Présente :

La collecte de données personnelles par les entreprises québécoises dans un but publicitaire sur Internet

Faculté de droit - Université de Montréal

Travail de session, À l'attention de monsieur le professeur Pierre Trudel.

Véronique ABAD

Session Automne 2002

Date de mise en ligne :10 mars 2003

Sommaire

Internet est aujourd'hui un espace incontournable en matière de publicité, que ce soit pour les entreprises qui exploitent un site sur Internet dont elles veulent faire la promotion ou pour d'autres dont les activités, sont, pour l'instant, basées exclusivement dans le « monde réel » comme le cinéma. La prolifération de messages publicitaires sur Internet en est la plus flagrante preuve. En effet, si Internet était au début des années 90 un médium principalement utilisé par les universitaires, sa démocratisation s'est traduite par une implantation des sociétés commerciales qui ont amenées avec elles les schémas d'économie classiques, et notamment la publicité. Le message commercial étant essentiel au fonctionnement d'une économie saine, en ce qu'il permet d'informer le consommateur, il était donc normal qu'il trouve, avec Internet, un nouveau médium où s'exprimer. Cependant la publicité sur Internet a développé des spécificités nouvelles reliées au fait que l'on peut désormais cibler les récipiendaires d'une campagne promotionnelle. Ce ciblage présuppose de connaître et d'identifier chaque internaute, de l'individualiser, ce qui signifie qu'il faut préalablement recueillir des informations le concernant. Ces données ont une grande valeur commerciale, car en plus de les utiliser à des fins propres, les entreprises peuvent aussi les vendre, par exemple en cas de faillite, comme un commerçant céderait sa clientèle.

Cependant, le fait que les informations collectées permettent d'identifier une personne soulève des problèmes relatifs à la vie privée. En effet, les internautes soucieux de leurs droits, sont souvent réticents quand on leur parle de constituer un dossier les concernant. Les raisons sont multiples, il peut s'agir simplement de la volonté d'être discret ou de ne pas vouloir que des informations soient connues. La peur de se voir voler son identité est aussi très souvent mentionnée.

Cette étude va dresser le portrait de la publicité sur Internet au Québec, en nous attachant d'abord à la présenter (1), puis nous analyserons les lois qui s'appliquent en matière de protection de la vie privée (2), afin d'avoir une vue globale de la situation.

1. **Les activités reliées à la publicité sur Internet**

La publicité est omniprésente aujourd'hui sur Internet ; bandeaux publicitaires, fenêtres pop-up et pourriel abondent dès que l'on se connecte au réseau. Il s'agit principalement de messages qui font la promotion de contenus disponibles sur Internet. En effet, des plus petites entreprises aux multinationales, tous les commerçants peuvent offrir une vitrine mondiale à leurs produits et créer un site pour les vendre en ligne. Car la cyberpublicité offre des perspectives nouvelles aux annonceurs (A.) en matière de ciblage du consommateur internaute. Cependant elle présuppose une bonne connaissance de ce dernier et par la même des procédés pour collecter des données le concernant (B.).

A. La Cyberpublicité

Les objectifs de la publicité en ligne diffèrent peu de ceux de la publicité traditionnelle. Premièrement, le but est de promouvoir l'image de marque, la notoriété d'une compagnie ou des produits et services qu'elle offre. Ensuite, comme une publicité sur un média traditionnel pour une boutique, elle vise à créer un trafic sur un site et ainsi augmenter les ventes. La différence ici est que l'internaute va se trouver immédiatement sur le site marchand grâce à un lien hypertexte intégré à la publicité. Son magasinage est donc énormément simplifié : plus besoin de garer la voiture ni de sortir de chez soi ! L'instantanéité va simplifier le processus de magasinage, donc d'achat. Dans ce sens là, on peut dire que la cyberpublicité est plus avantageuse pour le commerçant qu'une simple annonce insérée dans un journal. Ces remarques sont vraies aussi quand la publicité vise un produit, et que le lien hypertexte amène directement le consommateur sur la page où le bien est vendu. Mais la plus grande différence entre la publicité sur un support traditionnel et la cyberpublicité est que cette dernière *« est également utilisée en*

vue de constituer des bases de données de clients/prospects dans le but de recruter des nouveaux clients ou de fidéliser ceux-ci »[1]. Avant d'aborder cet aspect de base de données et de collecte d'informations sur les internautes (B.) il convient d'abord de présenter un panorama des techniques publicitaires (1.) et de marketing direct (2.).

1. Panorama des techniques publicitaires classiques

La publicité peut prendre sur Internet multiples formes. Certains ont même avancé que toute publication sur Internet était de la publicité[2]. Sans aller jusque là, nous préférons distinguer la publicité des activités plus directement reliées à la vente. Ainsi, un site comme Amazon qui propose des livres cumule une activité de vente, avec un moteur de recherche interne qui permet de trouver l'ouvrage désiré et une communication promotionnelle grâce à des liens vers des livres portant sur des sujets similaires et externes avec des publicités placées sur d'autres sites.

Nous concentrerons donc notre étude sur les trois techniques publicitaires les plus répandues : les bannières, les pop-ups et le spamming, qui sont propices à une personnalisation, à un ciblage pour l'internaute, et nous laisserons de coté les questions reliées aux métadonnées, au référencement et aux autres formes de publicité sur Internet qui, bien qu'elles soient fort intéressantes sur un plan juridique ne posent pas de problèmes relatifs aux données personnelles et à la vie privée sur Internet.

a) Les bandeaux ou bannières publicitaires

Assimilable, jusqu'à un certain point il est vrai, aux encadrés publicitaires présents dans les journaux, le bandeau est la forme la plus classique de promotion sur le web et

[1] Didier GOBERT, « La publicité sur Internet – le droit en (r)évolution », Colloque Internet et le droit , Tunis 4-6 mai 2000, et Revue Ubiquité, décembre 2000,n°7, p71, disponible sur http://www.droit.fundp.ac.be/Textes/publicite.pdf, visité le 8 octobre 2002. Citation page 3.
[2] Marie-Hélène CÔTÉ : « Application des lois nationales à l'Internet : Étude de l'encadrement juridique de la publicité », mémoire de maîtrise, Université de Montréal, janvier 1999.

constitue la grande majorité des investissements publicitaires[3]. Comme dans la presse écrite, le bandeau peut prendre plusieurs formes, vertical, horizontal, rectangulaire, carré etc… Il contient un lien hypertexte qui dirige les personnes, détournées de leur navigation initiale, vers le site dont la bannière fait la promotion ou directement vers l'objet ou le service annoncé.

Afin d'avoir un impact important sur l'internaute, les publicitaires se sont montrés très créatifs. Non seulement le message qui y est apposé est généralement très alléchant, mais les techniques utilisées visent à le rendre encore plus attractif. Nous parlons ici des *gifs* animés (des images, à ne pas confondre avec les *.gifs* dont nous parlerons plus loin), qui permettent d'afficher une publicité non statique à l'intérieur de la bannière. Les images défilent, le message commercial sera alors soit une suite de textes, soit une suite d'images, à la manière d'un dessin animé, qui lui donne un caractère audiovisuel attrayant.

L'évolution des langages de programmation et l'augmentation de la largeur de la bande passante, et donc de la vitesse de téléchargement ont aussi permis l'utilisation de techniques plus récentes.
D'abord les *applets javas*, petits programmes qui permettent d'insérer de façon non statique le bandeau dans la page web. Présenté sous un format minimal, le bandeau se déroule au passage de la souris, se superposant au texte –dont il empêche en général la lecture. Si l'on clique sur le lien qu'il contient, soit on arrivera sur une autre fenêtre, soit le site apparaîtra à l'intérieur même de la bannière. « *Le bandeau publicitaire devient ainsi un espace commercial à part entière, un mini site dans le site qui permet de mener l'internaute directement à l'achat* »[4]. Les *applets javas* sont aussi utilisés hors des bandeaux, c'est en effet la technique qui permet de faire apparaître d'attrayantes images animées qui traversent l'écran.

[3] Eric LABBÉ, Daniel POULIN, François JACQUOT et Jean-François BOURQUE, « Le guide juridique du commerçant électronique », Juris International, chap.7 p127, et disponible sur http://wwwjurisint.org./pub/05/fr/index.htm, visité le 17 septembre 2002 et voir aussi Didier GOBERT, « La publicité sur Internet – le droit en (r)évolution », loc.cit note 1, p4.
[4] Didier GOBERT, « La publicité sur Internet – le droit en (r)évolution », Id., p5.

Ensuite, les bandeaux peuvent être diffusés en *streaming* c'est à dire grâce à la lecture en transit. Technique désormais couramment utilisée pour diffuser de la musique (notamment en ce qu'elle évite les reproductions temporaires sur le disque dur, et donc permet un plus grand respect des droits d'auteurs), elle permet d'afficher une bannière sans la télécharger, donc de façon plus rapide, plus instantanée. Elle est également appréciée car ainsi la page web qui contient le bandeau est moins lourde, moins volumineuse, donc la publicité ne ralentit pas son affichage à l'écran. Enfin, la technologie *flash* est une technologie de compression qui « allège » le poids des bandeaux, donc qui permet d'y inclure plus de choses, comme du son, et de la vidéo, pour une durée de téléchargement égale.

Mais ce n'est pas tout. Dans la recherche des objectifs de rapidité, fluidité et interactivité, les publicitaires sont arrivés à dissocier le bandeau de la page où il apparaît, en utilisant un *AdServer*, qui est un serveur distinct de celui qui fournit le contenu de la page que l'on visite. Souvent même, c'est une autre compagnie, spécialisée dans la cyberpublicité qui exploite ce serveur, gérant les campagnes promotionnelles de différents annonceurs. Ceci explique pourquoi, quand on va plusieurs fois sur une page d'un site, même à quelques minutes d'intervalle, ce ne sont pas les même publicités qui s'affichent.

Nous effleurons ici déjà, la problématique principale de cette étude. En effet puisque les publicités ne sont plus solidaires de la page où elles apparaissent, il est alors possible de cibler le message en fonction de chaque internaute. Grâce à des techniques que nous verrons plus loin, les cyberpublicitaires savent non seulement quelles sont les publicités qui ont déjà été affichées pour chaque personne, ceci afin d'éviter les répétitions, mais en plus, disposant d'un profil de consommateur, ils peuvent orienter la sélection des publicités vers les centres d'intérêt spécifiques de l'internaute.

b) Le pourriel ou spamming

Le pourriel (amalgame très explicite de poubelle et de courriel), plus communément appelé *spamming* (qui tire son origine du Spam, une viande en boite de mauvaise qualité, ce qui est tout aussi suggestif) se définit comme « *l'envoi massif de courriers électroniques non sollicités* »[5].
Le pourriel est symptomatique du ciblage publicitaire. En effet si le message commercial est licite[6], et si aucune législation ne visant spécifiquement le pourriel n'ayant été adoptée au Canada, le pourriel présuppose la collecte des adresses Emails auxquelles il va être envoyé. Or une adresse Email est une donnée personnelle d'un internaute[7], et les modalités de sa collecte pourraient influencer sur la licéité de l'envoi du spam.

Le pourriel se présente sous la forme d'un message en format texte ou plus généralement en format HTML, plus coloré, imagé, donc plus attractif. Les internautes sont ainsi bombardés d'Emails qui, le plus fréquemment ont trait à des sites pornographiques, des propositions pour faire fortune, des voitures ou la possibilité d'acquérir un diplôme universitaire. Cependant la notion de pourriel est plus large que ces quelques exemples, puisqu'elle couvre aussi des envois que l'on peut considérer plus légitimes ou tout au moins, ayant un caractère moins déplaisant, comme les Emails publicitaires provenant de sites consultés régulièrement par l'internaute.

Le courrier électronique est un outil très avantageux pour les entreprises qui désirent faire de la publicité car il est peu coûteux, on peut sélectionner les récipiendaires en fonction d'un profil prédéterminé, et les messages peuvent contenir des liens hypertextes qui dirigeront les cyberconsommateurs intéressés sur le site annoncé.

---

[5] Thibault VERBIEST, « Publicité et Marketing sur Internet », 22 octobre 1999, p 3, Juriscom, disponible sur http://www.juriscom.ney/pro/1/ce19991022.htm, visité le 23 octobre 2002.
[6] Voir notamment Québec (Procureur général) c. Irwin Toys Ltd. [1989] 1 R.C.S. 927, où la Cour Supérieure explique que « *Nous ne pouvons donc écarter une activité humaine du champ de la garantie de la liberté d'expression en se basant sur le contenu ou la signification. En effet, si l'activité transmet ou tente de transmettre une signification, elle a un contenu expressif et relève à première vue du champs de la garantie* ».

Cependant, le pourriel est en général mal perçu par l'internaute qui consulte ses Emails, et qui désapprouve cette méthode intrusive. En effet, il peut être gênant d'ouvrir son courrier, avec quelqu'un dans son bureau pour recevoir un message vantant les mérites d'un site classé XXX. Le spam est aussi peu apprécié par les exploitants de service Internet, car il encombre les mémoires des serveurs et la bande passante, et leur cause des difficultés techniques[8].

c) Les messages interstitiels ou les pop-ups

Un pop-up est le message qui apparaît dans une autre fenêtre qui s'ouvre spontanément quand l'internaute passe d'une page web à une autre. Page web entièrement dédiée à un message commercial, elle peut prendre plusieurs formats, rectangulaire ou carrée, petite ou couvrant tout l'écran. De plus, il suffit souvent de rafraîchir la page que nous voulions consulter originellement pour revoir s'ouvrir d'autres pop-ups. Comme les bandeaux non solidaires de la page web qui les accueille, les pop-ups sont gérés par des entreprises de publicités spécialisées comme Gator, et Cibleclick par exemple, qui peuvent cibler leurs envois en fonction du profil du consommateur.

Les pop-up sont souvent considérés comme irritants à cause de leur prolifération rapidement incontrôlable, et parce qu'utilisant les ressources de l'ordinateur ce qui peut le ralentir ; ce qui s'additionne au fait que la fenêtre s'ouvre sur celle que l'on consulte, ce qui a pour conséquences de gêner la navigation de l'internaute. Pourtant, ils sont très à la mode auprès des publicitaires actuellement. Parmi les plus populaires on trouve notamment ceux qui font la promotion de casinos en ligne, de cartes de crédit, et ceux qui proposent de retrouver nos anciens camarades de classe.

Ces formes de publicité ont un avantage sur la promotion dans les médias traditionnels ; elles permettent de cibler le récipiendaire du message, c'est l'avènement du marketing one-to-one.

---

[7] Nous approfondirons ces notions au paragraphe A. 2 .

2. Le marketing *one-to-one* ou marketing direct

Comme nous venons de le voir, Internet offre des possibilités fabuleuses pour les publicitaires pour qui ciblage est synonyme de réduction des coûts et hausse de l'efficacité des campagnes. Enfin, le monde dont ils ont tant rêvé, sans pour autant oser imaginer qu'il existerait réellement un jour, ce monde est à leur portée ! Comme l'explique Bob Tedeschi « *the utopian vision of true "one-to-one marketing" as e-commerce companies like to put it, is predicated on gleaning as much information as possible about a customer and building a storefront tailored to that particular individual. After gathering personal data and tracking a shoppers movements within the site, Internet retailers can display products to suit that customer's tastes and price range, or list customized specials and sales* »[9].

Afin d'être à même de réaliser des opérations de marketing direct, c'est à dire diriger les publicités vers des personnes déterminées dont on a établit un profil détaillé et personnalisé, les entreprises doivent collecter des renseignements sur les internautes. Il s'agit de savoir tout (ou presque) ce qu'un *e-consummer* potentiel fait quand il navigue sur Internet : quels sites il visite, quelles recherches il fait et sur quels moteurs spécialisés, et éventuellement les services et produits qu'il achète, voire même ceux qui composent son ordinateur. Deux sortes d'informations sont ici visées : les données personnelles et les données non nominatives.

Les données non nominatives sont celles qui peuvent être collectées par exemple, lorsqu'un internaute visite un site, y rempli un petit questionnaire anodin ou répond à un sondage, puis va d'une page à une autre. Grâce à des moyens techniques, le logiciel gestionnaire du site est alors en mesure de dresser son portrait général, et en l'incluant

---

[8] Voir Eric LABBÉ, op.cit., note 3, p131.

[9] Bob TEDESCHI, « Targeter marketing confronts privacy concerns », New York Times, 1999/10/05, disponible sur http://www.nytimes.com/library/tech/99/05/cyber/commerce/10commerce.html, cité dans Ann BARTOW « Women as targets : the gender-based implications of online consumer profiling », », Comment to the Department of Commerce and Federal Trade Commission, (P994809, Docket N° 990811219-9219-01), 8 novembre 1999, disponible sur http://www.ftc.gov/bcp/profiling/comments/bartow.htm, visité le 21 octobre 2002 et voir aussi Thierry LEONARD, « E-marketing et protection des donnés à caractère personnel », p2, 23/05/2000, disponible sur http://www.droit-technologie.org/2_1.asp?dossier_id=22&motcle=e-marketing&mode=motamot, visité le 21 octobre 2002.

dans un profil global d'internautes qui partagent certains de ses goûts, il en déduira qu'il est probable qu'il apprécie ou non les mêmes choses, tel qu'il est indiqué dans le profil. La collecte de données non nominatives permet donc un premier ciblage, mais qui va s'avérer souvent bien insatisfaisant et imprécis. Il faut donc coupler ces informations avec des données nominatives, afin d'être en mesure de réaliser des opérations de marketing direct.

Les données personnelles sont définies dans la Loi sur la protection des renseignements personnels et des documents électroniques[10] comme « *tout renseignement concernant un individu identifiable, à l'exclusion du nom et du titre d'un employé d'une organisation et des adresses et numéro de téléphone de son lieu de travail* ». Les termes de la Loi sur la protection des renseignements personnels dans le secteur privé[11] sont plus larges[12], puisqu'ils ne, et peut-être un peu plus clairs : « *Est un renseignement personnel, tout renseignement qui concerne une personne physique et permet de l'identifier* ». En pratique un renseignement personnel peut être le nom, le prénom, l'âge, le numéro de téléphone, l'adresse de courriel, l'adresse IP, le numéro de carte de crédit d'un individu…, soit toute donnée dès qu'elle permet d'identifier une personne en particulier.

Les renseignements personnels sont à la base de toutes les techniques de marketing direct ou marketing one-to-one. Disposant d'un profil très précis sur chaque personne, qui se complète à chaque connexion, la publicité qui sera envoyée par les entreprises de publicité comme par les logiciels personnels aux sites visités sera potentiellement très proche des goûts, du pouvoir d'achat et des besoins de l'internaute et génèrera donc potentiellement plus de réponse, de réactions positives, de feedback, voire

[10] L.C. 2000, ch.5, appelée loi C-6, ou PIPEDA, ci après « Loi fédérale ». Cette loi a été très inspirée par les recommandations de l'OCDE du 23 septembre 1980, signées par le Canada en 1984.
[11] L.R.Q., Ch. P-39, article 2, entrée en vigueur le 1er janvier 1994, ci-après « Loi québécoise ».
[12] En effet, ne comprenant pas les exceptions relatives au lieu de travail et aux membres d'une organisation de la Loi fédérale, le texte québécois ne fait pas de distinction quant à la protection de la vie privée pendant les activités reliées à l'emploi et celles qui ont lieu dans l'intimité du domicile. Pourtant la Cour Suprême a fait cette distinction en 1988 dans l'arrêt R. v. Dyment [1988] 2 S.C.R. 417.

éventuellement d'achats[13]. Les bénéfices de telles opérations de marketing ne sont pas spécifiques aux annonceurs. Les consommateurs ne sont pas forcément contre une certaine personnalisation si cela leur facilite la navigation et les recherches en ligne[14]. Comme il est agréable lors d'opérations commerciales traditionnelles que le vendeur se souvienne de nos goûts, la gestion informatisée de nos habitudes de consommation personnalise les sites fréquentés, les individualise, nous en fait des lieux familiers et nous apprécions les raccourcis et autres facilités d'utilisations qui sont à notre disposition. Le marketing one-to-one cherche donc à recréer les relations client-vendeur qui étaient inexistantes jusque là dans le monde virtuel[15].

[13] R. KONRAD rapporte dans « Your PC's enemy within : spyware, adware constroversies show why Net needs new laws », news.com, 26 juin 2002, disponible sur http://news.com.com/2009-1023-937457.html, visité le 21 octobre 2002, que lors d'une campagne, Gator a ciblé les personnes qui remplissait les trois critères suivants : des mères, qui étaient conscientes de faire attention à leur beauté et qui avaient de l'influence. Les résultats de la campagne en termes de click sur les publicités ont été de 24%, ce qui est énorme comparé au 0,2% habituel pour les pop-ups en général et le petit 0,01% pour les bannières. L'efficacité du ciblage est donc irréfutable. Par contre, « *it's impossible to say whether the better rates translate into higher sales* » (id., p4), ce qui est assez logique, car on peut penser que si le consommateur achète en ligne, il n'achètera pas chez son détaillant habituel, et de plus, il peut aussi consulter le produit en ligne et aller l'acheter dans une boutique traditionnelle. Des chiffres sur l'éfficacité des publicités en lignes seraient donc très difficiles à établir.

[14] M. PASTORE, « Web users will share information for better service », Cyberatlas, 5 avril 2000, disponible sur http://cyberatlas.Internet.com/markets/advertising/article/0,1323,5941_335011,00.html, visité le 22 octobre 2002.

[15] Voir notamment E. BARCHECHAT, « Une lecture critique du one-to-one », Commerce électronique, Marketing et Libertés, Cahier Laser n°2, Paris, Ed. 00h00, p89 à 104, cité dans Thierry LÉONARD ; « E-Marketing et protection des données à caractère personnel », Droit & Nouvelles Technologies, 23 mai 2000, disponible sur http://www.droit-technologie.org/2_1.asp?dossier_id=22&motcle=e-marketing&mode=motamot, visité le 21 octobre 2002.

B. Les procédés de collecte des données :

Mais comment toutes ces informations sont-elles collectées ? Il nous faut distinguer deux situations : celle où l'internaute donne volontairement de l'information, et celle ou les données sont collectées à son insu.

1. La divulgation volontaire d'informations

Elle a lieu a de multiples occasions au cours des activités sur Internet, il suffit pour cela de s'inscrire à un concours ou à un jeu, de s'abonner à une newsletter, de s'identifier à l'entrée d'un site a l'aide d'un mot de passe créé préalablement ou non, de participer à des groupes de discussions, plus communément appelés *chats*, ou de répondre à un de ces multiples questionnaires en ligne[16].

A notre humble avis, et faute d'un sondage venant confirmer nos dires, la majorité des internautes, en faisant toutes ces opérations désormais banales, n'a pas conscience de donner des informations précieuses pour les publicitaires, tout comme les utilisateurs des cartes de points des grands magasins ne voient dans cette habitude qu'un moyen pour obtenir des cadeaux gratuits. Les commerçants ne sont pas des philanthropes par définition, les cadeaux ne sont là que pour nous inciter à leur permettre d'enregistrer nos habitudes de communication.

Considérant que toutes ces informations transmises par nos soins sur Internet peuvent non seulement servir pour des procédés de marketing direct pour les sites que nous consultons mais aussi être vendues et servir à des compagnies dont nous ne connaissons pas l'existence et qui sont potentiellement émettrices de pourriel ou

[16] Des séminaires sont aujourd'hui organisés pour apprendre aux gestionnaires de site à récolter un maximum d'informations sur les personnes qui viennent visiter leur site, voir notamment, « Transformer le trafic en chiffres d'affaires : jeux-concours, référencement, marketing viral », séminaire du 3 décembre 2002, proposé par le

gestionnaires de serveurs de pop-ups, nous ne saurions que recommander prudence et parcimonie dans le processus d'éssaiminage des données nous concernant. Nous disposons d'un contrôle a priori qu'il serait peut-être judicieux d'exercer surtout si l'on considère les techniques existantes pour collecter des informations à notre insu et bien souvent, sans que l'on puisse s'en rendre compte.

2. La collecte non transparente de données

Si aux débuts d'Internet, l'anonymat était la règle, avec « *nobody knows you're a dog* »[17] pour credo, les technologies ont bien évolué, et nombreuses sont celles qui permettent la collecte des données sournoisement, c'est à dire sans le consentement des internautes, sans même qu'ils en soient avertis.

a. Les données issues de l'utilisation des protocoles de communication

D'après une étude menée par Jean-Marc Dinant[18], informaticien au plus grand centre de recherches en informatique et en droit : le CRID de Namur, le protocole TCP/IP qui est à la base des communications sur Internet serait à l'origine de fuites potentielles d'information. Prenant l'exemple de la circulation des Emails, il démontre que leur circulation se fait sans considération des frontières ou de la distance ; un courrier envoyé de Namur vers Bruxelles sera passé successivement par la Suisse, la France, la Suède et la Finlande, et son acheminement aura donc été assuré en partie par des opérateurs étrangers (entreprises commerciales, devons nous le rappeler ?) qui sont en mesure de les enregistrer et ainsi de composer des bases de données comprenant les adresses IP, les adresses Email, les noms en clair de l'expéditeur et bien souvent du

---

Benchmark Institut, disponible sur http://www.benchmark.fr/ebn.asp?pid=106&seminaire=6870&id_fils=8, visité le 24 novembre 2002.

[17] Cette célèbre expression est tirée d'une caricature de Peter Steiner publiée dans le New –Yorker, du 5 juillet 1993, Vol.69 (LXIX) no. 20 en page 61, disponible sur http://www.unc.edu/courses/jomc050/idog.html, visité le 24 novembre 2002.

[18] Jean-Marc DINANT : « Les traitements invisibles sur Internet », présenté lors d'une conférence à l'Institut Universitaire International à Luxembourg, juillet 1998, disponible sur http://www.droit.fundp.ac.be/crid/eclip/Luxembourg.html, visité le 8 octobre 2002.

destinataire. Le tableau est alarmiste, cependant rien n'indique que tous notre courrier électronique est ainsi enregistré. Pourtant, rien n'indique le contraire.

M. Dinant, dans son étude exhaustive, explique aussi qu'il existe des programmes que le gestionnaire d'un site peut utiliser pour savoir si un utilisateur est connecté sur son serveur, il s'agit en l'espèce de la commande Ping suivie de l'adresse IP sur laquelle on cherche des renseignements.

Pour résumer, le protocole de navigation ainsi que les langages de programmation supposent une discussion incessante entre l'ordinateur de l'internaute et différents et multiples serveurs. La plus grande partie de ces communications n'est pas visible à l'internaute et peut donner lieu à une collecte d'information par des tiers. Cependant, cet échange de données est inhérent au bon fonctionnement de l'Internet, contrairement à celui que nous allons présenter maintenant.

b. Les données issues de l'utilisation normale des potentialités d'Internet

Principalement, les informations sont recueillies dans deux hypothèses ; lors de la navigation sur Internet et lors de l'installation et utilisation de logiciels.

Lors de ses excursions sur le web, l'internaute fait immanquablement une bonne récolte de divers petits programmes dont il ne connaît pas à priori la présence sur son ordinateur : les cookies, les spywares et autres fichiers *.gif*,. La littérature sur ces sujets est très abondante, nous nous contenterons donc de les présenter brièvement[19].

[19] Pour des explications sur les cookies et spywares, lire notamment J.-M. DINANt, « Les traitements invisibles sur Internet », id., note 18 , et Stephanie OLSEN « Is your E-mail watching you ? », CNET.com, 4 avril 2002, disponible sur http://news.com.com/2100-1023-875992.html, visité le 21 octobre 2002, CEXX.org : « Advertising spyware : News Upd.exe », disponible sur http://www.cexx.org/newsupd.htm, et « Adware, spyware and other unwanted « malware » - and how to remove them, disponible sur http://www.cexx.org/adware.htm, et « The trouble with spyware & advertising-supported software », disponible sur http://www.cexx.org/problem.htm, visités le 26 octobre 2002, PEST PATROL : « Beyond viruses », disponible sur http://www.pestpatrol.com/Whitepapers/BeyondViruses0302.asp, visité le 26 octobre 2002, Evan HANSEN, John BORLAND et Rachel KONRAD « Your PC's enemy within » 26 juin 2002, disponible sur http://news.com.com/2009-1023-937457.html, visité le 21 octobre 2002., Commissaire à l'information et à la protection de la vie privée / Ontario : « La vie privée sur Internet : soyez sur vos gardes », août 2001, disponible sur http://ipc.on.ca/francais/pubpres/papers/primer-f.pdf, visité le 26 octobre 2002, Major R. Ken PIPPIN, « Consumer

Les cookies et les spywares sont des fichiers installés sur les disques durs qui enregistrent les visites de l'internaute. Ils y sont déposés lors du premier passage sur un site et permettent de savoir si une personne est déjà venue, et ce qu'elle y a fait. La différence entre les cookies et les spywares réside dans le fait que le premier ne va servir qu'à connaître les activités sur un site ce particulier, alors que le spyware va avoir un champ d'investigations beaucoup plus vaste, s'intéressant à tous ce qui est fait par l'internaute, même sur des sites différents. Un cookie va aussi servir aux publicitaires pour savoir quelles ont été les publicités qui ont été envoyées à un ordinateur, et ainsi permettre une rotation, une diversification du contenu des pop-ups et des bannières.

Si au départ le cookie était le moyen pour permettre au commerce électronique d'exister, c'est à dire grâce auquel le site identifiait un client et son « panier » avec ses achats, on peut considérer le spyware comme sa dérive à but publicitaire.

Un spyware, que l'on appelle parfois fichier *.gif*, va non seulement enregistrer les noms des sites visités par l'internaute, mais aussi ses achats, les fichiers qui ont été téléchargés, le type d'explorateur Internet utilisé et même parfois l'adresse Email.

Même la boite à lettres électronique n'est pas à l'abri[20] ; lors de la réception de pourriel, si le malheureux « spammé » clique sur le lien hypertexte, que ne manque jamais de contenir le message, alors un cookie, voire un spyware, sera déposé sur son disque dur, permettant ainsi à l'émetteur de contrôler si son mail a été lu.

Quelques exemples précis démontreront que ces propos ne sont pas inutilement alarmistes. Certaines publicités pour les casinos en ligne (des pop-ups au spam) sont gérées à l'aide de cookies appelés PAgent, Vegas Palm Casino, KFH, Media Loads, et

---

privacy on the Internet : it's surfer beware », 47 A.F.L. Rev. 125, Garry M. SCHOBER, Ann BARTOW, Chris HOOFNAGLE, Phyllis BORZI, « Colloquium on privacy & security », transcription, 50 Buff. L. Rev. 703, printemps / été 2002, et André POST « The dangers of spyware », Symantec, disponible sur http://securityresponse.symantec.com/avcenter/reference/danger.of.spyware.pdf, visité le 15 octobre 2002.

[20] Voir notamment Stephanie OLSEN, « Is your E-mail watching you ? », id., note19.

WinEME, quant à openme.exe, il génère une avalanche de publicité pornographique sous toutes ses formes, après seulement vingt minutes d'installations !

Mais les intrusions dans l'intimité des ordinateurs des internautes ne se limitent pas à ces situations. Il faut avoir conscience que souvent, lorsqu'on télécharge un logiciel gratuit sur Internet, ce dernier contient un spyware. Les exemples sont légion ; le jeu « Yo Mamma, Osama », créé par TwistedHumor.com, installe secrètement le cookie WNAD.EXE, qui transmet de l'information personnelle et génère des pop-ups, et s'il prend l'envie à l'internaute d'utiliser Kazaa, le logiciel de Peer-to-peer installera aussi Cydoor, dlder.exe et bdeviewer.exe, trois spywares qui se chargerons d'encombrer son ordinateur de multiples publicités.

Ce n'est hélas pas tout, un ordinateur, même s'il n'a jamais été connecté à Internet peut contenir un spyware ! Les cartes–son vendues par Créative Labs contiennent le fichier newsupd.exe qui connecte l'ordinateur à Internet et envoie de l'information[21].

Toutes ces applications génèrent un énorme flux de données personnelles[22] exploitable par les entreprises dans des buts publicitaires. Cet exposé un peu technique, aux saveurs alarmistes (ou tout au moins alarmées) avait pour but de présenter la situation factuelle, telle que tout internaute la vit au quotidien. L'impression générale est celle d'une anarchie : invasion de l'Internet par les publicités, et collecte sauvage d'informations. Pourtant des règles législatives encadrent cette activité.

---

[21] Voir CNET News.com Staff, « Creative Labs accused of spying », 13 juin 2001, disponible sur http://news.com.com/2100-1040-268361.html?legacy=cnet, visité le 26 octobre 2002.

[22] D'après le rapport de la Federal Trade Commission « Privacy online : a report to congress », juin 1998, disponible sur http://www.ftc.gov/reports/privacy3/exeintro.htm, visité le 22 octobre 2002, **92%** des sites web collectent des données personnelles et d'après M. J. CULNAN « Georgetown Internet Privacy policy Survey : Report to the Federal Trade Commission », disponible sur http://www.msb.edu/faculty/culnanm/gippshome.html, **93%** des sites collectent de l'information personnelle. Ces statistiques ont été citées dans C. F. CARLTON, « The right to privacy in Internet commerce : a call for new federal guidelines and the creation of an independant privacy commission », 16 Saint John's Journal of Legal Commentary 393, printemps/été 2002, p17.

2. Les dispositions législatives qui encadrent la collecte de données personnelles au Québec

Avant de présenter les règles qui protègent les renseignements personnels au Québec, donc auxquelles les entreprises québécoises sont soumises, il n'est pas inutile de rappeler qu'Internet, médium international, ne reconnaît pas les frontières. Ce que signifie en pratique cette remarque désormais banale, c'est que même si toutes les entreprises ayant leur siège social au Québec respectaient les législations à la lettre, les données personnelles des internautes de la belle province seraient quand même menacées, ou tout au moins collectées sans égard aux dispositions de la Loi sur la protection des renseignements personnels dans le secteur privé. En effet, l'internaute ne surfe pas que sur des sites québécois voire canadiens ! Une grande proportion du contenu disponible sur Internet provient de l'Europe et surtout des États-Unis. La loi qui s'applique à leur contenu est d'abord celle du lieu de leur siège social[23], et ce même en matière de publicité et de protection des renseignements personnels. Or c'est une lapalissade que de dire que les lois nationales diffèrent ! La solution serait d'envisager un consensus mondial, mais l'adoption d'une convention internationale sur un sujet aussi sensible que la vie privée est à notre avis, aussi utopique que la paix dans le monde.

En effet, la vie privée est une notion intimement liée à la culture de chaque pays, et est traduite en conséquence non seulement dans les habitudes et les attentes des citoyens, mais aussi dans les droits nationaux. Par exemple, dans les pays de culture anglo-saxonne comme la Grande-Bretagne et les États-Unis, la majorité des maisons n'ont pas de volets extérieurs aux fenêtres mais des rideaux, elles ne sont pas non plus, en général, entourées de murs de pierres et la protection de la vie privée est assurée par

[23] Dans certaines situations, et en application de critères établis par le droit international privé et la jurisprudence, un site peut se voir imposer le respect de dispositions d'un droit étranger, mais en règle générale, un site doit respecter le droit du pays où est son siège social voire ses serveurs; c'est pour cette raison que souvent des entreprises vont aller s'installer dans des pays comme les Barbades pour y installer des sites au contenu prohibé. Pour une présentation des critères en matière de compétence des tribunaux étrangers et de droit applicable, voir Michael GEIST, « Is there a there there ? Towards greater certainty for Internet jurisdiction », disponible sur http://aix1.uottawa.ca/%7Egeist/geistjurisdiction-us.pdf, visité le 14 novembre 2002.

les textes d'une manière sectorielle, afin de protéger les plus faibles, notamment les enfants. Ainsi alors que l'Europe considère le droit à la vie privée comme un droit de l'homme fondamental, consacré dans les textes législatifs nationaux[24] comme communautaires[25], les États-Unis préfèrent l'apprécier comme *« a commodity that can and should be controlled through the free market approach* »[26], un droit économique autorégulé par le marché. Les positions sont donc on ne peut plus opposées. Quant au Québec, on y trouve une situation particulière pour un pays d'Amérique du Nord où l'influence des États-Unis est généralement palpable. En effet, le droit à la vie privée est consacré dans le Code Civil du Québec[27], à l'article 35 dans ces termes : « *Toute personne a droit au respect de sa réputation et de sa vie privée. Nulle atteinte ne peut être portée à la vie privée d'une personne sans que celle-ci ou ses héritiers y consentent ou sans que la loi l'autorise* ». Cet article faisait écho à un texte plus ancien ; la Charte des droits et libertés de la personne[28] de 1975 qui dans son article 5 garantissait que « *Toute personne a droit au respect de sa vie privée* ». On sent ici l'influence européenne, voire française dans le droit québécois.

Cependant, comprendre ce qui motive l'existence ou l'absence de législation spécifique ne change rien aux problèmes soulevés par la disparité des régimes juridiques. Pourtant des tentatives d'harmonisation ont été faites dans ce sens avec les principes de l'OCDE[29], une résolution des Nations Unies[30] et avec la Directive

---

[24] Voir Cynthia CHASSIGNEUX, « La protection des données personnelles en France », Lex Electronica, vol.6, n°2, hiver 2001, disponible sur http://www.lex-electronica.org/articles/v6-2/chassigneux.htm, visité le 22 septembre 2002.

[25] Voir la Convention de sauvegarde des droits de l'homme et des libertés fondamentales, signée à Rome, 4.XI.1950, disponible sur http://conventions.coe.int/treaty/fr/Treaties/Html/005.htm, visité le 22 novembre 2002.
et par exemple la directive 2002/58/CE du Parlement européen et du Conseil du 12 juillet 2002 concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques), JOCE, 31 juillet 2002, L 201/37.

[26] L. C. KRAMER, « Private eyes are watching you : consumer online privacy protection – lessons from home and abroad », 37 Texas International Law Journal 387, printemps 2002, p2.

[27] L.Q. 1991, c. 64

[28] L.R.Q. C-12, disponible notamment sur http://www.canlii.org/qc/loi/c12/tout.html, visité le 30 octobre 2002.

[29] Adoptés par le Conseil, le 23 septembre 1980, les principes sont : une collecte limitée avec le consentement de la personne, le principe de la qualité des renseignements qui vise notamment leur véracité, l'utilisation spécifique, le principe d'une utilisation limitée (quant à sa communication à des tiers notamment), le principe de sécurité, le droit d'accès, le principe selon lequel les entreprises doivent établir des politiques de vie privée, et enfin, celui selon lequel une personne doit être désignée responsable dans l'entreprise du devenir des données.
Les principes, non contraignants et très proches de ceux de la législation fédérale, sont disponibles sur http://www.cpsr.org/cpsr/privacy/privacy_international/international_laws/1980_oecd_privacy_guidelines.txt, visité

européenne concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques[31] qui a été ratifiée par plusieurs pays ne faisant pas partie de l'Union Européenne, comme le Canada. Les États-Unis, menacés de se voir exclus du marché européen ont demandé une l'attribution d'un régime dérogatoire, ce qui a donné lieu aux accords du Safe Harbour, dont l'application est surveillée par le FTC. Beaucoup serait à écrire à ce sujet, mais ce n'est pas l'objectif de cette étude que nous voulons centrée sur la situation québécoise. Pourtant, en examinant les dispositions qui gèrent la collecte des renseignements personnels au Québec, nous devrons garder à l'esprit la situation internationale, qui rend tout système national protecteur des données récoltées sur ses citoyens insatisfaisant.

Deux textes législatifs existent au Québec ; d'abord la Loi sur la protection des renseignements personnels et les documents électroniques, de stature fédérale, communément appelée projet de loi C-6 ou, PIPEDA et la Loi sur la protection des renseignements personnels dans le secteur privé qui régit les données permettant l'identification des personnes depuis 1992 au Québec.
La première partie de la loi fédérale traite de la protection des renseignements personnels. Cette loi entrera en vigueur à compter du premier janvier 2004 pour toutes les entreprises qui collectent, ou utilisent des renseignements personnels dans le cadre d'activités commerciales[32].

Nous avons déjà comparé leurs définitions de la notion de données personnelles, nous pouvons nous attacher maintenant plus en détail à leur contenu. Les dispositions que

---

le 23 novembre 2002. Une version plus récente a été publiée en l'an 2000, intitulée : « Principes directeurs pour les multinationales », disponibles sur http://www.oecd.org/FR/about/0,,FR-about-93-3-no-no-no-0,00.html, visité le 23 novembre 2002.

[30] Résolution 45/95 du 14 décembre 1990, adoptant les principes directeurs pour la réglementation des fichiers informatisés contenant des données à caractère personnel, disponible sur http://www.unhchr.ch/french/html/menu3/b/71_fr.htm, visité le 23 novembre 2002.

[31] Directive 95/46/CE, publiée au Journal officiel L 281 du 23.11.1995, p31.

[32] Article 72 de la Loi fédérale. Il faut aussi noter que la première partie de la Loi est en vigueur depuis le 1er janvier 2001 et s'applique à toute organisation gouvernementale et à toute entreprise qui génèrent des flux trans-provinciaux de données personnelles. Enfin, pour les organisations qui gèrent des renseignements personnels relatifs à la santé, elle s'applique depuis le 1er janvier 2002.

ces lois contiennent sont de deux ordres. On trouve d'abord celles relatives au consentement (A.) et celles relatives au traitement des données (B).

A. Le consentement

Le consentement de la personne quant à la collecte des données personnelles est un élément fondamental commun aux deux textes. Il est rendu obligatoire par les deux lois.

1. Le consentement dans la Loi fédérale

La Loi fédérale intègre par son article 5 (1), les principes énoncés dans la norme nationale du Canada intitulée Annexe 1, *Code type sur la protection des renseignements personnels*[33]*,* dont l'article 4 . 3 dispose que « *toute personne doit être informée de toute collecte, utilisation ou communication de renseignements personnels qui la concernent et y consentir à moins qu'il ne soit pas approprié de le faire*» et l'article 4 . 3.1 précise qu'« *il faut obtenir le consentement de la personne concernée avant de recueillir des renseignements personnels à son sujet et d'utiliser ou de communiquer les renseignements recueillis* » . La Loi québécoise lui fait écho par son article 14 qui est rédigé en ces termes : « *le consentement à la communication ou à l'utilisation d'un renseignement personnel doit être manifeste, libre, éclairé et être donné à des fins spécifiques* ».

D'après ces dispositions, il est plutôt clair que les entreprises publicitaires devront obtenir le consentement des internautes afin de collecter des données les concernant. Il existe tout un débat en Europe notamment où l'on se demande si le consentement doit avoir lieu avant la collecte des données ou après, c'est à dire avant son utilisation, il s'agit de savoir si l'on va privilégier un système d'*opt-in* ou d'*opt-out*. La question est d'importance car le premier est nettement plus protecteur de la vie privée des internautes que le second. Il signifierait que les entreprises devraient demander

l'autorisation des internautes avant d'implanter un spyware sur leur disque dur, ce qui aurait sans doute pour conséquence de réduire énormément le volume de logiciels espions implantés et consécutivement le volume d'informations collectées. Pratiquement, l'internaute pourrait refuser de profiter des techniques de marketing direct, puisque moins d'information le concernant serait détenue par les publicitaires. De plus, il ne faudrait pas que les sites web conditionnent l'accès à leur site à la fourniture de renseignements dont la collecte ne serait pas légitime, car cela fausserait le choix, la volonté de l'internaute. Le système de l'opt-out serait plus favorable aux entreprises qui pourraient collecter les données personnelles et s'en servir jusqu'à ce que l'individu concerné leur fasse savoir qu'il ne désire plus que les informations le concernant continuent d'être encore utilisées. Cela signifie aussi que même dans cette optique, les entreprises auraient des obligations ; notamment celle de mettre à la disposition des internautes un moyen pour leur faire parvenir leur avis de rétractation.

La solution envisagée par le Canada peut paraître claire au premier abord, mais certaines dispositions de la loi fédérale se contredisent. L'article 4 .3.1 de l'Annexe 1 dispose bien qu' «*il* ***faut*** *obtenir le consentement de la personne concernée* ***avant de recueillir des renseignements personnels*** *à son sujet* », et semble consacrer un système d'opt-in dans le droit canadien, mais avec des exceptions prévues aux articles 7 (1), 7 (2) et 7 (3) de la Loi qui précisent que dans certaines hypothèses l'entreprise n'a pas à obtenir de consentement. Il s'agit notamment des situations où la collecte est faite à des fins statistiques, journalistiques, ou pour transmission ultérieure à des services de police ou de justice ou pour répondre à une situation d'urgence mettant en danger la vie d'un individu. L'article 7 (1) b) envisage l'hypothèse où l'individu qui aurait connaissance de la collecte fausserait l'exactitude des données transmises, et permet donc aux entreprises de ne pas demander de consentement pour cette situation précise. Une autre exception est celle de l'article 7 (1) a) qui stipule que lorsque « *la collecte du renseignement est manifestement dans l'intérêt de l'intéressé et* [que] *le consentement ne peut être obtenu auprès ce celui-ci en temps opportun* » l'entreprise peut recueillir des renseignements personnels sans le consentement de l'individu. Les situations où

[33] CAN/CSA-Q830-96

une telle exception pourrait jouer ne sont pas très claires, car avec la rapidité des moyens de communications fournis par Internet, diminue les hypothèses ou un consentement ne pourrait être obtenu en « *temps opportun* » ; par exemple, une fenêtre pop-up, dont on connaît la rapidité d'apparition, pourrait servir pour recueillir le consentement, et peut-être ainsi donner quelques lettres de noblesses à une application souvent décriée.

Mais la situation n'est pas si simple, en effet, après avoir posé le principe de l'opt-in à l'article 4. 3.1, l'Annexe 1 de la Loi fédérale décrit les formes du consentement à l'article 4. 3.7.
Si le premier alinéa reflète bien une situation d'opt-in, l'alinéa b) lui, propose une forme de consentement qui s'apparente à l'opt-out, où l'internaute est présumé consentir s'il ne coche pas une case. La prise de position fédérale n'est donc pas très claire.

Pour finir, l'article 5 (2) de la Loi fédérale stipule que « *l'emploi du conditionnel dans l'annexe 1 indique qu'il s'agit d'une recommandation et non d'une obligation* », donc certaines dispositions de ladite annexe n'ont pas force obligatoire. Nous pouvons donc en conclure que cette loi nous conseille éventuellement un système d'opt-in comprenant des exceptions, mais qu'un système d'opt-out serait tout aussi possible.

2. Le consentement dans la Loi québécoise

Qu'en est-il de la Loi québécoise ? La Loi sur la protection des renseignements personnels dans le secteur privé vient préciser les modalités d'application des articles du Code civil du Québec en matière de protection des renseignements personnels[34]. Ces dispositions exigent, elles aussi, le consentement de la personne dont les renseignements sont collectés dans des termes clairs ; « *L'utilisation des renseignements contenus dans un dossier n'est permise, une fois l'objet du dossier accompli, qu'avec le consentement de la personne concernée* »[35] et « *elle ne peut, sans*

[34] Voir article 1 de la Loi Québécoise.
[35] Article 12 de la Loi Québécoise

le consentement de l'intéressé […], *les communiquer à des tiers ou les utiliser à des fins incompatibles avec celles de sa constitution* ».

Cependant, et la différence est fondamentale, il faut noter que la loi parle de l'*utilisation* des renseignements, et non pas de la collecte, donc nous pouvons en déduire que le droit québécois protège les données personnelles postérieurement à leur compilation. Le consentement étant exigé spécifiquement pour leur utilisation, il semblerait qu'il ne soit pas nécessaire lors du processus de collecte. Il semble donc clair que la Loi québécoise introduise un système d'opt-out, c'est à dire que les entreprises québécoises peuvent recueillir les renseignements nominatifs des internautes sans les en informer au préalable, et n'ont qu'à obtenir leur consentement au moment où ils voudront les utiliser.

Au moment de la collecte des renseignements, les entreprises n'ont qu'une obligation d'information, selon les dispositions de l'article 8. Cette information doit préciser cinq éléments : l'objet du dossier qu'elle constitue, l'utilisation qui sera faite des renseignements, les personnes qui y auront accès, l'endroit où il sera stocké et les droits d'accès et de rectification de la personne sur laquelle l'entreprise établit un dossier[36]. Cette obligation d'information vient encadrer le système d'opt-out, en permettant à l'internaute de savoir que des informations le concernant sont glanées en vue de constituer une base de données. En pratique, dans l'optique qui nous intéresse, cela signifierait que les entreprises québécoises doivent prévenir les personnes qui viennent surfer sur leurs sites que des renseignements personnels les concernant sont compilés, et les informer des cinq éléments que nous venons d'énumérer. Cela ne signifie pas qu'elles doivent préciser aux internautes par quels moyens elles réalisent cette collecte, donc les prévenir qu'elles utilisent des cookies.

Un autre article vient encadrer la collecte. L'article 5 précise que « *la personne qui recueille des renseignements personnels afin de constituer un dossier sur autrui ou d'y consigner de tels renseignements ne doit recueillir que les renseignements nécessaires*

[36] Nous reparlerons de ce point plus en détails dans le chapitre B.

à l'objet du dossier ». A priori cette disposition pourrait limiter le volume d'informations collectées, cependant, quand on parle de marketing direct, tout comportement de l'internaute est susceptible d'intéresser les entreprises afin de permettre un meilleur ciblage. Il faudra donc attendre que la jurisprudence se prononce sur la question afin de définir quels sont les « *renseignements nécessaires à l'objet* » du marketing direct. De plus, le deuxième alinéa de cet article 5 précise que *« ces renseignements doivent être recueillis par des moyens licites* ». Similairement, il faudra que la jurisprudence se prononce sur ce point afin de déterminer quels sont les « *moyens licites* », c'est à dire, par exemple, si les spywares en font partie.

La Loi québécoise, dont la définition des données personnelles était plus large que celle de la Loi fédérale et qui donc pouvait laisser présumer une protection plus grande de ces renseignements, se révèle à la lecture de ses dispositions, plutôt favorable aux entreprises dans le sens où les obligations qu'elle fait peser sur leurs épaules sont relativement légères quant à la collecte des renseignements personnels et introduisent un régime d'opt-out dans le droit québécois. Cette légèreté est d'autant plus manifeste qu'il existe une exception à l'obligation d'obtenir un consentement préalable à l'utilisation des renseignements collectés. Il s'agit d'une hypothèse très particulière, que l'on trouve à l'article 23 de la loi qui précise qu' « *une personne qui exploite une entreprise peut, sans le consentement des personnes concernées, utiliser, à des fins de prospection commerciale ou philanthropique, une liste nominative*[37] *de ses clients, de ses membres ou de ses employés* ». Ce qui veut dire lorsqu'un internaute achète sur un site web, ou s'inscrit à une newsletter et devient ainsi un membre de la communauté de ce site, et que pour ce faire, il donne son nom, son adresse et son numéro de téléphone, ledit site marchand a le droit de constituer une base de données avec ces éléments spécifiques, qui sont, notons-le, plus restreints que ceux qui peuvent être contenus dans un dossier, et d'utiliser ces informations sans avoir à demander de consentement préalable. Cette disposition visait certainement à l'époque de l'entrée en

[37] Une liste nominative est définie à l'article 22 de la Loi fédérale comme « *une liste de noms, adresses ou numéros de téléphone de personnes physiques* ». Cette définition ne le précise pas, mais une adresse Email pourrait, à notre avis être couverte par la portée de cet article, ce que l'on peut notamment déduire de l'utilisation du pluriel au mot *adresses*.

vigueur de la loi, en 1993, les activités de publicités traditionnelles que peuvent faire les commerçants, comme envoyer à domicile les catalogues présentant leur collection. Transposée à l'ère numérique, elle autorise les sites marchands, qui ne sont bien souvent que des représentations en ligne d'entreprises existant dans le monde réel, à collecter des données nominatives qui pourront éventuellement servir à envoyer de la publicité par voie de poste et par voie d'Émail. L'étendue d'une telle collecte sera nettement plus grande que celle qui était traditionnellement visée, cela n'en fait pas automatiquement une disposition mal adaptée qu'il faudrait changer. Cependant, il est bon demander si cette disposition ne légitimerait pas l'envoi de pourriel à la condition de respecter le second alinéa de l'article 23 qui précise que même dans cette situation, l'utilisateur de la liste « *doit accorder aux personnes concernées une occasion valable de refuser que des renseignements personnels soient utilisés à de telles fins* ». Ainsi, si comme nous le soupçonnons cet article encadre l'envoi de pourriel, il nous faut déduire de ce dernier alinéa que le message contenu dans le spam devrait aussi inclure, par exemple un lien qui mènerait l'internaute vers une page où il pourrait se retirer de la liste nominative.

Nous venons de passer en revue les dispositions relatives au consentement, et nous avons pu constater que les deux lois organisaient un régime différent en la matière. Elles contiennent aussi des dispositions relatives au traitement des données, qu'il nous faut maintenant aborder.

B. Le traitement des données

Par « traitement des données », nous voulons aborder l'utilisation des renseignements personnels, la confidentialité et le droit d'accès. Les deux textes y font référence.

1. L'utilisation des renseignements personnels

S'agissant d'abord de l'utilisation des renseignements personnels, le principe est celui de la spécificité. L'article 14 de la Loi québécoise précise en effet que « *le consentement à la communication ou à l'utilisation d'un renseignement personnel doit être manifeste, libre, éclairé et être donné à des fins spécifiques. Ce consentement ne vaut que pour la durée nécessaire à la réalisation des fins pour lesquelles il a été demandé* ». De même, l'article 4.5 de l'Annexe 1 contient des dispositions similaires, exprimés dans des termes peu différents : « *les renseignements personnels ne doivent pas être utilisés ou communiqués à des fins autres que celles auxquelles ils ont été recueillis à moins que la personne concernée n'y consente ou que la loi ne l'exige. On ne doit conserver les renseignements personnels qu'aussi longtemps que nécessaire pour les réalisations déterminées* ». Plusieurs points sont importants dans ces articles.

D'abord le principe de la spécificité. Qu'il s'agisse d'un système d'opt-in ou d'opt-out, donc que l'on parle de la Loi fédérale comme de la Loi québécoise, l'utilisation des renseignements personnels doit être conforme à ce que les entreprises ont déclaré lors de la collecte. En pratique cela signifie que les entreprises doivent se munir d'une politique de vie privée[38] qui décrit leurs pratiques, que cette politique doit être visible et facilement accessible sur le site afin que les internautes puissent en prendre connaissance. Cela veut aussi dire que ces entreprises doivent se conformer à leur politique, et ne pas utiliser les renseignements personnels pour des finalités qu'elles auraient omis de préciser, de peur de rebuter les internautes. Les politiques de vie privée des entreprises canadiennes disponibles actuellement sur les sites Internet sont généralement rédigées dans des termes assez clairs. Elles commencent généralement par une introduction où l'entreprise assure aux internautes qu'elle est consciente de l'importance de la vie privée[39], puis elles précisent quelles informations sont collectées,

[38] La Loi fédérale dans l'article 4.1.4 d) de l'Annexe 1 précise que « *les organisations doivent assurer la mise en œuvre des politiques et des pratiques destinées à donner suite aux principes, y compris* : […] *la rédaction des documents explicatifs concernant leur politiques et leurs procédures* ».

[39] Voir par exemple la politique de Sprint Canada, qui précise : « *Sprint Canada Inc.[1] recognizes that your right to privacy is an important issue. We understand your interest in maintaining your anonymity and protecting your private information while using our telecommunications products and services. As a result, Sprint Canada manages*

la personne avec qui communiquer et comment elles sont utilisées. Lors de cette étape, la politique précisera dans de nombreux cas, précise que l'information sera communiquée aux tiers affiliés, qui peuvent être notamment des partenaires commerciaux et qui s'en serviront à des fins de marketing[40]. On peut aussi remarquer que certains sites ne disposent pas de politique de vie privée[41], et que d'autres proposent une politique de confidentialité minimale[42]. Il faudra non seulement qu'ils prennent conscience que la Loi fédérale va entrer en vigueur pour toutes les entreprises au premier janvier 2004 et qu'ils devront s'y conforment, mais aussi que les sites québécois réalisent rapidement l'existence d'une loi provinciale en la matière.

Mais revenons aux dispositions législatives qui encadrent l'utilisation des renseignements personnels. Outre le fait d'imposer la rédaction d'une politique de vie privée aux gestionnaires de sites, et en vertu du principe de spécificité des consentements, elles requièrent que pour toute utilisation nouvelle des renseignements personnels, non prévue initialement, il faudra à nouveau obtenir le consentement des personnes concernées. Cette obligation découle de la formulation de l'article 14 de la Loi québécoise et est explicitement requise par l'article 4.2. 4 de l'Annexe 1 qui dispose que, « *à moins que les nouvelles fins auxquelles les renseignements sont destinés ne soient prévues par une loi, il faut obtenir le consentement de la personne concernée avant d'utiliser les renseignements à cette nouvelle fin* ».

2. La confidentialité

Les deux lois font aussi peser sur les sites qui collectent des renseignements personnels une obligation de confidentialité, avec l'article 10 de la Loi québécoise et l'article 4.1.3 de l'Annexe 1, en vertu desquels il faut « *appliquer des mesures de*

---

your personal information with great care as reflected through this privacy policy. », disponible sur http://www.sprintcanada.ca/Privacy/ , visité le 21 novembre 2002.

[40] Voir notamment, les politiques d'Organon Canada, disponibles sur http://organon.ca/privacy_policy.asp, visité le 22 novembre 2002, Sprint Canada, disponible sur http://www.sprint.ca/general/privacy.php3, visité le 22 novembre 2002, et CanadaTravel, disponible sur http://www.canadatravel.ca/privPolicy.asp, visité le 22 novembre 2002.

[41] Voir notamment Recettes.qc.ca, des recettes simples, disponible sur http://www.recettes.qc.ca/, visité le 22 novembre 2002, et Top Québec, disponible sur http://top-quebec.virtualave.net/, visité le 22 novembre 2002.

[42] Voir notamment Planète Québec, disponible sur http://planete.qc.ca/confiden.asp, visité le 22 novembre 2002.

sécurité propres à assurer le caractère confidentiel des renseignements »[43] et « *fournir un degré comparable de protection aux renseignements qui sont en cours de traitement pas une tierce partie* »[44]. Ces dispositions peuvent sembler incongrues puisque depuis le début de cette étude, nous parlons de la circulation de la vente et de l'utilisation de renseignements personnels. Or, l'obligation de confidentialité doit se comprendre par rapport au principe de la spécificité des consentements. En effet, si un internaute donne son consentement pour que ses informations personnelles soient utilisées afin de personnaliser un site précis, celui qui collecte les renseignements, et que lors de la personnalisation du site une autre entreprise arrive à s'emparer des données, cette dernière pourra s'en servir, même si cette activité sera illégale car sans consentement. Car, les renseignements personnels ont une grande valeur intrinsèque pour tous les publicitaires, et il est très difficile de trouver l'origine de la fuite de données nominatives. Le site qui récolte des informations personnelles est donc responsable de leur utilisation, et du fait qu'elles ne doivent être utilisées que par les personnes ou partenaires désignés dans la politique de vie privée.

3. Le droit d'accès

Enfin, les internautes disposent d'un droit d'accès à leurs renseignements personnels détenus par les entreprises commerciales en ligne. Ce droit est consacré par l'article 27 de la Loi québécoise selon lequel « *toute personne qui exploite une entreprise et détient un dossier sur autrui doit, à la demande de la personne concernée, lui en confirmer l'existence et lui donner communication des renseignements personnels la concernant* ». Cet article doit se lire de concert avec l'article 11 qui dispose que « *toute personne qui exploite une entreprise doit veiller à ce que les dossiers qu'elle détient sur autrui soient à jour et exacts au moment où elle les utilise pour prendre une décision relative à la personne concernée* », car afin d'assurer l'exactitude des données personnelles, il faut que les personnes intéressées puissent y avoir accès pour éventuellement les rectifier. Le texte de la Loi fédérale est rédigé dans des termes clairs : « *une organisation doit informer toute personne qui en fait la demande de*

[43] Article 10 de la Loi québécoise.

l'existence de renseignements personnels qui la concernent, de l'usage qui en est fait et du fait qu'ils ont été communiqués à des tiers, et lui permettre de les consulter. Il sera aussi possible de contester l'exactitude et l'intégralité des renseignements et d'y apporter les corrections appropriées »[45]. L'autre intérêt de ces dispositions est de permettre à l'internaute d'accéder aux dossiers les concernant pour éventuellement estimer le volume d'informations détenues, et peut-être réévaluer la pertinence de son consentement.

Ce bref aperçu nous permet non seulement d'évaluer l'ensemble des règles législatives applicables au Québec, mais il a aussi mis en relief quelques-unes des disparités qui existent entre les dispositions provinciales et fédérales. Or, nous évoquions précédemment l'intérêt, voire la nécessité de législations harmonisées afin d'assurer une véritable protection des renseignements personnels sur Internet. Nous voyons donc que la situation n'est pas simple à l'intérieur même du Canada.

Sur le plan international, depuis la décision[46] de la Commission européenne du 20 décembre 2001 constatant, conformément à la directive 95/46/CE[47] du Parlement européen et du Conseil, le niveau de protection adéquat des données à caractère personnel assuré par la Loi canadienne, le Canada est donc considéré comme ayant une législation conforme aux exigences européennes, ce qui lui assure la sécurité des échanges électroniques de données personnelles avec les autres pays membres.

Le principal problème pour un internaute qui voudrait agir en justice dans l'hypothèse où des renseignements personnels auraient été utilisés sans son consentement, serait de trouver l'origine de la fuite ou de la mauvaise utilisation voire de la collecte non

---

[44] Article 4.1.3 de l'Annexe 1.
[45] Article 4.9 de l'Annexe 1. Les dispositions relatives à l'exactitude des renseignements se retrouvent aux articles 4.6 et suivants.
[46] Publiée au Journal officiel des Communautés européennes L. 2/13, du 4 janvier 2002.
[47] Publiée au Journal Officiel des Communautés européennes L. 281 du 23 novembre 1995, p31.

documentée. Nous l'avons vu, de multiples techniques permettent d'obtenir des données sur les personnes qui visitent un site, sans que ceux-ci ne s'en aperçoivent. La jurisprudence en la matière est développée aux États-Unis[48], mais elle reste embryonnaire au Canada.

Certains répondent à ce problème en prônant l'utilisation de logiciels protecteurs de la vie privée comme Popup Free 1.5, Zone Alarm 2.6.362, Exit Popup Terminator 3.0, ou PopUp Buster 2.0[49]. S'ils empêchent l'installation de tout cookie ou de spyware sur notre ordinateur, ils peuvent avoir des conséquences imprévues. D'abord, certains sites conditionnent leur accès à l'implantation d'un cookie sur notre disque dur, comme par exemple les sites des banques qui requièrent un haut niveau d'authentification pour des besoins de sécurité. D'autres sites, où pourtant le besoin de sécurité est moins évident, font de même et installer ces logiciels peut réduire considérablement le volume des sites auxquels nous auront accès. Ensuite, nous l'avons vu, pour pouvoir faire fonctionner les paniers d'achats, les sites marchants ont besoin d'utiliser des cookies. Très peu de ces logiciels permettent de sélectionner ceux que l'on accepte. Il faut noter cependant que le World Wide Web Consortium[50] par l'intermédiaire de ses recommandations est à l'origine de modifications techniques dans les fureteurs Internet : par exemple Internet Explorer propose désormais une option pour accepter plus ou moins de cookies en fonction de leurs qualités[51].

---

[48] Voir notamment le « scandale DoubleClick », une entreprise qui voulait, lors de l'acquisition d'une société, fusionner les banques de données pour en constituer une plus grande, un arrangement a eu lieu le 21 mars 2002: In re DoubleClick Inc. Privacy Litigation, 154F. Supp. 2d., l'affaire Quicken.com où l'entreprise état accusée de collecter de l'information personnelle sans en avertir les internautes : In re Intuit Privacy Litigation, 138 F. Supp. 2d 1272 (C.D. Cal. 2001), l'affaire America Online : In re America Online, Inc. Version 5.0 Software Litigation, 168 F.Supp. 2d 1359 (S.D. Fla.2001), voir aussi In re Toys'R Us, Inc., Privacy Litigation, Master file No. C 00-2746 MCC, 2001 (N.D. Cal. Oct. 9, 2001).

[49] Tous ces logiciels sont proposés au téléchargement, notamment sur CENT Networks, http://news.com.com/2009-1023-937861.html, visité le 15 octobre 2002.

[50] Disponible sur http://www.w3.org/, visité le 15 octobre 2002.

[51] Cette option est accessible en cliquant sur Outils/Options Internet/Confidentialité/ puis on choisit le niveau désiré. Bien que souvent décriée comme étant insatisfaisante car ne permettant qu'une protection de la vie privée minimale, cette option a au moins le mérite d'exister.

Cependant, ces solutions techniques ne sont que des succédanées et ne peuvent satisfaire les juristes que nous sommes. Dans de nombreux cas, les entreprises ont besoin de collecter de l'information, Internet leur permet de cibler les destinataires des messages, ce qui engendre, lorsque cela est fait judicieusement, des résultats satisfaisants pour les annonceurs comme pour les internautes. Là où le bas blesse, c'est lorsque les sites abusent de la collecte d'informations et inondent leurs victimes de pourriel et de pop-up, qui sont pour le moins irritants. Il faudrait que ces entreprises prennent conscience non seulement de l'existence de lois encadrant la pratique, mais aussi qu'il n'est pas dans leur intérêt à long terme de continuer d'agir de la sorte, car les internautes s'éduquent relativement vite, et l'on peut envisager que l'utilisation de logiciels pour bloquer l'introduction de cookies sur les disques durs va augmenter dans les années qui viennent, pénalisant leurs activités. Cette prise de conscience semble amorcée d'après William Adkinson, de la Progress and Freedom Foundation[52], qui dans un rapport datant de mars 2002 constate que les sites collectent moins d'informations, qu'ils utilisent moins de cookies permettant de connaître le comportement de l'internaute sur d'autres sites, que les politiques de vie privées sont plus présentes et plus complètes, que les consommateurs ont plus l'opportunité de choisir la façon dont seront utilisées leurs informations et que certains sites ont même introduit un système d'opt-in. Cette prise de conscience ne doit pas s'arrêter la, les entreprises doivent continuer leurs efforts, éventuellement en adoptant des normes au niveau international. Elles doivent ainsi s'attacher à gagner la confiance des internautes, c'est un pré-requit nécessaire à l'avenir du commerce électronique.

[52] William F. ADKINSON, Jr, Jeffrey A. EISENACH et Thomas M. LENARD « Privacy online : a report on the information practices ans policies of commercial web site », rapport remis à The Progress & Freedom Foundation, mars 2002, disponible sur http://www.pff.org/publications/privacyonlinefinalael.pdf, visité le 21 octobre 2002.

Bibliographie

Table de la législation

Loi sur la protection des renseignements personnels et des documents électroniques, L.C. 2000, ch.5

Loi sur la protection des renseignements personnels dans le secteur privé, L.R.Q., Ch. P-39

Code Civil du Québec, L.Q. 1991, c. 64

Charte des droits et libertés de la personne, L.R.Q. C-12.

Convention de sauvegarde des droits de l'homme et des libertés fondamentales, Rome, 4.XI.1950

Directive 95/46/CE, concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques, Journal officiel des Communautés européennes L 281 du 23.11.1995, p31.

Décision de la Commission européenne du 20 décembre 2001 constatant, conformément à la directive 95/46/CE du Parlement européen et du Conseil, le niveau de protection adéquat des données à caractère personnel assuré par la Loi canadienne, Journal officiel des Communautés européennes L. 2/13, du 4 janvier 2002

Table des jugements

Québec (Procureur général) c. Irwin Toys Ltd. [1989] 1 R.C.S. 927

R. v. Dyment [1988] 2 S.C.R. 417

Monographies et recueils

GAUTRAIS, V. : Droit du commerce électronique, Montréal, Éd.Thémis, 2002.

GEIST, M. A. : Internet Law in Canada, New-York, Captus Presse, 2000

L'HEUREUX, N. : Droit de la consommation, Montréal, Ed . Yvon Blais, 2000

TRUDEL, P. et F. ABRAN : Droit du Cyberespace, Montréal, Éd. Thémis, 1997

TRUDEL, P. et F. ABRAN : Droit de la radio et de la télévision, Montréal, Thémis, 1991

YOUNG, D. M. et B. R. FRASER : Canadian Advertising and Marketing Law, Toronto, Carswell, 1990

Articles de Revues

ADKINSON, W.F.JR., J. A. EISENACH, et T. M. LENARD : « Privacy online : a report of the information practices and policies of commercial web sites », mars 2002, Progress & Freedom Foundation, disponible sur http://www.pff.org/publications/privacyonlinefinalael.pdf, visité le 21 octobre 2002.

BARRETT, J. : « Customer data integration technology : a privacy solution », juillet 2002, 19 n° 7 Computer and Internet Lawyer 8

BARTOW, A. : « Women as targets : the gender-based implications of online consumer profiling », », Comment to the Department of Commerce and Federal Trade Commission, 8 novembre 1999, disponible sur http://www.ftc.gov/bcp/profiling/comments/bartow.htm, visité le 21 octobre 2002.

BENDER , D. : « Privacy Law », novembre 2002, 17 Practising Law Institute / Patents, Copyrights, Trademarks and Literary Property Course Handbook series 563.

BRAINBRIDGE, D. : « The Directive on Electronic Commerce », octobre 2000, Intellectual Property & Information Technology Law, Vol 5, i. 5.

BUIS G. : « Aspects internationaux de la publicité et des promotions sur Internet », 47 Revue Droit de la Communication – Commerce électronique, 1846, éditions JCP 23 nov. 2000, disponible sur http://www.recrulex.com/fr/commun/droitsenligne/droits.asp?secteur=nouvelles_technologies&ID_ntic=27, visité le 8 octobre 2002.

BUREAU DE VÉRIFICATION DE LA PUBLICITÉ : « Recommandation publicité sur Internet », octobre 1998, disponible sur http://www.bvp.org/documents/deonto/internet/contenu.htm, visité le 8 octobre 2002.

CAHEN, M. : « L'Email Marketing », Avocat Online, 2002, disponible sur http://www.murielle-cahen.com/p_mail2.asp, (Premier article) et sur http://www.murielle-cahen.com/p_mail3.asp (deuxième article), visités le 8 octobre 2002.
CAHEN, M. : « Le spamming », Avocat Online, 2002, disponible sur http://www.murielle-cahen.com/p_spamming.asp, visité le 8 octobre 2002.

CARLTON, C.F. : « The right to privacy in Internet commerce : a call for new federal guidelines and the creation of an independant privacy commission », printemps / été 2002, 16 Saint John's Journal of Legal Commentary 393.

CATLETT J. : « Re : online profiling projet – comment P994809 », Comment to the Department of Commerce and Federal Trade Commission, 18 octobre 1999, disponible sur : http://www.ftc.gov/bcp/profiling/comments/catlett.htm, visité le 21 octobre 2002.

CAUSIN, L. : « Internet et la publicité », Les chroniques Juritel, 2e trimestre 1999, disponible sur http://www.juritel.com/juri2000/chroniquePage.asp?Index=40 , visité le 8 octobre 2002.

CHASSIGNEUX, C. : « La protection des données personnelles en France », Lex Electronica, vol. 6, n°2, hiver 2001, disponible sur http://www.lex-electronica.org/articles/v6-2/chassigneux.htm, visité le 22 octobre 2002.

CÔTÉ, M.-H. : « Application des lois nationales à l'Internet : Etude de l'encadrement juridique de la publicité », mémoire de maîtrise, Université de Montréal, janvier 1999.

DÉCHAMPS, F. : « Internet et Marketing : la technique de l'opt-in a convaincu les autorités européennes », Recrulex, disponible sur http://www.recrulex.com/fr/commun/droitsenligne/droits.asp?secteur=nouvelles_technologies&ID_ntic=22, visité le 9 octobre 2002.

DINANT, J.-M. : « Les traitements invisibles sur Internet », présenté lors d'une conférence à l'Institut Universitaire International à Luxembourg, juillet 1998, disponible sur http://www.droit.fundp.ac.be/crid/eclip/Luxembourg.html, visité le 8 octobre 2002.

DILLON, J. et M. HILDEBRAND, J. KLOSEK : « Top strategies for minimising the risk of privacy lawsuits and enforcement actions », octobre 2002, 19 n°10 Computer and Internet Lawyer 28.

GOBERT, D. : « La publicité sur Internet – Le droit en (r)évolution », décembre 2000, Revue Ubiquité, n°7, p71, disponible sur http://www.droit.fundp.ac.be/Textes/publicite.pdf, visité le 8 octobre 2002.

GOLDMAN, R. : « Understanding Internet Co-Branding Deals », 1999, 16 Computer High Technology Law Journal 65.

GREENSPAN, R. : « Online marketers tighten privacy », 29 mars 2002, disponible sur http://cyberatlas.Internet.com/markets/advertising/article/0,1323,5941_1000931,00.html visité le 21 octobre 2002.

M GEIST, « Is there a there there ? Towards greater certainty for Internet jurisdiction », disponible sur http://aix1.uottawa.ca/%7Egeist/geistjurisdiction-us.pdf, visité le 14 novembre 2002.

HANSEN, E. et J. BORLAND, R. KONRAD : « Your PC's enemy within : spyware, adware constroversies show why Net needs new laws », 26 juin 2002, disponible sur http://news.com.com/2009-1023-937457.html, visité le 21 octobre 2002.

HELMS, S.C. : « Translating privacy values with technology », été 2001, 7 B. U. J. SCI. & TECH. L. 288.

HERTZ, L. M. : « Advertising regulation on the Internet », juin 2002, 19 n°6 Computer and Internet Lawyer 18.

HETCHER, S. A. : « Norm Proselytizers create a privacy entitlement in Cyberspace », été 2001, 16 Berkeley Tech. L.J. 877.

KERR, C. L., et O. MERZGER : « Online privacy : new developments and issues in a changing world », juin 2002, 701 Practising Law Institute / Patents, Copyrights, Trademarks and Literary Property Course Handbook series 303.

KRAMER, L.C. : « Private eyes are watching you : consumer online privacy protection – lessons from home and abroad », printemps 2002, 37 Texas International Law Journal 387.

LE BORNE, M. : « L'industrie de la publicité en ligne adopte sa "Privacy Policy" », Droit et nouvelles technologies, disponible sur http://www.droit-technologie.org/1_2.asp?actu_id=437, visité le 9 octobre 2002.

LE CLAINCHE, J. : « Doubleclick devant la justice américaine : une démonstration efficace », 2002, droit-ntic.com, disponible sur http://www.droit-ntic.com/news/afficher.php?id=38, visité le 27 septembre 2002.

LEONARD, T. : « E-Marketing et protection des données à caractère personnel », 23 mai 2000, disponible sur http://www.droit-

technologie.org/2_1.asp?dossier_id=22&motcle=e-marketing&mode=motamot, visité le 21 octobre 2002.

LESSER, S. R. : « Privacy law in the Internet era : new developments and directions », juin 2002, 701 Practising Law Institute / Patent, Copyrights, Trademarks and Literary Course Handbook Series 115.

LOLIVIER, M. : « Les lignes directrices révisées de la Chambre de commerce internationale en matière de publicité et de marketing sur Internet », Gaz. Pal. 23 mai 1999, II, p7.

OLSEN, S. : « DoubleClik nearing privacy settlements », 29 mars 2002, disponible sur http://news.com.com/2100-1023-871654.html?tag=rn, visité le 21 octobre 2002.

OLSEN, S. : « Is your Email watching you? », 4 avril 2002, disponible sur http://news.com.com/2100-1023-875992.html, visité le 21 octobre 2002.

PASTORE, M. : « Web users will share information for better service », 5 avril 2000, disponible sur http://cyberatlas.Internet.com/markets/advertising/article/0,1323,5941_335011,00.html, visité le 21 octobre 2002.

PIPPIN, R. K. : « Consumer privacy on the Internet : It's surfer beware », 1999, 47 A.F. L. Rev. 125.

POLACK, M. : « Opt-in government : Using the Internet to empower choice – Privacy application », printemps 2001, 50 Cath. U. L. Rev. 653.

POST, A. : « The dangers of spyware », Symantech Ltd., disponible sur http://securityresponse.symantec.com/avcenter/reference/danger.of.spyware.pdf, visité le 21 octobre 2002.

ROLLO, A . : « The new litigation thing : consumer privacy », avril 2002, 1301 Practising Law Institute / Corporate Law and Practice Course Handbook Series 9.

RUBIN, P.H. et T. M. LENARD : « Privacy and the commercial use of personal information », juillet 2001, Progress and Freedom Foundation's Project, disponible sur http://www.pff.org/RubinLenard.pdf, visité le 21 octobre 2002.

SANDHANA, L. : « There's no place to hide », 26 aout 2002, disponible sur http://wired.com/news/print/0,1294,54598,00.html, visité le 20 septembre 2002.

SHIELDS, R. : « Les renseignements personnels accessibles au public et la loi sur la protection des renseignements personnels et les documents électroniques au Canada », McCarty Trétault, 12 octobre 2000, disponible sur http://dsp-psd.communication.gc.ca/Collection/C2-537-2000F.pdf, visité le 10 octobre 2002.

SHACHTMAN, N. : « A new code for anonymous web use », 12 juillet 2002, disponible sur http://wired.com/news/print/0,1294,53799,00.html, visité le 20 septembre 2002.

SHEN, A. : « Re : online profiling projet – comment P994809 », Comment to the Department of Commerce and Federal Trade Commission, 8 novembre 1999 http://www.ftc.gov/bcp/profiling/comments/shen.htm, visité le 21 octobre 2002.

SHERIDAN, M. G. : « Coverage issues raised by E-mail and the Internet », avril 2002, Illinois Institute for Continuing Legal Education 13-1.

SHOBER, G.M., et A. BARTOW, C. HOOFNAGLE, P. BORZI : « Colloquium on privacy & security », printemps / été 2002, 50 Buff. L. Rev. 703.

SIEGEL, T.H. : « International legal issues that can impact your online business », 711 Practising Law Institute / Patents, Copyrights, Trademarks and Literary Property Course Handbook series 265.

SINGH, K.C. : « Re : online profiling projet – comment P994809 », Comment to the Department of Commerce and Federal Trade Commission, 8 novembre 1999 http://www.ftc.gov/bcp/profiling/comments/ckunwarchandrajeetsingh.htm, visité le 21 octobre 2002.

VARILLE, N. : « La publicité et Internet », décembre 1997, n°98 H Cahier – Lamy Droit de l'informatique, 12.

VERBIEST, T. : « Publicité et Marketing sur Internet », 22 octobre 1999, Juriscom, disponible sur http://www.juriscom.ney/pro/1/ce19991022.htm, visité le 23 octobre 2002.