

La responsabilité des prestataires techniques Internet au Québec

Eloïse Gratton¹

Les lois de la société numérique : Responsables et responsabilités

Conférence organisée par le Programme international de coopération scientifique

(CRDP / CECOJI)

Montréal, 7 octobre 2004

Lex Electronica, vol. 10, n°1, Hiver 2005

<http://www.lex-electronica.org/articles/v10-1/gratton.htm>

INTRODUCTION	1
I. RESPONSABILITÉ ENVERS LES TIERS : CONTENU ILLICITE	3
I.1. PRINCIPE GÉNÉRAL : ABSENCE D'OBLIGATION DE SURVEILLANCE ACTIVE.....	3
I.2. TRANSMETTEUR	4
I.3. FOURNISSEUR DE SERVICES DE <i>CACHING</i>	6
I.4. HÉBERGEUR.....	7
II. RESPONSABILITÉ ENVERS LES CLIENTS : VIE PRIVÉE ET SPAM	9
II.1. PROTECTION DES RENSEIGNEMENTS PERSONNELS DU CLIENT ET DROIT À L'ANONYMAT	9
II.1.1 <i>Adresses Courriel</i>	10
II.1.2 <i>Messages Électroniques</i>	12
II.1.3 <i>Adresses IP</i>	14
II.1.4 <i>Promesse Contractuelle du FSI</i>	15
II.2. TRANSMISSION DE SPAM.....	16
II.2.1 <i>Envoi de Messages Électroniques Non Sollicités</i>	17
II.2.2 <i>Suspension de Compte pour Envoi de Spam</i>	18
CONCLUSION	19

INTRODUCTION

Les prestataires techniques fournissant des services sur Internet (ou « FSI ») sont les organisations qui interviennent dans l'accomplissement d'une tâche effectuée entre le point d'expédition d'une transmission de document et le point de réception final du document. Ces prestataires techniques peuvent inclure le simple transporteur de documents technologiques, lequel fournit les services d'un réseau de communication exclusivement pour la transmission de documents technologiques soit le fournisseur d'accès à, ou de services, Internet ou encore le fournisseur de connectivité (ci-après le « transmetteur »). Le prestataire offrant des services d'antémémorisation (ou services de *caching*), lequel est un service comportant la conservation par le prestataire des éléments d'une page Web que lui fournit son client dans un serveur (ou un ordinateur intermédiaire) afin de permettre, aux personnes qui ont droit d'accès à l'information,

¹ Avocate chez Mendelsohn, egratton@mendelsohn.ca.

l'accès à ladite page Web, de façon plus efficace en utilisant des *proxies*² (ci-après le « fournisseur de services de *caching* »)³ est également visé. Finalement, ces prestataires techniques peuvent également inclure le prestataire offrant des services de conservation de documents technologiques sur un réseau de communication (ci-après l'« hébergeur »).

Ces FSI peuvent être responsables face aux tiers ou face à leurs clients, et ce, à plusieurs niveaux.

La quantité d'informations circulant sur Internet fait en sorte que beaucoup de documents ou informations peuvent avoir un caractère illicite, soit affecter les droits d'auteur de tiers, être diffamatoire envers certains individus ou affecter d'autres tiers. Dans un premier temps, les FSI, que ce soit des transmetteurs, des fournisseurs de services de *caching* ou encore des hébergeurs, peuvent être tenus responsables face aux tiers pour le caractère illicite de l'information ou de documents qu'ils diffusent. Ces FSI sont les messagers de documents ou encore les intermédiaires qui jouent un rôle dans la transmission d'informations ou de documents qui peuvent avoir un contenu illicite. Ils sont souvent les premiers visés lors de la transmission ou diffusion d'information ou document dommageable, et ce, pour plusieurs raisons : (i) ces prestataires techniques sont souvent présents suite à une activité illicite et sont parfois plus facilement identifiables que l'auteur du document ou de l'information à caractère illicite; (ii) même dans l'éventualité où l'auteur de l'information ou document illicite est identifiable, ce dernier peut être situé dans un pays doté d'un système judiciaire inopérant; et (iii) l'auteur de l'information ou du fait dommageable peut se trouver insolvable tandis que le FSI visé est l'intermédiaire qui risque d'être solvable et en bonne santé financière.

Les FSI qui offrent certains services à des individus doivent nécessairement collecter leurs renseignements personnels, afin entre autres d'être en mesure d'offrir les services demandés, de gérer le compte du client ou à des fins de facturation. Certains FSI ont également accès à certains autres types de données électroniques telles que les données de connexion de leur client. Dans un deuxième temps, les FSI qui ont accès aux renseignements personnels de certains de leurs clients ou utilisateurs sur Internet ont certaines obligations relativement à la protection de ces renseignements. Leurs obligations de confidentialité peuvent découler soit de la promesse faite à ces individus (soit dans le cadre par exemple d'une politique adoptée en matière de protection de renseignements personnels ou encore du contrat intervenu entre le prestataire et son client) ou encore de leurs obligations imposées par les lois en matière de protection de renseignements personnels.

Finalement et dans un troisième temps, les FSI peuvent dans certains cas être tenus responsables d'avoir fait parvenir des courriels publicitaires non sollicités à leurs clients. Les problèmes de *spam* (ou « pourriels ») faisant couler beaucoup d'encre et étant un problème tellement grandissant qu'il force les autorités à se pencher sur la réglementation de l'envoi de courriels non sollicités, les FSI doivent être prudents et s'assurer d'avoir l'autorisation requise de l'abonné en question avant d'effectuer ce type d'envoi promotionnel. Certains FSI pourraient être tentés de

² Les proxies sont des intermédiaires entre le navigateur de l'utilisateur et le serveur Web.

³ En d'autres mots, le document est reproduit sur un serveur et l'utilisateur de l'Internet peut y avoir accès sans devoir requérir au serveur où le document est originellement situé.

suspendre le compte de leur client qui envoie du *spam*. La jurisprudence rendue en cette matière détaille les circonstances au cours desquelles un FSI peut légitimement suspendre un compte sans encourir de responsabilité envers son client.

Le présent article traitera des questions de responsabilité des prestataires techniques Internet au Québec envers les tiers quant au caractère illicite des documents transmis ou hébergés; à leurs obligations de respect des renseignements personnels de leurs clients; et finalement, aux questions de responsabilité pour l'envoi de *spam* à leurs clients ou à leur droit de suspendre un compte pour le motif que leur client détenant le compte envoie du *spam*.

I. RESPONSABILITÉ ENVERS LES TIERS : CONTENU ILLICITE

Au niveau du cadre légal, la *Loi concernant le cadre juridique des technologies de l'information* (« LCCJTI ») a été adoptée par le Parlement québécois en juin 2001⁴. Elle organise le statut juridique des documents, peu importe leur support. Cette loi prévoit, entre autres, des règles traitant de la responsabilité des prestataires de services agissant, à divers titres, en tant qu'intermédiaire dans l'hébergement ou la transmission de documents. Les dispositions de la LCCJTI complètent les principes généraux de la responsabilité civile énoncés à l'article 1457 du Code civil du Québec. La responsabilité des FSI, comme de toute autre personne, lorsqu'elle est engagée, découle nécessairement d'une faute de leur part. La responsabilité du prestataire sera engagée lorsqu'il aura été démontré un comportement que n'aurait pas eu une personne prudente et diligente placée en pareilles circonstances.

La LCCJTI trouvera application dès que le prestataire technique est domicilié au Québec ou si le préjudice dont se plaint la victime s'est manifesté au Québec. Cette loi détermine quel comportement les FSI doivent adopter afin de ne pas être tenus responsables. Toutefois, leur responsabilité n'est pas automatiquement engagée s'ils n'adoptent pas les comportements suggérés étant donné que la LCCJTI précise que ces agissements pouvant entraîner la responsabilité des prestataires sont non limitatifs.

I.1. Principe général : Absence d'obligation de surveillance active

Les FSI qui offrent des services sur un réseau de communication ou qui y conservent ou y transportent des documents technologiques ne sont pas tenus d'en surveiller l'information, ni de rechercher des circonstances qui pourraient indiquer que les documents permettent la réalisation d'activités à caractère illicite.⁵ Ces prestataires techniques ne doivent toutefois prendre aucun moyen pour empêcher la personne responsable de l'accès aux documents d'exercer ses fonctions, notamment en ce qui a trait à la confidentialité, ou pour empêcher les autorités responsables d'exercer leurs fonctions, conformément à la loi, relativement à la sécurité publique ou à la prévention, à la détection, à la preuve ou à la poursuite d'infractions.⁶

⁴ *Loi concernant le cadre juridique des technologies de l'information*, L.R.Q., chapitre C-1.1.

⁵ *Loi concernant le cadre juridique des technologies de l'information*, L.R.Q., chapitre C-1.1, art. 27.

⁶ *Loi concernant le cadre juridique des technologies de l'information*, L.R.Q., chapitre C-1.1, art. 27, al. 2.

Le FSI ne commet donc pas de faute en n'exerçant pas de surveillance active car il est exempt de le faire. Toutefois, cette exemption cesse au moment où le prestataire interfère avec la personne responsable du document ou de l'accès au document, le cas échéant, et qu'il commence à avoir un rôle actif dans la transmission du, ou l'accès au, document, que ce soit en se mêlant à l'accès aux documents ou en s'interposant entre les autorités légales et le document.

I.2. Transmetteur

Le transmetteur, soit le prestataire de services de courriel qui n'intervient que pour assurer la transmission des documents expédiés par ou à son abonné sur le réseau au moyen de son serveur, a souvent un rôle de simple transporteur de documents ou d'informations. Les transmetteurs qui offrent des services au public, aussi appelés les «common carriers», comme par exemple Bell Sympatico, ne sont généralement pas responsables du contenu des documents transmis pour ou par leurs clients, et ce, contrairement aux éditeurs et aux distributeurs de contenu. En effet, les transmetteurs doivent d'ailleurs rester neutres quant au contenu qu'ils transportent et ne peuvent pas régir le contenu ou influencer le sens ou l'objet des télécommunications qu'ils acheminent pour le public.⁷

Les dispositions de la LCCJTI précisent un principe général selon lequel le transmetteur n'est pas responsable des actions accomplies par autrui au moyen des documents qu'il transmet ou qu'il conserve durant le cours normal de la transmission du document et pendant le temps nécessaire pour en assurer l'efficacité.⁸ Le transmetteur n'est donc pas responsable des messages qui seraient de nature illégale ou illicite qui sont soit reçus ou encore expédiés par un de ses clients.

Toutefois, la LCCJTI émet quatre exceptions et situations qui peuvent engager la responsabilité du transmetteur. La première situation est le fait pour le transmetteur d'être à l'origine de la transmission du document.⁹ Puisque dans ce cas il a décidé lui-même de transmettre un document, il est logique que sa responsabilité puisse être engagée car alors il a un rôle actif dans la transmission d'un document qui pourrait être de nature illicite. La LCCJTI précise comme deuxième situation le fait pour le transmetteur de sélectionner ou de modifier l'information du document transporté.¹⁰ Dans ce cas, ce geste est considéré comme étant de nature éditoriale et le transmetteur est considéré avoir participé à la décision de transmettre l'information. Sa responsabilité peut donc être engagée.

Troisièmement, la LCCJTI mentionne que le transmetteur qui sélectionne la personne qui transmet le document, qui le reçoit ou qui y a accès peut engager sa responsabilité.¹¹ Le raisonnement pour potentiellement tenir le transmetteur responsable dans ce cas est le fait que le transmetteur, qui décide de la personne qui transmet le document ou qui le reçoit, joue un certain rôle actif et fait plus que simplement transporter ou transmettre l'information. Finalement, la LCCJTI précise la quatrième situation où le transmetteur peut engager sa responsabilité, soit

⁷ *Loi sur les télécommunications*, L.C, 1993, c- 38, art. 36.

⁸ *Loi concernant le cadre juridique des technologies de l'information*, L.R.Q., chapitre C-1.1, art. 36.

⁹ *Loi concernant le cadre juridique des technologies de l'information*, L.R.Q., chapitre C-1.1, art. 36, al. 1.

¹⁰ *Loi concernant le cadre juridique des technologies de l'information*, L.R.Q., chapitre C-1.1, art. 36, al. 2.

¹¹ *Loi concernant le cadre juridique des technologies de l'information*, L.R.Q., chapitre C-1.1, art. 36, al. 3.

lorsque ce dernier conserve le document à transmettre plus longtemps que nécessaire pour sa transmission. Dans ce cas, sa responsabilité peut être engagée étant donné le fait que le transmetteur est en possession du document et exerce un contrôle physique sur ce dernier.

Il est à noter que ces quatre situations mentionnées au deuxième alinéa de l'article 36 ne forment pas une liste exhaustive des situations pouvant impliquer la responsabilité du transmetteur, l'article 36, deuxième alinéa, précisant que ce dernier peut engager la responsabilité du transmetteur « notamment » s'il participe autrement à l'action d'autrui dans les quatre situations détaillées ci-dessus. Pour ce motif, la responsabilité du transmetteur en dehors de ces situations énumérées peut être engagée du moment que le transmetteur assume un rôle actif dans la transmission des informations ou documents de, ou destinés à, ses clients.

Au niveau fédéral, dans un arrêt de principe récent dans lequel la LCCJTI ne s'appliquait pas, la Cour suprême du Canada a unanimement soutenu que les FSI qui jouent un rôle de transmetteurs de documents ne peuvent pas être tenus responsables des violations des lois canadiennes sur le droit d'auteur commises par leurs abonnés.¹² La Cour a en effet considéré que les FSI qui fournissent simplement les moyens pour la télécommunication des documents publiés, donc qui agissent à titre de transmetteurs d'informations, sont, par conséquent, protégés de la responsabilité en vertu de la *Loi sur le droit d'auteur* du Canada,¹³ laquelle considère que les participants d'une communication qui fournissent seulement les moyens de télécommunication nécessaires ne sont pas réputés être des communicateurs au sens de cette loi.¹⁴

Ce jugement marque le point culminant de plusieurs années de litiges et d'appels réglementaires, lesquels ont débuté en 1995 lorsque la SOCAN¹⁵ a demandé au Tribunal canadien du droit d'auteur d'imposer des redevances, connues sous le nom de « Tarif 22 », sur les FSI agissant à titre de transmetteurs qui facilitaient le transfert d'œuvres publiées sur Internet. La préoccupation principale était le téléchargement de fichiers musicaux. La SOCAN a fait valoir que ces FSI contrefaisaient les droits des détenteurs d'un droit d'auteur de communiquer et d'autoriser la communication de leur œuvre au public se trouvant dans la *Loi sur le droit d'auteur*.¹⁶ La Cour a conclu que la connaissance de contrefaçon potentielle de la part d'abonnés ne rend pas un FSI responsable d'avoir autorisé la contrefaçon car les FSI agissant à titre de transmetteurs sont en droit de présumer que leurs facilités seront utilisées conformément à la loi, et ces FSI ne concèdent aucune licence ou permission à des abonnés qui permettent la contrefaçon.

Le jugement canadien est conforme aux dispositions de la LCCJTI où le FSI se fait octroyer un niveau élevé de protection contre les méfaits de ses utilisateurs pour autant que le rôle du FSI est limité à héberger et/ou à fournir l'accès à l'utilisateur, et que ce dernier agit en toute bonne foi.

¹² *Société canadienne des auteurs, compositeurs et éditeurs de musique c. Association canadienne des fournisseurs Internet*, [2004] CSC 45.

¹³ *Loi sur le droit d'auteur*, L.R. 1985, ch. C-42.

¹⁴ *Loi sur le droit d'auteur*, L.R. 1985, ch. C-42, art. 2.4(1)(b).

¹⁵ La SOCAN est la Société canadienne des auteurs, compositeurs et éditeurs de musique.

¹⁶ Cette obligation se trouve à : *Loi sur le droit d'auteur*, L.R. 1985, ch. C-42, art. 3(1)(f).

I.3. Fournisseur de Services de *Caching*

L'antémémorisation ou le *caching* est l'entreposage des éléments d'une page Web dans un serveur ou un ordinateur intermédiaire (serveur « proxy ») de manière à pouvoir accéder plus efficacement à cette page. Le but de l'utilisation de cette méthode est l'amélioration de la sécurité et de la vitesse de transfert de documents ou données vers le client. Les dispositions de la LCCJTI régissant les fournisseurs de services de *caching* indiquent le principe général à l'effet que ce type de prestataire n'est pas responsable des actions accomplies par autrui par le biais de ces documents.¹⁷ Son activité est dans ce cas assimilée à celle du transmetteur.

Toutefois, le fournisseur de services de *caching* peut engager sa responsabilité, notamment s'il participe autrement à l'action d'autrui : (i) dans les cas d'exceptions détaillés pour le transmetteur sous la sous-section 0;¹⁸ (ii) en ne respectant pas les conditions d'accès au document;¹⁹ ou (iii) en prenant des mesures pour empêcher la vérification de qui a eu accès au document.²⁰ Dans toutes ces situations, le fournisseur de services de *caching* a un rôle actif au niveau de la diffusion d'un document puisqu'il participe dans la décision entourant cette diffusion, soit en décidant des conditions d'accès au document ou encore en s'interposant dans cette décision de diffusion du document. Sa responsabilité peut donc être engagée.

Le fournisseur de services de *caching* peut également engager sa responsabilité en ne retirant pas promptement du réseau ou en ne rendant pas l'accès au document impossible alors : (i) qu'il a de fait connaissance qu'un tel document a été retiré de là où il se trouvait initialement sur le réseau; (ii) qu'il n'est pas possible aux personnes qui y ont droit d'y avoir accès; ou (iii) du fait qu'une autorité compétente en a ordonné le retrait du réseau ou en a interdit l'accès.²¹

Dans l'Affaire *Tariff 22*²² discutée davantage sous la section 0, la responsabilité du FSI fournissant des services de *caching* a été soulevée. Le Tribunal canadien du droit d'auteur a refusé de retenir la responsabilité des FSI agissant à titre de transmetteur en raison de l'exception prévue à l'article 2.4(1)(b) de la *Loi sur le droit d'auteur* qui mentionne que les participants d'une communication qui fournissent seulement les moyens de télécommunication nécessaires tels que les transmetteurs ne sont pas réputés être des communicateurs. La Cour d'appel du Canada avait trouvé que cette exception ne s'appliquait pas aux FSI fournissant des services de *caching* car dans ce cas, ces FSI ne sont plus de simples facilitateurs du procédé de télécommunication, mais ils deviennent des communicateurs et ils s'assujettissent à une responsabilité pour contrefaçon du droit d'auteur.

La Cour suprême du Canada a accepté la conclusion selon laquelle les FSI font partie de l'exception prévue à l'article 2.4(1)(b) estimant que le test approprié était d'étudier chaque

¹⁷ *Loi concernant le cadre juridique des technologies de l'information*, L.R.Q., chapitre C-1.1, art. 37, al. 1.

¹⁸ *Loi concernant le cadre juridique des technologies de l'information*, L.R.Q., chapitre C-1.1, art. 37, al. 2 (1).

¹⁹ *Loi concernant le cadre juridique des technologies de l'information*, L.R.Q., chapitre C-1.1, art. 37, al. 2 (2).

²⁰ *Loi concernant le cadre juridique des technologies de l'information*, L.R.Q., chapitre C-1.1, art. 37, al. 2 (3).

²¹ *Loi concernant le cadre juridique des technologies de l'information*, L.R.Q., chapitre C-1.1, art. 37, al. 2 (4).

²² *Société canadienne des auteurs, compositeurs et éditeurs de musique c. Association canadienne des fournisseurs Internet*, [2004] CSC 45.

opération de façon individuelle afin de déterminer si un FSI agit simplement à titre de canal de communications pour d'autres personnes, ou s'il agit à un autre niveau. La Cour a toutefois conclu que la pratique de la mise en antémémoire ou *caching* ne viciait pas l'exception prévue à l'article 2.4(1)(b) de la *Loi sur le droit d'auteur* car celle-ci est une heureuse conséquence des améliorations de la technologie Internet et qu'elle ne devrait avoir aucune incidence légale sur les communications :

« L'antémémoire est une belle invention issue du progrès de la technologie Internet, elle n'a aucune incidence sur le contenu et, au vu de l'al. 2.4(1)b) de la Loi, elle ne devrait avoir aucun effet juridique sur la communication intervenant entre le fournisseur de contenu et l'utilisateur final. La « mise en antémémoire » est dictée par la nécessité d'offrir un service plus rapide et plus économique. Elle ne devrait pas emporter la violation du droit d'auteur lorsqu'elle a lieu uniquement pour de telles raisons techniques et bénéficie donc de la protection prévue à l'al. 2.4(1)b). »

La mise en antémémoire ou les services de *caching* dictés par le besoin d'offrir un service plus rapide et économique ne devraient pas, lorsqu'ils sont utilisés seulement à des fins techniques, entraîner une responsabilité de droit d'auteur pour le fournisseur de services de *caching*.

I.4. Hébergeur

L'hébergeur est celui qui met des documents appartenant à son client à la disposition du public sur Internet en les plaçant sur son serveur. Les dispositions de la LCCJTI régissant les fournisseurs de services d'hébergement énoncent un principe général selon lequel l'hébergeur n'est pas responsable des activités accomplies par la personne utilisant le service d'hébergement au moyen des documents hébergés par l'utilisateur ou à la demande de celui-ci.²³ L'analogie la plus simple et logique à utiliser afin de bien comprendre le régime de responsabilité de l'hébergeur est la comparaison avec le propriétaire d'un lieu, puisque ce dernier n'est, de façon générale, pas tenu responsable des actes commis par des tiers sur ses lieux, en autant que les actes illicites, le cas échéant, soient commis à son insu.

Cette exonération de responsabilité pour l'hébergeur ne peut être invoquée s'il est démontré que l'hébergeur a de fait connaissance du caractère illicite du document diffusé sur Internet. Dans ce cas, l'hébergeur se doit de prendre les moyens pour rendre l'accès aux documents impossible ou pour autrement empêcher la poursuite de cette activité et ce, sans délai. L'hébergeur peut en effet engager sa responsabilité, notamment s'il a de fait connaissance que les documents conservés servent à la réalisation d'une activité à caractère illicite ou s'il a connaissance de circonstances qui la rendent apparente et qu'il n'agit pas promptement pour interdire l'accès aux documents ou pour autrement empêcher la poursuite de cette activité.²⁴

Il est à noter que la connaissance de la nature illicite de l'information hébergée n'est toutefois pas nécessairement l'unique situation où la responsabilité de l'hébergeur peut être engagée. L'article 22 de la LCCJTI ne constitue pas une liste exhaustive des situations au cours desquelles un hébergeur qui y est visé peut engager sa responsabilité car au 2^e alinéa, cet article énonce que

²³ *Loi concernant le cadre juridique des technologies de l'information*, L.R.Q., chapitre C-1.1, art. 22, al. 1,

²⁴ *Loi concernant le cadre juridique des technologies de l'information*, L.R.Q., chapitre C-1.1, art. 22, al. 6,

l'hébergeur peut engager sa responsabilité « *notamment* » s'il a de fait connaissance du caractère illicite des informations ou documents hébergés, sous-entendant qu'il peut également être tenu responsable dans d'autres types de situations non détaillées.

Dès le moment où l'hébergeur a connaissance du caractère illicite de l'activité associée aux documents qu'il conserve ou auxquels il donne accès, ce dernier doit agir. Étant donné que les hébergeurs n'ont pas l'obligation de surveiller le contenu au sens de l'article 26 de la LCCJTI, ils sont présumés avoir connaissance du caractère illicite des informations ou de documents hébergés que lorsqu'ils sont avisés de ce caractère illicite à moins que : (i) l'information ou le document hébergé émane de l'hébergeur ou que ce dernier a lui-même pris la décision d'effectuer la diffusion de l'information ou document illicite; ou (ii) il est démontré que l'hébergeur exerce une surveillance, constante ou occasionnelle, d'un site Internet.²⁵ Dans ces deux cas, l'hébergeur est présumé avoir connaissance du contenu ou caractère illicite des informations ou documents hébergés. En cas inverse, l'hébergeur est présumé avoir connaissance de ce caractère illicite uniquement si une personne porte ce caractère à son attention.

La LCCJTI ne précise pas à partir de quel moment l'hébergeur a une obligation d'agir et de retirer les documents qui ont un caractère illicite. Dans les cas où la notion du caractère illicite de l'information ou document est claire et n'est aucunement matière à débat, l'hébergeur doit agir dès la réception d'une plainte et retirer les informations ou documents illicites.

Un problème peut survenir dans le cas où le caractère illicite de l'information ou document n'est pas clair ou évident.

La LCCJTI ne précisant pas le moment à partir duquel l'hébergeur doit agir, il serait surprenant que l'intention du législateur soit telle que l'hébergeur doive retirer les informations ou documents hébergés dès lors qu'un tiers l'informe du fait que ces informations ou documents ont un caractère illicite et ce, compte tenu du fait que dans bien des cas, la notion du caractère illicite de l'information ou document est matière à débat. Le droit de supprimer une information ou un document devrait exister uniquement à partir du moment où le caractère sérieux de la plainte est établi.

De plus, l'hébergeur qui retire une information ou un document appartenant à son client sans s'être assuré du véritable caractère sérieux de la plainte et du caractère illicite de cette information ou document pourrait engager sa responsabilité et s'exposer à se faire poursuivre par son client.

L'hébergeur doit, lors de la réception d'une notification visant le contenu hébergé, agir avec prudence et diligence raisonnable. L'auteur Pierre Trudel dans son article intitulé *La responsabilité civile sur Internet selon la Loi concernant le cadre juridique des technologies de l'information*, suggère que lorsque le caractère illicite du document visé est matière à controverse, l'obligation de l'hébergeur d'agir ne commencera qu'à compter du moment où le caractère illicite aura été établi :

²⁵ Trudel, Pierre, *La responsabilité civile sur Internet selon la Loi concernant le cadre juridique des technologies de l'information*, Développements récents en droit de l'Internet, service de l'information permanente, Barreau du Québec, Éditions Yvon Blais, 2001, p. 124.

« *Il nous paraît (...) que le seuil de connaissance à partir duquel la responsabilité de l'intermédiaire est engagée est la connaissance confirmée, par un tiers indépendant du caractère effectivement illicite du document. La connaissance à partir de laquelle est engendrée la responsabilité n'est pas celle qui résulte de la seule réception d'une plainte mais vise plutôt le moment où le caractère illicite devient manifeste.* »²⁶

La connaissance confirmée, par un tiers indépendant, du caractère effectivement illicite de l'information ou du document pourrait être l'obtention par l'hébergeur d'une opinion juridique. Dès que cette opinion confirme le caractère illicite, alors l'hébergeur devra agir promptement, sans délai, suite à la réception de l'opinion et retirer les informations ou documents illicites, le cas échéant.

Si la plainte est mal fondée, alors l'hébergeur n'a pas à supprimer ou censurer le contenu hébergé. Si la plainte est bien fondée, l'hébergeur doit rendre l'accès aux informations ou documents impossible ou encore empêcher la poursuite de l'activité illicite. L'auteur Pierre Trudel mentionne que l'hébergeur qui doit agir doit prendre les moyens possibles compte tenu des ressources dont il dispose et des circonstances dans lesquelles il agit.²⁷ L'hébergeur qui pose les gestes nécessaires afin de corriger la situation sans délai n'engagera pas sa responsabilité.

II. Responsabilité envers les clients : Vie privée et Spam

II.1. Protection des renseignements personnels du client et droit à l'anonymat

Depuis le 1er janvier 2001, la *Loi sur la protection des renseignements personnels et les documents électroniques*²⁸ (« LPRPDÉ ») s'applique aux entreprises fédérales. Le Commissaire à la protection de la vie privée du Canada, un agent du Parlement qui relève directement de la Chambre des communes et du Sénat, a généralement compétence pour entendre toute plainte relative à un FSI car ces derniers (par exemple les FSI agissant à titre de transmetteurs) sont des entreprises fédérales selon la définition de la *LPRPDÉ*.

Au Québec, la *Loi sur la protection des renseignements personnels dans le secteur privé*,²⁹ en vigueur depuis 1994, régit également la collecte et l'utilisation de renseignements personnels. Cette loi ayant été jugée comme étant substantiellement similaire à la loi fédérale *LPRPDÉ*,³⁰ c'est la loi québécoise qui s'applique en matière intra-provinciale.³¹ Cela signifie que même si

²⁶ Trudel, Pierre, *La responsabilité civile sur Internet selon la Loi concernant le cadre juridique des technologies de l'information*, Développements récents en droit de l'Internet, service de l'information permanente, Barreau du Québec, Éditions Yvon Blais, 2001, p. 126.

²⁷ Trudel, Pierre, *La responsabilité civile sur Internet selon la Loi concernant le cadre juridique des technologies de l'information*, Développements récents en droit de l'Internet, service de l'information permanente, Barreau du Québec, Éditions Yvon Blais, 2001, p. 130.

²⁸ *Loi sur la Protection des renseignements personnels et les documents électroniques*, 2000, ch. 5.

²⁹ *Loi sur la protection des renseignements personnels dans le secteur privé*, L.R.Q., chapitre P-39.1.

³⁰ Décret d'exclusion visant des organisations de la province de Québec, C.P. 2003-1842 19 novembre 2003, <http://canadagazette.gc.ca/partII/2003/20031203/html/sor374-f.html> (Dernier accès: 5 janvier 2005)

³¹ Il est à noter que la Colombie Britannique et l'Alberta ont également leurs lois depuis 2003, lesquelles lois ont été jugées comme étant substantiellement similaires à LPRPDÉ en octobre dernier et lesquelles s'appliquent également en matière intra-provinciales. Voir : Industrie Canada, Communiqué, *Les organisations de l'Aberta et*

c'est la *LPRPDÉ* qui régit de façon générale les FSI, la loi québécoise pourrait régir certains autres prestataires techniques sur Internet, par exemple un hébergeur, dans l'éventualité où ce dernier est une entité québécoise ou qu'il héberge des sites à partir d'un serveur situé au Québec. Uniquement l'analyse de la *LPRPDÉ* sera effectuée dans le présent article. Quoique la *LPRPDÉ* et la loi québécoise soient substantiellement similaires, le lecteur doit prendre note que la loi québécoise pourrait s'appliquer dans certains cas et que pour ce motif des variances pourraient être notées.

La *LPRPDÉ* définit « renseignement personnel » comme étant : « *Tout renseignement concernant un individu identifiable, à l'exclusion du nom et du titre d'un employé d'une organisation et des adresse et numéro de téléphone de son lieu de travail.* »³²

Certains nouveaux types de données collectés par l'entremise de l'Internet tels que les adresses courriel, les messages électroniques et les adresses Internet Protocol (IP) ne sont pas nécessairement ou automatiquement inclus dans la définition de renseignement personnel. Un prestataire technique sur Internet peut être tenu responsable de la collecte, de l'utilisation ou de la divulgation illégale de certaines de ces données en vertu de la *LPRPDÉ* ou encore d'une loi provinciale ayant été jugée comme étant substantiellement similaire. Pour ce motif, une analyse des décisions rendues par le Commissaire à la protection de la vie privée peut être utile afin de déterminer quel genre d'activité peut engager la responsabilité d'un FSI.

II.1.1 Adresses Courriel

Les adresses courriel personnelles sont de façon générale considérées comme des renseignements personnels et sont donc régies par la *LPRPDÉ*.³³ Dans certains cas, deux ou plusieurs individus partagent une même adresse courriel. Dans ce cas, l'adresse n'identifie pas un individu mais plutôt un groupe d'individus et il n'est pas clair si dans cette éventualité l'adresse courriel est régie par la *LPRPDÉ*. Étant donné que les informations relatives à une adresse courriel n'identifient pas toujours si cette dernière est relative à un seul individu ou à plus qu'un individu, les organisations qui collectent ou utilisent ce genre de données dans le cours de leurs activités commerciales devraient être prudentes et traiter ce type de données comme étant des renseignements personnels.

La définition de « renseignement personnel » de *LPRPDÉ* exclue expressément de cette définition les informations relatives aux informations d'affaires d'un individu, soit plus précisément le nom et le titre d'un employé d'une organisation et les adresse et numéro de téléphone de son lieu de travail. Une incertitude subsistait jusqu'à tout récemment car l'adresse

de la Colombie-Britannique exemptées de l'application de la Loi fédérale sur la protection des renseignements personnels, Ottawa, le 3 novembre 2004. <http://www.ic.gc.ca/cmb/welcomeic.nsf/0/85256a5d006b972085256f410046bca7?OpenDocument> (Dernier accès: 5 janvier 2005)

³² *Loi sur la Protection des renseignements personnels et les documents électroniques*, 2000, ch. 5, art. 2 (1).

³³ Voir par exemple les conclusions d'enquêtes suivantes où le Commissaire à la protection de la vie privée a traité les adresses courriel comme étant des renseignements personnels: Conclusions d'enquête de *LPRPDÉ* #2, *Messages électroniques non sollicités d'un fournisseur de services Internet*, 3 juillet 2001; Conclusions d'enquêtes de *LPRPDÉ* #277, *L'envoi collectif d'un message entraîne la communication des adresses électroniques des participants à un concours*, 2 septembre 2004.

courriel de travail n'est pas expressément exclue dans cette définition. Cela pouvait être interprété de deux façons : (i) le législateur a volontairement omis d'inclure l'adresse courriel de cette exclusion afin de s'assurer que toutes les adresses courriel, incluant les adresses courriel de travail soient considérées comme étant des renseignements personnels et soient régies par la *LPRPDÉ*; ou (ii) il s'agit plutôt d'un simple oubli du législateur d'inclure l'adresse courriel du lieu de travail dans l'exclusion prévue dans la définition de « renseignements personnel » et l'adresse courriel du lieu de travail n'est pas régie par la *LPRPDÉ*.

Une décision récemment rendue par l'Assistante Commissaire à la protection de la vie privée Heather Black précise le statut des adresses courriel de travail et confirme que ces dernières doivent être considérées comme étant des renseignements personnels au sens de la *LPRPDÉ*.³⁴ Il est à noter que la *Loi sur la protection des renseignements personnels dans le secteur privé*³⁵ ne contient pas d'exclusions en ce qui a trait aux informations d'affaires d'un employé d'une organisation et que pour ce motif, les adresses courriel, même celles d'un employé d'une organisation, sont depuis toujours considérés comme étant des renseignements personnels selon cette loi québécoise.

La collecte d'adresses courriel ou son utilisation ou divulgation à des tiers par un FSI sans le consentement des individus détenant ces adresses sont donc des activités illégales. Les prestataires techniques doivent s'assurer d'agir en conformité avec la *LPRPDÉ* (ou la loi québécoise, le cas échéant) afin de ne pas encourir leur responsabilité. Par exemple, ces derniers doivent s'assurer d'utiliser les adresses courriel uniquement aux fins pour lesquelles ces adresses ont été obtenues. Les FSI doivent s'assurer d'avoir obtenu le consentement des individus concernés avant de vendre leurs adresses courriel à des publicitaires. Ils doivent garder à l'esprit qu'ils peuvent utiliser ces adresses courriel dans le cadre d'une campagne publicitaire par courriel uniquement en conformité avec la loi relative à la protection des renseignements personnels qui s'applique et l'entente régissant le prestataire et l'individu en question, le cas échéant.³⁶

Les FSI doivent s'assurer de protéger les renseignements personnels de leurs abonnés au moyen de mesures de sécurité correspondant à leur degré de sensibilité et ce, contre la perte, le vol, la consultation, la communication, la copie, l'utilisation ou la modification non autorisées.³⁷ Le respect de ce principe est important lorsque les FSI désirent réaffecter une adresse courriel qui appartenait à un client à un autre individu.

En 2002, un client d'un FSI a déposé une plainte au Commissaire à la protection de la vie privée alléguant que son FSI agissant à titre de transmetteur n'avait pas adopté de mesures de sécurité adéquates pour protéger ses renseignements personnels.³⁸ Plus précisément, il alléguait que la

³⁴ Conclusions d'enquête, Dossier 6100-00780, 6100-00781, Plaignant Michael Geist, 1er Décembre 2004.

³⁵ *Loi sur la protection des renseignements personnels dans le secteur privé*, L.R.Q., chapitre P-39.1.

³⁶ Pour plus de détails relativement à la responsabilité des FSI en matière d'envoi de *spam*, veuillez vous référer à la Section 0 du présent article.

³⁷ *Loi sur la Protection des renseignements personnels et les documents électroniques*, 2000, ch. 5, principe 4.7.1 de l'annexe 1.

³⁸ Conclusions d'enquête de LPRPDÉ #41, *Un client s'objecte quand une compagnie lui annonce qu'elle a cédé son compte de courriel*, 15 mars 2002.

compagnie, en réaffectant son adresse électronique à un autre client, avait permis à une tierce partie de consulter ses renseignements personnels sans que lui-même soit au courant et sans qu'il y consente.

L'enquête a démontré que le client avait effectué une demande de jonction de comptes pour fins de facturation. Pour ce motif, le FSI avait procédé à une démarche technique complexe par laquelle les comptes de courriel sont isolés et mis en réserve en attendant la jonction des comptes de service principaux. Normalement, une fois la jonction accomplie, les comptes de courriel doivent être sortis de la réserve et réaffectés à l'abonné. L'enquête a confirmé que suite à une erreur matérielle du personnel du FSI, ce compte avait plutôt été placé dans une réserve sans être réaffecté à l'abonné plaignant et qu'il n'avait jamais été réaffecté ou cédé à un autre client. Pour ce motif, la plainte a été jugée comme non fondée. Malgré le fait que cette décision ne donne pas de détails quant au délai à respecter par le FSI avant de réaffecter une adresse courriel d'un ancien abonné à un nouveau client, cette décision est un rappel aux FSI qu'ils doivent être prudents dans la réaffectation d'adresses courriel.

II.1.2 Messages Électroniques

Un message électronique est un renseignement personnel et sa collecte ou utilisation est régie par la *LPRPDÉ*. En 2002, dans une décision du Commissaire à la protection de la vie privée,³⁹ un FSI agissant à titre de transmetteur accusé d'avoir retenu les messages électroniques adressés à un compte suspendu a été rendu coupable d'une infraction au sens de la *LPRPDÉ*.⁴⁰ Dans cette affaire, une cliente a effectué une plainte au Commissaire à la protection de la vie privée du fait que son FSI avait fait une utilisation de ses messages électroniques (soit de ses renseignements personnels) à une fin autre que celle à laquelle ils avaient été recueillis, et ce, sans son consentement. La plaignante alléguait que son FSI continuait de recevoir et d'emmagasiner ses messages électroniques sans les lui communiquer alors que son compte était suspendu pour non-paiement, et ce, en attendant de recevoir le paiement des arriérés et même lorsque son compte fut annulé.

Le FSI alléguait que le compte de la plaignante était officiellement réputé être toujours suspendu, et non annulé, et qu'elle pourrait réactiver le compte et récupérer ses messages électroniques sur paiement des arriérés. De plus, sa position était que sa politique de suspension, prévoyant notamment l'emmagasinage et la conservation des messages électroniques jusqu'au paiement, constituait une norme de l'industrie qu'une personne raisonnable jugerait appropriée. Le FSI a soutenu que la plaignante avait consenti à cette politique et pratique en signant la convention de service initiale. Il est à noter que suite à la plainte, le FSI a pris des mesures pour préciser la politique et les pratiques de suspension dans sa convention de service. Toutefois, le FSI a maintenu que l'explication initiale avait été suffisamment claire pour que la plaignante la comprenne.

³⁹ Conclusions d'enquête de LPRPDÉ #41, *Un client s'objecte quand une compagnie lui annonce qu'elle a cédé son compte de courriel*, 15 mars 2002.

⁴⁰ Voir la *Loi sur la Protection des renseignements personnels et les documents électroniques*, 2000, ch. 5, principes 4.3, 4.3.2 et 4.5, annexe 1; et paragraphe 5(3)].

Le Commissaire à la protection de la vie privée a constaté que la pratique normale de l'industrie était effectivement de continuer d'accepter les messages électroniques, de les emmagasiner et d'en refuser l'accès au client dont le compte est suspendu. Ce dernier était d'avis que la convention initiale n'était pas claire sur la pratique du FSI en cas de suspension de compte et que pour ce motif, le FSI avait contrevenu au principe de la *LPRPDÉ* selon lequel toute personne doit être informée de toute collecte, utilisation ou communication de renseignements personnels qui la concernent et y consentir.⁴¹ Suivant ce principe, il faut informer la personne au sujet de laquelle on recueille des renseignements et obtenir son consentement, les organisations devant faire un effort raisonnable pour s'assurer que la personne est informée des fins auxquelles les renseignements seront utilisés.⁴² Pour que le consentement soit valable, les fins doivent être énoncées de façon que la personne puisse raisonnablement comprendre de quelle manière les renseignements seront utilisés ou communiqués.

Le Commissaire à la protection de la vie privée a conclu que l'entreprise, ayant utilisé les renseignements personnels de la plaignante sans son consentement à des fins autres que celles auxquelles elle les avait recueillis, contrevenait au principe 4.5 de la *LPRPDÉ* lequel indique que 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.

Le Commissaire à la protection de la vie privée a donc conclu que l'entreprise, ayant par la suite pris des mesures pour expliquer en termes compréhensibles ses pratiques de suspension des comptes, se conformait désormais aux principes 4.3, 4.3.2, 4.5 de l'annexe 1 et au paragraphe 5(3) de la *LPRPDÉ*.

Cette décision énonce donc le principe selon lequel un FSI qui agit à titre de transmetteur ne peut pas retenir les messages électroniques de son abonné (par exemple en cas de non paiement) sans encourir sa responsabilité au sens de la *LPRPDÉ*, à moins que cette pratique ait été convenue et énoncée clairement dans l'entente liant le FSI et son client.

Même si un FSI peut utiliser cette pratique d'emmagasiner et de conserver des messages, le fait est qu'il est possible que certains messages soient importants et que le défaut d'informer le destinataire de leur existence ou l'expéditeur de leur défaut de livraison puisse avoir certaines conséquences néfastes pour le client et même pour l'expéditeur qui croit que ses messages ont été livrés. Pour ce motif, les FSI qui emmagasinent les messages électroniques adressés aux détenteurs de comptes suspendus et leur refusent l'accès devraient adopter une pratique de renvoyer ces messages électroniques aux expéditeurs avec un avis indiquant qu'ils n'ont pu être livrés. Le Commissaire à la protection de la vie privée recommande d'ailleurs que les FSI prennent des mesures pour permettre au détenteur d'un compte suspendu d'avoir accès aux messages électroniques que l'entreprise a déjà reçus mais que le client n'a pas encore récupérés, au moment de la prise d'effet de la suspension. Ces recommandations résument les pratiques d'affaires exemplaires qui devraient être suivies par tout FSI.

⁴¹ Voir la *Loi sur la Protection des renseignements personnels et les documents électroniques*, 2000, ch. 5, principe 4.3, annexe 1.

⁴² Voir la *Loi sur la Protection des renseignements personnels et les documents électroniques*, 2000, ch. 5, principe 4.3.2, annexe 1.

II.1.3. Adresses IP

Plusieurs utilisateurs considèrent que l'Internet est un forum anonyme. La plupart des expéditeurs peuvent utiliser un pseudonyme, advenant qu'ils aient à dévoiler un nom. Pour ce motif, l'unique façon de retracer un utilisateur est souvent par l'entremise de son adresse de protocole Internet (ou *adresse IP*), soit un ensemble de 4 chiffres unique à chaque utilisateur à tout moment. Ces adresses IP peuvent être retracées au niveau du FSI (particulièrement le FSI agissant à titre de transmetteur), lequel peut être en mesure d'identifier son client à partir de l'adresse IP ainsi qu'à partir de la date et de l'heure d'enregistrement. Ainsi, lorsque des déclarations diffamatoires sont enregistrées ou qu'un certain utilisateur semble avoir fait une utilisation de son service Internet qui enfreint les droits de propriété intellectuelle de tiers, la partie demanderesse qui n'a généralement accès qu'à l'adresse IP de l'expéditeur ou de l'auteur de l'activité illicite fera appel au FSI afin d'obtenir des informations relatives à l'identification de cet expéditeur ou auteur fautif. Un FSI peut être réticent à divulguer l'identité et les renseignements personnels de son client.

Le 31 mars 2004, la Cour fédérale du Canada a rejeté la requête de l'Association de l'industrie canadienne de l'enregistrement (la « CRIA ») pour contraindre certains FSI agissant à titre de transmetteurs à divulguer l'identité de 29 utilisateurs anonymes qui partageaient des fichiers musicaux sur Internet.⁴³

Dans un premier temps, pour en arriver à sa décision, la Cour a établi que la CRIA n'avait pas présenté de preuves *prima facie* de violation du droit d'auteur par les partageurs de fichiers. La Cour a soutenu que le fait de copier des fichiers à des fins personnelles, ainsi que le stockage de ces fichiers sur un répertoire de données partagées qui peut être accessible par le biais d'un réseau poste à poste ne constituait pas une violation du droit d'auteur. De plus, la Cour a soutenu que le simple entreposage de copies personnelles de fichiers musicaux sur un répertoire de données partagées où elles sont accessibles par le biais d'autres ordinateurs n'était pas une violation de l'article 80(1) de la *Loi sur le droit d'auteur*.⁴⁴ Il n'y avait aucune preuve que les prétendus contrevenants avaient distribué ou autorisé la reproduction d'enregistrements. En se référant à la récente décision de la Cour suprême du Canada dans l'affaire *CCH Canadienne Limitée c. Le Barreau du Canada*,⁴⁵ la Cour a déclaré qu'il n'existait aucune différence importante entre le fait de placer une photocopieuse dans une pièce remplie d'œuvres protégées par le droit d'auteur et le fait d'entreposer des copies personnelles de fichiers musicaux dans un répertoire de données partagées accessibles par d'autres usagers Internet. Il doit y avoir un acte positif de la part du propriétaire de distribuer les enregistrements. Il n'est pas suffisant d'établir que les prétendus contrevenants ont simplement rendu les enregistrements accessibles en ligne.

⁴³ *BMG Canada Inc. v. John Doe* (F.C.), [2004] 3 F.C. 241, 2004 FC 488. <http://www.canlii.org/ca/cas/fct/2004/2004fc488.html> (Dernier accès: 5 janvier 2005)

⁴⁴ Cet article mentionne que ne constitue pas une violation du droit d'auteur protégeant tant l'enregistrement sonore que l'œuvre musicale ou la prestation d'une œuvre musicale qui le constituent, le fait de reproduire pour usage privé l'intégralité ou toute partie importante de cet enregistrement sonore, de cette œuvre ou de cette prestation sur un support audio.

⁴⁵ *CCH Canadienne Ltée c. Barreau du Haut-Canada*, [2004] 1 R.C.S. 339, 2004 CSC 13. <http://www.canlii.org/ca/jug/csc/2004/2004csc13.html> (Dernier accès : 5 janvier 2005)

Certains autres motifs au soutien de la décision de la Cour de rejeter la requête sont pertinents en ce qui a trait à la protection des renseignements personnels des clients du FSI. La Cour a mentionné comme autre motif le fait que le droit à la protection des renseignements personnels des clients des FSI l'emporte sur l'intérêt public de divulguer leur identité, car il y avait une sérieuse possibilité d'identifier un client de FSI innocent.⁴⁶

La CRIA entend faire appel de cette décision et les FSI devraient s'informer du suivi de cette affaire étant donné que cela affecte leurs obligations de divulguer certain type de renseignements personnels de leurs clients.

II.1.4. Promesse Contractuelle du FSI

Un FSI a un intérêt quant à la conservation de l'anonymat de ses abonnés dans le but de conserver une bonne réputation d'affaire. Un autre type de responsabilité du FSI peut découler de la supposition de l'anonymat par le client du FSI. Plusieurs FSI promettent de ne pas divulguer d'informations qui révéleraient l'identité de leurs utilisateurs au sein de leurs politiques en matière de confidentialité ou de leurs modalités d'utilisation. Ces derniers ne le feront que rarement sur simple demande et ils exigeront un jugement de la cour ou un mandat de perquisition, selon le cas.

Lorsqu'un FSI reçoit un avis de présentation d'une requête ou demande en justice, il doit tout d'abord décider de prendre position ou non et, dans l'affirmative, il doit déterminer sa ligne de conduite. Les FSI dont la politique de protection de renseignements personnels et les modalités d'utilisation comprennent une clause spécifiant, par exemple, qu'ils ne dévoileront pas l'identité de leurs utilisateurs « sauf dans le cadre d'une ordonnance d'un tribunal » se trouvent dans une bonne position, puisqu'ils peuvent décider qu'ils ne prendront pas position et peuvent plus facilement divulguer l'identité de leurs clients sans encourir leur responsabilité.

Les FSI qui ont promis d'assurer la confidentialité sans cette exception sont, potentiellement, dans une position plus précaire. Il ne fait aucun doute qu'ils devraient se conformer à une ordonnance d'un tribunal si cette dernière est émise. Toutefois, ayant fait cette promesse à leurs utilisateurs, ils pourraient facilement être critiqués pour leur défaut de s'opposer à la requête. En effet, en 2000 aux États-Unis, le FSI Yahoo! a été poursuivie par un expéditeur qui s'identifiait sous le pseudonyme « Aquacool » pour s'être conformée à ce qui semblait être une assignation juridiquement valide.⁴⁷ La plainte d'Aquacool reposait, essentiellement, sur le fait que Yahoo! n'avait pas insisté sur les formalités de procédure qui se seraient appliquées en temps normal, que Yahoo! avait promis une plus grande protection en matière de confidentialité que celle qui a été offerte en adhérant à l'assignation par subpoena et que Yahoo! avait négligemment présenté de manière inexacte ses modalités de services puisqu'elle n'avait pas avisé le client avant de divulguer son identité. Bien que cette poursuite fut abandonnée et qu'aucune poursuite similaire a été entreprise au Canada, cette poursuite demeure un rappel aux FSI qu'il est important de déclarer de façon claire dans leur politique en matière de protection de renseignements

⁴⁶ Il est à noter que l'adresse IP réfère à un ordinateur et non à un individu.

⁴⁷ *Aquacool c. Yahoo!*, Re: subpoenas to bulletin board providers for personal information about anonymous posters. U.S. District Court, C.D.Cal., Filed on May 11, 2000. <http://www.techlawjournal.com/courts/aquacool/20000511com.htm> (Dernier accès : 5 janvier 2005)

personnels et modalités d'utilisation leur position dans l'éventualité où l'identité d'un abonné est recherchée par un tiers, puis de s'y tenir.

Le FSI, et non l'utilisateur, reçoit l'avis de requête. S'il ne s'oppose pas à l'ordonnance, la partie véritablement intéressée, soit l'expéditeur, ne sera pas en mesure de défendre son anonymat avant qu'il ne soit trop tard. Une pratique prudente suggère que le FSI avise l'utilisateur de la poursuite en cours et lui transmette tout document signifié. Cette procédure permet à l'expéditeur d'obtenir des conseils et d'assister en son nom propre afin de soulever des arguments sur la conservation de son anonymat. Toutefois, les FSI qui désirent ne pas avoir à aviser leurs abonnés des requêtes imminentes devraient préciser ce fait dans leur politique de protection des renseignements personnels ou dans leurs modalités d'utilisation, et inclure une clause prévoyant que le FSI a le droit contractuel de révéler l'identité de l'abonné sur simple demande, et ce, sans avis préalable à l'abonné.

II.2. Transmission de Spam

Au Canada, la *LPRPDÉ* oblige les organisations à offrir aux citoyens canadiens certaines garanties relativement à la collecte et à l'utilisation de leurs renseignements personnels. Les adresses courriel, lesquelles sont utilisées dans la transmission de *spam*, sont considérées comme étant des renseignements personnels. Pour ce motif, les FSI qui désirent utiliser les adresses courriel de leurs clients afin de faire la promotion de certains de leurs nouveaux produits ou services peuvent le faire uniquement dans certaines circonstances détaillées ci-dessous.

La politique canadienne sur le *spam* a été initialement articulée dans un document émanant de la section du commerce électronique de Industrie Canada en 1999.⁴⁸ Ce document suggérait qu'une législation anti-spam n'était pas nécessaire à ce stade étant donné que le *spam* pouvait être adressé dans certains cas en utilisant les lois existantes telles que le Code criminel et la *LPRPDÉ*. Avec le volume grandissant de *spam* en 2000 et 2001, Industrie Canada a publié en janvier 2003 un autre document de discussion intitulé : « Télémercatique : Offrir un choix au consommateur et créer des possibilités d'affaires » qui traite de différentes questions incluant la responsabilité des FSI, de la valeur des logiciels et des politiques anti-spam et discute du rôle du gouvernement dans le combat contre le *spam*.⁴⁹ En mai 2004, Industrie Canada a publié son plan d'action anti-pourriel pour le Canada,⁵⁰ lequel discute de l'utilisation de lois et réglementations existantes et de l'appui par le Canada aux efforts globaux dans la lutte contre le *spam*.

En 2003 et 2004, certains projets de loi anti-spam ont été proposés au Canada. Malgré le fait que ces projets n'ont pas été adoptés comme lois en date de ce jour, la Ministre de l'industrie est depuis 2004 en train de considérer une loi pour combattre le problème de *spam*.⁵¹ Industrie Canada a également développé en 2003 un code volontaire intitulé : *Code Canadien de pratiques*

⁴⁸ Industrie Canada, *L'internet et le courrier électronique en vrac non sollicité, MULTIPOSTAGE Document de discussion*, Juillet 1999.

⁴⁹ Industrie Canada, *Télémercatique: Offrir un choix au consommateur et créer des possibilités d'affaires*, Document de discussion, Janvier 2003.

⁵⁰ Industrie Canada, *Un Plan d'action anti-pourriel pour le Canada*, Mai 2004.

⁵¹ CBC News, *Canadian anti-spam law may be in works*, le 4 Février 2004.

pour la protection des consommateurs dans le commerce électronique,⁵² lequel vise à établir des standards pour le commerce électronique et les courriels publicitaires. Par exemple, les marchands faisant affaires en ligne ne doivent pas transmettre des courriels publicitaires aux consommateurs sans leur consentement, à moins que ces derniers possèdent une relation d'affaires existante avec ces consommateurs. De plus, tout courriel publicitaire doit mentionner de façon claire une adresse courriel de retour valide et doit mentionner en langage clair et concis une procédure simple selon laquelle les consommateurs désirant ne plus recevoir de courriels publicitaires peuvent informer le marchand de ce désir.⁵³

II.2.1. Envoi de Messages Électroniques Non Sollicités

En 2001, une cliente s'est plainte au Commissaire à la protection de la vie privée que son FSI, en lui envoyant des communications électroniques non sollicitées, ait utilisé sans son consentement des renseignements personnels la concernant,⁵⁴ à savoir son adresse électronique, et ce, en contravention de la *LPRPDÉ*.⁵⁵ Le FSI de la plaignante lui avait fait parvenir plusieurs messages électroniques non sollicités portant sur ses services. Le FSI soutenait qu'il était en droit d'envoyer de tels messages, en vertu des modalités et conditions de l'entente d'abonnement, qui comprenait une clause de consentement.

La plaignante, dont le premier abonnement d'un an était un cadeau d'un ami, n'avait pas étudié personnellement ces modalités, mais elle en a pris connaissance par la suite, lors du renouvellement de son abonnement.

Le Commissaire à la protection de la vie privée s'est référé au principe énoncé à l'article 4.3 de l'annexe 1 de la *LPRPDÉ* selon lequel 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. Après avoir examiné l'entente d'abonnement du FSI en question, le Commissaire à la protection de la vie privée était d'avis que la pratique d'envoi de communications électroniques périodiques à la clientèle était décrite clairement dans l'entente. Par conséquent, il a jugé qu'il était raisonnable que les clients du FSI s'attendent à recevoir, de temps à autre, de pareilles communications. De plus, il a considéré que la plaignante avait consenti à cette pratique en renouvelant son abonnement. Il a conclu que le FSI n'avait donc pas contrevenu au principe énoncé à l'article 4.3 et que la plainte était non fondée.

La jurisprudence est donc claire à l'effet que le *spam* ou l'envoi de courriels publicitaires par le FSI à son client est prohibé, à moins qu'il ne soit permis dans l'entente liant le FSI et son client.

⁵² Industrie Canada, *Code Canadien de pratiques pour la protection des consommateurs dans le commerce électronique*, Janvier 2003 <http://www.strategis.ic.gc.ca/pics/ca/consumerprotection03.pdf> (Dernier accès : 5 Janvier 2005)

⁵³ Industrie Canada, *Code Canadien de pratiques pour la protection des consommateurs dans le commerce électronique*, Janvier 2003, Principe 7.2. <http://www.strategis.ic.gc.ca/pics/ca/consumerprotection03.pdf> (Dernier accès : 5 Janvier 2005)

⁵⁴ Conclusions d'enquête de LPRPDÉ #2, *Messages électroniques non sollicités d'un fournisseur de services Internet*, 3 juillet 2001;

⁵⁵ *Loi sur la Protection des renseignements personnels et les documents électroniques*, 2000, ch. 5, principe 4.3., annexe 1.

II.2.2. Suspension de Compte pour Envoi de Spam

En 1999, la Cour supérieure de l'Ontario dans l'affaire *1267623 Ontario Inc. contre Nexx Online Inc.*⁵⁶ s'est penchée sur la pratique qui consiste à effectuer des envois massifs par courrier électronique de messages publicitaires non sollicités. Dans cette affaire, 1267623 Ontario Inc. (« 1267623 ») exploitait un commerce de vente au détail de meubles et effectuait sa publicité aux consommateurs par le biais d'Internet. Nexx Online Inc. (« Nexx »), un FSI se spécialisant dans l'hébergement sur son serveur de sites appartenant à des tiers, avait en août 1998 conclu une entente avec 1267623 aux termes de laquelle Nexx acceptait d'héberger sur son serveur, pour une période d'un an, le site Internet de 1267623.

Cinq mois plus tard, Nexx commence à recevoir des plaintes d'internautes relativement à la distribution massive par 1267623 de messages non sollicités. L'entente liant Nexx à son propre FSI contenait une disposition prohibant l'envoi par Nexx, ou par ses clients, de messages publicitaires non sollicités. Nexx avisa immédiatement 1267623 qu'une telle distribution massive de courriels non sollicités n'était pas permise et que si elle ne cessait pas cette pratique, Nexx se réservait le droit de résilier l'entente. 1267623 a alors, tout en conservant son site sur Nexx, retenu les services d'un tiers dont le site n'était pas hébergé par Nexx pour continuer l'envoi de ses courriels.

Nexx a alors désactivé le site Internet de 1267623. 1267623 prétendait que cette désactivation de son site Internet constituait une violation de l'entente et a donc demandé à la cour d'obliger Nexx à héberger son site Internet. Nexx plaidait que 1267623 avait violé les règles de conduite non écrites et évolutives régissant l'usage d'Internet (la « netiquette ») par l'envoi de *spam* et qu'elle est en défaut aux termes de l'entente intervenue entre les parties, laquelle prévoyait que 1267623 devait suivre les règles généralement acceptées de la *netiquette* lorsqu'elle envoyait des messages par courrier électronique. L'entente prévoyait également le droit pour Nexx d'imposer les conditions supplémentaires à ses clients et le droit pour ces derniers de mettre fin à l'entente s'ils refusaient ces conditions.

Après avoir consulté la jurisprudence américaine sur la question, la cour a d'abord conclu que l'envoi de *spam* par courrier électronique est contraire aux règles de la netiquette. La cour a aussi conclu que l'entente permettait à Nexx d'aviser 1267623 de l'existence d'une nouvelle condition, dans ce cas l'interdiction d'effectuer l'envoi de *spam*, le refus de 1267623 de cette nouvelle condition permettant à Nexx de mettre fin à l'entente. La demande de 1267623 a donc été rejetée.

Cette décision confirme le principe selon lequel l'envoi de *spam* est considéré comme étant contraire aux règles de la *netiquette*. Les FSI qui désirent pouvoir suspendre ou annuler le compte d'un client pour l'envoi de *spam* par ce dernier devraient spécifier ce droit dans l'entente intervenant entre le FSI et leur client. Une définition de *spam* devrait être incluse dans l'entente afin d'éviter les problèmes. Certains FSI ont entrepris d'autres initiatives en vue de combattre le *spam*. Par exemple, MSN Hotmail interdit à ses abonnés d'envoyer plus de 100 messages

⁵⁶ *1267623 Ontario Inc. c. Nexx Online Inc.* [1999] O.J. no. 2246.

électroniques par jour.⁵⁷ Les individus ou organisations désirant utiliser leur compte afin d'envoyer du *spam* vont donc s'assurer de faire affaires avec un autre FSI que MSN Hotmail.

CONCLUSION

Sur Internet, plusieurs prestataires techniques peuvent accomplir diverses fonctions reliées à la communication ou à la transmission d'information ou de documents. Chaque prestataire peut être unique dans le genre de service ou fonction qu'il détient et une analyse du rôle de ce FSI est souvent utile afin d'être en mesure de déterminer la responsabilité qu'il a envers son client et envers les tiers sur Internet.

En ce qui a trait à la responsabilité des FSI envers les tiers, la *Loi concernant le cadre juridique des technologies de l'information* dispense les prestataires techniques de l'obligation de surveillance active. Toutefois, dans l'éventualité où le FSI joue un rôle actif dans la transmission du document ou qu'il reçoit une plainte d'un tiers alléguant qu'un document transmis, diffusé ou hébergé a un caractère illicite et que le caractère illicite du document n'est pas évident, le FSI doit sans délai se doter d'un avis juridique indépendant, confirmant le caractère illicite du document qui est l'objet de la plainte. Le FSI doit retirer le document promptement si le caractère illicite est confirmé ou refuser de retirer le document si la plainte apparaît non fondée.

En ce qui a trait à la responsabilité des FSI envers leurs clients, une analyse des décisions rendues relativement à la protection des renseignements personnels ou à l'envoi de *spam* nous démontre que dans plusieurs cas, la responsabilité du FSI peut être évitée si l'entente régissant ce prestataire et son client est bien rédigée et traite de certains points sensibles. En effet, le cadre contractuel est important car dans bien des cas, la loi sur la protection des renseignements personnels qui s'appliquerait autrement est écartée afin de faire place au contrat qui régie les parties.

L'idée n'est pas d'inclure plusieurs clauses limitatives de responsabilité abusives mais au contraire de s'assurer de bien cerner l'utilisation que le FSI compte faire des renseignements personnels collectés et de bien divulguer, d'une façon raisonnablement compréhensible, ses activités et ses politiques en matière de protection de renseignements personnels. Également, les politiques du prestataire en cas de défaut de paiement, ses droits de suspendre un compte et le droit des parties d'envoyer des courriels promotionnels et les conséquences de cette activité doivent être précisées dans l'entente régissant les parties afin d'éviter des litiges inutiles. Finalement, les FSI doivent être prudents dans la réaffectation d'adresses courriel d'anciens clients.

⁵⁷ Stefanie Olsen, *Hotmail restricts outgoing messages*, CNET News, March 24, 2003. <http://news.com.com/2100-1025-993774.html> (Dernier accès : 14 Janvier 2005)