'obligation de fournir un logiciel bloquant les *pop-up ads* ? En effet, dans l'affaire AOL étudiée plus haut, le premier fournisseur d'accès mondial s'est engagé à offrir à ses abonnés un tel dispositif.

Enfin, même en l'absence de dispositions légales, nous avons pu constater que le droit français dispose d'outils, sur le terrain de l'article 1382 du Code civil en matière de concurrence déloyale, ou avec les dispositions du Code de la propriété intellectuelle, permettant de réprimer les abus rendus possibles par une technique facilement maîtrisable.

Conclusion générale.

A l'heure où la difficile articulation des textes existants est une source d'insécurité juridique pour les commerçants qui utilisent Internet, cette confusion nuit également à la protection des internautes. Or, avec l'entrée en vigueur de la nouvelle directive « Vie privée et communications électroniques », une clarification en faveur des internautes est en train de voir le jour, et la France devra respecter le délai imparti pour sa transposition, prévue avant le 31 octobre 2003.

Même si, jusqu'à présent, le droit positif a su démontrer sa capacité à régler efficacement les situations inédites, une harmonisation européenne semble nécessaire afin de lutter contre la publicité non sollicitée sur Internet, au niveau international.

En effet, il n'est plus nécessaire, aujourd'hui, de démontrer combien Internet se joue, par nature, des frontières nationales. Dans un tel contexte, l'harmonisation engagée par le législateur européen est évidemment bienvenue ; mais elle ne saurait suffire.

D'une part, une même publicité non sollicitée peut atteindre sur Internet, des consommateurs et des concurrents aussi bien d'un côté de l'Atlantique que de l'autre ; comment alors s'assurer, pour une entreprise européenne par exemple, qu'elle ne sera pas victime aux États-Unis de concurrence déloyale par ce biais, alors même qu'en Europe le droit communautaire lui assure une certaine protection ? Il apparaît donc nécessaire que les dispositions protectrices soient rédigées en termes aussi proches que possibles, au-delà du simple choix de l'*opt-in*.

D'autre part, il semble nécessaire d'organiser une protection identique contre toutes les formes de publicité non sollicitée sur Internet. Il n'est en effet pas acceptable qu'alors que la question du *spamming* est en passe d'être réglée, celle des *pop-up ads* reste noyée dans une sorte d'expectative juridique, où chacun « pioche » dans la masse de textes spéciaux et généraux disponibles en matière de droit des nouvelles technologies, de protection du consommateur, de droit de la concurrence.

Dans ces conditions, il appartient sans doute au législateur communautaire non seulement de s'inspirer en matière de protection de l'internaute des exemples américain et français, mais également d'aligner au plus vite le régime des *pop-up ads* sur celui du *spam*.

Lexique technique.

— *Cookies* : informations échangées entre un navigateur et un serveur web, pouvant être stockées sur le disque dur du client. Leur usage est décrié pour des raisons évidentes de sécurité. Les *cookies* sur le web sont des données au format texte, obtenues par le concepteur de la page web, soit parce qu'elles se réfèrent directement au site visité, soit parce que l'utilisateur a rempli un formulaire.

— *Netiquette* : ensemble minimum de règles de conduite sur Internet. Ces règles de conduite sont valables dans tous les pays, pour tout le monde.

— *Opt-in / opt-out* : manière dont sont collectées les données personnelles (en particulier des adresses électroniques) des internautes. On distingue quatre possibilités d'inscription d'un internaute à une liste de diffusion. Dans la liste qui suit, la liberté de choix de l'internaute est de plus en plus réduite.

1. *Opt-in* actif : l'internaute doit volontairement cocher une case ou faire défiler un menu déroulant pour que son adresse (ou d'autres données) soient utilisées ultérieurement à des fins commerciales.
2. *Opt-in* passif : une case est déjà pré-cochée ou un menu déroulant déjà positionné sur oui (à la question voulez-vous recevoir des sollicitations ultérieures ?). Avec l'*opt-in*, l'accord de l'internaute est explicite.
3. *Opt-out* actif : Il faut cocher une case ou sélectionner un menu déroulant pour ne pas recevoir de message ultérieurement. On considère l'accord de l'internaute comme acquis par défaut, implicite.
4. *Opt-out* passif : en s'inscrivant à un service, l'internaute est automatiquement inscrit à une liste de diffusion sans qu'il ait la possibilité de changer cela au moment de l'inscription. La désinscription ne peut se faire qu'après l'inscription. L'accord de l'internaute est demandé a posteriori.

— *Peer-to-peer* : partage des ressources et des services par échange direct entre systèmes. Contrairement au modèle client / serveur, chaque système est une entité réseau complète qui

remplit à la fois le rôle de serveur et celui de client. Avec le *peer-to-peer*, les ordinateurs personnels ont le droit de faire partie du réseau. Le *peer-to-peer* désigne donc une classe d'applications qui tirent partie des ressources matérielles ou humaines qui sont disponibles sur le réseau Internet.

— *Pop-up* : fenêtre qui s'ouvre par-dessus les autres, généralement de plus petite taille. Lorsque la fenêtre s'ouvre *sous* les autres, on parle de *pop-under*.

— *Proxy* : serveur de proximité ou passerelle Internet, qui agit comme un filtre, gérant le trafic entre un réseau privé et Internet. Physiquement, c'est un vaste espace disque localisé chez le fournisseur d'accès qui sert à stocker les pages web les plus consultées par les abonnés, afin qu'elles s'affichent plus rapidement. Un *proxy* ne s'avère efficace qu'avec un nombre restreint d'utilisateurs. Un *proxy* est surtout utile pour économiser de la bande passante (le débit vers Internet offert aux abonnés). Enfin, un *proxy* demande des temps d'accès plus longs pour obtenir une page Web.

— *Spamming* : envoi massif – et parfois répété- de courriers électroniques non sollicités, le plus souvent à caractère commercial, à des personnes avec lesquelles l'expéditeur n'a jamais eu de contact et dont il a capté l'adresse électronique dans les espaces publics de l'Internet : forums de discussion, listes de diffusion, annuaires, sites Web, etc.

— *Spyware* (ou logiciel espion) : partie d'un programme qui récolte des données sur son utilisateur et les transmet à une tierce personne (par exemple une régie publicitaire). Les *spywares* sont présents essentiellement dans les logiciels gratuits et certains refusent de fonctionner sans leur(s) *spyware(s)*.

— *SSL* : *Secure Sockets Layer*, protocole de chiffrement des données, qui atteint en France 128 bits en national et 56 bits à l'international. *SSL* permet de garantir la confidentialité des données, comme le requiert entre autres le paiement en ligne sur Internet.

Bibliographie.

OUVRAGES GÉNÉRAUX :

BALLE Fr., *Médias et sociétés*, Montchrestien, 2001, Paris, 873 p.

DEBBASCH Ch. (sous la direction), *Droit des médias*, Dalloz référence, 2002, Paris, 1184 p.

MALAURIE Ph. et AYNÈS L., *Droit civil – les obligations*, 10^{ème} ed., éditions Cujas, 1999, Paris, 834 p.

OUVRAGES SPÉCIALISÉS :

GAUTIER P.-Y., *Propriété littéraire et artistique*, 4^{ème} ed., PUF, Collection droit fondamental, 2001, Paris, 840 p.

LUCAS A., DEVÈZE J., FRAYSSINET J., *Droit de l'informatique et de l'Internet*, PUF, Thémis, 2001, Paris, 754 p.

ARTICLES ET NOTES :

FEDERAL TRADE COMMISSION, Five Years Protecting Consumers Online, décembre 1999.

FRANKREICH, J. et FOURGOUX L., Internet et la concurrence déloyale, 2001.

FRAYSSINET J., Nouvelles technologies de l'information et de la communication et protection des libertés des consommateurs, *Cahiers Lamy droit de l'informatique et des réseaux*, n° 127, juillet 2000, p. 7.

GIRAUDEL A., Les liens hypertextes face au droit, *Juriscom.net*, juin 1998.

GRYNBAUM L., Contrats et responsabilité, revue *Communication Commerce Électronique*, Avril 2002, éd. Juris Classeur, pp. 24-25. TGI Rochefort-sur Mer, 28 février 2001, Ch. G. c/ Sté France Télécom Interactive SA, TGI Paris, référé, 15 janvier 2002 : P. V. c/ Sté Liberty Surf et a., pp. 25-27.

GRYNBAUM L., Projet de loi « pour la confiance dans l'économie numérique » : encore un petit effort de rigueur juridique pour un « contrat électronique » fiable, *Dalloz 2003* n° 11, pp. 746-749.

ISENBERG D., Are Pop-up Advertisements On The Web Illegal? *Gigalaw*, novembre 2002.

MARNA Ch., Courriers électroniques publicitaires et responsabilités, *Actualité jurisprudentielle, Dalloz 2002*, n° 13, p. 1138.

MARTIN D. et RYAN M., Pop-ups Abound, But Most Advertisers Remain Inline, *Spotlight on Advertising*, Nielsen NetRatings, 29 août 2002.

PICOVSKI G., Concurrence déloyale et site web, *Legalbiznext.com*.

SÉDAILLAN V., Internet et droits d'auteur, *Autour du Libre 2002*, INT Evry, 29 Mai 2002.

SÉDAILLAN V., La directive européenne « Vie privée et communications électroniques », *Légipresse* n°198, Janvier février 2003, pp 12-15.

STANFORD GRADUATE SCHOOL OF BUSINESS, Double Click and Internet Privacy, case number P-32, août 2000.

VARET V., Le cadre juridique du *spam* : état des lieux, *revue Communication Commerce Électronique*, éd. Juris-Classeur, septembre 2002, p. 14.

Table des matières.

SOMMAIRE.....	2
INTRODUCTION.....	3
PREMIÈRE PARTIE : LE SPAMMING, PAR MICHELLE CRISTOFARI.....	6
INTRODUCTION.....	6
I. L'ENCADREMENT JURIDIQUE DU SPAMMING PAR LES RÈGLES DU DROIT DE LA CONCURRENCE... 8	8
A. <i>La difficile application des entraves à la concurrence à la pratique du spamming.</i>	9
1. Le <i>spamming</i> , une pratique anticoncurrentielle ?	9
2. Le <i>spamming</i> , une pratique restrictive de concurrence ?	10
B. <i>Le spamming, une pratique déloyale, attentatoire à la Netiquette.</i>	12
1. L'engagement de la responsabilité des « spammeurs » face aux atteintes à la Netiquette.....	12
2. Applications jurisprudentielles.....	14
II. LE CADRE JURIDIQUE FLOU DU SPAMMING.....	16
A. <i>Les tentatives d'éclaircissement des directives européennes sur le spamming.</i>	17
1. Le choix de l' <i>opt-out</i> par la première directive relative à la protection des consommateurs en	
matière de contrats à distance.....	17
2. La liberté de choix laissée aux États membres : les directives 97/66/CE et 2000/31/CE.....	18
3. La consécration de l' <i>opt-in</i> par la directive « Vie privée et communications électroniques ».....	19
B. <i>L'interdiction ambiguë du spamming par le projet de loi LEN.</i>	21
1. La protection de l'internaute.....	21
2. Une protection difficilement applicable.....	22
CONCLUSION.....	24

DEUXIÈME PARTIE : POP-UP ADS ET SPYWARES, PAR RUBIN SFADJ.....	25
INTRODUCTION.....	25
I. LA PUBLICITÉ EN LIGNE ET LE CONSOMMATEUR.....	26
A. <i>L'avant-garde : le droit américain.</i>	27
1. Les normes adoptées.....	27
2. Les affaires AOL et Double Click.....	29
B. <i>Le droit français, en gestation.</i>	33
1. L'apport communautaire.....	33
2. Le droit interne.....	35
II. LA PUBLICITÉ EN LIGNE ET LA CONCURRENCE.....	38
A. <i>Le droit américain : l'affaire Gator</i>	38
1. L'aspect technique.....	38
2. L'application des règles de concurrence.....	40
B. <i>L'applicabilité des règles de concurrence en France</i>	43
1. La concurrence déloyale.....	43
2. La propriété intellectuelle.....	45
CONCLUSION.....	47
CONCLUSION GÉNÉRALE.....	48
LEXIQUE TECHNIQUE.....	49
BIBLIOGRAPHIE.....	51
TABLE DES MATIÈRES.....	53