LE COMMERCE D'INFORMATIONS PERSONNELLES profite-t-il au consommateur ?

Rapport final du projet de recherche présenté
au Commissariat à la protection de la vie privée
et au Bureau de la consommation d'Industrie Canada

par

l'union des consommateurs

Juin 2007

Rapport de recherche publié par :

l'union des consommateurs

6226 rue Saint-Hubert, 3e étage
Montréal (Québec) H2S 2M2

Téléphone : 514-521-6820
Sans frais : 1 888 521-6820
Télécopieur : 514-521-0736

union@consommateur.qc.ca
www.consommateur.qc.ca/union

Membres de l'Union des consommateurs
ACEF Abitibi-Témiscamingue
ACEF Amiante – Beauce – Etchemins
ACEF de l'Est de Montréal
ACEF de l'Île-Jésus
ACEF de Lanaudière
ACEF Estrie
ACEF Grand-Portage
ACEF Montérégie-est
ACEF du Nord de Montréal
ACEF Rive-Sud de Québec
Association des consommateurs pour la qualité dans la construction
Membres individuels

L'Union des consommateurs est membre de l'Organisation internationale des consommateurs (CI), une fédération regroupant 234 membres en provenance de 113 pays.

Rédaction du rapport
- Me Marie-Eve Rancourt

Avec la collaboration
- du comité Télécommunication, Télédiffusion, Inforoute et Vie privée

Direction de rédaction
- Me Marcel Boucher

ISBN 978-2-923405-20-9

L'Union des consommateurs remercie Industrie Canada et le Commissariat à la protection de la vie privée pour l'aide financière accordée à ce projet de recherche. Les opinions exprimées dans ce rapport ne sont pas nécessairement celles du Commissariat à la protection de la vie privée, ni celles d'Industrie Canada ou celles du Gouvernement du Canada.

Pour faciliter la lecture du texte et éviter la redondance systématique, nous avons choisi d'utiliser le masculin générique pour désigner les deux genres.

TABLE DES MATIERES

L'UNION DES CONSOMMATEURS, *la force d'un réseau*

L'Union des consommateurs est un organisme à but non lucratif qui regroupe plusieurs Associations coopératives d'économie familiale (ACEF), l'Association des consommateurs pour la qualité dans la construction (ACQC) ainsi que des membres individuels.

La mission de l'Union des consommateurs est de représenter et défendre les droits des consommateurs, en prenant en compte de façon particulière les intérêts des ménages à revenu modeste. Les interventions de l'Union des consommateurs s'articulent autour des valeurs chères à ses membres : la solidarité, l'équité et la justice sociale, ainsi que l'amélioration des conditions de vie des consommateurs aux plans économique, social, politique et environnemental.

La structure de l'Union des consommateurs lui permet de maintenir une vision large des enjeux de consommation tout en développant une expertise pointue dans certains secteurs d'intervention, notamment par ses travaux de recherche sur les nouvelles problématiques auxquelles les consommateurs doivent faire face; ses actions, de portée nationale, sont alimentées et légitimées par le travail terrain et l'enracinement des associations membres dans leur communauté.

L'Union des consommateurs agit principalement sur la scène nationale, en représentant les intérêts des consommateurs auprès de diverses instances politiques, réglementaires ou judiciaires et sur la place publique. Parmi ses dossiers privilégiés de recherche, d'action et de représentation, mentionnons le budget familial et l'endettement, l'énergie, les questions liées à la téléphonie, la radiodiffusion, la télédistribution et l'inforoute, la santé, l'alimentation et les biotechnologies, les produits et services financiers, les pratiques commerciales, ainsi que les politiques sociales et fiscales.

Finalement, dans le contexte de la globalisation des marchés, l'Union des consommateurs travaille en collaboration avec plusieurs groupes de consommateurs du Canada anglais et de l'étranger. Elle est membre de l'*Organisation internationale des consommateurs* (CI), organisme reconnu notamment par les Nations Unies.

INTRODUCTION

Le droit à la vie privée est souvent défini comme le droit d'un individu à ne pas être importuné ou à ne pas voir des renseignements personnels qui le concernent recueillis, utilisés ou dévoilés sans son consentement. Par ailleurs, ce droit à la vie privée est depuis toujours considéré comme un attribut propre aux personnes physiques, qui ne peut être revendiqué par une entreprise ou un organisme. Avec la libéralisation des échanges et le développement des technologies, la question de la protection de la vie privée et des renseignements personnels suscite de plus en plus d'intérêt au sein de la population canadienne et est également source d'inquiétude.

Vu leur utilité, notamment à des fins de marketing, les renseignements personnels ont acquis une valeur qui a amené les entreprises à en faire un objet de commerce. La collecte et la vente de renseignements personnels font aujourd'hui partie des activités commerciales au même titre que la vente de produits ou services. En effet, bien que se pratiquant majoritairement à l'insu du consommateur, le recours à ce commerce est aujourd'hui partie intégrante de la commercialisation, de la mise en marché ou même de l'offre de certains biens ou services. D'ailleurs, la particularité de ce commerce et la rapidité de son évolution ont poussé plusieurs pays à légiférer afin d'encadrer ses méthodes et ses fins.

Au cours des vingt-cinq dernières années, on a vu naître de plus en plus de codes et de normes visant à encadrer le commerce de renseignements personnels. D'abord volontaires, ces normes, au fil du temps et devant l'ampleur prise par ce phénomène, sont devenues, dans plusieurs pays, obligatoires. Si certains pays, comme les États-Unis, ont choisi la voie de l'encadrement volontaire, d'autres, comme les pays européens ou le Canada, ont plutôt choisi de légiférer et de baliser par des lois la cueillette et l'utilisation des renseignements personnels.

Au Canada, le droit à la protection de la vie privée est un droit fondamental qui a été reconnu par les tribunaux comme étant protégé par la Charte canadienne des droits et libertés. Ce droit est également enchâssé dans la Charte des droits et libertés de la personne du Québec et protégé par diverses dispositions du Code civil du Québec. Un des corollaires du droit à la protection de la vie privée est la nécessité d'assurer la protection des renseignements personnels des individus, renseignements qui ne peuvent être recueillis, conservés, utilisés ou divulgués qu'en suivant certaines règles et en respectant certaines conditions, énoncés dans les lois fédérales et provinciales relatives à la protection des renseignements personnels. Or, si certaines pratiques sont conformes aux différentes dispositions de ces lois, d'autres semblent évoluer aux limites de la légalité.

Les renseignements personnels associés à un consommateur sont des données extrêmement précieuses pour les commerçants. S'il est courant de voir les institutions financières, les compagnies d'assurance ou les locateurs de logement avoir recours à des agents de renseignements personnels afin de vérifier, par exemple, la solvabilité d'un individu, ces renseignements sont également de plus en plus utilisés pour la commercialisation de produits et services. En effet, depuis le début des années 90, on assiste à une nouvelle utilisation des renseignements personnels, soit le marketing personnalisé, dit « *one-to-one* », dont l'objectif est d'individualiser l'offre pour chaque client en fonction de son profil, chose que rendent possible la collecte et la compilation de renseignements personnels, grandement facilitées par l'usage d'internet.

L'autoroute de l'information, terrain très vaste, éminemment difficile à superviser, facilite l'utilisation de plusieurs dispositifs qui permettent de recueillir ou d'utiliser des renseignements à l'insu de la personne qui fait l'objet de la collecte, voire même de voler à des fins frauduleuses certaines informations confidentielles. Ces renseignements s'avèrent fort utiles pour les commerçants puisqu'ils leur offrent non seulement la possibilité de faire la promotion de leurs produits auprès de ce consommateur, mais également, grâce aux techniques de profilage, d'optimiser leurs chances de réaliser une transaction en orientant cette promotion en fonction de ses goûts et intérêts.

Le potentiel économique et l'avantage concurrentiel dont peut tirer profit le détenteur de ces renseignements soulèvent plusieurs inquiétudes concernant notamment le consentement du consommateur quant à la cueillette et l'utilisation de ses renseignements personnels, la sécurité qui entoure le stockage de ces données ou les recours qui lui sont offerts. Conscients des dérapages qui pourraient découler d'un tel commerce, les élus canadiens ont choisi d'assujettir le secteur privé à diverses exigences.

Puisque de plus en plus de consommateurs sont confrontés à des clauses octroyant aux commerçants le droit d'utiliser à des fins commerciales leurs renseignements personnels et que se répandent les méthodes qui permettent de recueillir et d'utiliser des renseignements à l'insu des consommateurs, il convient d'examiner si le commerce des renseignements personnels profite de quelque manière aux consommateurs et si les lois de protection des renseignements personnels remplissent adéquatement le rôle qu'elles devaient jouer.

À cette fin, nous étudierons les lois encadrant la protection des renseignements personnels au niveau fédéral et au niveau provincial québécois et le contexte dans lequel elles ont été adoptées, afin d'établir les objectifs qu'elles visaient. Nous avons par la suite recensé les différentes méthodes de cueillette de renseignements et leur fonctionnement ainsi que l'usage qui est fait des renseignements ainsi recueillis.

Nous terminerons notre analyse en tentant d'identifier les avantages et désavantages que peut présenter pour le consommateur le commerce de renseignements personnels et les risques qu'il peut présenter.

Nous conclurons finalement avec des recommandations qui portent tant sur les pratiques commerciales actuellement en vigueur que sur les règles qui les encadrent.

LOIS ET NORMES APPLICABLES

Au Canada, les règles qui visent la protection des renseignements personnels dans le secteur privé se retrouvent à la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDÉ)[1], qui s'applique de prime abord à toutes les organisations qui exercent des activités commerciales. La LPRPDÉ énonce les règles de base pour la cueillette, l'utilisation et la communication des renseignements personnels par le secteur privé dans le cadre de leurs activités. La Loi fédérale prévoit, à son article 26(2)b, que des lois provinciales pourront s'appliquer à certaines entreprises en lieu et place de la législation fédérale, pour peu qu'une loi jugée essentiellement similaire à la Loi fédérale ait été adoptée par les autorités provinciales. Sera considérée comme une loi similaire à la LPRPDÉ :« *une loi qui établit, en matière d'information, un jeu fondamental de pratiques équitables allant dans le sens de la norme de la CSA et qui prévoit la mise sur pied d'un mécanisme indépendant de surveillance et des recours pour les personnes qui auront été lésées* »[2]. La LPRPDÉ continuera toutefois dans tous les cas à s'appliquer aux entreprises du secteur privé qui sont de juridiction fédérale ainsi qu'à celles qui exercent des activités interprovinciales ou internationales.

Jusqu'à présent, le Québec, l'Alberta et la Colombie-Britannique ont adopté des législations jugées essentiellement similaires en matière de protection des renseignements personnels,[3] tout comme l'Ontario en ce qui a trait aux renseignements personnels sur la santé[4]

Entrée en vigueur en 1994, soit 10 ans avant la LPRPDÉ, la loi québécoise, *Loi sur la protection des renseignements personnels dans le secteur privé* (LPRPSP), a naturellement été à ce jour source d'une jurisprudence beaucoup plus abondante que la loi fédérale. Par ailleurs, bien que les dispositions de ces deux lois se ressemblent, on y retrouve tout de même certaines différences, qui peuvent être assez significatives et sur lesquelles nous reviendrons un peu plus loin.

---

[1] *Loi sur la protection des renseignements personnels et des documents électroniques*, L.C. 2000, ch.5.
[2] Comité sénatorial permanent des affaires sociales, des sciences et de la technologie, 2 décembre 1999 [En ligne] http://canadagazette.gc.ca/partI/2002/20020803/html/notice-f.html#i5 (consulté le 21 février 2007).
[3] Au Québec : *Loi sur la protection des renseignements personnels dans le secteur privé*, L.R.Q., chapitre P-39.1 ; Décret d'exclusion visant des organisations de la province de Québec C.P. 2003-1842, 19 novembre 2003 Gazette du Canada partie II, Vol. 137, no 25 — Le 3 décembre 2003 [En ligne] http://canadagazette.gc.ca/partII/2003/20031203/html/sor374-f.html (consulté le 25 juin 2007),
En Alberta : *Personal Information Protection Act,* S.A. 2003, ch. P-6.5 ; Décret d'exclusion visant des organisations de la province d'Alberta, C.P. 2004-1163, 12 octobre 2004, Gazette du Canada, partie II Vol. 138, No. 22 — Le 3 novembre 2004, [En ligne] http://canadagazette.gc.ca/partII/2004/20041103/html/sor219-f.html (consulté le 25 juin 2007);
En Colombie-Britannique : *Personal Information Protection Act*, S.B.C. 2003, ch. 63 ; Décret d'exclusion visant des organisations de la province de la Colombie-Britannique, C.P. 2004-1164 12 octobre 2004, Gazette du Canada partie II, Vol. 138, No. 22 — Le 3 novembre 2004, [En ligne] http://canadagazette.gc.ca/partII/2004/20041103/html/sor220-f.html (consulté le 25 juin 2007),
[4] *Loi de 2004 sur la protection des renseignements personnels sur la santé*, L.O. 2004, ch. 3, Annexe A *Décret d'exclusion visant des dépositaires de renseignements sur la santé de la province d'Ontario*, C.P. 2005-2224 Le 28 novembre 2005, Gazette du Canada partie II Vol. 139, No. 25 — Le 14 décembre 2005. [En ligne] http://canadagazette.gc.ca/partII/2005/20051214/html/sor399-f.html (consulté le 25 juin 2007).

Le présent chapitre propose d'abord un bref survol des normes et accords ayant vu le jour en matière de protection de la vie privée au niveau international, pour ensuite examiner le contexte national, afin d'évaluer les motivations qui ont été à l'origine des normes adoptées et les buts poursuivis par le législateur lors de l'élaboration de ces normes. Nous terminerons le chapitre par un examen comparatif des lois provinciales et fédérale.

Protection de la vie privée et lois sur la protection des renseignements personnels

Le contexte international

L'intérêt pour un encadrement de la protection de la vie privée par le biais du droit d'accès aux renseignements personnels remonte au début des années soixante-dix. En effet, dans le contexte d'un développement sans précédent des nouvelles technologies, qui permettent notamment d'accroître considérablement l'accès des individus et des entreprises à des ordinateurs de plus en plus performants, on voit naître des intérêts antagonistes où s'opposent, d'une part, le désir d'un accès illimité à l'information que ces nouvelles technologies rendent possible et facilitent et, d'autre part, la volonté d'assurer la protection de la vie privée. Comme le mentionne l'Organisation de coopération et de développement économique (OCDE) :

> *« Cette préoccupation très répandue s'explique notamment du fait que les ordinateurs sont partout utilisés pour le traitement des données à caractère personnel, que les possibilités d'enregistrement, de comparaison, de rapprochement et de choix des données à caractère personnel, ainsi que d'accès à ces dernières, se sont considérablement élargies et que la fusion de la technologie des ordinateurs et de celle des télécommunications risque de mettre les données à caractère personnel simultanément à la disposition de milliers d'utilisateurs géographiquement dispersés, de même qu'elle permet la mise en commun des données et la création de réseaux de données complexes à l'échelon national et international. Il s'avère particulièrement urgent d'étudier certains problèmes, notamment ceux que posent les nouveaux réseaux internationaux de données et la nécessité de concilier les intérêts antagonistes liés, d'une part, à la protection de la vie privée et, de l'autre, à la liberté de l'information, afin de pouvoir pleinement exploiter les possibilités des technologies modernes du traitement de l'information, dans la mesure où cela est souhaitable. »*[5]

Entre les années soixante-dix et quatre-vingt, plus du tiers des pays membres de l'OCDE ont adopté une ou plusieurs lois visant à protéger les personnes physiques contre l'utilisation abusive de données les concernant et à leur reconnaître le droit d'accéder à ces données en vue d'en vérifier l'exactitude et d'exiger, le cas échéant, des corrections[6]. Dans les États à structure fédérale, des lois de ce type ont été adoptées tant par l'entité nationale que par les provinces ou les États. Ces lois ont, pour la plupart, été promulguées après 1973.

Les approches adoptées par les différents pays afin de protéger la vie privée ont de nombreuses caractéristiques communes. Parmi ces points communs se retrouvent quelques principes fondamentaux : assigner, selon les objectifs et les besoins de cette collecte, des

[5] OCDE « Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données à caractère personnel » 23 septembre 1980 C(80)58/Final, p. 5 [En ligne] http://www.oecd.org/document/0,2340,fr_2649_34255_1815225_1_1_1_1,00.html (consulté le 26 janvier 2007).

[6] *Ibid.*

limites à la collecte des données à caractère personnel, limiter aux finalités déclarées l'utilisation des données recueillies, créer des processus visant à permettre aux personnes physiques de connaître l'existence de dossiers contenant des renseignements les concernant et leur donner la possibilité de consulter ces dossiers et, le cas échéant, de faire corriger les informations y apparaissant.

Dans le but d'harmoniser les différentes lois nationales afin que celles-ci ne créent pas de distorsions à la concurrence, d'encadrer les problématiques reliées à la sécurité, au caractère confidentiel, et aux flux transfrontières des données, l'OCDE a mis sur pied en 1978 un groupe ad hoc d'experts sur les obstacles aux mouvements transfrontières des données. Ce groupe fut chargé d'élaborer des lignes directrices relatives « *aux règles fondamentales régissant le mouvement transfrontière des données à caractère personnel et la protection des libertés individuelles, en vue de favoriser l'harmonisation des législations nationales (…).* »[7] Les travaux du Groupe se sont effectués en étroite collaboration avec le Conseil de l'Europe et la Communauté européenne. Les objectifs des lignes directrices qu'a élaborées le Groupe étaient de :

> *«a) faire accepter aux pays membres certaines normes minimales de protection de la vie privée et des libertés individuelles eu égard aux données à caractère personnel ;*
>
> *b) Réduire au minimum les différences entre les règles pratiques intérieures des pays membres en la matière ;*
>
> *c) Veiller à prendre en considération, dans la protection des données à caractère personnel, les intérêts d'autres pays membres et la nécessité d'éviter des ingérences injustifiées dans le flux de données à caractère personnel entre pays membres ;*
>
> *d) Éliminer dans la mesure du possible, les raisons qui pourraient inciter les pays membres à restreindre les flux transfrontières de données à caractère personnel à cause des risques éventuels liés à ces flux. »*[8]

C'est donc dans un contexte de libéralisation des échanges, y compris une libéralisation du commerce de renseignements personnels, que s'inscrivent ces lignes directrices. En effet, bien que l'objet de ces lignes directrices soit la protection des renseignements personnels, leur but avoué était d'assurer une protection minimale de ces renseignements dans le cadre du développement du libre-échange, que l'OCDE voulait favoriser. La protection des données personnelles ne devait pas entraver au-delà du strict nécessaire la libre circulation des données. Comme le mentionne le document de l'OCDE : « *les lignes directrices (…) tout en admettant certaines restrictions à la libre circulation des données à caractère personnel à travers les frontières, cherchent à diminuer la nécessité de telles restrictions et, partant, à renforcer la notion de libre circulation de l'information entre pays*. »[9]

Le 23 septembre 1980, le Conseil de l'OCDE adoptait les *Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données à caractère personnel* (ci-après, Lignes directrices.) Ces Lignes directrices revêtent la forme d'une recommandation, les pays devant tenir compte, dans leurs législations nationales, de principes et objectifs qui y sont énoncés.

---

[7] *Ibid*., p. 7.
[8] *Ibid*., p. 34.
[9] *Ibid.*

Les Lignes directrices motiveront, par la suite, l'adoption par le Parlement européen et le Conseil européen, de la directive du 24 octobre 1995 relative à la *Protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données*[10]. Les législations nationales des pays membres devront être modifiées afin d'assurer leur conformité à cette nouvelle directive. Par ailleurs, il importe de souligner que cette directive européenne contient une disposition qui interdit aux organismes européens d'échanger des renseignements personnels avec les organismes d'autres pays, à moins que lesdits pays n'aient eux-mêmes mis en place des garanties adéquates assurant le droit des individus à la protection de leurs renseignements personnels. Le caractère adéquat du niveau de protection offert par un organisme situé dans un pays tiers s'appréciera au regard de toutes les circonstances quant aux données et à leur transfert, notamment la nature des données, la finalité et la durée du traitement envisagé, le pays d'origine et de destination finale, les règles de droit générales ou sectorielles en vigueur dans le pays tiers, ainsi que les règles professionnelles et les mesures de sécurité qui y sont respectées. Cette règle compte quelques exceptions, notamment si l'individu a consenti au transfert ou si ce transfert est nécessaire à l'exécution du contrat auquel l'individu est partie. Dans le cas où le pays tiers ne possède pas de législation relative à la protection des renseignements personnels, le transfert pourra tout de même être effectué dans la mesure où le destinataire offre des garanties suffisantes, qui peuvent notamment consister en des clauses contractuelles.[11] C'est dans ce contexte qu'un dialogue s'est établi entre l'Union européenne et les États-Unis afin de convenir d'un système qui assurerait la protection des données à caractère personnel transférées entre États membres de l'Union européenne et les États-Unis.[12] Les *Safe Harbour Principles*, considérés comme assurant un niveau de protection adéquat au sens de la directive 95/46/CE ont finalement été adoptés en juillet 2000, par la Commission européenne, après près de deux ans de négociation entre les pays membres de cette institution et les États-Unis.[13]

Contrairement aux pays européens, les États-Unis ont plutôt choisi l'approche non réglementaire, basée sur des codes volontaires. Cette stratégie, énoncée dans le document produit en 1997 par la Maison blanche et intitulé *A Framework for Global Electronic Commerce* (FGEC), favorise les initiatives provenant du secteur privé et vise à éviter une réglementation excessive du commerce électronique. En juin 1998, la Federal Trade Commission (FTC) a effectué une enquête sur les pratiques observées sur plus de 1400 sites internet en vue d'évaluer le respect des principes fondamentaux en regard d'un traitement équitable de l'information. L'enquête a révélé que de nombreux sites ne respectaient pas de façon acceptable les principes visant la protection de la vie privée. En effet, près de 85 % des sites recueillaient des renseignements auprès des consommateurs alors que seulement 14 % donnaient avis de leurs pratiques de traitement de l'information. Seulement 2 % des entreprises dont les sites avaient été étudiés s'étaient dotées d'une politique complète à ce chapitre.[14] En ce qui concerne les sites Web destinés aux enfants, la FTC a constaté que 89 % recueillaient

[10] Union européenne, *Directive 95/46/EC du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques et à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données*, Journal officiel no L.281, 23/11/1995, p. 31. para.25(2).
[11] *Ibid*. art. 26.
[12] POULLET, Yves, *Les Safe Harbour Principles, une protection adéquate ?* Paris, 17 juin 2000, [En ligne] http://www.juriscom.net/uni/doc/20000617.htm#_ftn10 (consulté le 26 janvier 2007).
[13] CHASSIGNEUX, Cynthia, *Aterritorialité des atteintes face aux logiques territoriales de protection juridique et problème de l'absence d'homogénéité des législations protectrices (quid des Safe Harbour Principles)*, *Lex Electronica*, vol. 9, n°2, Numéro Spécial, hiver 2004, p. 3 [En ligne] http://www.lex-electronica.org/articles/v9-2/chassigneux.htm (consulté le 22 janvier 2007).
[14] Pour qu'une politique soit complète, elle doit être affichée sur le site internet de l'organisation. Si elle n'y figurait pas, la politique était donc considérée comme incomplète.

des renseignements personnels alors que seulement 23 % demandaient aux enfants d'obtenir la permission de leurs parents avant de fournir ces informations. Ceux qui permettaient aux parents d'exercer un contrôle sur la collecte et l'utilisation de ces renseignements représentant une proportion encore plus faible.[15]

Donnant suite à ce rapport, la *Children's Online Privacy Protection Act of 1998*[16] (COPPA) qui vise à réglementer les questions liées à la protection de renseignements personnels pour les sites internet destinés aux enfants de moins de 13 ans a été adoptée et est entrée en vigueur le 21 avril 2000. Outre cette loi, la cueillette et l'utilisation des renseignements personnels aux États-Unis restent encadrées uniquement par l'autoréglementation, c'est-à-dire « *des normes volontaires développées et acceptées par ceux qui prennent part à une activité* », et ce, malgré le fait que les rapports de la FTC de 1998 et 1999 soulèvent l'inefficacité de cette approche.[17]

La FTC et le United States Department of Commerce ont organisé en 1999 le *Public Workshop on Online Profiling,* auquel ont participé les principales entreprises de publicité sur internet. Lors de cette rencontre, les membres de l'industrie ont annoncé la création d'un Groupe de travail, la *Network Advertising Initiative* (NAI) afin de mettre sur pied une proposition d'auto-réglementation destinée aux membres de l'industrie du profilage en ligne[18]. Malgré cette initiative, le rapport de de la FTC de 2000 tirera les même conclusions quant à l'inefficacité de l'autoréglementation, la majorité suggérant que le recours à la législation sera nécessaire pour protéger adéquatement les renseignements personnels et la vie privée des consommateurs sur internet.[19] À ce jour, cependant, outre la COPPA, aucune loi n'a été mise en place afin d'améliorer cette protection.

Lors de la Conférence ministérielle de l'OCDE, tenue à Ottawa en octobre 1998 , "*Un monde sans frontières : concrétiser le potentiel du commerce électronique mondial*", les pays membres de l'OCDE ont adopté la *Déclaration relative à la protection de la vie privée sur les réseaux mondiaux*[20] dans laquelle ils réaffirment leur engagement relativement aux Lignes directrices et invitent les pays non membres, les organisations internationales, l'industrie et les entreprises à respecter les principes et objectifs qui y sont énoncés.

---

[15] United States Federal Trade Commission (FTC), "*Privacy Online: A Report to Congress*", 1998, p. 2, [En ligne] http://www.ftc.gov/reports/privacy3/priv-23a.pdf (consulté le 10 avril 2007).
[16] *Children's Online Privacy Protection Act of 1998,* 15 U.S.C. §§ 6501-6506.
[17] United States Federal Trade Commission (FTC), *Op. cit*., note 16, p. 40 et "*Self-Regulation and Online Privacy: A Report to Congress*", 1999, p.12 [En ligne] http://www.ftc.gov/os/1999/07/privacy99.pdf (consulté le 10 avril 2007).
[18] United States Federal Trade Commission (FTC), "*Online Profiling: A Report to Congress" 2000*, p. 7 [En ligne] http://www.ftc.gov/os/2000/06/onlineprofilingreportjune2000.pdf (consulté le 25 juin 2007)
[19] *Ibid*., p. 21
[20] OCDE, *Déclaration relative à la protection de la vie privée sur les réseaux mondiaux,* C(98)177 [En ligne] http://webdomino1.oecd.org/horizontal/oecdacts.nsf/Display/440238D7718F359EC1257089002B8482?OpenDocument (consulté le 25 janvier 2007).

Le contexte national

L'adoption des *Lignes directrices* par les pays membres de l'OCDE et l'adhésion du Canada, en 1984, à ces lignes directrices ont été à la source de l'engagement du gouvernement fédéral à encourager le secteur privé à adopter des codes volontaires pour la protection des renseignements personnels.[21] Toutefois, à la fin des années 80, le Commissaire à la protection de la vie privée, qui avait le mandat de surveiller le respect de la *Loi sur la protection des renseignements personnels*[22] et de promouvoir le droit des personnes à la vie privée, s'inquiétait du peu de progrès accomplis et réclamait des mesures législatives fédérales qui obligeraient les organisations sous réglementation fédérale à élaborer de tels codes.[23]

Conscient du potentiel économique que peut représenter le commerce électronique et inquiet des freins que risque d'y mettre toute réglementation trop restrictive, le gouvernement du Canada a commencé à élaborer, dans la deuxième moitié des années 90, des stratégies et politiques portant sur des considérations commerciales, juridiques, technologiques et sociales reliées au commerce électronique et visant à répondre aux préoccupations en matière de protection de la vie privée suscitées par ce marché.[24] En 1994, le Président de la chambre des communes, Gilbert Parent, lors du discours du trône, annonçait que le gouvernement allait mettre en œuvre une stratégie canadienne concernant l'autoroute de l'information.[25] Au mois d'avril de la même année, le gouvernement fédéral formait le Comité consultatif sur l'autoroute de l'information (CCAI). Le mandat de ce Comité consistait à « *déterminer comment le mieux aménager et utiliser l'autoroute de l'information au bénéfice culturel, économique et social de tous les Canadiens (…) et comment en arriver à un équilibre approprié entre la concurrence et la réglementation.*»[26]

Parallèlement à l'engagement du gouvernement d'offrir un cadre réglementaire permettant une protection adéquate des internautes et de leur vie privée, des normes volontaires issues d'un processus de consultation entre le secteur privé, le gouvernement et les groupes de défense des droits des consommateurs et de la vie privée verront le jour. Élaborées sous la gouverne de l'Association canadienne de normalisation (CSA), ces normes volontaires s'appuient sur dix principes qui visent à établir un équilibre entre, d'une part, le droit à la vie privée des individus et, d'autre part les besoins en matière de renseignements des entreprises privées. Considéré comme une norme volontaire, le Code type de la CSA a été conçu pour servir de modèle que les entreprises peuvent adopter et modifier selon leur situation particulière.

En 1996, la Conférence pour l'harmonisation des lois au Canada (CHLC), un organisme indépendant qui travaille à l'uniformisation des lois à travers le pays, a recommandé

---

[21] Commissaire à la protection de la vie privée du Canada, Rapport annuel 1984-1985, Ottawa, Approvisionnements et Services Canada, 1985.

[22] *Loi sur la protection des renseignements personnels* L.R., 1985, ch. P-21. Cette loi vise la protection des renseignements personnels relevant des institutions fédérales. Le poste de Commissaire à la protection de la vie privée a été créé en vertu de l'article 53 de cette loi.

[23] Commissaire à la protection de la vie privée du Canada, Rapport annuel 1988-1989, Ottawa, Approvisionnements et Services Canada, 1989; Rapport annuel 1989-1990, Ottawa, Approvisionnements et Services Canada, 1990.

[24] SMITH, Margaret, *La protection des renseignements personnels et le commerce électronique : L'État de la question*, 31 mai 2000, [En ligne] http://dsp-psd.tpsgc.gc.ca/Collection-R/LoPBdP/BP/prb0005-f.htm#(94)txt (consulté le 29 janvier 2007).

[25] Débat de la Chambre des communes, volume 133, no. 002, 1ere session, 35e Législature, p. 1547.

[26] Santé Canada, Comité consultatif sur l'autoroute de l'information - *infostructure canadienne de la santé* [En ligne] http://www.hc-sc.gc.ca/hcs-sss/ehealth-esante/infostructure/ihac_ccai_f.html (consulté le 20 avril 2007).

l'élaboration d'une loi régissant la protection des renseignements personnels dans le secteur privé. Les objectifs de cette loi devaient être les suivants :

> *« ◆ Traiter également toutes les entreprises et toutes les organisations non gouvernementales, peu importe leur taille ou leur type d'activités;*
> *◆ Traiter toutes les données personnelles sur un pied d'égalité, abstraction faite de leur degré de sensibilité;*
> *◆ S'appuyer sur des principes établis, comme ceux énoncés dans le Code type sur la protection des renseignements personnels de l'Association canadienne de normalisation;*
> *◆ Établir un mécanisme administratif pour superviser la mise en œuvre de la loi (comme les commissions existantes de protection des données);*
> *◆ Investir la commission de protection des données du pouvoir de sensibiliser le public au sujet de la protection des données dans le secteur privé;*
> *◆ Pourvoir à des enquêtes sur les plaintes et à une médiation, mais seulement après l'application du processus de traitement des plaintes de l'entreprise (à supposer qu'il y en ait un et qu'il fixe des délais clairs et brefs), tout en prévoyant que, dans des cas exceptionnels, on puisse adresser une plainte directement à la commission;*
> *◆ Permettre à la commission de publier les noms des entreprises qui ne respectent pas la loi sur la protection des données; et*
> *◆ Prévoir des mesures dans les cas d'infraction à la loi. »*[27]

En 1996, dans un rapport intitulé *La société canadienne à l'ère de l'information*, Industrie Canada déclarait qu'il fallait reconnaître le droit à la vie privée sur le plan législatif, particulièrement en ce qui concerne la conservation de renseignements personnels dans des bases de données électroniques.[28] La même année, les ministres fédéraux de l'Industrie et de la Justice annonçaient que le gouvernement fédéral allait légiférer afin de protéger la vie privée.

En janvier 1998, Industrie Canada et le ministère de la Justice ont rendu public un document de travail sur la protection des renseignements personnels, qui soulignait notamment que la confiance des consommateurs était essentielle à la croissance de l'économie de l'information. D'après le document, « *une loi qui définit un ensemble de règles communes pour la protection des renseignements personnels aidera à renforcer cette confiance et à instaurer un système équitable où l'usage abusif des renseignements personnels ne pourra conférer un avantage concurrentiel.* »[29] Selon Industrie Canada, l'objectif avoué de l'instauration d'un tel cadre législatif visant la protection des renseignements personnels tenait d'abord et avant tout à des préoccupations commerciales : « *Afin de créer les conditions favorables à la croissance du commerce électronique au Canada, le gouvernement s'est engagé à élaborer un cadre législatif destiné à protéger les renseignements personnels dans le secteur privé, sans pour autant nuire à la circulation des informations, atout dont le pays a absolument besoin pour soutenir la concurrence sur le marché mondial.* »[30] Beaucoup moins élaboré que le document du CHLC, le document de travail d'Industrie Canada mentionne qu'afin d'atteindre cet objectif, une loi fédérale est nécessaire et qu'une telle loi devrait tenir compte des quatre éléments clés suivants :

---

[27] SMITH, Margareth *Op. cit*, note 25.
[28] Canada, ministère de l'Industrie, *La société canadienne à l'ère de l'information : Pour entrer de plain-pied dans le XXIe siècle*, Ottawa, 1996, p. 25.
[29] Canada, Industrie Canada, Justice Canada, Groupe de travail sur le commerce électronique. *La protection des renseignements personnels : Pour une économie et une société de l'information au Canada*, Ottawa, janvier 1998, p. 6.
[30] *Ibid.*

- Des obligations fondées sur des pratiques équitables de traitement de l'information;
- Des dispositions administratives pour un organe de surveillance afin de garantir la reddition de comptes;
- Des attributions pour des autorités de supervision et des tribunaux;
- Des pouvoirs et responsabilités qui favoriseront l'information du public et garantiront un réel respect des obligations.[31]

En vue de renforcer la confiance des consommateurs, le Canada visait ainsi, par l'adoption de normes et lois visant la protection des renseignements personnels, à mettre en place des mécanismes susceptibles d'éviter les fraudes et abus qui peuvent résulter de la cueillette et de l'utilisation anarchique de ce type de renseignements. Vu, toutefois, l'importance de la collecte et de l'utilisation des renseignements personnels dans le cadre d'activités commerciales, la législation qui visait prioritairement à faciliter le commerce se devait de trouver, par le biais d'un encadrement qui respecterait les éléments clés, le juste équilibre entre des normes qui seraient suffisantes pour assurer la confiance du public face à la protection des renseignements et une réglementation qui n'aurait pas pour effet de constituer une barrière au commerce et à la libre circulation des informations.

Organisations et activités commerciales

Le 1 janvier 2004, la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDÉ) entrait intégralement en vigueur.[32] Cette Loi s'applique à toute « *organisation à l'égard des renseignements personnels (…) qu'elle recueille, utilise ou communique dans le cadre d'activités commerciales (…)* »[33] Ainsi, à l'exception des activités des entreprises non fédérales oeuvrant dans une province ayant adopté une loi essentiellement similaire, les activités commerciales exercées sur le territoire canadien par toute organisation du secteur privé sont encadrées par cette Loi.

Le terme « organisation » contenu dans la loi fait référence non seulement aux associations, sociétés de personnes, personnes et organisations syndicales, mais aussi à un individu, s'il est engagé dans une activité commerciale.[34] Par activité commerciale, la LPRPDÉ entend « *Toute activité régulière ainsi que tout acte isolé qui revêtent un caractère commercial de par leur nature, y compris la vente, le troc ou la location de listes de donneurs, d'adhésion ou de collecte de fonds* ». Dans une fiche d'information datée de 2004, le Commissariat à la protection de la vie privée expliquait comme suit l'application de la LPRPDÉ aux œuvres de charité et aux organismes sans but lucratif.

---

[31] *Ibid*., p. 11.

[32] Commissariat à la protection de la vie privée, Fiche d'information, *Se conformer à la Loi sur la protection des renseignements personnels et les documents électroniques,* « L'entrée en vigueur de la *LPRPDÉ* s'est faite par étape. D'abord, à compter de janvier 2001, la Loi s'est appliquée à la collecte, à l'utilisation et à la communication de renseignements personnels concernant des clients et des employé(e)s par des organisations de compétence fédérale dans le cadre de leurs activités commerciales. Elle visait également les renseignements vendus au-delà des frontières provinciales et territoriales. Ensuite, en janvier 2002, le champ d'application de la Loi s'est étendu aux renseignements médicaux personnels recueillis, utilisés ou communiqués par ces organisations.
À compter du 1er janvier 2004, l'application de la *LPRPDÉ* est de portée générale — c'est-à-dire que la Loi vise tous les renseignements recueillis, utilisés ou communiqués par toutes les organisations du secteur privé dans le cadre de leurs activités commerciales, sauf dans les provinces qui auront, d'ici là, adopté des lois réputées être similaires à la loi fédérale. »

[33] LPRPDÉ art.4.

[34] LPRPDÉ art.2(1).

> *« La présence d'activités commerciales constitue l'élément le plus important afin de déterminer si un organisme est ou non assujetti à la Loi. (…)*
>
> *Le fait qu'un organisme soit ou non sans but lucratif ne permet pas de déterminer de façon concluante la mesure dans laquelle la Loi s'applique. Les expressions « sans but lucratif » ou « à but non lucratif » sont des expressions techniques qui ne figurent pas dans la LPRPDÉ. En fait, ce n'est pas parce qu'un organisme détient le statut d'organisme sans but lucratif qu'il est automatiquement dispensé des obligations découlant de la Loi.*
>
> *La plupart des organismes sans but lucratif ne sont pas assujettis à la Loi parce qu'ils n'exercent pas d'activités commerciales. C'est généralement le cas pour ce qui est de la majorité des œuvres de charité, des associations de hockey mineur, des clubs, des groupes communautaires et des organismes de défense des droits. La collecte de droits d'adhésion, l'organisation d'activités de club, l'établissement d'une liste de noms et d'adresses de membres et l'envoi de bulletins de nouvelles n'entrent pas dans la définition d'activités commerciales, et il en est de même pour les collectes de fonds. (…)*
>
> *Selon la définition contenue dans la Loi, il est évident que la vente, le troc ou la location de listes d'adhésion ou de donneurs constituent une activité commerciale. Par conséquent, il faut obtenir un consentement pour communiquer cette information.»* [35]

Le Commissariat à la protection de la vie privée du Canada précisant qu'il n'est pas nécessaire que l'argent soit en jeu pour qu'une activité soit de nature commerciale, il faut bien avouer qu'une incertitude persiste quant aux caractéristiques précises qui permettraient de déterminer qu'une activité est considérée comme une activité commerciale au sens de la LPRPDÉ. Un échange de service en contrepartie d'une somme d'argent ne serait, ainsi, pas nécessairement non plus une activité commerciale, comme en fait foi une décision rendue en 2006 par la Commissaire adjointe, qui a considéré qu'une école privée ne menait aucune activité commerciale au sens de la loi[36] et que, comme l'école n'était pas soumise à la LPRPDÉ, la Commissaire n'avait pas compétence pour enquêter. La Commissaire adjointe base sa décision sur l'examen de l'activité principale de l'établissement, qui est l'éducation, et sur le fait que les objectifs de l'organisme ne sont pas de procurer un profit aux propriétaires de l'établissement.

Ces conclusions basées sur l'activité principale et les objectifs de l'organisme, plutôt que sur le caractère propre de l'activité, qui détermineraient l'assujettissement de l'organisme à la LPRPDÉ semblent difficilement conciliables avec la lettre de la loi et avec l'interprétation offerte par le Commissariat en 2004 et mentionnée plus haut. Ainsi, si la définition de ce que constitue une « activité commerciale » laisse place à interprétation et que l'état actuel du droit et de la

---

[35] Commissariat à la protection de la vie privée du Canada. *Fiche d'information : Application de la Loi sur la protection des renseignements personnels et les documents électroniques aux œuvres de charité et aux organismes sans but lucratif*. [En ligne] http://www.privcom.gc.ca/fs-fi/02_05_d_19_f.asp (consulté le 2 mai 2007).

[36] Commissariat à la protection de la vie privée du Canada. Conclusions de la Commissaire - *Résumé de conclusions d'enquête de #345: Une école privée non assujettie à la LPRPDÉ* (Le 5 juillet 2006). [En ligne] http://www.privcom.gc.ca/cf-dc/2006/345_20060705_f.asp (consulté le 2 juin 2007). On soulignera le fait que la publication par le Commissariat à la protection de la vie privée de simples résumés plutôt que de décisions qui présenteraient de façon plus élaborée les motifs et les arguments qui les appuient ne facilite par l'interprétation par le biais de ces décisions.

jurisprudence ne nous permet pas d'établir avec certitude les paramètres juridiques de ce terme, la détermination de l'assujettissement à la loi fédérale de certains organismes pourrait aussi être incertaine.

Renseignements personnels

Quant à la définition de ce que constituent des « renseignements personnels » la LPRPDÉ stipule qu'il s'agit de : « *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* »[37]. Ces renseignements « *peuvent être factuels ou subjectifs, consignés ou non, au sujet d'une personne identifiable, quelle que soit la forme sous laquelle elle est présentée, c'est-à-dire : son âge, son nom, son numéro d'identification, son revenu, son origine ethnique ou son groupe sanguin ; ses opinions, les évaluations à son sujet, les commentaires à son propos, les mesures disciplinaires prises à son égard et son état civil; ses dossiers d'employé, son dossier de crédit, son dossier de prêts, son dossier médical, l'existence d'un conflit entre cette personne et un commerçant, ses intentions (par exemple, faire l'acquisition de biens ou de services, ou changer d'emploi)* »[38].

Principes

On notera que le code élaboré par la CSA a été incorporé dans la LPRPDÉ et représente le corps de la législation fédérale. Le code définit les obligations et responsabilités des organisations concernant la cueillette, l'utilisation et la communication de renseignements personnels. Les dix principes qu'on y retrouve, reproduits et détaillés ci-dessous, constituent les principales obligations des entreprises et organisations relativement au traitement des renseignements personnels.

Les principales règles énoncées dans la LPRPDÉ sont les suivantes :

1. Responsabilité : Une organisation est responsable des renseignements personnels dont elle a la gestion et doit désigner une ou des personnes qui devront s'assurer du respect des principes de la LPRPDÉ. Les coordonnées de ces personnes doivent être accessibles au public et l'agent responsable de la protection de la vie privée doit posséder l'autorité nécessaire pour remplir ses fonctions et ses obligations ;
2. Détermination des fins de la collecte des renseignements : Les fins auxquelles des renseignements personnels sont recueillis doivent être déterminées par l'organisation avant la collecte ou au moment de celle-ci. De même, l'utilisation et/ou la diffusion qui en seront faites doivent être portées à la connaissance du consommateur ;
3. Consentement : Toute personne doit être informée de toute collecte, utilisation ou communication de renseignements personnels qui la concernent et y consentir (sauf dans certains cas spécifiques[39]). Le consentement doit être obtenu avant et au moment de la collecte, et une autre fois si une nouvelle utilisation des renseignements personnels est envisagée, et ce, peu importe que les renseignements aient été obtenus directement de la personne concernée ou d'une tierce partie à moins qu'il ne soit pas approprié d'obtenir tel consentement ;

[37] LPRPDÉ art.2
[38] Commissariat à la protection de la vie privée. Fiche d'information, *Se conformer à* la *Loi sur la protection des renseignements personnels et les documents électroniques.* [En ligne] http://www.privcom.gc.ca/fs-fi/02_05_d_16_f.asp (consulté le 3 mai 2007).
[39] LPRPDÉ art.7, LPRPSP, art. 18 à 25 ; PIPA Alberta art. 14, 17, 20 ; Pipa Colombie-Britannique art. 12, 15, 18. et voir infra les renseignements personnels à caractère public.

4. Limitation de la collecte : L'organisation ne peut recueillir que les renseignements personnels nécessaires aux fins déterminées et doit procéder de façon honnête et licite. Il est interdit de recueillir plus de renseignements que nécessaire. Un individu pourra de plein droit refuser de divulguer des informations personnelles qui ne seraient pas nécessaires à la réalisation de la transaction[40];
5. Limitation de l'utilisation, de la communication et de la conservation : 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 la réalisation des fins déterminées ;
6. Exactitude : Les renseignements personnels doivent être aussi exacts, complets et à jour que l'exigent les fins auxquelles ils sont destinés. Les organisations sont tenues de faire tous les efforts nécessaires pour éliminer la possibilité d'utiliser des renseignements personnels inexacts ou périmés ;
7. Mesures de sécurité : Les renseignements personnels doivent être protégés au moyen de mesures de sécurité correspondant à leur degré de sensibilité. Ces mesures comprennent non seulement la sécurité du réseau pour préserver l'intégrité des données contre l'intrusion des pirates informaticiens ou autres menaces du même type, mais aussi la sécurité physique telle que des portes verrouillées et l'accès limité aux individus concernés ;
8. Transparence : Une organisation doit faire en sorte que des renseignements précis sur ses politiques et ses pratiques concernant la gestion des renseignements personnels soient facilement accessibles et compréhensibles ;
9. Accès aux renseignements personnels : Une organisation doit informer toute personne qui en fait la demande de l'existence de renseignements personnels qui la concernent, de l'usage qui en est fait et de l'éventuelle communication de ces renseignements à des tiers et doit lui permettre de consulter ces renseignements. Il doit aussi être possible de contester l'exactitude et l'intégralité des renseignements et d'y faire apporter les corrections appropriées. Par contre, l'accès pourra être refusé si certains de ces renseignements contiennent des informations confidentielles ou des renseignements concernant d'autres personnes ;
10. Possibilité de porter plainte à l'égard du non-respect des principes : Toute personne doit être en mesure de se plaindre du non-respect des principes énoncés ci-dessus en communiquant avec le ou les responsables au sein de l'organisation concernée. Ainsi, les organisations doivent prévoir des procédures de plaintes simples et accessibles, faire enquête sur les plaintes reçues et, lorsque la plainte s'avère fondée, apporter des changements nécessaires aux pratiques et politiques de traitement des informations.

[40] Le Commissaire à la protection de la vie privée a ainsi jugé fondée la plainte d'un demandeur qui s'opposait à une vérification de son crédit comme condition d'ouverture d'un compte en banque. Commissariat à la protection de la vie privée du Canada. Conclusions de la Commissaire - *Résumé de conclusions d'enquête en vertu de la LPRPDÉ #40 : Un demandeur s'oppose à une vérification de son crédit comme condition d'ouverture d'un compte bancaire*. (12 mars 2002) [En ligne] http://www.privcom.gc.ca/cf-dc/2002/cf-dc_020312_f.asp (consulté le 3 mai 2007)

Le contexte provincial

Dès les années soixante-dix, le Québec fait figure de précurseur en matière de protection de la vie privée en adoptant plusieurs lois visant à encadrer l'utilisation de certains renseignements personnels et leur accès. La première de ces initiatives fut l'adoption de la *Loi sur la protection du consommateur*[41], qui assurait à toute personne le droit d'accès à son dossier de crédit. Par la suite, d'autres lois, comme le Code des professions[42], ont consacré des principes aujourd'hui considérés fondamentaux, comme le secret professionnel et le caractère confidentiel des renseignements personnels. C'est dans ce contexte que le Québec adoptera, en 1994, la *Loi sur la protection des renseignements personnels dans le secteur privé* (LPRPSP). À ce jour, deux autres provinces, l'Alberta et la Colombie-Britannique ont adopté dans leur province respective une loi semblable, toutes deux titrées *Personal Information Protection Act*, (PIPA) et entrées en vigueur, pour les deux provinces, le 1er janvier 2004. Ces lois provinciales ont été considérées comme des lois essentiellement similaires à la loi fédérale, ce qui signifie qu'elles s'appliquent sur les territoires respectifs des provinces, en lieu et place de la LPRPDÉ, aux activités intraprovinciales des organisations du secteur privé qui ne sont pas de compétence fédérale exclusive[43].

Le Québec sera, par le biais de la LPRPSP, la première entité en l'Amérique du Nord à légiférer sur la collecte, l'utilisation, la communication et la conservation des renseignements personnels dans le secteur privé. Cette Loi s'appliquera aux renseignements personnels « *qu'une personne recueille, détient, utilise ou communique à des tiers à l'occasion de l'exploitation d'une entreprise* »[44] dans la province de Québec.

Renseignements personnels

La LPRPSP définit, à son article 2, le terme « renseignement personnel » comme étant « *tout renseignement qui concerne une personne physique et permet de l'identifier.* » La jurisprudence de la Commission d'accès à l'information vient compléter cette définition, précisant que le renseignement visé est celui qui « *cerne les caractéristiques de l'individu : il se définit par rapport à cette personne et à celle-là seulement. C'est une donnée objective qui fonde son existence sur un être en chair et en os*»[45]. Un renseignement personnel, au sens de la LPRSP permet donc de caractériser et de distinguer une personne d'une autre. Les caractéristiques peuvent être partielles, mais substantielles : son âge, le montant de sa retraite, des recommandations à son sujet, etc[46].

Organisations

« Entreprise » s'entend au sens, assez large, que lui donne le Code civil du Québec à l'article 1525, soit: «*l'exercice par une ou plusieurs personnes, d'une activité économique organisée,*

[41] L.R.Q., chapitre P-40.1.
[42] L.R.Q., chapitre C-26.
[43] Commissariat à la protection de la vie privée, mandat et mission du CPVP, [En ligne] http://www.privcom.gc.ca/aboutUs/index_f.asp (consulté le 1 juin 2007).
[44] LPRPSP, art.1.
[45] Commission d'accès à l'information, Claude Stebenne c. Assurance-vie Desjardins, décision du 16 décembre 1994, P-0020, p. 5, [En ligne] http://www.cai.gouv.qc.ca/07_decisions_de_la_cai/01_pdf/jurisprudence/940366de.pdf (consulté le 20 mai 2007).
[46] *Ibid*.

qu'elle soit ou non à caractère commercial, consistant dans la production ou la réalisation de biens, leur administration ou leur aliénation, ou dans la prestation de services »[47].

Les deux autres lois provinciales s'appliquent également, sauf exceptions, à toute organisation, relativement aux renseignements personnels qu'elle recueille, utilise ou communique à des tiers.

La PIPA albertaine définit le terme organisation pour inclure les corporations, les associations non incorporées, les syndicats, les partenariats et les individus qui mènent des activités commerciales.[48] Quant à la notion de «renseignement personnel», elle la définit comme constituant un renseignement relatif à une personne identifiable.[49] La Loi précise que ne sont toutefois pas inclus les renseignements qui permettent de contacter un individu à une place d'affaires, pourvut qu'ils ne soient utilisés qu'à ces fins.[50]

La PIPA de la Colombie-Britannique s'applique aussi, sauf exception, à toute organisation, la définition incluant nommément les fondations et les organismes à but non lucratif. Un renseignement personnel est ici aussi une information relative à un individu identifiable. La Loi précise que ne sont pas inclus les renseignements qui permettent de contacter un individu à une place d'affaires, incluant son nom, son titre, l'adresse et les numéros de téléphone et de fax de la place d'affaires de même que son adresse de courriel[51].

Les différences entre la législation fédérale et les législations provinciales

Organismes visés

On notera une différence dans la portée des lois provinciales et de la LPRPDÉ. Comme nous l'avons mentionné précédemment, la loi fédérale s'applique aux organisations exerçant des activités commerciales, excluant ainsi, à toutes fins pratiques, les activités des organismes à but non lucratif et des œuvres de charité. Les lois provinciales, quant à elles, ont une portée plus large et s'appliquent aussi à de telles organisations. Si la loi de la Colombie-Britannique, par exemple, mentionne les organismes à but non lucratif dans sa définition d'«organisation», la Loi albertaine, pour sa part, prévoit que les organismes à but non lucratif seront visés pour ce qui est des renseignements personnels recueillis, utilisés ou divulgués dans le cadre d'activités commerciales[52]. On soulignera aussi une différence quant au traitement des renseignements dits à caractère public.

---

[47] *Code civil du Québec*, L.Q., 1991, c. 64, article 1525 – Le texte intégral de la Loi peut être consulté [En ligne] sur le site Internet de l'Institut canadien d'information juridique (IIJCan), [En ligne] http://www.canlii.org/qc/legis/loi/ccq/20050513/tout.html (page consultée le 10 juillet 2005).
[48] *PIPA* Alberta, art. 1(i).
[49] *PIPA* Alberta, art. 1(k).
[50] *PIPA* Alberta, art. 4(3)d.
[51] *PIPA* Colombie-Britannique, art 1 et Centre de ressources Ogilvy Renaud, « L'adresse électronique professionnelle : renseignement personnel ou information à caractère public ? » (2005) [En ligne] http://www.ogilvyrenault.com/fr/ResourceCenter/ResourceCenterDetails.aspx?id=897&pId=43
[52] *PIPA* Alberta, art. 56(2). En contraste avec la décision de la Commissaire adjointe citée plus haut (LPRPDÉ #345, *Op. cit.,* 30), on soulignera que la Loi albertaine prévoit expressément, à son article 56 (1), l'assujettissement des écoles privées.

Renseignements personnels à caractère public

Alors qu'en Colombie-Britannique et au Québec, les règles relatives à la collecte, la détention, l'utilisation et la communication ne s'appliquent pas aux renseignements personnels qui ont un caractère public (information personnelle disponible dans l'annuaire téléphonique ou diffusée par les télévisions ou les journaux, etc.)[53], les lois albertaine et fédérale restreignent l'exemption à une utilisation qui serait faite pour les seules fins pour lesquelles les renseignements ont été rendus publics[54].

Ces différences entre les législations provinciales ont pour effet de soumettre les entreprises, selon les provinces, à des règles différentes. Elles ont aussi pour effet, si les activités commerciales ont lieu entre différentes provinces, de créer une incertitude quant aux critères et définitions applicables.

Organismes chargés de l'application de la loi

Alors qu'au niveau fédéral, c'est le Commissariat à la protection de la vie privée qui est chargé d'assurer le respect de la LPRPDÉ, les provinces ont confié l'application de leur loi à un organe quasi judiciaire, soit l'Office of the Information and Privacy Commissioner en Alberta et en Colombie-Britannique et la Commission d'accès à l'information pour le Québec. La différence entre les pouvoirs qui ont été octroyés à ces organismes a un impact direct sur l'administration des lois et le traitement des plaintes.

Le Commissariat à la protection de la vie privée s'est vu confier par le fédéral un rôle d'ombudsman, soit un rôle de conciliation et de médiation. Les décisions du Commissaire ne sont que des recommandations et n'ont aucune force contraignante. Si, suite à la décision du Commissaire, un plaignant se considère toujours lésé, il lui sera possible, en vertu de l'article 14 de la LPRPDÉ, de porter sa cause devant la Cour fédérale. Il pourrait notamment demander à la Cour de rendre obligatoire la décision du Commissaire ou, dans le cas d'une décision jugée non fondée par le Commissaire, de rendre une nouvelle décision, suite à l'examen des pratiques de l'organisation contre laquelle la plainte initiale a été déposée. Le rôle de la Cour ne sera pas d'examiner le rapport du Commissaire, mais bien de poser un regard nouveau sur les preuves avancées par les deux parties[55]. Si la Cour accueille la requête, elle pourra ordonner à l'organisation de revoir ses pratiques et/ou ordonner le paiement au requérant de dommages-intérêts. On soulèvera que cette procédure en deux temps, d'abord, devant le Commissariat puis devant la Cour fédérale, a pour effet, en plus de compliquer le processus, de rendre public un débat auquel les requérants, puisqu'il porte justement sur une violation de leur vie privée ou de confidentialité, pourraient préférer conserver le caractère confidentiel.[56] Très peu de plaignants se sont à ce jour prévalus de ce droit d'appel[57]. On soulignera que la Cour fédérale

[53] *Personal Information Protection Act*. B.C. Reg. 473/2003 art.6 (le règlement prévoit que ces renseignements sont exclus seulement si l'individu a eu l'occasion de refuser son inclusion dans le registre public) ; LPRPDÉ art.1.
[54] *Personal Information Protection Act Regulation*, Alta. Reg. 366/2003; art.7; *LPRPDÉ* art. 7 et 26.
[55] Commissariat à la protection de la vie privée. Fiche d'information. *Les demandes d'audience à la cour en vertu de la LPRPDÉ*. [En ligne] http://www.privcom.gc.ca/fs-fi/02_05_d_31_f.asp (consulté le 10 mai 2007).
[56] LAWFORD, John. *Consumer privacy Under PIPEDA : How Are We Doing ?* (2004) Public Interest Advocacy Center (PIAC). [En ligne] http://www.piac.ca/files/pipedareviewfinal.pdf (consulté le 2 juin 2007).
[57] Sur plus de 1400 plaintes reçues par le Commissaire à la protection de la vie privée, seulement 9 ont été commentées par la Cour fédérale (KERR, Ian « *Submission to the House of Commons Standing*

n'a jamais, jusqu'à présent, octroyé de dommages-intérêts à un plaignant dans le cadre d'un dossier portant sur des questions de vie privée.[58]

Pour ce qui est des organismes provinciaux, la Commission d'accès à l'information, par exemple, pourra «*rendre toute ordonnance qu'elle estime propre à sauvegarder les droits des parties et décider de toute question de fait ou de droit*.»[59] Elle pourra également ordonner à une entreprise de «*donner communication, de rectifier un renseignement ou de s'abstenir de le faire*»[60] et ses décisions sont exécutoires dans les trente jours. La PIPA de l'Alberta et celle de la Colombie-Britannique octroient également au Commissaire de la province dans laquelle elles s'appliquent de tels pouvoirs.[61] La loi de la Colombie-Britannique, tout comme la loi québécoise donne trente jours à l'entreprise pour se conformer à la décision de la Commissaire, alors que la loi albertaine étend ce délai à cinquante jours.[62]

Les différences dans les rôles conférés aux organes provinciaux et fédéral se reflètent aussi dans les pouvoirs de surveillance et d'enquête qui leur ont été confiés. Alors qu'en vertu des lois provinciales le Commissaire peut faire enquête sur n'importe quelle organisation concernant sa politique de gestion des renseignements personnels[63], la loi fédérale stipule pour sa part que le Commissaire doit, avant de procéder à la vérification des pratiques de l'entreprise, avoir « *des motifs raisonnables de croire que [l'organisation] a contrevenu à l'une des dispositions de la section 1 ou n'a pas mis en œuvre une recommandation énoncée dans l'annexe 1 (…)* »[64]. Ainsi, le Commissaire qui agit en vertu de la LPRPDÉ n'a pas le pouvoir d'effectuer de sa propre initiative des enquêtes aléatoires afin de vérifier les politiques et les comportements des organisations relativement aux renseignements personnels qu'ils sont susceptibles de recueillir. Cette exigence de «motifs raisonnables» peut s'avérer un obstacle à l'application et au respect de la loi, attendu qu'elle permet une contestation par l'entreprise visée d'une vérification que le Commissaire voudrait effectuer.[65]

Committee on Access to Information, Privacy and Ethics on the Personal Information Protection and Electronic Documents Acts (PIPEDA) » [En ligne] http://www.cippic.ca/en/projects-cases/privacy/submissions/IK_PIPEDA_Review_Submission_(final)_FORMATTED.pdf p. 15, (consulté le 20 avril 2007).

[58] *Ibid.*

[59] *LPRPSP*, art.55

[60] *Ibid*.

[61] *PIPA* Alberta et Colombie-Britannique art.52.

[62] *PIPA* Alberta art.54 ; PIPA Colombie-Britannique art.53.

[63] *LPRPSP*, art. 80.2 à 81 ; *PIPA* Alberta et Colombie-Britannique art. 36 à 44.

[64] *LPRPDÉ*, art. 18(1).

[65] C'est ce qu'a fait Equifax qui, suite à une enquête amorcée par le Commissaire, a intenté une action en contrôle judiciaire visant à faire abandonner cette vérification, au motif que le Commissaire n'avait pas de « motifs raisonnables » d'intenter une telle action et ce, malgré le fait que quatre plaintes individuelles avaient été déposées à l'Office de la protection du consommateur concernant les pratiques d'Équifax. Canadian Internet Policy and Public Interest Clinic (CIPPIC) « *Submission to the House of Commons Standing Committee on Access to Information, Privacy and Ethics on the Personnal Information Protection and Electronic Document Act (PIPEDA)* » 28 novembre 2006, pp. 8-9. Par contre, le 14 mars 2007, Équifax a conclu une entente avec le Commissariat à la protection de la vie privée et s'est désistée de la contestation judiciaire qu'elle avait déposée en Cour fédérale. (Commissariat à la protection de la vie privée , Communiqué*, La Commissaire à la protection de la vie privée collabore avec Equifax au parachèvement d'une vérification*, 16 mars 2007, [En ligne] http://www.privcom.gc.ca/media/nr-c/2007/nr-c_070316_f.asp (consulté le 18 mars 2007).

Dispositions pénales

Les législations provinciales prévoient, en cas de contravention à certaines de leurs dispositions ou en cas d'entrave aux enquêtes menées en vertu de ces lois, que les organismes chargés de l'application de la loi peuvent imposer des amendes aux contrevenants. Dans ce cas, autant la personne morale que le dirigeant, l'administrateur ou le représentant de cette personne morale pourront se voir imposer une amende.[66] Les lois provinciales ne prévoient pas, par contre, l'octroi de dommages-intérêts au plaignant par le Commissaire. En vue d'obtenir le paiement de tels dommages, le plaignant devra procéder en vertu des règles générales de droit de sa province[67].

Aucune disposition pénale n'a été incorporée à la LPRPDÉ. Ni le Commissariat à la protection de la vie privée ni la Cour fédérale n'ont donc le pouvoir d'imposer aux contrevenants quelque amende ou pénalité que ce soit. Comme nous l'avons vu plus haut, la Cour fédérale, lorsqu'elle rend une décision en vertu de la LPRPDÉ, a le pouvoir d'ordonner le paiement au requérant de dommages-intérêts.

Inclusion des adresses de courriel comme renseignements personnels

Mis à part les cas où l'adresse électronique d'une personne est composée de son nom, il ne semble pas qu'une adresse de courriel puisse permettre d'identifier une personne ou être associée à une personne identifiable. L'adresse électronique d'un individu fait-elle partie des renseignements visés par les lois sur la protection des renseignements personnels ?

La Commissaire adjointe, dans une décision rendue en 2005, a répondu par l'affirmative à cette question, en ce qui a trait à tout le moins aux adresses électroniques liées au travail. Dans cette affaire, des courriels non sollicités ont été expédiés, aux fins de marketing, à des adresses électroniques qui avaient été cueillies dans des répertoires auxquels le public avait accès et dans un répertoire auquel n'avaient accès que les membres d'une association particulière. S'agissant en l'espèce d'une adresse électronique professionnelle et non personnelle, la Commissaire conclut que :

> *« L'article de la Loi énonçant les définitions qui lui sont applicables prévoit les types de renseignements qui ne sont pas protégés par la Loi, plus particulièrement les nom et titre d'un employé d'une organisation et les adresse et numéro de téléphone de son lieu de travail. Puisque l'article 2 ne précise pas les adresses de courriel d'affaires, la Commissaire adjointe a conclu qu'il s'agissait des renseignements personnels d'un individu aux fins de la Loi. »68*

Si une adresse électronique professionnelle constitue un renseignement personnel, a fortiori, une adresse électronique personnelle devra-t-elle être considérée comme telle en vertu de la LPRPDÉ. La Commissaire adjointe avait d'ailleurs précédemment reconnu comme fondée une autre plainte relative à une transmission d'adresses de courriel[69].

---

[66] *LPRPDÉ,* art.91 à 93 ; *PIPA* Alberta art. 59 ; *PIPA* Colombie-Britannique art.56.
[67] *PIPA* Alberta, art.60 ; *PIPA* Colombie-Britannique, art.57.
[68] Commissariat à la protection de la vie privée, Conclusions de la Commissaire - *Résumé de conclusions d'enquête en vertu de la LPRPDÉ #297*, *Courriels non sollicités pour fins de marketing*, 28 avril 2005. [En ligne] http://www.privcom.gc.ca/cf-dc/2005/297_050331_01_f.asp (consulté le 3 mai 2007).
[69] Commissariat à la protection de la vie privée, Conclusion de la Commissaire - *Résumé de conclusions d'enquêtes en vertu de la LPRPDÉ #277 : L'envoi collectif d'un message entraîne la communication des adresses électroniques des participants à un concours,* 2 septembre 2004. [En ligne] http://www.privcom.gc.ca/cf-dc/2004/cf-dc_040902_02_f.asp (consulté le 10 mai 2007).

Le site du Commissariat à la protection de la vie privée mentionne par ailleurs nommément les adresses de courriel comme faisant partie des renseignements personnels : «*Le courriel est un moyen commode et économique de communiquer. Votre adresse électronique ainsi que le contenu de vos messages personnels constituent des renseignements personnels.»*[70]

Comme nous l'avons vu plus tôt, les lois de l'Alberta et de la Colombie-Britannique ont inclus les adresses de courriel professionnelles dans la liste des renseignements qui ne sont pas protégés, la loi albertaine précisant que l'exemption ne s'applique que pour les utilisations conformes aux fins prévues par la diffusion ou l'affichage de ces renseignements[71].

Le fait que ces deux lois provinciales aient retenu une approche similaire à celle de la loi fédérale, excluant spécifiquement les renseignements professionnels de l'application de la loi, et le fait que les adresses de courriel aient été nommément mentionnées dans la liste des renseignements personnels, il y a fort à parier que les adresses de courriel personnelles seront aussi considérées en vertu de ces lois, comme constituant un renseignement personnel.

La loi québécoise, outre l'exclusion générale visant les renseignements à caractère public, ne prévoit pour sa part aucun régime particulier pour les coordonnées au travail. Faute de jurisprudence, on peut se demander si, en vertu du libellé de la loi québécoise, une adresse de courriel constitue un renseignement personnel, soit un renseignement « qui concerne une personne physique et permet de l'identifier». Il apparaît évident qu'une simple adresse de courriel pourra permettre d'individualiser son propriétaire si apparaissent dans cette adresse le nom de famille et le prénom de l'utilisateur. Une adresse anonyme pourrait poser un problème autre. Selon certains analystes, l'interprétation favorisée par le Commissariat à la protection de la vie privée pourrait *«avoir un impact sur l'interprétation de la loi québécoise, d'autant plus que le Commissaire fédéral à la vie privée a le pouvoir de consulter les autorités provinciales et de conclure des accords afin d'uniformiser les pratiques en matière de protection des renseignements personnels*. »[72]

---

70 Commissariat à la protection de la vie privée. Fiche d'information, Protégez vos renseignements personnels sur Internet. [En ligne] http://www.privcom.gc.ca/fs-fi/02_05_d_13_f.asp#003 (consulté le 15 mai 2007).

71 On rappellera que c'est à une limite semblable qu'est soumise l'exclusion visant les renseignements à caractère public dans les lois albertaine et fédérale, alors que cette limite ne s'applique pas en Colombie-Britannique et au Québec, en vertu desquelles les renseignements à caractère public ne sont pas protégés.

72 Centre de ressources Ogilvy Renaud. *Op. cit.*, note 52

CUEILLETTE DE RENSEIGNEMENTS PERSONNELS

Impact de la croissance du secteur des télécommunications

Les développements technologiques de ces dernières années et l'introduction de la fibre optique sur le marché ont permis de révolutionner l'univers des télécommunications. Ce développement a eu et continue d'avoir une incidence directe sur les possibilités relatives à la cueillette et l'utilisation de renseignements personnels et, par le fait même, sur la protection de la vie privée. En effet, internet, tel qu'on le conçoit aujourd'hui, était simplement inimaginable il y a 25 ans. Le premier serveur, apparu en 1990 et signalant la naissance du *World Wide Web (W.W.W.)* ne permettait de visiter que quelques sites internet, pour la plupart, américains.[73] À cette époque, la vitesse moyenne d'une connexion internet privée variait entre 2400 et 9600 bits/sec.[74] Avant les années 1990, le secteur des télécommunications se concentrait sur deux fonctions principales, soit le téléphone et la télécopie. Ce n'est que quelques années plus tard, avec l'implantation d'internet, que l'usage des télécommunications s'étendra à de multiples fonctions : lecture de journaux, achat de biens et services, consultation de documents, publication de petites annonces, paiements en ligne, etc. Avec l'augmentation de la vitesse des connexions, qui atteint couramment les 10Gbits/sec[75], avec la numérisation de l'information et de sa transmission, combinée à l'accroissement phénoménal de la puissance des processeurs[76] et de leur accessibilité au public, le potentiel informatique a augmenté de façon exponentielle. Puisqu'on estime que la puissance d'un ordinateur double tous les 18 mois et que pendant ce temps, les prix diminuent de moitié,[77] il est maintenant facile et abordable d'acquérir du matériel informatique performant, ce qui permet notamment de cueillir et d'emmagasiner une quantité impressionnante d'informations.

Ces développements informatiques ont entraîné des bouleversements dans la société moderne, qui est passée de l'ère industrielle à l'ère de l'information. La numérisation est appliquée à toutes les informations, y compris celles qui concernent directement les êtres humains, qui ont aujourd'hui une existence numérisée complexe, soit un ensemble d'informations qui donnent accès à de nombreuses sphères d'activités et de services : travail, santé, éducation, finance, loisirs, etc. Parmi ces informations qui permettent à un individu de s'identifier et qui sont maintenant amassées dans les banques de données informatisées, on retrouve des renseignements aussi divers que : numéros d'assurance sociale, d'assurance maladie, permis de conduire, folios, noms d'utilisateurs et mots de passe permettant l'accès à divers dossiers ou services, code permanent, adresse, date de naissance, numéro de téléphone, etc. Ces

[73] POULLET, Yves, Consultative Committee of the Convention for the Protection of Individuals with regard to automatic processing of personal data, « *Report on the Application of Data Protection Principles to the Worldwide Telecommunication Networks* » (2004) Strasbourg, Conseil de l'Europe, p. 6.
[74] *Ibid*., p. 7.
[75] *Ibid*. (En référence avec de l'équipement informatique moyen, des prototypes permettant évidemment d'atteindre des vitesses beaucoup plus grandes).
[76] *Ibid.,* En 1987, un ordinateur moyen avait un processeur de 8 MegaHertz (MHz) avec 640 Kilobytes (KB) de mémoire vive (RAM) et un disque dur de 20 megabytes. En 2004, un ordinateur moyen possède un processeur de 2.4 GHz (soit 300 fois la puissance de celui de 1987), 256 MB de mémoire vive (RAM) (soit 400 fois plus qu'en 1987) et un disque dur avec une capacité de 60 GB (soit 3000 fois la capacité de stockage d'informations).
[77] *Ibid.*

renseignements sont fort précieux pour ceux qui les détiennent, car ils permettent d'identifier et de connaître l'individu qu'ils concernent, au point même de permettre le vol d'identité.

Un accès aussi facile à ce lot d'informations permet d'entrer facilement et rapidement en communication avec un individu et se faire une idée de ses intérêts et activités. Conjugué à une capacité de stockage accrue et une facilité du traitement de l'information, cela a eu pour conséquence de donner une valeur marchande accrue à ces renseignements, auxquels les entreprises ont maintenant couramment recours afin de connaître les clients et consommateurs avec lesquels ils ont des relations d'affaires… ou avec lesquels elles désirent en avoir. Car, si les agents de renseignements personnels furent parmi les premiers à commercialiser les renseignements des individus, principalement en vue d'établir des dossiers de crédit, les renseignements qui sont aujourd'hui recueillis grâce, notamment, aux techniques informatiques sont beaucoup plus diversifiés et l'information qui peut en être tirée bien plus éloquente.

Afin d'analyser le fonctionnement du commerce d'informations personnelles, il convient d'étudier préalablement les méthodes qu'utilisent les entreprises pour recueillir des renseignements sur les consommateurs. Nous avons séparé ces différentes méthodes en deux catégories principales, soit la cueillette faite suite à la divulgation explicite par le consommateur de renseignements le concernant et la cueillette faite à son insu. Comme nous le verrons, ces différentes méthodes permettront aux entreprises d'obtenir une foule d'informations sur les individus. Avant d'examiner ces différentes méthodes, nous nous pencherons rapidement sur le type d'entreprises qui pratiquent la cueillette d'informations.

Organisations recueillant des renseignements personnels

Parmi les organisations qui recueillent le plus couramment des renseignements personnels, on relève notamment les divers services gouvernementaux, les organismes à but non lucratif, les entreprises commerciales et les agents de renseignements personnels, chacun procédant à cette cueillette pour des motifs et dans des buts différents et faisant des renseignements ainsi recueillis une utilisation différente : utilisations administratives, communication, divulgation d'information ou de publicités, marketing, commerce de renseignements personnels, etc.

Pour ce qui est du transfert de renseignements personnels, les gouvernements transmettent souvent d'une agence à l'autre les renseignements pertinents sur les contribuables, mais ne les divulguent généralement pas aux entreprises. Certaines agences gouvernementales dévoileront par contre certains renseignements généraux élaborés à partir des renseignements personnels recueillis auprès des individus (statistiques de revenu, de santé, etc.), renseignements qui seront par la suite utilisés par les entreprises pour orienter leurs stratégies commerciales. Il convient toutefois de préciser ici que les agences gouvernementales sont soumises à des lois de protection des renseignements personnels différentes, qui s'appliquent uniquement au secteur public, soit une loi fédérale s'appliquant aux organismes fédéraux[78] et des lois provinciales, chaque province ayant adopté sa propre loi régissant les organismes provinciaux[79].

[78] *Loi sur la protection des renseignements personnels dans le secteur public*, L.R., 1985, ch. P-21.
[79] Au Québec : *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels,* L.R.Q., chapitre A-2.1.

Les organismes à but non lucratif, pour leur part, procèderont plutôt à des échanges de leurs listes de donateurs ou loueront parfois ces listes à des courtiers en renseignements[80]. La Croix-Rouge canadienne, par exemple, reconnaît dans sa politique de protection des renseignements personnels avoir recours à de telles pratiques[81].

Les entreprises qui détiennent des renseignements personnels sur les consommateurs les ont généralement recueillis dans le cadre de leurs activités commerciales comme détaillants ou fournisseurs de services[82]. Si plusieurs entreprises conserveront ces renseignements exclusivement pour un usage interne, d'autres choisiront de les vendre, les louer ou les échanger à des fins commerciales, selon les pratiques de l'entreprise.

L'agent de renseignements personnels, quant à lui, a vu ses activités spécifiquement encadrées dans la LPRPSP qui le définit comme étant celui qui *« fait le commerce de constituer des dossiers sur autrui, de préparer et de communiquer à des tiers des rapports de crédit au sujet du caractère, de la réputation ou de la solvabilité des personnes concernées par ces dossiers*.»[83] L'agent de renseignement personnel a un statut particulier et doit obligatoirement être inscrit, au Québec, auprès de la Commission d'accès à l'information pour exercer ses activités, ce que nous étudierons un peu plus loin. L'Alberta et la Colombie-Britannique ont elles aussi prévu des dispositions spécifiques entourant la pratique des agences de renseignements personnels. La Colombie-Britannique a intégré dans sa PIPA diverses dispositions s'appliquant spécifiquement aux agences de renseignements personnels[84] alors que L'Alberta a plutôt choisi d'utiliser une loi distincte[85].

Les méthodes de cueillette

La cueillette directe

La collecte directe se résume en substance à la divulgation volontaire, par le consommateur, de renseignements personnels, lorsqu'il complète, par exemple, un formulaire ou une demande qui requièrent ce type de renseignements. On trouve de nombreux exemples de ces occasions de divulgation volontaire : abonnement à une revue ou un journal, achat de billets d'avion, achats à distance de biens ou services, etc. On remarquera quand même que, quoique cette divulgation soit volontaire, l'achat à distance oblige le consommateur à la divulgation d'informations qu'il n'aurait pas eu à dévoiler si les mêmes achats avaient été faits à la place d'affaire du commerçant.

---

[80] LAWSON, Philippa et al., « *On the Data Trail : How detailed information about you gets into the hands of organizations with whom you have no relationship* » Canadian Internet Policy and Public Interest Clinic, [En ligne] http://www.cippic.ca/en/news/documents/May1-06/DatabrokerReport.pdf p. 8. (consulté le 15 mars 2007).

[81] Croix-Rouge canadienne, *Politique sur la collecte, l'utilisation et la divulgation de renseignements personnels* « (…) Nous pouvons échanger les noms et les coordonnées de nos donateurs avec d'autres organismes humanitaires, de bienfaisance et sans but lucratif accrédités, aux fins d'activités de financement. » [En ligne] http://www.croixrouge.ca/article.asp?id=010958&tid=001 (consulté le 4 avril 2007)

[82] LAWSON Philippa, *Op. cit.,* note 81.

[83] *LPRPS*P, art.70.

[84] *PIPA* art. 1(4), 9(6), 12(1)g, 15(1)g, 15(1)k, 2392)a, 23(3.1), 51 c), 52(1)iv.

[85] *Fair Trading Act*, R.S.A. 2000, c. F-2.

Outre ces informations que le consommateur divulguera directement et qui seront indispensables en vue d'acquérir le bien ou le service (nom, prénom, coordonnées et numéro de cartes de crédit), les entreprises ont recours à d'autres méthodes de cueillette en vue d'obtenir certains renseignements complémentaires, méthodes qui, bien qu'elles requièrent un certain degré de divulgation volontaire, sont nettement moins explicites et plus intrusives.

Les cartes de fidélité

Les cartes de fidélité permettent à leurs émetteurs de compiler les habitudes de consommation des détenteurs. Une étude du *Canadian Broadcasting Corporation* (CBC) faite en 2004 a démontré que 76 % des consommateurs canadiens possèdent au moins une carte de fidélité (*Air Miles, Sears*, etc.). Les renseignements que les entreprises acquièrent par le biais de ces cartes sur les habitudes des consommateurs peuvent être utilisés afin d'établir le portrait d'un consommateur ou son profil psychologique. Ces données, compilées, peuvent par la suite être transmises à des partenaires d'affaires, des télévendeurs, etc.

Les détenteurs de ces cartes, qui les présentent à chaque achat en échange de points bonis, rabais, etc., acceptent donc de divulguer à des entreprises qui ils sont, ce qu'ils achètent et où ils l'achètent. Par exemple, Sears émet une carte de fidélité qui, selon leur publicité, donne droit à une foule d'avantages : « *L'un des programmes les plus complets au Canada, le Club Sears vous permet de recevoir jusqu'à 3 % du montant de vos achats effectués avec une carte Sears en cartes Récompenses Sears*. » D'apparence inoffensives, de telles cartes de fidélité, utilisées dans différents commerces, épiceries, pharmacies, permettent à l'entreprise de récolter une foule d'informations sur le consommateur, informations que le consommateur n'est pas nécessairement conscient de divulguer et dont il peut fort bien ignorer la portée : renseignements sur son état de santé, ses habitudes de consommation, ses déplacements, sa consommation d'alcool, l'importance accordée à l'image et même ses habitudes sexuelles!

Les informations ainsi récoltées se retrouvent compilées dans un système informatique qui permet de dresser un profil de chaque consommateur. Ces informations peuvent par la suite être utilisées ou revendues à des commerçants, manufacturiers, distributeurs, fabricants pour leur permettre de faire du marketing ciblé, c'est-à-dire rejoindre un certain type de consommateur qui sera intéressé par leurs produits. Si ce type de renseignements, sous forme purement statistique, est d'une aide inestimable pour les entreprises, on imagine aisément la valeur de ce type de profil lorsqu'il est personnalisé et que pourront lui être adjointes les coordonnées du consommateur.

La carte fidélité Air Miles, administré par le groupe Loyalty, mentionne dans sa politique de confidentialité que :

« les renseignements personnels sont récoltés aux fins suivantes (…) :

- *Communiquer l'information et les offres aux adhérents et aux commanditaires;*
- *Comprendre et analyser les réponses, les besoins et les préférences des adhérents;*
- *Élaborer, améliorer, commercialiser et offrir des produits et des services qui répondent à ces besoins»*[86]*. (nos soulignés)*

Cela implique bien entendu que la cueillette de renseignements personnels et le partage de ces renseignements, comme le stipule clairement leur politique de confidentialité, ne se limitent pas

[86] Air Miles, Politique de confidentialité, [En ligne] https://www.airmiles.ca/servlet/ContentServer?pagename=Airmiles/Visitors/Privacy (consulté le 2 avril 2007).

à celles des coordonnées personnelles du client, mais qu'elle s'étendra également aux achats effectués, afin de pouvoir compiler l'ensemble de ces données et les utiliser ultérieurement :

> *« Avec votre consentement, la collecte de renseignements personnels nous permet :*
> - *de vous identifier;*
> - *d'établir et de maintenir une relation harmonieuse avec vous, en vous assurant le meilleur service à long terme;*
> - *d'établir une compréhension de vos besoins et admissibilité pour des produits et services et vous soumettre des offres de Sears ou de certains de ses partenaires commerciaux tiers »*[87].

On soulignera l'utilisation de l'expression « *avec votre consentement* ». Attendu que la politique de confidentialité de Sears fait partie de ses engagements envers sa clientèle, le consommateur qui demande une carte Sears en accepte automatiquement les termes, consentant implicitement aux conditions que fixe l'entreprise, soit la collecte d'information permettant de l'identifier et le partage de ces informations que la loi interdit à l'entreprise de partager sans le consentement du consommateur. Attendu, par ailleurs, que ce consentement vise l'ensemble des activités de l'entreprise pour ce qui est du traitement des informations personnelles et que le consommateur n'est pas libre de refuser les utilisations que prévoit en faire l'entreprise, utilisations dont il n'est par ailleurs en aucun moment clairement informé, il va de soi que ces méthodes sont, en ce qui a trait à la transparence, beaucoup plus sujettes à caution.

Les concours, enquêtes, sondages ou formulaires pour l'achat de biens ou services

Les renseignements personnels de ceux qui répondent à des concours ou sondages sont souvent récoltés et analysés par les entreprises qui les ont recueillis. S'ils peuvent être compilés de façon anonyme dans le seul but de connaître la popularité d'un produit, ils peuvent également être rattachés à l'individu qui y a répondu et servir d'outil de profilage.

Le groupe *Sondages Canadiens* offre la possibilité de participer à des sondages rémunérés sur internet. Un observateur avisé découvrira, en cliquant à droite, au bas de l'écran, la politique de confidentialité, qui lui apprendra, en petits caractères, ce que l'entreprise compte faire des informations qui lui sont fournies :

> *« Nous recueillons de l'information de nos membres par voie de formulaires en ligne. Nos membres soumettent leur nom, leur adresse, leur adresse de courrier électronique, leur âge, ainsi que de l'information concernant des données démographiques et/ou réponse à toute autre question choisie par nos annonceurs. (…) L'information recueillie par CanadaSurveyPanel.com pour nos annonceurs est la propriété de nos annonceurs et ne sera partagée qu'avec l'annonceur. Chaque annonceur contrôle leur utilisation de l'information recueillie. »*[88]

Ainsi, s'il désire connaître l'utilisation qui pourra être faite des renseignements qu'il a fournis par le biais du sondage, le consommateur devra, en plus de celle du sondeur, consulter la politique de vie privée des différents annonceurs afin de savoir quels renseignements sont conservés, de quelle façon ils sont utilisés et à qui ils pourront être transmis.

---

[87] Sears Canada, Politique de confidentialité, [En ligne] http://www.sears.ca/gp/browse.html/ref=sc_bb_l_0_43336011_9/002-6473987-6706404?ie=UTF8&node=43339011&no=43336011&searsBrand=core&me=A10FHFRJZ0GJG3 (consulté le 10 avril 2007).

[88] Sondages canadiens, Politique de confidentialité, [En ligne].: http://sondagescanadiens.com/?p=privacy (consulté le 20 mars 2007).

L'entreprise Publisac, propriété du groupe Transcontinental, effectue actuellement un concours sur internet, par le biais duquel elle recueille des renseignements personnels. La politique de vie privée qui y est rattachée stipule que :

« En outre, de temps à autre, nous pouvons utiliser vos renseignements personnels aux fins suivantes :

- *repérer les erreurs, fraudes, vols et autres activités illégales et en protéger Transcontinental et d'autres tiers, et vérifier la conformité à l'égard des politiques et obligations contractuelles de Transcontinental;*
- *comprendre vos besoins et préférences, notamment pour communiquer avec vous et effectuer des sondages, de la recherche et des évaluations;*
- *obtenir des relevés vérifiés concernant le nombre d'abonnés par publication;*
- *réaliser des opérations commerciales, y compris l'achat, la vente, la location, la fusion, le regroupement ou tout autre type d'acquisition, d'aliénation, de titrisation ou de financement auquel prend part Transcontinental;*[89]
- *toute autre fin que nous pouvons vous indiquer de temps à autre. »*

(nos soulignés)

Ainsi, le consommateur divulgue ses renseignements personnels, ses goûts, ses préférences, ses achats, à de nombreuses occasions, non seulement lors de ses transactions commerciales, mais également en participant à des activités promotionnelles. La quantité et le degré de sensibilité des informations divulguées peuvent varier considérablement d'une fois à l'autre. Ces informations sont généralement enregistrées et peuvent être combinées à des renseignements récoltés par d'autres voies afin de permettre aux entreprises d'avoir un portrait encore plus détaillé d'un consommateur précis.

Utilisation de techniques informatiques afin de recueillir des renseignements personnels

Une étude américaine, la Georgetown Internet Privacy Policy Survey, a examiné en 2000 dans quelle mesure les sites internet commerciaux recueillaient de l'information sur les consommateurs avec lesquels ils transigeaient ainsi que le type de renseignements recueillis. L'enquête a révélé que 92,8% des 361 sites évalués recueillaient au moins un type de renseignement nominatif (nom, adresse électronique, adresse postale, etc.), 56,8% recueillaient au moins un type de renseignement démographique (sexe, préférences, code postal, etc.) et 56,2% des sites recueillaient à la fois des renseignements nominatifs et des renseignements démographiques, 6.6 % seulement ne recueillant aucun renseignement nominatif ou démographique.[90]

Le développement des nouvelles technologies a non seulement permis d'accroître l'usage et la grosseur des bases de données informatiques et de faciliter leur accès et le traitement des données, il a également permis de développer de nombreux programmes ou fichiers permettant de recueillir, souvent à leur insu, les renseignements personnels d'internautes en vue de garnir ces banques de données. Voici donc un portrait des différentes techniques informatiques actuellement utilisées et un survol de leur fonctionnement et du type de renseignements qu'elles servent à recueillir.

[89] Groupe Transcontinental. Politique de confidentialité. [En ligne] http://www.transcontinental.com/confidentialite.html (consulté le 5 avril 2007).
[90] Étude citée par : SMITH, Margaret, *Op. cit.*, note 25.

Les fichiers témoins (cookies)

Les fichiers témoins, communément appelés *cookies*, sont des fichiers qui sont déposés sur le disque dur d'un internaute lorsqu'il visite un site internet et qui collectent certaines informations qu'il retransmet au site qui l'a émis. Leur durée de vie peut être très courte (*cookies* non persistants), se limitant uniquement au temps de visite du site, ou être de plusieurs années (*cookies* persistants) selon le choix du serveur qui l'aura implanté. Ils peuvent aussi demeurer sur le disque dur jusqu'à ce que l'internaute ne s'en débarrasse lui-même. Une fois la durée de vie du *cookie* expirée, le fureteur de l'internaute ne délivrera plus les informations qu'il contient.

L'information recueillie par les fichiers témoins sera généralement beaucoup plus détaillée dans le cas des *cookies* persistants, dévoilant notamment les choix de navigation de l'internaute (les sites qu'il a visités, les pages qui l'ont intéressé) et permettant d'aller jusqu'à communiquer les allégeances politiques de l'internaute, sa religion, son origine ethnique, etc. Si les renseignements recueillis ne sont pas en soi des renseignements personnels, ces renseignements deviendront des renseignements personnels au sens de la loi s'ils peuvent être rattachés à un individu identifiable, par exemple si l'internaute s'est enregistré sur le site ayant émis le fichier témoin[91]. Puisque de nombreux sites demandent aux visiteurs de s'inscrire afin d'avoir accès au contenu du site ou de pouvoir faire des achats, dans de telles circonstances, l'internaute sera appelé à fournir son identité personnalisant ainsi les informations fournies.

Les *cookies* non persistants ne posent pas vraiment de problèmes en matière de protection des renseignements personnels puisqu'ils n'existent que le temps de la visite d'un internaute sur un site, visent principalement à faciliter l'accès au site et son utilisation et sont supprimés une fois la visite terminée. Un exemple de ce type de *cookie* est le panier d'achat (*shopping cart*) utilisé par la plupart des sites d'achat en ligne qui enregistre les divers items que désire acheter l'internaute avant qu'il ne procède au paiement.[92]

Les *cookies* persistants, quant à eux, fournissent des renseignements que le responsable du site internet qui les a implantés pourra consulter dès que l'internaute retournera sur le site qui a émis ce *cookie*, ce dernier transmettant à ce moment les renseignements qu'il a accumulés.[93] Le gestionnaire du site pourra dès lors utiliser ces renseignements pour adapter les offres, publicités et informations qu'il affichera lorsque cet internaute retournera sur son site, afin de personnaliser sa visite et, surtout, d'influencer ses choix de consommation.

La Commission Nationale de l'Informatique et des Libertés (CNIL), sur son site internet, dévoile quelques exemples pratiques de l'utilisation qui peut être faite de cookies afin de recueillir des renseignements personnels :

> *« dans la rubrique de ce site intitulée « Comment déclarer vos traitements ? », vous avez la possibilité de commander des formulaires de déclaration à la CNIL en nous laissant vos coordonnées. Nous aurions pu à cette occasion déposer dans votre ordinateur un cookie contenant ces coordonnées. Libre à nous, ensuite, de faire le lien entre votre adresse IP et votre adresse postale afin de prendre connaissance de manière nominative du parcours que vous avez suivi. Tiens, vous avez consulté tel*

[91] « Les cookies démystifiés » [En ligne] http://www.tactika.com/cookie/cookie5.htm (consulté le 18 mars 2007).
[92] FORTIER, Caroline. « Les cookies, le profilage et les intrusions dans la vie privée » [En ligne].http://www.lexum.umontreal.ca/cours/internet2000/forc/forc.html (consulté le 18 mars 2007).
[93] ROUILLÉ-MIRZA Ségolène, « Les collectes de données personnelles à l'insu des internautes » (2001) mémoire de DESS droit du multimédia et de l'informatique, Université Panthéon-Assas Paris II, p. 8.

> *dossier thématique ! Tiens, vous avez consulté tel communiqué de presse… Nous aurions pu ainsi, à votre insu, constituer un premier profil de votre comportement, associé à vos coordonnées ! »*[94]

Les fichiers témoins persistants sont principalement utilisés à des fins commerciales. En enregistrant les goûts, les intérêts et les caractéristiques d'un internaute, une entreprise peut par la suite lui proposer des informations ou des produits qui seront plus susceptibles de l'intéresser, de lui présenter une publicité plus précisément ciblée.

Le célèbre marchand *Amazon*, par exemple, utilise les deux types de *fichiers témoins*. Dans sa Déclaration de confidentialité, l'entreprise mentionne que parmi la liste de renseignements qu'*Amazon.ca* recueille et analyse automatiquement figurent :

> *« l'adresse IP utilisée pour connecter votre ordinateur au réseau internet, votre nom d'utilisateur, votre adresse électronique, votre mot de passe Amazon.ca, les renseignements relatifs à votre système et à vos connexions, telles que le type et la version de votre fureteur, votre système d'exploitation et la plate-forme. Nous analysons également votre historique d'achats sur les différents sites Amazon (que nous mettons parfois en corrélation avec l'historique d'achats d'autres consommateurs pour établir nos listes de meilleures ventes, par exemple) le parcours URL complet vous ayant conduit sur notre site, votre parcours sur le site lui-même (y compris la date et l'heure de connexion, les produits que vous avez recherchés et les pages que vous avez consultées) et votre parcours pour sortir de notre site web. Nous recueillons également votre numéro de témoin (cookie) ainsi que le numéro de téléphone à partir duquel vous avez appelé notre service à la clientèle. »*[95]

En plus de ces renseignements, d'autres ont été divulgués volontairement par le consommateur. La déclaration de confidentialité d'Amazon.ca stipule à ce sujet que :

> *« Vous nous fournissez des renseignements personnels chaque fois que vous effectuez une recherche, passez une commande, utilisez un forum de discussion, participez à un concours, répondez à un questionnaire ou contactez notre service à la clientèle. (…)Ce faisant, vous pouvez nous avoir fourni des données comme vos nom, adresse et numéro de téléphone ; les données relatives à votre carte de crédit ; les nom, adresse et numéro de téléphone de personnes à qui vos achats ont été expédiés ; les nom, adresse et numéro de téléphone des personnes figurant dans vos coordonnées 1-Click ; le contenu des commentaires et des courriels que vous nous avez fait parvenir ; ainsi que certaines informations financières. »*[96]

Par conséquent, lorsqu'on fait la somme des renseignements qui ont été divulgués de façon volontaire et de ceux qui ont été recueillis à l'aide de techniques informatiques, on s'aperçoit que le total des renseignements recueillis peut être considérable. Par ailleurs, bien qu'il soit possible pour l'internaute, en ajustant les paramètres de son fureteur, de refuser les fichiers témoins, certains sites ne permettront tout simplement pas l'accès aux internautes qui les refusent, la plupart recommandant d'ailleurs aux internautes de les accepter afin

---

[94] Commission Nationale de l'Informatique et des Libertés « vos traces » Les cookies, [En ligne] http://www.cnil.fr/index.php?id=170 (consulté le 25 Juin 2007).
[95] Amazon.ca. *Déclaration de confidentialité*. [En ligne] http://www.amazon.ca/gp/help/customer/display.html/701-8773470-7208349?ie=UTF8&nodeId=918814 (consulté le 30 mars 2007).
[96] *Ibid.*

« d'agrémenter » leur visite du site. L'invitation d'Amazon.ca, par exemple, est assez convaincante :

> *« (…) Les cookies vous permettent de profiter pleinement de certaines fonctions les plus intéressantes d'Amazon.ca. C'est pourquoi nous vous recommandons de les laisser activés. »*[97]

Ticketpro y va d'une suggestion semblable :

> *« Des témoins sont utilisés afin de vous procurer un contenu personnalisé tout en sauvegardant votre mot de passe vous permettant également de sauvegarder les renseignements personnels et financiers si vous le désirez. Ces témoins peuvent être désactivés avec la commande « Aide ». Cependant, cette désactivation pourrait rendre inaccessibles certaines parties du Site. »* [98]

Les logiciels malveillants (malware)

Le monde de l'internet regorge de types différents de logiciels malveillants. Aux fins de notre recherche, nous nous attarderons plus spécifiquement à ceux qui recueillent de l'information. Généralement classés dans la catégorie des logiciels espions (*spyware*), ces logiciels collectent de l'information sur l'internaute après s'être installés, à son insu, sur son ordinateur.[99] Les logiciels espions sont principalement développés par des entreprises qui offrent de la publicité sur internet, afin de récolter de l'information sur l'internaute pour des fins de publicité en ligne[100] ou directement par des concepteurs de programmes, qui les insèrent dans certains programmes, généralement disponibles gratuitement sur le web, en vue de se financer, en vendant, par exemple, les informations recueillies par ces logiciels.[101] Dans un cas comme dans l'autre, le but sera commercial.

Le logiciel espion est composé de trois mécanismes. D'abord, un mécanisme d'installation : le logiciel sera souvent rattaché à un programme téléchargé et installé par un utilisateur (le programme de téléchargement de musique Kazaa, par exemple, contient le logiciel espion *cydoor*). Le logiciel espion pourra aussi s'installer par lui-même, par le biais de failles de sécurité des fureteurs. Il y a ensuite le mécanisme de cueillette de l'information (dans le cas de *cydoor*, toutes les recherches et téléchargements effectués via Kazaa seront enregistrés). Vient enfin le mécanisme de transmission de l'information à un tiers qui sera généralement le concepteur du logiciel ou une entreprise.[102] Certains logiciels espions (les publiciels, ou *adwares)* pourront aussi afficher automatiquement, selon l'information recueillie, des offres publicitaires, parfois adaptées au profil de l'internaute, qui sera établi en fonction de sa navigation sur internet.

Les informations recueillies par les logiciels espions varient en fonction du type de logiciel et peuvent aller d'un relevé des sites internet visités aux numéros de cartes de crédit en passant par les mots-clés saisis lors d'une recherche, des renseignements personnels de l'internaute ou des achats faits sur internet, etc.[103]

---

[97] *Ibid.*
[98] Ticketpro. Politique de confidentialité. [En ligne] http://www.ticketpro.ca/confidentiel_fr.html (consulté le 10 avril 2007).
[99] Wikipedia « Logiciel espion » [En ligne] http://fr.wikipedia.org/wiki/Logiciel_espion (consulté le 8 mai 2007).
[100] *Ibid.*
[101] *Ibid.*
[102] *Ibid.*
[103] *Ibid.*

Les données de connexion (fichiers logs)

Les données de connexion, communément appelées fichiers *logs*, permettent, comme leur nom l'indique, de collecter des données liées à la connexion de l'internaute. Chaque site possède ses propres fichiers *logs* qui reflètent les activités qui ont eu lieu lors des connexions sur le site. Ces fichiers, comparables à un journal en format texte, recueillent, pour chaque page visitée sur le site en question, un certain nombre de renseignements[104], incluant l'adresse IP de l'ordinateur qui a accédé au site ou à la page, sa configuration, le type de navigateur utilisé, les dates et heures de connexion, le nombre de pages vues, le site d'origine et de destination, etc.

Les fichiers logs ne recueillent pas, en eux-mêmes, de renseignements personnels puisqu'ils ne sont associés qu'à une adresse IP, soit le numéro, ou adresse, anonyme, assignée à chaque ordinateur qui se connecte à internet. Il n'en demeure pas moins que les données qui sont recueillies sous forme de journal de la navigation d'un internaute anonyme peuvent permettre d'en apprendre beaucoup sur ce dernier. Un exemple éloquent a d'ailleurs récemment retenu l'attention : un document mis en ligne par AOL en août 2006, dans lequel figuraient les recherches effectuées par des millions d'internautes américains, a alerté le public sur les risques d'identification que présentent les données de connexion. Si les données ainsi diffusées ont permis de conclure, par exemple, que 45 % des clics se font sur le premier résultat de recherche affiché, il a aussi été établi que, par le biais de croisements, ces données permettaient de dresser un profil de chaque internaute. En effet, le numéro, anonyme, attribué à chaque utilisateur permettait de recenser l'ensemble des recherches qu'un utilisateur donné avait pu effectuer au cours des trois derniers mois, de connaître les mots-clés qu'il avait soumis, les dates et heures des recherches, ainsi que les adresses de sites visités.

Cette pratique a soulevé de sérieuses préoccupations, du fait que malgré le fait que les données soient anonymes, « *la liste des recherches associées à chaque identifiant a permis à de nombreux pisteurs de retrouver la trace d'internautes, d'identifier leurs numéros de sécurité sociale, leurs adresses parfois, jusqu'à leurs noms pour certains. En observant la seule liste des requêtes quotidiennes, sur plusieurs mois, il n'est souvent pas difficile de comprendre les préoccupations de l'internaute, d'imaginer son intimité, voire de retrouver son identité.* »[105]

Le fichier *log* rattache en effet les données à une adresse IP, c'est-à-dire à un ordinateur précis. En soi, ces données peuvent servir, notamment, à profiler les individus, comme le démontre l'exercice auquel se sont livrés des journalistes du Guardian qui ont conclu que :

> *« Le numéro 17556639 est un homme, qui a une passion pour le football portugais et vit dans une ville de Floride. Visiblement, il apprend que sa femme a une relation extraconjugale et les requêtes qu'il effectue sur son moteur décrivent l'évolution de sa relation : "Ma femme ne m'aime plus". Il cherche à "interrompre son divorce" puis à prendre une "revanche sur sa femme" avant de regarder les propres symptômes de son malaise : "manque d'alcool", "symptômes du manque d'alcool" (à 10 heures du matin) et "problème d'érection". Le 1er avril, il chercha un médium local pour lui "prédire son futur". »*[106]

[104] Adcom Internet, « les fichiers logs » [En ligne] http://www.adcom.fr/expertise/fichier_log.htm (consulté le 13 avril 2007).
[105] *Ibid.*
[106] « Big Brother et les fichiers logs » [En ligne] http://www.futura-sciences.com/news-big-brother-fichiers-log_9682.php (consulté le 13 avril 2007).

116874	thompson water seal	2006-05-24 11:31:36	1	http://www.thompsonswaterseal.com
116874	express-scripts.com	2006-05-30 07:56:03	1	http://www.express-scripts.com
116874	express-scripts.com	2006-05-30 07:56:03	2	https://member.express-scripts.com/
116874	knbt	2006-05-31 07:57:28		
116874	knbt.com	2006-05-31 08:09:30	1	http://www.knbt.com
117020	naughty thoughts	2006-03-01 08:33:07	2	http://www.naughtythoughts.com
117020	really eighteen	2006-03-01 15:49:55	2	http://www.reallyeighteen.com
117020	texas penal code	2006-03-03 17:57:38	1	http://www.capitol.state.tx.us
117020	hooks texas	2006-03-08 09:47:08		
117020	homicide in hooks texas	2006-03-08 09:47:35		
117020	homicide in bowie county	2006-03-08 09:48:25	6	http://www.tdcj.state.tx.us
117020	texarkana gazette	2006-03-08 09:50:20	1	http://www.texarkanagazette.com
117020	tdcj	2006-03-08 09:52:36	1	http://www.tdcj.state.tx.us
117020	naughty thoughts	2006-03-11 00:04:40	1	http://www.naughtythoughts.com
117020	cupid.com	2006-03-11 00:08:50		

Extrait du fichier divulgué par AOL[107]

Comme le mentionnait Michael Arrington, sur le site de TechCrunch:

> *« The most serious problem is the fact that many people often search on their own name, or those of their friends and family, to see what information is available about them on the net. Combine these ego searches with porn queries and you have a serious embarrassment. Combine them with "buy ecstasy" and you have evidence of a crime. Combine it with an address, social security number, etc., and you have an identity theft waiting to happen. The possibilities are endless. »*[108]

On s'aperçoit donc que les données récoltées par le biais des techniques informatiques peuvent ne pas être ou rester aussi anonymes ou innocentes qu'elles le paraissent à première vue. On comprend qu'il devient dès lors difficile de déterminer le type de renseignements qui tombe vraiment sous le coup de la définition de renseignements personnels, si des données anonymes permettent elles aussi d'identifier la personne qui soumet ces renseignements… ou à qui on les soutire.

La cueillette d'adresse (harvesting)

La cueillette d'adresse, mieux connue sous le nom de *harvesting*, est le procédé par lequel une adresse de courriel est automatiquement cueillie, sur les sites internet sur lesquels elle peut apparaître, en vue d'être ajoutée à une liste d'envoi. Des logiciels ont en effet été conçus pour ratisser internet et enregistrer toute adresse de courriel qui figure sur des sites web, des

[107] *Ibid.*.
[108] Tech Crunch, [En ligne] http://www.techcrunch.com/2006/08/06/aol-proudly-releases-massive-amounts-of-user-search-data/ (consulté 10 avril 2007).

blogues, etc. Aussitôt qu'une adresse électronique apparaît en ligne, il y a donc de fortes chances qu'elle soit rapidement cueillie aux fins de pollupostage et ajoutée à une liste destinée à la revente.[109]

La vente de listes d'adresses électroniques est maintenant chose courante. Comme ces listes peuvent servir aussi bien à des envois massifs qu'à des envois plus ciblés, le prix de telles listes varie selon les caractéristiques, plus ou moins pointues, des coordonnées qui s'y retrouvent.[110]

L'hameçonnage (phishing)

La technique frauduleuse connue sous le nom d'hameçonnage porte, en anglais, le nom plus éloquent de « *phishing* », néologisme anglo-saxon qui mêle "*fishing*" (pêche - le pirate essayant de piéger un « poisson » dans l'océan des utilisateurs d'internet) et «*phreaking*» (technique de piratage contre les systèmes téléphoniques utilisée dans les années 80, le terme est généralement utilisé en anglais pour désigner une fraude informatique).[111] L'hameçonnage consiste à envoyer massivement des courriers électroniques qui semblent provenir d'une entreprise légitime, en vue de tromper la vigilance du consommateur qui croira qu'il est en contact avec un tiers de confiance. Le courriel indiquera par exemple que l'entreprise a besoin de vérifier certaines informations et invitera l'internaute à lui fournir ces informations confidentielles (numéro de compte de banque, mot de passe, etc.), par retour de courriel ou sur un site qui reproduit fidèlement la charte graphique de l'organisme (banque, grandes entreprises, etc.), sur lequel l'internaute sera invité à se rendre par le biais d'hyperliens et qui captera les renseignements confidentiels du « poisson ».

On remarquera ici que ce n'est pas le système informatique qui est manipulé par cette voie, mais bien son utilisateur. Par ailleurs, si ce type de fraude ne dépend pas des technologies informatiques, ces fausses représentations étant parfaitement réalisables par téléphone, il faut avouer que la possibilité de procéder par envois électroniques massifs facilite considérablement le travail des fraudeurs, qui peuvent jeter en même temps et à peu de frais une quantité phénoménale de « lignes » et attendre de voir si quelqu'un mordra, ce qui réduit aussi grandement le risque d'être pris.

Les techniques d'hameçonnage se perfectionnent toujours davantage et il peut être aujourd'hui extrêmement difficile pour les consommateurs de les détecter. Au Canada, presque toutes les institutions financières ont servi d'appât pour des tentatives d'hameçonnage.[112] Les hameçonneurs raffinent leurs procédés, faisant des envois plus ciblés. Récemment, un courriel identifié comme provenant du groupe financier Desjardins (rédigé en français, chose que l'on voyait rarement auparavant) invitait le destinataire à se rendre, par le biais d'un hyperlien affiché dans le courriel, vers un site qui reproduisait parfaitement celui de Desjardins et où on lui demandait, s'il voulait continuer à avoir accès aux services AccèsD, de mettre à jour certaines

[109] POELLHUBER, David, « La sécurité du courriel ? Perspective annuelle et solutions en entreprise » [En ligne] http://www.zerospam.ca/docu/le-contexte-de-la-securite-du-courriel.html (consulté le 18 mars 2007).
[110] Par exemple, 2 millions d'adresses électroniques sans caractère spécifique peuvent se vendre à 99 dollars américains et 100 000 adresses d'abonnés d'AOL, à 100 dollars américains. LABBÉ, Éric, "*Le Spamming et son contrôle*", décembre 1997. [En ligne] . http://www.droit.umontreal.ca/~labbee/ (consulté le 26 mars 2007).
[111] Wikipedia, « Hameçonnage » [En ligne] http://fr.wikipedia.org/wiki/Hame%C3%A7onnage (consulté le 10 avril 2007)
[112] *Ibid.*

données personnelles. L'internaute qui fournissait les informations demandées avait par la suite la fâcheuse surprise de découvrir qu'il s'était fait vider son compte de banque.

L'identification par radio fréquence

L'identification par radio fréquence (radio frequency identification, RFID) permet de recueillir à distance et de conserver des informations. Les radioétiquettes, destinées à remplacer les codes à barres des produits, sont de petits objets qui peuvent être collés ou incorporés à des produits, tissus, ou autres et même à des êtres vivants. « *Ces radio-étiquettes comprennent une antenne associée à une puce électronique qui leur permet de recevoir et de répondre aux demandes de requête radio émises par l'émetteur-récepteur.* »[113] Alors que les codes à barres ne permettent que de donner un numéro pour une classe de produits, les radio identifiants peuvent permettre de donner à chaque objet un numéro unique, qui permet de tracer le déplacement des objets d'un endroit à un autre, depuis la chaîne de production jusqu'au consommateur final, et ce, tout en étant fort abordables [114]

Cette nouvelle technologie est considérée par de nombreux industriels comme la solution technologique ultime à tous les problèmes de traçabilité. L'utilisation de minuscules puces électroniques incluses dans une étiquette permettrait bien entendu, selon ses promoteurs, de faciliter considérablement la vie des consommateurs. En effet, comme le mentionne Xavier Lemarteleur :

> *« Qui n'a pas rêvé de ne plus avoir à faire la queue aux caisses de son supermarché, les achats étant comptabilisés automatiquement par une lecture à distance des articles, ou encore de ne plus avoir à sortir son coupon de transport en commun, de ne plus chercher ses clefs pour ouvrir son automobile (ce qui existe déjà chez certains constructeurs) ou sa maison ? C'est que nous promet l'utilisation des RFID. »*[115]

Les potentialités de cette technologie sont énormes et l'inventivité des ingénieurs garantit que le nombre d'applications possibles s'accroît de jour en jour… soulevant au même rythme de nombreuses inquiétudes quant à la protection de la vie privée des consommateurs. Les radioétiquettes peuvent recueillir et transmettre une quantité importante d'informations sur le consommateur, et ce, à son insu. En effet, la simple lecture des différentes étiquettes que pourrait porter un consommateur lors de son entrée dans un commerce (vêtements qu'il porte, objets contenus dans ses poches, dans un sac, etc.) pourrait permettre de recueillir une foule de renseignements sur cet individu. Pour peu que le récepteur soit assez puissant, on pourrait même envisager un inventaire rapide de ce qui pourrait se trouver étiqueté à l'intérieur de son domicile. Par ailleurs, les RFID pouvant également être utilisés dans différentes pièces d'identité (passeport, permis de conduire, cartes d'assurance maladie, cartes de crédit, etc.), il serait possible à ce récepteur de capter des informations permettant du même coup d'identifier les individus. Les inquiétudes sont bien entendu multipliées quand on considère que quiconque possède un récepteur serait à même de recueillir ces renseignements.

Cette technologie n'est pas actuellement très répandue et peu de renseignements personnels sont à ce jour effectivement recueillis de cette façon. Par conséquent, nous ne reviendrons pas

[113] Wikipedia, « Radio-identification » [En ligne] http://fr.wikipedia.org/wiki/Radio-identification (consulté le 17 avril 2007).
[114] Moins de 20 cents l'unité. CNIL, [En ligne] http://www.cnil.fr/index.php?id=1063 (consulté le 17 avril 2007).
[115] LEMARTELEUR, Xavier, « Traçabilité contre vie privée : Les RFID» [En ligne] http://www.juriscom.net/uni/visu.php?ID=587 (consulté le 16 avril 2007).

sur cette méthode de cueillette au cours de notre étude, mais nous tenions à la mentionner, car elle semble appelée à se développer au cours des prochaines années et pourrait éventuellement être une technique prisée pour recueillir des renseignements qui, accessoirement, pourraient comprendre des renseignements personnels.

UTILISATION DES RENSEIGNEMENTS PERSONNELS

La collecte et l'utilisation des renseignements personnels par les commerçants sont une pratique qui ne date pas d'hier et qui existait bien avant l'arrivée d'internet. En effet, une des premières entreprises à avoir découvert le potentiel commercial que pouvaient présenter les renseignements personnels des consommateurs fut la Polk Company, entreprise de vente de véhicules motorisés, fondée en 1870 aux États-Unis. Polk, le fondateur, récoltait les informations qui apparaissaient aux permis des consommateurs qui achetaient un véhicule afin de pouvoir les contacter dans le cas d'un éventuel rappel du manufacturier. Il a cependant rapidement constaté qu'en combinant le type de véhicule acheté et le moment de l'achat avec les renseignements personnels tels le nom, l'adresse et l'âge des propriétaires, il avait en main des données qu'il pouvait facilement vendre aux entreprises de publicité qui les utilisaient à leur tour afin d'établir le style de vie, le salaire et la probabilité, pour chaque individu, d'être intéressé à l'achat de tel ou tel produit.[116]

Il existe, au Canada, un marché florissant de renseignements personnels et l'utilisation à des fins commerciales de ces renseignements présente un intérêt grandissant pour les entreprises qui désirent rejoindre les consommateurs canadiens qui, en 2004, dépensaient 277 milliards de dollars dans le commerce de détail. Statistiquement, les Canadiens répondent aux offres par envois directs 25 % plus souvent que ne le font les Américains ; ils reçoivent moins d'envois que ces derniers et 84 % lisent entièrement les envois reçus[117]. Ces données signalent des occasions d'affaires avantageuses que plusieurs convoitent. Ainsi, les entreprises déploient des ressources de plus en plus importantes en vue de connaître les consommateurs, leurs goûts, leurs intérêts, leurs opinions, leurs préoccupations, mais aussi leurs faiblesses et leurs vices… afin, comme ils le prétendent, de mieux satisfaire le consommateur, mais surtout pour mieux le convaincre d'acheter leur produit.

Du marketing ciblé au profilage

Avec l'évolution des nouvelles technologies, le mode de consommation des individus s'est rapidement modifié. Si, traditionnellement, les consommateurs avaient l'habitude de se déplacer et de se rendre dans les différents commerces pour magasiner, louer ou acheter un bien ou un service, ils sont aujourd'hui de plus en plus nombreux à faire leur magasinage ou leurs achats sur internet, dans le confort de leur foyer. Conscientes de cette réalité, la majorité des entreprises québécoises possèdent aujourd'hui un site internet. Ce nouveau mode de consommation rend précieux les renseignements que les entreprises peuvent recueillir sur l'internaute, ses goûts et ses préférences puisqu'ils lui permettent de transmettre de l'information qui correspond à ses attentes, optimisant du même coup les chances de conclure une transaction. Pas de déplacement, pas de file d'attente, pas de foules… les nouvelles techniques de commercialisation proactives utilisées par les entreprises visent à aller chercher

[116] SHOLTZ, Paul, *Economics of Personnal Information Exchange.* First Monday 5(9). [En ligne] http://www.firstmonday.org/issues/issue5_9/sholtz/index.html (consulté le 4 avril).
[117] Double Click, The Smart Marketing Report, « *Abacus Canada and Canada Post Borderfree Give Direct Marketers Access to Canada's Growing Consumer Market* » [En ligne] http://www3.doubleclick.com/market/2005/02/dc/direct.htm?&c=0502_smr&id_lead=newsletter&id_source=newsletter_0502 (consulté le 4 avril).

le consommateur chez lui et à l'amener à effectuer ses achats immédiatement, plutôt que d'attendre qu'il vienne à eux. C'est dans ce contexte que se sont multipliées les techniques de commercialisation et, par le fait même, les entreprises spécialisées dans la cueillette, le traitement ou l'analyse de données.

Le site de Postes Canada Libres-frontières, une entreprise qui offre des services de marketing et agit comme intermédiaire entre les entreprises et les consommateurs est éloquent :

> *« En offrant des outils de segmentation de la clientèle permettant de trouver les meilleurs clients éventuels en fonction du profil du consommateur du détaillant, une planification de la diffusion et une série de campagnes de marketing intégré et d'analyses pertinentes, Postes Canada Libres-frontières aide ses partenaires à élargir leurs marchés. »*[118]

Il s'agit donc d'une nouvelle approche de commercialisation, que permettent, d'une part, la conjugaison des nouvelles technologies et, d'autre part, une cueillette de renseignements personnels plus ciblée, plus personnalisée et, donc, plus efficace. Alors qu'en moyenne, seulement 6,4 % des consommateurs ouvrent un courriel promotionnel (ce qui ne garantit pas que le contenu est lu), ce taux grimpe à plus de 30 % lorsque le message est personnalisé[119], ce qui explique en soi l'importance accordée par les commerçants à la collecte et au traitement des renseignements personnels des consommateurs.

Si certaines entreprises utilisent les renseignements personnels des consommateurs qu'elles auront recueillis directement, dans le cadre de leurs activités commerciales, d'autres feront affaire avec des entreprises qui se spécialisent dans la cueillette et le traitement de renseignements. Ces entreprises soumettent aux commerçants ou aux agences de publicité des listes de clients potentiels, profilés en fonction des produits et services offerts, ou fournissent des renseignements additionnels sur des clients de l'entreprise en vue de leur permettre de détailler leur profil.

De véritables réseaux de commercialisation en ligne, appelés régies publicitaires, se sont ainsi développés. Ces régies permettent à des entreprises de déléguer à certaines agences, telles DoubleClick, la gestion de la publicité qu'ils affichent sur leurs sites. Les entreprises ayant adhéré à DoubleClick lui permettent de récolter des informations sur l'ensemble des internautes qui visitent leur site au moyen de fichiers témoins. Dès lors, les informations récoltées au sujet d'un internaute sont beaucoup plus détaillées et serviront à établir un profil précis de l'individu permettant ainsi de lui afficher des publicités qui seront plus susceptibles de correspondre à ses goûts et intérêts.[120]

La Commission Nationale de l'informatique et des Libertés (CNIL) réfère, au sujet de la notion de profilage, à : « *la capacité de traitement des ordinateurs, pour, au regard des caractéristiques définies a priori ou déterminées après une étude statistique, classer des*

---

[118] Poste Canada Libres-frontières, [En ligne] http://www.libres-frontieres.net/fr/business/media/releases/2005-05-17.jsp (consulté le 10 avril 2007).

[119] NANTEL, M., « *La publicité Web à la croisée des chemins* » La Presse, 30 janvier 2004, [En ligne] http://www.inoxmedia.ca/carnet/archives/000263.html (consulté le 5 avril 2007).

[120] CHASSIGNEUX, Cynthia, « *La protection des informations à caractère personnel* » dans le Guide juridique du commerçant électronique, sous la direction de LABBE E., POULIN D., JACQUOT F., BOURQUE J-F., Montréal, 2001, [En ligne] http://www.jurisint.org/pub/05/fr/index.htm (consulté le 10 avril 2007).

individus et prendre des décisions à leur égard. »[121] Les différents renseignements recueillis sont classés par « segments », en vue d'établir une segmentation comportementale, « *une technique permettant de construire, au sein de la clientèle d'un établissement ou d'une entreprise, des classes homogènes de clients appelés segments, en fonction des comportements observés.* »[122] Le marketing ciblé profitera donc du profilage pour établir un portrait général du consommateur et de son mode de vie sur la base de ses habitudes de consommation, ses intérêts, ses goûts, etc., afin, sur la base de ces informations, de lui faire parvenir de la publicité personnalisée.

Internet offre aux publicitaires les outils nécessaires pour atteindre à peu de frais la clientèle ainsi ciblée. NetWorldMedia, une agence de marketing offrant le service de ciblage comportemental sur internet, explique le fonctionnement de son service :

> *« Jean Tremblay est à la recherche d'une nouvelle voiture. En magasinant sa prochaine voiture en ligne, Jean visite certains sites dédiés aux automobiles du réseau NetWorldMedia tel que GuideAuto.com, Essais-auto.com ou AutoConseils.ca, et clique sur une publicité de General Motors qui l'intéresse.*
>
> *Dès lors que notre système aura enregistré au moins 2 actions démontrant l'intérêt de Jean envers les voitures, il sera considéré comme un profil "Acheteur automobile".*
>
> *Par la suite, dans les 30 prochains jours, peu importe quel site Jean visitera sur le réseau de 150 sites NetWorldMedia, Jean sera exposé plus souvent à des bannières publicitaires reliées à l'automobile telle que Ford, GM, Toyota, etc. »*[123]

Il ne faut cependant pas confondre ce type de ciblage avec le ciblage contextuel qui consiste pour sa part à afficher la publicité en fonction du contenu d'une page plutôt qu'en fonction du profil de l'internaute. Alors que le ciblage comportemental évaluera la navigation préalable de l'internaute pour lui afficher des publicités relatives aux divers champs d'intérêt observés, le ciblage contextuel n'affichera les publicités relatives à un champ d'intérêt particulier que lors de la navigation sur les sites qui concernent ce même champ d'intérêt. Le ciblage comportemental est donc beaucoup plus complexe (et plus coûteux) que le ciblage contextuel, car il nécessite l'identification de l'internaute et la cueillette de renseignements le concernant, réalisées grâce aux différentes techniques informatiques décrites précédemment. Adam Sohn, le directeur des services en ligne de Microsoft affirme que le profilage comportemental permet d'augmenter de 76 % les chances qu'un internaute clique sur la publicité qu'on lui présente.[124]

L'accès à des listes de données personnelles est aussi offert aux entreprises qui désirent rejoindre le consommateur autrement que par mode virtuel. Il s'agira le plus souvent de listes de nom et d'adresse de personnes qui possèdent une ou des caractéristiques communes : abonnement à tel type de revue, réponse à tel type d'offre postale, type de carte de crédit détenue, groupe d'âge précis, etc.[125] Le numéro de téléphone et/ou l'adresse électronique feront parfois également partie des renseignements qui apparaîtront à la liste. Le prix de la liste

---

[121] Commission Nationale de l'informatique et des libertés (CNIL) « Dix ans d'informatique et de liberté » 1998, Economica, p. 37.
[122] ROUILLÉ-MIRZA, Ségolène, *Op .cit.,* note 94, p. 18.
[123] Networld Media, [En ligne] http://networldmedia.net/FR/annonceurs-internet/ciblage-comportemental/ciblage-comportemental.html (consulté le 13 avril 2007).
[124] MINTZ, Jessica « Microsoft Adds Behavioral Marketing » Associated Press, 27 décembre 2006 [En ligne] http://www.msnbc.msn.com/id/16370058/ (consulté le 27 mars 2007).
[125] LAWSON, Philippa et Al., *Op. cit.*, note 81, p. 9.

variera en fonction des critères demandés et de la méthode de livraison de la liste (disquette, CD-ROM, courriel, etc.) et sera fixé, dans la plupart des cas, en fonction d'une utilisation unique.[126] Plutôt que d'être transmise à l'entreprise qui l'achète, cette liste pourra être transmise par l'entreprise qui désire conserver le contrôle sur ses listes directement au Bureau d'envoi postal qui préparera et enverra le courrier aux personnes ciblées. Certaines restrictions pourront s'appliquer à l'utilisation des listes, comme l'interdiction d'offrir certains produits ou services (par exemple produits et services destinés exclusivement aux personnes de 18 ans ou plus).[127]

En vue de rassembler les renseignements les plus complets possible, les entreprises tentent, de plus en plus, de mettre en commun leurs banques de données. De tels échanges permettent de dresser des profils encore plus précis des consommateurs. La société DoubleClick, la plus grande agence de publicité sur internet, parlait en ces termes des avantages que pourrait présenter le croisement des renseignements qu'elle détient :

> *« Pour ce qui est du ciblage, notre idéal serait de savoir tout sur tout le monde. Nous tentons actuellement de recouper nos données avec celles d'Amazon.com, leader dans le domaine de la vente par internet. Jusqu'ici nous connaissons l'adresse IP des ordinateurs – le numéro qui les identifie de manière unique et permet de la situer géographiquement – et les habitudes de leurs utilisateurs. Nous pouvions savoir que tel internaute s'était connecté tant de fois à tel site durant les trois dernières semaines et quel avait été son parcours de navigation : s'il visitait souvent des sites de foot, etc. Avec la base de données d'Amazon.com, nous disposerons aussi de ses nom, prénom, adresse et numéro de téléphone. »*[128]

Si l'entente avec Amazon ne s'est pas concrétisée, une autre a plutôt été conclue, avec Abacus, une coopérative de renseignements. Sur son site internet, Abacus précise l'utilité de son approche :

> *« A cooperative database allows consumer activity to be viewed not from the narrow perspective of purchases made with one company but those made right across the mail order spectrum with many different organisations. »*[129]

Le ciblage comportemental peut se faire autant à partir des renseignements recueillis par le biais de la divulgation volontaire par le consommateur dans le cadre d'une relation commerciale que par celui d'une collecte de données effectuée grâce à des techniques informatiques, ou de la combinaison des renseignements obtenus par ces deux méthodes. Par ailleurs, outre la publicité par internet, la publicité numérique individualisée devrait s'accroître dans les années à venir. En effet, bien qu'il n'en soit encore qu'à ses balbutiements au Canada, ce type de diffusion de la publicité permettra notamment de rejoindre le consommateur en lui envoyant des offres sur son téléphone portable ou sur les consoles de jeu connectées à internet. Les commerces de quartiers pourront ainsi envoyer des promotions à toute personne qui passerait dans les environs et qu'ils auraient repérée par les balises GPS qui seront bientôt intégrées dans la plupart des téléphones portables.[130]

---

[126] *Ibid.*
[127] *Ibid.*
[128] BOYER, Joël « La révolution d'internet » Petites affiches, 10 novembre 1999.
[129] Abacus*, The Abacus Alliance : What is the Abacus Alliance ?*, site d'Abacus, Teddington, Royaume-Uni, 2006 [En ligne] http://www.abacusalliance.com/The%5FAbacus%5FAlliance/ (consulté le 4 avril 2007).
[130] BENHAMOU, Laurence, « La publicité de l'ère numérique traque les consommateurs » La Presse, 28 mars 2007, [En ligne]

Études de cas

DoubleClick

DoubleClick est une entreprise américaine fondée en 1996, qui se consacre principalement à la publicité sur internet. À l'aide de *cookies* persistants, DoubleClick établit à leur insu le profil de millions d'internautes qui visitent les membres de son réseau et leur fait par la suite parvenir, individuellement et selon le profil détecté, les publicités de ses partenaires commerciaux.[131] DoubleClick, qui récolte de l'information sur plus de 11 000 sites web aurait, entre 1996 et 2000, accumulé plus de 100 millions de profils d'internautes[132]. Selon Media Metrix, 45,8 % des internautes des États-Unis ont visité, au mois de décembre 1998 seulement, au moins un site faisant partie du réseau de DoubleClick.[133] Les *cookies* persistants, qui enregistrent à partir de leur installation sur le disque dur de l'internaute toute navigation ultérieure permettront à DoubleClick de détecter les sites visités par l'internaute, les recherches qu'il a effectuées, les produits qu'il a achetés ou visionnés[134] et d'établir son profil. Par ailleurs, DoubleClick utilise également ses fichiers témoins afin de savoir quelles publicités ont été envoyées à l'internaute, afin d'éviter que celui-ci voie sans cesse s'afficher la même publicité.[135]

Ce suivi des activités des individus en vue du profilage commercial soulève bien entendu de sérieuses préoccupations relativement à la protection de la vie privée. Comme le mentionne Jason Catlett, président du groupe Junkbuster, dédié à la lutte contre le marketing intrusif (*privacy invading marketing*) :

> *« The web sites in Doubleclick's surveillance network have to disclose the fact in their privacy policies, but there's no requirement that consumers be asked to consent to Doubleclick's profiling. The vast majority of people online would want to be asked before profiles are built about them, and this should be required by law. The European Union is starting to requiring this, and for years Doubleclick's European operations have been years far less intrusive than its US ones. »*[136]

Par ailleurs, l'entreprise a soulevé un tollé parmi les organisations de protection de la vie privée lorsqu'elle a annoncé l'achat de la coopérative de renseignements personnels Abacus. Si l'information recueillie par DoubleClick était à ce jour anonyme, il lui serait maintenant possible, en fusionnant les banques de données des deux entreprises, de relier à un individu identifié toutes les informations recueillies. Suite à la levée de boucliers qui a suivi l'annonce de l'achat d'Abacus, DoubleClick a tenu à rassurer la population en précisant qu'il n'avait pas l'intention de fusionner les renseignements personnels détenus par chacune des entreprises. Si cette déclaration a suffi à rassurer la Federal Trade Commission, qui a approuvé la transaction malgré les contestations, Jason Catlett précise que, en l'absence de normes contraignantes, rien ne garantit que cette fusion de renseignements n'aura pas lieu :

> *« DoubleClick seems to have convinced the FTC that it did not actually associate names and addresses with its previously anonymous cookies, despite the fact that this was their*

---

http://www.cyberpresse.ca/article/20070328/CPACTUEL/70328065/1015/CPACTUEL (consulté le 28 mars 2007).

[131] FORTIER, Caroline, *Op. cit.*, note 93.

[132] *Ibid.*.

[133] EPIC (Electronic Privacy Information Center) «The Cookie Page» [En ligne] http://www.epic.org/privacy/internet/cookies (consulté le 3 avril 2007).

[134] RODGER, Will, «Activists Charge DoubleClick Double Cross» USA Today, États-Unis,7 juin 2000.

[135] FORTIER, Caroline, *Op. cit.*, note 93.

[136] CATLETT, Jason, « FTC drops investigation of DoubleClick.» [En ligne] http://www.junkbusters.com/new.html#DCLK (consulté le 18 avril 2007).

> *stated intention prior to their backdown in March. Even assuming that DoubleClick did not actually get around to matching up any of its massive stockpiles of online and offline data, they are still technically able to do so, and they continue to collect huge amounts of identified and identifiable information in ways that are unfair and unacceptable violations of privacy. »*[137]

La filiale américaine d'Abacus détenant une base de données contenant les noms, adresses, numéros de carte de crédit, numéros de téléphone et habitudes de consommation de 90% des foyers américains,[138] le profilage précis que permet la fusion des renseignements détenus par les deux entreprises est associé à une intrusion massive dans la vie privée des individus. L'achat, le 13 avril 2007, de DoubleClick par Google (pour 3,1 milliards de dollars[139]), que David Rosenblatt, PDG de DoubleClick, commentait ainsi : *« Google is the absolute perfect partner for us, combining DoubleClick's cutting edge digital solutions for both media buyers and sellers with Google's scale and innovative resources will bring tremendous value to both our employees and clients. » ne fera certainement pas en sorte de rassurer les critiques.*

Les agents de renseignements personnels

> *« Est un agent de renseignements personnels toute personne qui, elle-même ou par l'intermédiaire d'un représentant, fait le commerce de constituer des dossiers sur autrui, de préparer et de communiquer à des tiers des rapports de crédit au sujet du caractère, de la réputation ou de la solvabilité des personnes concernées par ces dossiers. »*[140]

La LPRPSP stipule que tout agent de renseignements personnels qui exploite une entreprise au Québec, doit obligatoirement être enregistré afin de mener ses activités commerciales. Une centaine d'agents de renseignements personnels sont ainsi enregistrés au Québec. Parmi celles-ci figure notamment Équifax, une des agences de crédit les plus connues. Ces entreprises recueillent de l'information sur le crédit et peuvent notamment fournir des renseignements personnels à une compagnie d'assurance, un employeur ou un locateur potentiel, à condition que la personne concernée ait donné à la personne qui désire obtenir ces renseignements son consentement à la cueillette auprès d'un tiers.

Or, il appert d'une récente enquête menée par l'émission de reportages *La facture*[141] que certaines agences procèdent à la divulgation même si elles n'ont pas de preuve que le requérant a obtenu le consentement nécessaire. Odette Oger, vice-présidente d'Équifax Canada, explique :

> *«Nous avons des centaines de milliers de demandes (…). C'est certain que nous ne demandons pas d'avoir une copie du consentement pour toutes les transactions!»*

L'enquête dévoile que des agences de renseignements personnels ont par ailleurs également obtenu et divulgué des informations bancaires qui n'apparaissent pourtant pas au dossier de crédit. En effet, il appert que des employés d'institutions financières fournissent à certaines agences, moyennant rémunération, des renseignements concernant les clients de l'institution,

---

[137] *Ibid.*
[138] FORTIER Caroline, *Op. cit.*, note 93.
[139] Press Release (Google et DoubleClick) [En ligne] http://www.doubleclick.com/us/about_doubleclick/press_releases/default.asp?p=572 (consulté le 18 avril).
[140] *LPRPSP*. art.70 et suivants.
[141] *La facture*, émission du 13 février 2007, Radio-Canada, Montréal, Québec, [En ligne] http://www.radio-canada.ca/actualite/v2/lafacture/niveau2_13625.shtml (consulté le 17 avril 2007).

que les agences revendent par la suite à leurs propres clients. Les agences de renseignements personnels et les banques n'ont pas été les seules entreprises visées par l'enquête. En effet, Bell est également pointée du doigt : à partir d'un simple numéro de téléphone, Bell a divulgué à l'enquêteur le nom de l'abonné, celui de sa conjointe, leur adresse, un second numéro de téléphone, de même que le nom de la compagnie enregistrée au nom de l'abonné. Si Bell reconnaît que la divulgation provient effectivement de son entreprise, elle assure qu'il s'agit d'un cas isolé.

Même si la Loi exige le consentement préalable de l'intéressé pour toute cueillette de renseignements personnels, la possibilité d'acheter sans trop de mal des renseignements personnels sur autrui témoigne de l'importance que prend actuellement ce commerce pour les entreprises et les profits qu'elles peuvent en tirer. Les rapports commandés par *La facture* dans le cadre de son enquête lui ont coûté entre 200 $ et 500 $ l'unité. Le type de renseignements que divulguent les agents de renseignements personnels pourra être déterminant dans le choix d'une entreprise de transiger avec tel individu ou de ne pas le faire, lui refusant ses produits ou ses services, selon les renseignements obtenus.

Cette enquête soulève évidemment de graves inquiétudes concernant la protection des renseignements personnels et leur divulgation, d'autant plus que les entreprises concernées font l'objet d'un encadrement plus serré que la moyenne. De plus, la possibilité, démontrée par les enquêteurs de l'émission *La facture*, d'acheter illégalement des renseignements personnels concernant un individu soulève de nombreuses questions relatives aux utilisations réelles qu'en font les entreprises et au respect des lois entourant la protection de ces renseignements.

Les manquements à la loi de la part des agences de renseignements personnels semblent être un phénomène répandu. Bien que ces agences qui exercent leurs activités dans les autres provinces n'aient pas d'obligation de s'enregistrer comme c'est le cas au Québec, elles sont tout de même elles aussi, soumises à certaines dispositions particulières de la loi[142]. Par contre, les lois de l'Alberta et de la Colombie-Britannique n'étant entrées en vigueur qu'en janvier 2004, aucune décision n'a été rendue, jusqu'à présent, à l'encontre de ces entreprises par les Commissaires de ces deux provinces[143]. Toutefois, le Commissariat à la protection de la vie privée du Canada a reçu de nombreuses plaintes concernant ces entreprises et la Commissaire a rendu douze décisions en faveur des plaignants[144]. Parmi les violations à la LPRPDÉ reconnues par la Commissaire, huit portaient sur le non-respect du principe 4.9 de l'annexe 1 et des articles 8(3) et (5), qui traitent du droit d'accéder à son dossier dans un délai de trente jours,[145] Deux décisions ont portées à la fois sur la violation du principe 4.3, relatif à l'obtention du consentement de la personne concernée avant la divulgation de renseignements personnels

[142] *PIPA* Colombie-Britannique art. 1, 9(6), 12(1)g, 15(1)g,k, 23(2)(3.1), 51c), 52(2) ainsi que le *Business Practices and Consumer Protection Act*, SBC 2004, c.2, art.106-112 ; *PIPA* Alberta art. 1c), 14g), 17g), 20o) ainsi que le *Fair trading Act* R.S.A. 2000 c.F.2, art.3 et 43 à 51.

[143] Depuis l'entrée en vigueur de la Loi, le Commissaire de la Colombie-Britannique n'a rendu que 9 décisions, (Office of the Information Privacy Commissioner for British Columbia, *Private sector- orders,* [En ligne] http://www.oipcbc.org/sector_private/orders_decisions/orders_2006.htm (consulté le 1 juin 2007)), alors que le Commissaire de l'Alberta en a rendu 12, (Office of the Information Privacy Commissioner for Alberta, *Orders and Investigation Report - orders*, [En ligne].http://www.oipc.ab.ca/orders/orders.cfm (consulté le 1 juin 2007).

[144] Plaintes jugées fondées par la Commissaire (en date du 25 juin 2007): Conclusions de la Commissaire - *Résumé de conclusions d'enquête en vertu de la LPRPDÉ #59, 64, 67, 102, 124, 134, 150, 182, 187, 291, 317, 326*

[145]Conclusions de la Commissaire - *Résumé de conclusions d'enquête en vertu de la LPRPDÉ #59, 64, 67, 102, 124, 134, 187, 291*

la concernant, et du principe 4.7 qui exige la mise en place de mesures de sécurité adéquates[146]. Une décision a porté sur la violation du principe 4.5, qui impose aux organisations de limiter la durée de conservation des renseignements personnels qu'elles recueillent[147] et une autre sur le non-respect du principe 4.10.4, qui oblige l'organisation à faire enquête sur les plaintes et à prendre des mesures appropriées si cette plainte est jugée fondée.[148]

[146] Conclusions de la Commissaire - *Résumé de conclusions d'enquête en vertu de la LPRPDÉ #150 et 317*
[147] Conclusions de la Commissaire - *Résumé de conclusions d'enquête en vertu de la LPRPDÉ #326*
[148] Conclusions de la Commissaire - *Résumé de conclusions d'enquête en vertu de la LPRPDÉ #182*

ANALYSE DE LA LEGALITE DES PRATIQUES DES ENTREPRISES

Le consentement du consommateur à la collecte et au partage des renseignements personnels qui le concernent est au cœur des lois qui visent la protection de ce type de renseignements, attendu que seul ce consentement permet au consommateur de conserver un certain contrôle sur les renseignements qui circuleront à son sujet. Il importe donc d'évaluer dans quelle mesure les entreprises auxquelles le consommateur divulgue –volontairement ou non– ses renseignements personnels, respectent l'encadrement qui leur est imposé par la loi en ce qui a trait à l'obtention du consentement lorsqu'elles recueillent, utilisent ou divulguent ces renseignements.

Dans le but de procéder à un tel examen, nous avons effectué, dans un premier temps, une analyse objective, à l'aide d'une grille d'analyse, des politiques de confidentialité en ligne de dix entreprises[149]. Dans un deuxième temps, puisque la question du consentement constitue le fondement des lois sur la protection des renseignements personnels, nous nous sommes attardés plus spécifiquement à cet aspect des politiques de protection de la vie privée et avons évalué la conformité de quelques une des clauses avec les obligations qui découlent des lois de protection des renseignements personnels.

L'enquête a été effectuée par une seule personne, entre le 10 et le 20 avril 2007. Les entreprises ont été sélectionnées de façon à représenter un échantillon d'activités commerciales diversifiées. Nous avons opté pour des entreprises établies, relativement bien connues du public et qui affichent un site Internet.

Les entreprises analysées étant soumises à la LPRPDÉ ou à la LPRPSP, les principes que nous avons choisi d'évaluer sont les principales dispositions communes qui ont été enchâssées dans la loi fédérale et dans la loi québécoise.

Notre grille d'analyse visait à évaluer si les politiques de confidentialité affichées en ligne par les organisations respectaient les principes essentiels des lois sur la protection des renseignements personnels :

- la cueillette, ainsi que l'utilisation et la divulgation qui seront faites des renseignements sont portées à la connaissance du consommateur ; (LPRPDÉ principe 4.2, LPRPSP art.8 ; détermination des fins de la collecte)
- le consommateur a la possibilité de refuser cette cueillette, utilisation et/ou communication ; (LPRPDÉ principe 4.3, LPRPSP art.9, 12 à 15 ; consentement)
- les renseignements recueillis sont limités à ceux qui sont nécessaires pour les fins spécifiées ; (LPRPDÉ principe 4.4, LPRPSP art.5, 9(2) ; limitation de la collecte)
- les renseignements ne sont conservés que pour une durée limitée ; (LPRPDÉ principe 4.5, LPRPSP art.12 ; limitation de l'utilisation de la communication et de la conservation)
- des mesures de sécurité protègent les renseignements recueillis ; (LPRPDÉ principe 4.7 et LPRPSP art. 10 ; mesures de sécurité)
- le consommateur peut s'adresser à un agent responsable des renseignements personnels pour avoir accès à son dossier, porter plainte ou pour tout autre renseignement ; (LPRPDÉ principe 4.9, LPRPSP art.27, 29 accès aux renseignements

[149] *Amazon.ca, Mountain Equipment Coop, 24/7 Real Media, Croix-Rouge canadienne, Cyberpresse.ca, Ikéa, Aéroplan, Réseau Admission, Air Canada, Ticketpro*

personnels et LPRPDÉ 4.10, LPRPSP art.32 à 36 possibilité de porter plainte à l'égard du non-respect des principes)

- la politique affichée est claire et compréhensible[150] ; (LPRPDÉ principe 4.8 at LPRPSP art.14 : transparence)

La grille des résultats ci-dessous nous a permis d'évaluer le contenu des politiques de protection de la vie privée et leur conformité avec les lois en vigueur. Comme nous l'avons vu précédemment, le consentement du consommateur à la cueillette, l'utilisation et la divulgation de ses renseignements personnels constituent le fondement des législations fédérale et provinciales. Afin de mesurer si les divers paramètres du consentement sont respectés, nous avons d'abord vérifié plusieurs aspects des politiques : la politique est portée expressément à la connaissance du consommateur (point 1) ; le consentement explicite est recherché (opt-in) (point 2) ; la politique indique quels renseignements seront recueillis, de même que l'utilisation et la divulgation qui en seront faites (point 3) ; la politique prévoit la possibilité de contrôler et/ou refuser l'utilisation et la divulgation de renseignements non nécessaires à la réalisation de la transaction (point 4 et 5) ; la politique prévoit une nouvelle demande de consentement en cas de modification des politiques de confidentialité, la présence d'une clause de modification unilatérale étant considérée comme un non-respect de ce principe (point 6) ; la protection des renseignements n'est pas assujettie à la politique non divulguée de tiers avec lesquelles l'entreprise échange des renseignements, de partenaires de l'entreprise, etc. (point 7); limitation de la cueillette aux renseignements nécessaires pour les fins de la transaction (point 8) ; indication d'une limite à la durée de la conservation des renseignements (point 9) ; mention de la possibilité, pour le consommateur, d'avoir accès aux renseignements personnels le concernant (point 11) ; gratuité de la procédure d'accès (point 12) ; mention d'une procédure de plainte en cas de non-respect des principes régissant la protection des renseignements personnels (point 13) ; désignation d'un agent des renseignements personnel qui peut être contacté par téléphone et numéro de téléphone (point 10) ; mention de l'existence de mesures de sécurité visant à assurer la protection des renseignements recueillis (point 14). Nous avons finalement évalué si la politique, prise dans son ensemble, nous apparaissait claire et compréhensible, de façon à permettre au consommateur, à la lumière de son contenu, de donner un consentement libre et éclairé (point 15).

Si la grille a permis une appréciation objective des politiques affichées, la discussion qui suit met en lumière quelques exemples des irrégularités que nous avons relevées, notamment des clauses qui contreviennent au droit en vigueur ou qui induisent le consommateur en erreur de même que des informations qui s'avèrent, suite à une vérification, erronées ou trompeuses.

[150] La grille d'analyse et les résultats sont reproduits plus avant dans le texte.

Grille des résultats

	Oui	Non	Non spécifié
1. Politique de confidentialité portée expressément à la connaissance du consommateur.	1	9	
2. Demande de consentement explicite (opt-in).	1	9	
3. Détermination des renseignements recueillis, de l'utilisation et/ou de la divulgation qui en seront faites.	8		2
4. Mention d'une possibilité de contrôler l'utilisation qui sera faite des renseignements personnels.	1	8	1
5. Possibilité de contrôler/refuser la divulgation des renseignements personnels.	1	8	1
6. Mention d'une demande de consentement express du consommateur si une nouvelle utilisation des renseignements personnels est envisagée.		8	2
7. Non-assujettissement à une politique de protection des renseignements personnels externe non divulguée.	5	5	
8. Limitation de la quantité de renseignements recueillis aux fins nécessaires à la réalisation de la transaction.	6	3	1
9. Indication d'une limite à la durée de conservation des renseignements recueillis	2	1	7
10. Indication d'un agent responsable des renseignements personnels avec coordonnées (incluant numéro de téléphone)*	3	7	
11. Mention de la possibilité de consulter les renseignements personnels**	3		7
12. Accès gratuit au dossier (ou moyennant des frais raisonnables).	3		7
13. Mention de la procédure de plainte.	4	6	
14. Mention des mesures de sécurité	5		5
15. Politique claire et compréhensible.	1	9	

* Nous avons jugé la présence d'un numéro de téléphone comme un élément essentiel d'une politique de protection de la vie privée afin que les consommateurs puissent non seulement porter plainte, mais également obtenir de l'information rapidement.

** Pour la consultation des renseignements personnels, nous avons considéré la présence d'un numéro de téléphone ou l'accès au compte personnel par le biais d'internet comme satisfaisant le critère de la possibilité de consulter ses renseignements.

Faits saillants

Il appert de notre enquête que les politiques de confidentialité ne sont pas, en règle générale, portées expressément à la connaissance du consommateur. Les politiques sont généralement accessibles sur le site de l'entreprise par le biais d'un hyperlien, mais ce lien est souvent affiché en petits caractères et est souvent difficile à apercevoir pour l'internaute. Par ailleurs, les politiques sont souvent difficiles à comprendre et portent à confusion, laissant souvent entendre que tels renseignements ne sont pas recueillis ou communiqués sans le consentement du consommateur alors que dans les faits, ils pourront l'être.

Certaines entreprises assujettissent à la divulgation obligatoire de renseignements personnels la conclusion de la transaction et même la simple utilisation du site internet.

La moitié des entreprises étudiées divulguent à des tiers dont les politiques de protection de la vie privée ne correspondent pas nécessairement aux leurs les renseignements des consommateurs qu'elles ont recueillis.

L'ensemble des entreprises étudiées affichent une clause qui prévoit la possibilité d'une modification de leur politique de protection de la vie privée, qui ouvre la porte à une modification de l'utilisation et de la communication des renseignements personnels sans que le consommateur soit consulté, contrairement à ce que stipulent les lois qui mentionnent que le consentement n'est valide que pour les fins pour lesquelles il a été demandé et que tout changement nécessite un nouveau consentement.

À une exception près, toutes les entreprises étudiées présument du consentement plutôt que de tenter d'obtenir du consommateur un consentement positif.

Analyse

La nature et la forme du consentement

Comme nous l'avons vu, les lois qui régissent la protection des renseignements personnels stipulent que les entreprises sont tenues, sauf dans certains cas spécifiques[151], d'obtenir le consentement préalable des individus pour toute cueillette, utilisation ou communication des renseignements personnels tel que défini par ces lois. Un individu pourra refuser de divulguer toute information personnelle qui ne serait pas nécessaire à la réalisation de la transaction. Les entreprises ne peuvent donc légalement assujettir l'accès à un bien ou à un service à la collecte de tout autre type de renseignement personnel[152].

Or, il appert que de nombreuses entreprises assujettissent la réalisation de la transaction à la divulgation de renseignements personnels qui vont bien au-delà de l'information nécessaire. Cette pratique est particulièrement courante lorsque les achats se font sur internet. L'entreprise *Amazon.ca*, par exemple, mentionne qu'elle récolte : nom, adresse et numéro de téléphone et données relatives à la carte de crédit de celui qui procède à un achat; les noms, adresse et numéro de téléphone du destinataire ; les nom, adresse et numéro de téléphone des personnes figurant dans les coordonnées *1-clik* de l'internaute, le contenu des commentaires et courriels transmis sur *Amazon*, certaines informations financières, l'adresse IP, le nom d'utilisateur,

[151] *LPRPDÉ* art.7, *LPRPSP* art.18 à 25, *PIPA* Alberta art. 14, 17, 20, *PIPA* Colombie-Britannique art. 12, 15, 18 et voir également *supra*, *Les renseignements personnels à caractère public.*
[152] *LPRPDÉ* annexe 1 principe. 4.3.3, *LPRPSP* art. 9.

l'adresse électronique, le mot de passe *amazon.ca*, les renseignements relatifs au système et aux connexions (par exemple : le type et la version du fureteur, le système d'exploitation et la plate-forme), l'historique d'achats faits sur Amazon, le parcours URL complet ayant conduit l'internaute sur le site, le parcours sur le site (y compris la date et l'heure de la connexion). Par ailleurs, les conditions d'utilisation d'*Amazon.ca* prévoient qu'il est impossible de refuser de consentir à la cueillette, l'utilisation et la divulgation des renseignements personnels:

> *« En utilisant le site Amazon.ca et les services qui y sont offerts, vous acceptez d'être lié par les présentes conditions d'utilisation et par toute politique, conditions et règles afférentes. Si vous refusez d'être lié par une quelconque des présentes conditions d'utilisation, il vous est interdit d'utiliser le site Amazon.ca. »*[153]

Les lois sur la protection des renseignements personnels requièrent également, selon le degré de sensibilité des renseignements recueillis, un consentement explicite, c'est-à-dire un consentement positif (*opt-in*). Dans les conclusions d'une enquête[154], après avoir cité le principe 4.3.4 de la LPRPDÉ, qui énonce que « *les organisations doivent tenir compte de la sensibilité des renseignements. Si certains renseignements sont toujours considérés comme sensibles, par exemple les dossiers médicaux ou le revenu, tous les renseignements peuvent devenir sensibles suivant le contexte.*», le Commissaire précise que le consentement positif est la méthode « *la plus appropriée et la plus respectueuse à utiliser en tout temps*, » mais que, dans certains cas, l'utilisation de la méthode du consentement négatif (*opt-out*), qui consiste à présumer du consentement sauf avis contraire, peut être justifiée si les conditions suivantes sont respectées:

> *« 1. les renseignements personnels doivent être nettement non sensibles de par leur nature et leur contexte;*
> *2. la communication doit être limitée et bien définie quant à la nature des renseignements personnels qui seront utilisés ou communiqués et à la mesure dans laquelle ils sont censés l'être;*
> *3. les intentions de l'organisation doivent être circonscrites et bien définies, énoncées d'une manière raisonnablement claire et compréhensible et signalées à la personne au moment de recueillir ses renseignements personnels;*
> *4. l'organisation doit mettre en place une procédure efficace, facile et peu coûteuse qui permet d'emblée à ses clients de se désister ou de retirer leur consentement relativement aux activités secondaires de marketing, et elle doit les en aviser au moment de recueillir leurs renseignements personnels. »* [155]

[153] Amazon.ca, Conditions d'utilisation. [En ligne] http://www.amazon.ca/gp/help/customer/display.html/701-8773470-7208349?ie=UTF8&nodeId=918816 (consulté le 13 avril 2007).
[154] Commissariat à la protection de la vie privée, Conclusion de la Commissaire - *Résumé de conclusions d'enquête en vertu de la LPRPDÉ #207 (2003): Une entreprise de téléphones cellulaires satisfait aux conditions rattachées au consentement négatif*. [En ligne] http://www.privcom.gc.ca/cf-dc/2003/cf-dc_030806_02_f.asp (consulté le 13 avril 2007).
[155] *Ibid*.

La Commission d'accès à l'information, bien qu'en d'autres termes, exige également que le consentement prévu à l'article 14 de la LPRSP[156] soit explicite. La Commission précise que le consentement est « *un acte réfléchi qui doit répondre à toutes ces caractéristiques :*

- ***Le consentement doit être manifeste**, c'est-à-dire évident, certain et indiscutable.*
- ***Le consentement doit être libre**, c'est-à-dire être donné sans contrainte.*
- ***Le consentement doit être éclairé**, c'est-à-dire qu'il doit être précis, rigoureux et spécifique. Ainsi, l'entreprise doit indiquer quels renseignements seront communiqués, à qui, pourquoi et comment, et quelles en seront les conséquences. La personne qui donne un consentement doit être suffisamment informée au sujet des communications qui seront effectuées pour qu'elle puisse porter un jugement éclairé sur la portée du consentement.*
- *Le consentement est également donné à des **fins spécifiques** et pour la **durée nécessaire** à la réalisation des fins pour lesquelles il a été demandé. La durée ne sera pas nécessairement reliée à un nombre de jours, de mois ou d'années, mais pourra faire référence à un événement déterminé ou une situation précise. »*[157]

Malgré cela, il ressort de notre analyse que très peu d'organisations recherchent le consentement explicite du consommateur. En effet, sur l'ensemble des pratiques analysées, seulement une entreprise (*Ikéa*) a adopté la formule de consentement positif (*opt-in*). Pour toutes les autres entreprises, non seulement le consentement était-il présumé plutôt que manifeste, il était tout simplement impossible, lors de la réalisation de la transaction, de retirer son consentement, malgré le fait que les lois stipulent que le consentement doit être obtenu avant ou au moment de la collecte des renseignements personnels.[158]

Lorsqu'il est possible, le retrait de consentement doit se faire par le biais de procédures écrites et complexes. Par exemple, Aéroplan mentionne dans sa politique que :

> *« Aéroplan ne recueillera, n'utilisera ni ne divulguera aucun renseignement personnel concernant un membre sans le consentement de celui-ci. »*[159]

Un peu plus loin, la politique précise que :

> *« nous fournirons à nos membres des explications détaillées sur les moyens mis à leur disposition pour faire rayer leur nom des listes que nous échangeons avec nos partenaires*[160] *(formulaire à remplir sur papier*[161]*) »*[162]

---

[156] *LPRPSP* art. 14.
[157] Commission d'accès à l'information. *Foire aux questions.* [En ligne] http://www.cai.gouv.qc.ca/11_foire_aux_questions/entreprises.html#theme8 (consulté le 16 avril 2007)
[158] *LPRPDÉ* Annexe 1 principe 4.3.1 ; *LPRPSP* art. 1 ; *PIPA* Colombie-Britannique art.6 ; *PIPA* Alberta art.7(1)
[159] Aéroplan. Politique sur la vie privée. [En ligne] http://www.Aéroplan.com/privacy/privacy_policy/privacy.do (consulté le 16 avril 2007)
[160] La liste des partenaires d'Aéroplan comprend notamment des compagnies aériennes, des hôtels, des compagnies de location de voiture, de cartes de crédit, de télécommunication, d'assurances, des compagnies pétrolières et des entreprises de commerce de détails. Au total, la liste contient plus d'une centaine d'entreprises. [En ligne] http://www.Aéroplan.com/earn_miles/our_partners/partner_contact_information.do (consulté le 16 avril 2007).
[161] Nous avons été incapables de trouver, [En ligne], les explications détaillées en question ou le formulaire papier dont Aéroplan fait mention, l'hyperlien y menant n'étant pas fonctionnel.
[162] Aéroplan. Politique sur la vie privée. [En ligne] http://www.Aéroplan.com/privacy/privacy_policy/privacy.do (consulté le 16 avril 2007).

L'imposition d'une procédure écrite a également été retrouvée dans la politique de la Croix-Rouge canadienne[163].

Cette façon de faire pourrait contrevenir à la Loi québécoise qui stipule à son article 25 qu'une « *personne qui désire retrancher d'une liste nominative ses renseignements personnels doit pouvoir le faire en tout temps au moyen d'une demande verbale ou écrite, auprès de toute personne qui détient ou utilise cette liste.* »[164]. À notre avis, l'intention du législateur étant de permettre au consommateur de retirer son consentement quand bon lui semble, le choix de la forme de l'avis devrait revenir au consommateur plutôt que d'être imposé par le commerçant. Une telle interprétation assurerait par ailleurs que le droit des individus de retirer leur consentement puisse être plus largement exercé, attendu que la nécessité d'un écrit ou toute autre procédure particulière imposée par le commerçant pourrait empêcher plusieurs personnes d'exercer son droit de retrait.

Le consentement à l'utilisation des renseignements personnels

L'exigence d'un consentement, tel que défini précédemment, s'applique non seulement à la cueillette, mais également à toute utilisation qui sera faite des renseignements recueillis. En vue de vérifier le respect de cette exigence, nous avons évalué de quelles façons étaient susceptibles d'être utilisés les renseignements recueillis et tenté de voir si cette utilisation avait été précédée d'un consentement valable de la part du consommateur.

Puisque, comme nous l'avons mentionné plus haut, une seule entreprise recherchait le consentement explicite du consommateur, de l'ensemble des entreprises étudiées, huit procédaient, sans un consentement positif, à des utilisations secondaires des renseignements recueillis.

Aéroplan, par exemple, détaille comme suit ses méthodes de cueillette, d'utilisation et de communication des renseignements:

> *« Aéroplan et ses partenaires s'échangent des renseignements personnels concernant les membres d'Aéroplan (…) sur les préférences des membres dans le but de leur offrir et de leur fournir des primes, avantages, produits, biens et services de qualité et ce, d'une manière efficace.*
>
> *(…) Afin d'offrir les services et privilège auxquels ils ont droit, Aéroplan est appelé à recueillir, utiliser et communiquer des renseignements à leur sujet. Ces renseignements peuvent avoir un caractère personnel.*
>
> *(…) Il peut arriver à l'occasion que nous communiquions des renseignements personnels à nos agences à des fins de traitement pour identifier quels membres seraient susceptibles de s'intéresser aux primes, avantages, produits, biens et services offerts par Aéroplan ou ses partenaires.*

---

[163] « *Lorsqu'un client ou un donateur ne consent pas à ce que ses renseignements personnels soient divulgués à d'autres organismes, tel que prévu par la présente politique, ou lorsqu'un client ne souhaite pas recevoir d'information sur d'autres services, il peut en informer la Société. Le cas échéant, il doit en aviser la Société par écrit, en s'adressant au programme en vertu duquel les renseignements personnels sont recueillis, au directeur général de la zone/division de la Société où il réside habituellement ou à l'agent de la protection de la vie privée de la Société, au siège social à Ottawa.* » Croix-Rouge Canadienne, Politique de confidentialité, [En ligne] http://www.croixrouge.ca/article.asp?id=010958&tid=001 (consulté le 13 avril 2007).

[164] *LPRPSP*, art.25. La loi fédérale et les autres lois provinciales précisent aussi, quant à elles qu'une personne doit pouvoir retirer son consentement en tout temps, mais sans mentionner la forme de l'avis. *LPRPDÉ*, annexe 1 principe 4.3.8 ; *PIPA* Colombie-Britannique et Alberta art.9

> *« (…) Aéroplan recueille des renseignements personnels pour les fins suivantes (…) : Mieux comprendre les préférences, besoins et intérêts des membres ; permettre à nos partenaires d'offrir à nos membres des primes, avantages, produits biens et services dans le cadre du programme Aéroplan.»*[165]

Il ressort de l'analyse de cette clause que des renseignements seront utilisés et communiqués pour des fins de marketing aux partenaires d'Aéroplan, soit plus d'une centaine d'entreprises. On remarquera que le libellé « *recours à des agences à des fins de traitement pour identifier quels membres seraient susceptibles de s'intéresser aux primes (…)* » semble signifier que ces agences dressent des profils de membres pour Aéroplan et ses partenaires.

Des politiques transparentes pour un consentement éclairé

Un consentement ne pourra être éclairé que si la personne qui le donne en comprend la portée. Tel consentement ne sera possible que si les politiques sont claires et transparentes, de façon à permettre au consommateur de savoir et de comprendre quels seront les renseignements qui seront recueillis et quelles utilisations en seront faites. Or, de l'ensemble des politiques analysées, une seule (*Mountain Equipment Coop*) remplissait ce critère. Voici quelques exemples de politiques qui, selon nous, induisent le consommateur en erreur, venant ainsi vicier son consentement.

Chez *Aéroplan*, une clause mentionne ce qui suit :

> *« Les renseignements personnels concernant les préférences, besoins et intérêts des membres sont utilisés pour identifier ceux d'entre eux qui sont les plus susceptibles d'être intéressés par les produits et services offerts par Aéroplan et ses partenaires. Ces renseignements sont utilisés exclusivement pour permettre à Aéroplan et à ses partenaires de proposer des primes, avantages, produits et services susceptibles d'intéresser les membres dans le cadre du programme Aéroplan. Aéroplan ne fournit aucun profil individualisé des membres à ses partenaires ou à des tiers. »*

La clause indique expressément que l'entreprise ne transmet pas de profil individualisé. Par contre, deux paragraphes plus loin, Aéroplan mentionne que :

> *« À l'occasion, Aéroplan peut également fournir à un partenaire une liste de membres qui répondent à certains critères généraux (…) »*

Une « liste de membres qui répondent à certains critères généraux » n'est-elle pas une liste de personnes correspondant à un certain profil ? La nuance entre la segmentation comportementale et le profil individualisé est à notre avis bien mince et la formulation de ces clauses trop susceptibles d'induire en erreur le consommateur.

Chez *Air Canada* :

> *« Le fait de réserver une place sur un vol ou d'adhérer à aircanada.com donne à Air Canada votre consentement implicite à l'utilisation des renseignements qui vous concernent aux fins demandées. (…) Air Canada n'utilise pas ni ne communique des renseignements personnels à des fins autres que celles pour lesquelles ils sont recueillis, sauf consentement explicite à cet égard de votre part ou sauf si la société y est tenue par la loi »*[166]

[165] Aéroplan. Politique sur la vie privée. [En ligne] http://www.Aéroplan.com/privacy/privacy_policy/privacy.do (consulté le 16 avril 2007).
[166] Air Canada. Politique de confidentialité. [En ligne]

Ainsi, nulle part dans sa politique, Air Canada ne mentionne qu'elle transfère les renseignements personnels qu'elle recueille à d'autres entreprises. L'entreprise les divulgue par contre à Aéroplan[167] qui, à son tour, transmet, comme nous l'avons mentionné précédemment, les informations qu'elle possède à plus d'une centaine de partenaires. Or, pour être au courant de ce fait, le consommateur devra consulter la politique de protection des renseignements personnels d'Aéroplan. Il nous semble que ce manque de transparence induit le consommateur en erreur quant à l'utilisation et la divulgation des renseignements qui le concernent et rend impossible un consentement éclairé.

La moitié des politiques de protection de la vie privée des entreprises que nous avons étudiées avaient recours à de telles clauses externes, obligeant le consommateur qui voudrait connaître l'ensemble des utilisations qui peuvent être faites de ces renseignements, à lire chacune des politiques des partenaires.

Si Aéroplan affichait sur son site une liste de plus d'une centaine de partenaires à qui les renseignements personnels étaient communiqués, d'autres ont recours à une liste non exhaustive empêchant ainsi le consommateur de connaître les éventuels détenteurs de ses renseignements. Par exemple, l'entreprise TicketPro mentionne, dans sa politique :

> *« Lorsque vous fournissez des renseignements personnels lors d'achat de billet sur le Site, vous consentez à ce que nous partagions vos renseignements, si nécessaire, avec nos agents, représentants, contractants, fournisseurs de services et partenaires d'événements, tels que promoteurs, artistes, exploitants, les ligues et autres tierces parties associées au billet ou au spectacle, à l'activité ou à l'événement (ci-après, les « Partenaires d'événements »).*
>
> *Il nous est impossible de vous offrir une option distincte de consentir ou non au partage de vos renseignements personnels avec les Partenaires d'événements. Les Partenaires d'événements peuvent utiliser vos renseignements personnels selon leur propre politique de confidentialité. Ils pourraient donc les utiliser pour communiquer avec vous ou les partager avec d'autres. Vous devez communiquer avec ces Partenaires d'événements pour les informer directement de votre décision en regard de l'utilisation de vos renseignements personnels.*
>
> *À l'exception de ce qui est autrement décrit dans la présente politique, nous n'avons aucun contrôle sur les pratiques en matière de renseignements personnels des Partenaires d'événements ou autres tierces parties. Comme il est décrit ci-haut, en achetant des billets sur le Site, en choisissant de recevoir des communications ou de participer à des concours, des tirages ou autres programmes associés à des tierces parties ou commandités par elles, en remplissant un formulaire d'inscription sur le Site, ou en choisissant autrement de nous permettre de partager vos renseignements personnels avec de tierces parties selon les conditions de la présente politique, vous nous autorisez à partager vos renseignements personnels avec les Partenaires*

http://www.aircanada.com/fr/about/legal/privacy/policy.html (consulté le 15 avril 2007).

[167] *Ibid.* « *En vous joignant à Air Canada.com, vous adhérez automatiquement à Aéroplan (…) pour que ces opérations soient possibles, le groupe Air Canada et les partenaires Aéroplan doivent échanger de l'information afin de s'assurer que votre compte est à jour et que les milles sont crédités et débités correctement.* »

> *d'événements et tierces parties en question et vous acceptez notre non-responsabilité en regard de leurs actions ou omissions.»*[168] *(nos soulignés)*

Les termes de cette politique de divulgation des renseignements personnels donnent à l'entreprise carte blanche, suite à un consentement obligatoire, pour une utilisation et une divulgation complètement arbitraire par TicketPro et ses partenaires des renseignements recueillis.

Limitation de la collecte et la durée de conservation des renseignements recueillis

Autant les lois provinciales que les lois fédérales obligent les organisations et entreprises à limiter la quantité de renseignements recueillis à ce qui est nécessaire aux fins pour lesquelles ils sont recueillis[169], de limiter la conservation des données dans le temps[170] et de permettre à une personne d'exiger que ses renseignements soient retirés de la liste qu'a pu monter celui qui a recueilli les renseignements.[171]

Encore une fois, les pratiques de certaines entreprises se sont révélées problématiques. Aéroplan, par exemple, mentionne qu'un membre dont le compte est inactif depuis 3 ans pourra demander la destruction des renseignements. En l'absence d'une demande de la part du membre, Aéroplan conservera ces données durant sept ans. Par ailleurs, si un membre désire *« mettre fin à son adhésion au programme, tous les renseignements le concernant qui sont détenus par Aéroplan sont archivés dans les 60 jours et conservés exclusivement à des fins de vérification de conformité jusqu'au terme de la période de trois ou sept ans.* »[172]

Au Réseau Admission on mentionne que, pour supprimer vos renseignements, vous devez communiquer avec le service à la clientèle. On précise toutefois que :

> *« La suppression du profil « mon compte » ne supprime pas tous les renseignements personnels ou autres contenus dans nos systèmes, puisque la majorité ou tous ces renseignements sont conservés afin de garder un historique de notre relation commerciale avec vous. »*[173]

La loi fédérale impose aux entreprises l'obligation d'élaborer des lignes directrices pour la conservation des renseignements personnels[174]. Le Commissariat à la protection de la vie privée énonce sur son site que « *vous ne devez conserver les renseignements personnels qu'aussi longtemps que nécessaire pour la réalisation des finalités déterminées (…) vous devez détruire, effacer ou dépersonnaliser les renseignements personnels dont vous n'avez plus besoin aux fins précisées (…)* »[175].

---

[168] Ticketpro. Politique de confidentialité. [En ligne] http://www.ticketpro.ca/confidentiel_fr.html (consulté le 3 avril 2007).
[169] *LPRPDÉ*, annexe 1 principe 4.4 et ss, *LPRPSP* art.5, *PIPA* Alberta et Colombie-Britannique art.11.
[170] *LPRPDÉ*, annexe 1 principe 4.5 et ss, *LPRPSP* art.12, *PIPA* Alberta, art.35, *PIPA* Colombie-Britannique art.35(2).
[171] *LPRPDÉ*, annexe 1 principe 4.3.8, *LPRPSP* art.24,25,26, *PIPA* Alberta et Colombie-Britannique, art. 9.
[172] Aéroplan. Politique *Op. cit.*, note 166.
[173] Réseau Admission. Politique de protection de la vie privée. [En ligne] http://www.admission.com/html/admission/policiesPrivacy.html?l=FR (consulté le 13 avril 2007).
[174] *LPRPDÉ*, annexe 1, principe 4.5.2.
[175] Commissariat à la protection de la vie privée, fiche d'information, « Se conformer à la *Loi sur la protection des renseignements personnels et les documents électroniques* » [En ligne] http://www.privcom.gc.ca/fs-fi/02_05_d_16_f.asp (consulté le 13 avril 2007).

Il est clair que la politique de conservation doit prévoir la durée de conservation des renseignements personnels[176]. À la lumière des dispositions législatives et de la jurisprudence, il est toutefois impossible de déterminer si la Commissaire, dans le cas où une entreprise aurait adopté une politique de conservation des données et prévu une durée de conservation, dispose des pouvoirs qui lui permettraient de déterminer si le délai de conservation prévu est abusif.

Les lois provinciales prévoient elles aussi une limite à la durée de conservation[177] et la Commission d'accès à l'information, précise sur son site que: « *Le dossier est conservé tant et aussi longtemps que l'objet pour lequel les renseignements ont été recueillis n'est pas accompli*.»[178] Une fois de plus, l'absence de jurisprudence sur ce sujet rend difficile l'établissement des balises de cette obligation.

Si la politique du Réseau Admission, qui refuse de supprimer les renseignements concernant un individu, va expressément à l'encontre des lois, on pourrait s'interroger sur la pertinence d'un délai de trois ou sept ans suivant l'accomplissement de l'objet premier de la cueillette que prévoient certaines entreprises pour mettre fin à la conservation des données personnelles.

La sécurisation des données

Les lois sur la protection des renseignements personnels obligent les entreprises à prendre des mesures de sécurité afin de protéger les renseignements personnels qu'elles recueillent.[179] Par conséquent, les entreprises ne peuvent s'exonérer des dommages que pourrait subir une personne dont les renseignements personnels ont été volés si des mesures raisonnables de sécurité n'étaient pas en place. Malgré tout, de nombreuses entreprises s'exemptent de toute responsabilité en cas de perte ou de vol de données.

La quantité de renseignements qu'accumulent les entreprises et la durée de leur conservation sont d'autant plus inquiétantes que la sécurité qui entoure le stockage et l'utilisation des données est également problématique. En effet, une étude réalisée récemment en Europe a indiqué que plus de la moitié des grandes entreprises européennes ne cryptent pas leurs données sortantes. Pourtant, 13 % des entreprises interrogées avouent avoir été victimes de violation de données confidentielles sortantes au cours de l'année précédente. Cette étude soulève une certaine inquiétude quant à la volonté réelle des entreprises de protéger les données confidentielles qu'elles détiennent et communiquent en contravention des obligations légales en vigueur. En effet, parmi les entreprises interrogées, « *plus de la moitié n'ayant pas recours au cryptage (59 %), disent ne pas en ressentir le besoin commercial, ce qui montre qu'un important travail de sensibilisation reste nécessaire sur les dangers de la violation de données et les solutions disponibles pour les prévenir.* »[180]

---

[176] Conclusion de la Commissaire - *Résumé de conclusions d'enquête en vertu de la LPRPDÉ #255 Remise en question des pratiques de collecte et de conservation de l'autorité aéroportuaire,* [En ligne] http://www.privcom.gc.ca/cf-dc/2003/cf-dc_031224_f.asp (consulté 1 juin 2007).
[177] PIPA Colombie-Britannique art. 35(2), PIPA Alberta art. 35.
[178] Commission d'accès à l'information, Foire aux questions, entreprises privées, *Les dossiers personnels dans les entreprises privées* [En ligne] http://www.cai.gouv.qc.ca/ (consulté le 13 avril 2007).
[179] *LPRPDÉ* art. 4.7 et ss ; *LPRPSP*, art 10, 11.
[180] « Les entreprises nonchalantes face aux courriels » La Presse Affaire, 12 avril 2007 [En ligne] http://technaute.lapresseaffaires.com/nouvelles/texte_complet.php?id=81,12399,0,042007,1345603.html&ref=cyberpresse (consulté le 13 avril 2007).

> *« Actuellement, ça leur coûte moins cher de rembourser les clients que de mettre des mesures de sécurité en place, prétend Alain Mercier conseiller principal au Centre de recherche informatique de Montréal. Ça pourrait coûter très cher pour avoir une mesure assez efficace et encore là, il va probablement y avoir une manière de la contourner. Ce qui peut arriver, c'est que les gens vont un peu perdre confiance en les transactions en ligne, continue-t-il. On est en train d'étirer l'élastique, mais jusqu'où va-t-on être capable d'équilibrer les choses, ça reste à voir. »*[181]

Il est actuellement difficile pour le consommateur de connaître les mesures de sécurité qui entourent la protection de leurs renseignements personnels puisque les politiques des entreprises n'en font généralement pas mention. On soulignera de plus que, attendu qu'aucune obligation n'est faite aux entreprises de dénoncer les vols de renseignements personnels dont elles pourraient être victimes, le consommateur pourra ainsi ne même pas savoir que des renseignements le concernant ont été volés à l'entreprise.

Autres considérations

Au cours de notre analyse, outre les problématiques directement reliées au consentement, nous avons noté plusieurs situations problématiques, notamment :

- Chez Aéroplan : Toute plainte ou demande d'enquête fera l'objet d'une enquête ou d'une réponse dans les 60 jours, alors que la loi a fixé comme délai maximal 30 jours[182] ;

- Chez deux entreprises (La Presse et Air Canada), il a été impossible de joindre la personne responsable de la protection de la vie privée au numéro affiché dans la politique de protection de la vie privée, parce qu'il n'était plus valide.

- Par ailleurs, les politiques de protection de la vie privée des entreprises étudiées sont difficilement accessibles sur leur site web, se trouvant en petits caractères au bas de l'écran. Cette pratique est très peu efficace sur le plan de la qualité communicationnelle, car elle oblige souvent le consommateur à faire défiler la page pour accéder au document recherché.[183]

- La longueur des politiques, les termes utilisés, le manque de transparence et leur complexité les rendent souvent incompréhensibles pour le consommateur.

En 2003, la Conférence internationale des Commissaires pour la protection des données a adopté une résolution qui souligne l'importance, pour les organisations, de donner des indications beaucoup plus précises sur la façon dont elles traitent et utilisent les données personnelles.[184] Les notices d'informations étant justement un excellent outil pour permettre aux individus de savoir de quelles façons sont utilisés les renseignements personnels recueillis à leur sujet, l'OCDE a procédé à une étude visant à analyser les notices d'informations sur la protection de la vie privée. L'étude souligne que, si 60 % des gens déclarent ne pas être

[181] CRAIG, Pierre, « Hameçonnage, ne soyez pas le poisson » émission La facture du 29 novembre 2005, Radio-Canada, Montréal, Québec, http://www.radio-canada.ca/actualite/v2/lafacture/niveau2_5811.shtml (consulté le 20 mars 2007).
[182] *LPRPDÉ* art.8(3), *LPRPSP* art.32, *PIPA* Colombie-Britannique art.53, *PIPA* Alberta art.54(1) qui prévoit, pour sa part, un délai de 50 jours.
[183] GAUTRAIS, Vincent, « La couleur du consentement » Montréal, 2003 p. 10 [En ligne] http://www2.droit.umontreal.ca/cours/ecommerce/_textes/consentement2003CPI.pdf
[184] Conférence internationale des Commissaires, [En ligne] http://www.privacyconference2003.org/resolution.asp (consulté le 10 avril 2007).

indifférents à ces politiques, la plupart ne les lisent pas. En outre, il ressort que, même lorsque les personnes prennent le temps de les lire, les politiques sont si complexes, longues et écrites dans un langage technique et juridique difficilement accessible, qu'elles en retiennent bien peu. L'étude conclut que les politiques actuellement affichées par les entreprises se révèlent inefficaces pour communiquer des informations. Elles sont trop longues et répétitives, contiennent du jargon juridique et financier, ne font pas ressortir les points importants et n'incitent pas les gens à les lire.[185] Par ailleurs, le consommateur qui désire transiger via internet procède ainsi parce qu'il a des attentes de vitesse et désire gagner du temps. Or, la lecture à l'écran requiert 25% plus de temps que la lecture sur support papier[186], exacerbant davantage la problématique que pose la longueur de la politique de protection de la vie privée.[187] L'étude démontre qu'il est facile d'améliorer une politique de protection de la vie privée notamment en ayant recours à des cases à cocher, des champs de signatures, des titres évocateurs, etc. Les trois quarts des personnes interrogées ont estimé qu'elles prêteraient davantage attention à ces politiques si elles étaient mieux présentées.[188]

En 2001, des organismes officiels des États-Unis[189] ont commandé une étude en vue de déterminer pourquoi les consommateurs ne lisaient pas les politiques de protection de la vie privée et de formuler des principes pour la rédaction de politiques qui seraient plus efficaces[190]. Cette étude visait à mettre sur pied des déclarations de politiques de protection de la vie privée simplifiées et de mesurer leur compréhension par une variété de consommateurs provenant de l'ensemble des États-Unis. Les chercheurs évaluaient la compréhension des politiques par le biais de plusieurs cycles de tests, menés sur une période de 12 mois. Le contenu et la présentation étaient modifiés à chaque cycle afin d'obtenir, à la conclusion de l'étude, un prototype de politique accessible et compréhensible. Une des conclusions de cette étude porte sur la nécessité de mettre en contexte les informations fournies, afin de faciliter leur compréhension par le consommateur. Par exemple, bien que l'on informe le consommateur que des renseignements les concernant peuvent être divulgués à des tiers, la plupart ignorent concrètement comment ces pratiques fonctionnent et comment elles peuvent se répercuter sur eux. Il ressort également de cette étude que l'information complexe doit être simplifiée afin de faciliter sa compréhension et permettre un consentement éclairé.

Par ailleurs, il ne faut pas négliger l'incidence que peut avoir le support électronique sur la compréhension des politiques de protection de la vie privée. En effet, plusieurs auteurs ont

---

[185] OCDE « Groupe de travail sur la sécurité de l'information et la vie privée » 24 juillet 2006, DSTI/ICCP/REG(2006)5/FINAL, p. 4. [En ligne] http://appli1.oecd.org/olis/2006doc.nsf/43bb6130e5e86e5fc12569fa005d004c/a56f6b2f04871d3fc12571b5003dac3f/$FILE/JT03212215.PDF (consulté le 13 avril 2007).

[186] NIELSON Jakob, « Writing for the Web » Sun microsystem, États-Unis, [En ligne] http://www.sun.com/980713/webwriting/

[187] GAUTRAIS, Vincent, *Op. cit.,* note 184, p. 8

[188] OCDE*, Op. cit.,* note 186, p. 8.

[189] Les organismes participants sont les suivants : Commission fédérale du commerce, Conseil des gouverneurs du Système fédéral de réserve, Société fédérale de garantie des dépôts, Service du contrôle de la monnaie, administration des mutuelles nationales de crédit, Commission des opérations de Bourse.

[190] KLEIMANN Communication Group Inc. « *Evolution of a Prototype : Financial Privacy Notice* », 28 février 2006, [En ligne] http://www.ftc.gov/privacy/privacyinitiatives/ftcfinalreport060228.pdf (consulté le 20 mars 2007).

souligné la moins bonne lisibilité des écrans en comparaison du papier,[191] précisant notamment que : « *Le document écran est source de beaucoup plus d'imprécisions, d'éventuels quiproquos, encore que l'usager ne manquera pas de faire preuve, face à un document électronique, de sa désinvolture habituelle. S'il se donne la peine de « scroller » (scrolling), c'est-à-dire de faire défiler le texte, il n'absorbe pas vraiment le contenu du texte et ne va pas voir d'éventuels liens hypertextes insérés dans le texte initial, pour finir par « cliquer » sans forcément avoir pleinement conscience de ce à quoi il s'engage.*»[192]

[191] GAUTRAIS, Vincent, *Op. cit.,* note 184, p. 8 ; voir également NIELSON, Jakob, *Op. cit.,* note 187, DILLON, Andrew « Reading from paper versus screens : a critical review of the empirical littérature » (1992) 35 Ergonomics, 1297-1326

[192] GAUTRAIS, V. et MACKAAY E., « Les contrats informatiques » dans Denys-Claude LAMONTAGNE, *Contrats spéciaux*, Cowansville, Éditions Yvon Blais, 2001, p. 296.

AVANTAGES, DESAVANTAGES ET DERAPAGES POSSIBLES

Bien que le monde virtuel d'internet soit différent du monde réel, permettant l'accès instantané à une foule d'information et de produits, il ne faut pas oublier que derrière nos écrans se trouvent une foule d'individus qui nous permettent d'avoir accès à tout ce matériel. En effet, mis à part les frais de connexion (et pour peu qu'il évite les sites payants), l'utilisateur d'internet peut naviguer à sa guise dans le monde virtuel sans aucuns frais additionnels. Pourtant, internet n'est pas gratuit et les différents administrateurs de sites internet doivent user d'ingéniosité afin de financer les débours qu'engendre l'opération d'un site. Ils y parviennent notamment par le biais de la publicité qui y sera affichée. Cette publicité permettra de générer des revenus pour les différents acteurs, publicitaires et commerçants. Plus l'administrateur d'un site connaît le profil des internautes qui visitent son site, plus la publicité qu'il y affiche pourra être efficace et rentable. Producteurs de sites web, hébergeurs, fournisseurs d'accès internet et publicitaires, tous tirent des bénéfices de la publicité sur internet, le consommateur représentant le dénominateur commun de leurs attentions et le générateur ultime de leurs revenus, par le biais de ses achats, mais aussi par les renseignements qu'il fournit et dont ils pourront faire commerce.

Quels sont les avantages que le consommateur tire, pour sa part, de ce commerce de renseignements personnels ?

Profilage

Les publicitaires clament haut et fort que le consommateur est l'ultime bénéficiaire de la cueillette, de l'échange et de la vente de renseignements personnels, puisqu'elles lui permettent d'avoir accès à plus d'information concernant de nouveaux produits et services, de recevoir une information plus ciblée selon ses goûts et préférences, qui pourra, ultimement, lui permettre de faire des choix mieux éclairés. Par ailleurs, les renseignements fournis par le consommateur ne sont pas toujours échangés ou vendus à des tiers, mais sont souvent conservés au sein d'une même entreprise afin d'agrémenter la prochaine relation qu'aura un consommateur précis avec cette même entreprise.

La chaîne d'hôtels Ritz-Carlton, par exemple, conserve les informations des clients qui ont séjourné dans ses hôtels. Les besoins exprimés et les choix de plus de 500 000 clients se retrouvent dans le système informatique de la chaîne hôtelière Customer Loyalty Anticipation Satisfaction System (CLASS) : renseignements concernant le séjour, notamment : la grandeur de lit utilisé, le type d'oreiller (plume ou mousse), la nourriture commandée, etc., bref, tout ce que le consommateur a choisi et qui indique ses préférences. Ces informations serviront à agrémenter son prochain séjour par le biais de services plus personnalisés[193].

Certains consommateurs apprécient cette personnalisation du service et de la publicité, qui optimise leur consommation et leur permet de correspondre davantage à leurs goûts et leurs attentes[194]. Par exemple, l'internaute qui visite fréquemment des sites reliés au voyage pourra

[193] O'HARROW, Robert Jr., « Consumers trade privacy for lower prices » Washington Post, December 31, 1998, p. A-1.
[194] Ponemon Institute, Revenue Science, Chapell & Associates, septembre 2004.

voir s'afficher des publicités de forfaits de voyage ou de rabais sur des billets d'avion, sans qu'il ait à effectuer des recherches supplémentaires. Le consommateur peut ainsi découvrir plus facilement des offres commerciales adaptées à ses centres d'intérêt et en bénéficier. Lors d'un récent sondage, 65% des consommateurs ont mentionné considérer que les publicités sont moins dérangeantes ou intrusives lorsqu'elles correspondent mieux à leurs intérêts ou à leurs besoins.[195]

À la source de la publicité ciblée se retrouve le profilage des individus. Si la technique du marketing personnalisé dit « *one to one* » permet au consommateur de se voir présenter des offres qui, selon le profil établi, devraient présenter un plus grand intérêt, il serait toutefois naïf de croire que ces pratiques ne visent qu'à satisfaire le consommateur. Comme le mentionne le site d'*Abacus*: *« As the majority of customers are often recruited at an initial loss, it is vital that they are encouraged to purchase from you again.* »[196] Ainsi, alors qu'internet est perçu comme étant ouvert, neutre et anonyme, l'effet du profilage est d'en faire un outil orienté et scrutateur, qui permet de manipuler les utilisateurs en choisissant pour eux le contenu qui leur sera présenté, leur fournissant une information limitée en fonction de leur navigation antérieure et des besoins des clients de l'agence de marketing.

Par ailleurs, l'augmentation fulgurante du nombre de bases de données contenant des renseignements personnels soulève de nombreuses questions, qui vont au-delà de l'aspect légal ou non des différentes méthodes utilisées. Comme le mentionne Solove:

> *« The problem with databases and the practices cure-ongles associated with them is that they disempowered people. They make people vulnerable by stripping them of control over their personnel information. There is no diabolical motive or secret plan for denomination ; rater, there is a web of thoughtless décisions made by low-level bureaucrates, standardized policies, rigid routines and a way of relating to individuals and their information that often becomes indifferent to their welfare. »*[197]

Un des problèmes dénoncés par les défenseurs du droit à la vie privée est notamment le danger que représente le recours systématique aux banques de renseignements personnels, notamment par certaines entreprises et même par les gouvernements, alors que rien ne garantit l'exactitude des renseignements qu'elles contiennent. Par ailleurs, l'utilisation de ces renseignements peut avoir un impact significatif, puisqu'elle peut influencer l'octroi de crédit, l'évaluation d'une demande d'emploi, l'inclusion de son nom sur une liste de terroristes ou de criminels potentiels, etc.

De plus, le profilage des consommateurs crée des catégories différentes de consommateurs, soient ceux qui sont susceptibles d'acheter et ceux qui ne le sont pas, des « bons » et « mauvais » consommateurs, catégorisation qui ouvre la porte à des pratiques discriminatoires de la part des entreprises. En juin 1995, la Cour de cassation française a jugé illégale la segmentation comportementale, c'est-à-dire l'attribution de caractéristiques à un individu identifiable basé sur des comportements d'achats ou de consommation, qu'effectuait une banque qui avait créé des catégories telles que « ne s'améliorera pas avec le temps », « laxiste », « moderniste », « difficile à convaincre », « méfiant ». Chaque client se voyait ainsi

---

[195] *Ibid*.

[196] Abacus, *Data Driven Solutions,* , site d'Abacus, Teddington, Royaume-Uni, 2006 [En ligne] http://www.abacusalliance.com/Data%5FDriven%5FSolutions/ (consulté le 15 avril 2007).

[197] SOLOVE, Daniel, « The Digital Person : Technology and Privacy in the Information Age » 2004, New York, États-Unis, p. 1.

attribuer un code et le personnel recevait des instructions quant à la manière d'aborder les clients d'un segment particulier.[198]

Par ailleurs, la prévalence de la commercialisation ciblée fait également craindre l'apparition de méthodes de plus en plus agressives et envahissantes, particulièrement sur internet. Par exemple, l'impossibilité d'accéder à un site sans avoir préalablement visionné au complet une publicité, la présence de publicité où la fonction permettant la fermeture de la fenêtre est dissimulée, l'activation de la publicité par hyperlien caché, etc. L'amélioration des techniques informatiques permettant le marketing ciblé risque d'entraîner une augmentation du recours par les entreprises à ce type de techniques, au grand dam des internautes qui jugent les fenêtres intempestives (*pop up*)[199] trois fois plus dérangeantes que les publipostages et neuf fois plus que les annonces télévisées[200]. Conçues pour permettre l'offre de produits et services le plus susceptible d'être achetés par le consommateur, les techniques de profilage risquent non seulement de venir modifier le web en présentant des publicités de plus en plus agressives, mais également d'exploiter les vulnérabilités de l'internaute en l'encourageant à surconsommer.

De façon générale, les techniques de cueillette de renseignements sur internet, parce que les renseignements sont recueillis et utilisés à l'insu de l'internaute, constituent une atteinte au respect de la vie privée et aux lois qui visent à la protéger. Ce sont entre autres les utilisations de ces différentes techniques qui sont à la source du profilage qui ont poussé plusieurs groupes à dénoncer leur utilisation de façon non conforme avec le respect des libertés individuelles et de la vie privée.[201] Par conséquent, il convient ici de se pencher sur ces différentes méthodes afin d'évaluer si elles peuvent constituer un avantage pour le consommateur.

Fichiers témoins (cookies)

Au départ, les fichiers témoins ont été conçus au bénéfice de l'internaute : aide-mémoire de l'ordinateur, ils visaient à permettre une navigation plus rapide et plus efficace, notamment lorsqu'un internaute retourne sur un site web déjà visité, en affichant par exemple automatiquement le site dans sa langue préférée, ou en entrant automatiquement son code d'utilisateur, sans que l'internaute ait à indiquer à chaque fois ces préférences. Ils permettent également à l'administrateur d'un site internet d'analyser le parcours des visiteurs sur son site et d'améliorer sa configuration. De plus, ils facilitent le magasinage en ligne en enregistrant au cours de sa navigation les items (et leurs caractéristiques sélectionnées) que désire se procurer le consommateur. Les fichiers témoins qui portent essentiellement sur la navigation et le comportement des internautes sur un site donné (nombre de visiteurs, de visites, de pages vues, etc.), compilés de façon anonyme, peuvent aussi permettre à l'administrateur d'améliorer le site (contenu, forme, ergonomie, etc.).

---

[198] DINANT, Jean-Marc, «Les traitements invisibles sur internet» [En ligne] http://dess-droit-internet.univ-paris1.fr/bibliotheque/rubrique.php3?id_rubrique=242 (consulté le 15 avril 2007).

[199] « Une fenêtre intruse ou fenêtre surgissante (en anglais *pop up window* ou *pop up* tout court) est une fenêtre secondaire qui s'affiche sans avoir été sollicitée par l'utilisateur devant la fenêtre de navigation principale lorsqu'on navigue sur internet. » Wikipedia, [En ligne] http://fr.wikipedia.org/wiki/Fen%C3%AAtre_intruse (consulté le 15 avril 2007).

[200] NANTEL M., *Op. cit.*, note 120.

[201] RISACHER Nancy, « Le procès de l'internet » Lamy, Droit de l'informatique et des réseaux, no. 102, avril 1998.

Par contre, l'utilisation des fichiers témoins soulève deux principales préoccupations du point de vue de leur conformité avec les lois sur la protection des renseignements personnels, premièrement parce qu'ils s'installent automatiquement sur les ordinateurs des internautes et souvent à leur insu et, deuxièmement, parce que l'internaute n'est pas en mesure de contrôler les informations qu'ils recueillent ni l'utilisation qui en est faite. En effet, les sites qui utilisent les fichiers témoins n'informent généralement pas les utilisateurs de la présence de ces fichiers et de la collecte de renseignements qu'ils effectuent. La collecte de renseignements se fait donc sans le consentement explicite de l'internaute. Par ailleurs, bien que plusieurs de ces informations soient anonymes, elles peuvent éventuellement être rattachées à un individu identifiable si celui-ci s'est enregistré sur le site. Par exemple, l'abonné à des revues ou journaux en ligne devra décliner son identité, tout comme celui qui effectue des achats ou qui s'abonne à une liste d'envoi. Dès lors, si ces sites ont implanté des *cookies* persistants sur l'ordinateur, l'information recueillie par la suite contiendra des renseignements personnels, puisque rattachés à un individu identifiable. On n'a qu'à penser à *Amazon.ca* dont les fichiers témoins, comme nous l'avons vu précédemment, recueillent une foule d'informations. Si un internaute est déjà enregistré ou qu'il a déjà effectué des achats sur ce site, ou s'il le fait éventuellement, Amazon.ca sera alors en mesure de rattacher les renseignements recueillis à sa personne, incluant notamment son identité complète et ses coordonnées.

Ainsi, s'il est raisonnable de croire que les renseignements recueillis par les *cookies* non persistants vont dans l'intérêt du consommateur puisqu'ils facilitent sa navigation et ses achats et que les renseignements recueillis ne sont pas de type nominatif, il en va autrement des *cookies* persistants. En effet, l'absence de consentement de l'internaute concernant l'implantation de tels fichiers sur son disque dur, de même que de la cueillette et l'utilisation subséquente qui seront faites des informations recueillies entraînent, pour le consommateur, une perte de contrôle totale des renseignements personnels le concernant, avec les risques de profilage et d'usurpation d'identité qu'une telle situation peut provoquer.

Comme le mentionne Jean-Marc Dinant, le problème majeur soulevé par les cookies est qu'ils :

> *« cristallisent symboliquement dans l'imaginaire social cette fameuse inversion du paradigme client-serveur. Le phénomène des cookies demeure socialement dur à accepter, parce qu'il permet à un site distant et éventuellement inconnu (c'est le cas des millions de fois par jour sur le réseau grâce à des firmes de cybermarketing (…) d'utiliser le disque dur du naviguant à son insu, en y stockant les données personnelles codées de l'internaute et en allant les y retrouver et les modifier à sa guise.*
>
> *La technique des cookies permet donc de marquer un utilisateur particulier avec certaines données qui le concernent et dont la signification est tout à fait hermétique. Il est techniquement possible d'inclure dans ces cookies des données sensibles que l'on aurait pu déduire de certaines réponses à des formulaires envoyés précédemment. En d'autres termes, si un site Internet révisionniste (moyennant une programmation adéquate) arrive à la conclusion qu'un utilisateur est juif, il pourra coller une étoile codée sur le dos de cet utilisateur de telle manière que chaque site de sa famille DNS puisse avoir vent de cette caractéristique, avant d'afficher une quelconque de ses pages »* [202].

[202] DINANT Jean-Marc, *Op. cit.*, note 199.

Logiciels espions (spyware)

Tout comme les fichiers témoins, le premier problème avec les logiciels espions est qu'ils s'installent automatiquement sur l'ordinateur de l'internaute et recueillent des renseignements à l'insu de l'internaute[203]. Les concepteurs de ces logiciels défendent leur légalité en précisant que leur présence est souvent spécifiée, le cas échéant, dans la licence d'utilisation du programme téléchargé. Or, bien peu d'utilisateurs lisent ces licences qui sont longues et complexes et, bien que l'utilisateur soit notifié de la présence du logiciel espion, on ne porte pas à sa connaissance le type de renseignements recueillis, ni l'utilisation et la divulgation ultérieures qui en sera faites.

De plus, outre le préjudice pouvant découler directement de la cueillette des renseignements personnels, les logiciels espions affectent également l'ordinateur de l'internaute de différentes façons, notamment en consommant de la mémoire vive, en utilisant de l'espace sur le disque dur, en mobilisant les ressources du processeur, en nuisant à d'autres applications, etc.[204]

Considérés comme une nuisance par l'ensemble des internautes, les logiciels espions sont décriés de par leurs actions perverses, non transparentes et souvent illégales. S'ils confèrent certains avantages, ce n'est certainement pas aux consommateurs, mais plutôt à l'industrie qui préfère utiliser cette technique pour récolter de l'information sur les internautes, par crainte de se voir opposer un refus, de leur part, dans le cas d'une demande explicite de cueillette de renseignements personnels.

Pourriel (spam)

Comme nous l'avons mentionné précédemment, l'adresse électronique d'une personne est considérée par la LPRPDÉ comme étant un renseignement personnel et suivant l'évolution actuelle de la jurisprudence, les autres provinces qui ont adopté une loi similaire pourraient également la considérer ainsi. Les communications non sollicitées aux fins de pollupostage sont probablement les utilisations les plus irritantes des renseignements personnels dont aient conscience les consommateurs.

Défendu par certains comme ayant la même valeur que la publicité qui peut être envoyée par la poste ou celle que l'on retrouve sur bande-annonce sur le web, le pourriel constitue, selon ses défenseurs, un moyen écologique et économique de publicité, facile à supprimer ou ignorer[205]. En ce sens, il permet à de petites entreprises de concurrencer des entreprises internationales en leur permettant de rejoindre, à un faible coût, un très grand nombre de personnes[206], permettant au consommateur de connaître certains produits qu'il n'aurait pas autrement connus. Cependant, le spamming peut être fort contrariant pour qui en est la cible, ne serait-ce que pour le temps que le destinataire doit passer à séparer les spams des courriels légitimes. De plus, les pourriels ne proposent que très rarement un produit éventuellement intéressant pour le consommateur, consistant souvent en des tentatives d'hameçonnage ou des publicités

[203] Par ailleurs, certains logiciels espions sont très difficiles à éliminer, étant parfois impossibles à enlever manuellement et nécessitant un logiciel spécial. Voir : « Le logiciel espion » [En ligne] http://www.dataprotex.be/fr/logiciel-espion.html (consulté le 7 mai 2007).
[204] *Ibid.*
[205] LABBE, Eric, *Op. cit.*, note 111.
[206] SCOTT, Richard, «The case for advertising on Usenet», [En ligne] http://hamilton.htcomp.net/apt/Internet_Advertising.htm (consulté le 7 mai 2007).

trompeuses, visant à récolter de l'information sur la personne en question et/ou lui soutirer de l'argent. Plusieurs sites ont d'ailleurs vu le jour afin de dénoncer les polluposteurs[207] et plusieurs États tentent, tant bien que mal, de mettre un terme à cette pratique.[208]

Cartes de fidélité

Les cartes de fidélité posent le problème du choix devant lequel est placé le consommateur : s'il désire profiter de certains avantages ou de certaines économies, il devra en échange accepter des intrusions à sa vie privée et consentir au partage de ses renseignements personnels. Elles posent aussi les problèmes de l'information et du consentement : pour effectuer un choix éclairé, encore faut-il que le consommateur soit avisé clairement de ce à quoi il s'engage. La gravité de l'érosion de la protection de la vie privée engendrée par cette pratique divise les consommateurs. Si certains y voient une intrusion dans leur vie privée, d'autres ne semblent pas croire que la collecte de renseignements puisse leur nuire, comme l'illustrent les témoignages de deux consommatrices américaines rapportés dans un article du Washington Post:

> *«Schafer and many other shoppers use their club cards and eagerly accept this choice. "I'm just buying Tide and English muffins and dog food," said Schafer, 35, who added that she would feel foolish passing up savings that others around her get. That afternoon she saved $2.50 on her purchases and earned bonus points for more discounts later. "Why spend a lot more money for something as boring as food?" she asked.*
>
> *Erskine, on the other hand, said she loathes the idea of a corporation sifting through the fine-grained details of something as personal as her food. As a result, on her receipt it was noted she paid an extra $10.47, or about 22 percent more for her groceries than she would have as a Safeway Club member. "I resent having to pay extra to protect my privacy," said Erskine, 30. "Why should I have to give up my information to be able to get a sale item?"»*[209]

Comme le mentionne Robert Gellman, un spécialiste de la vie privée, le manque de transparence entourant la pratique est problématique.

> *«All the marketers say, 'This benefits consumers.' And it does. But what they won't do is be honest about it. They won't explain exactly what they're doing.»*[210]

Ainsi, les principales critiques faites aux cartes de fidélité portent sur la quantité impressionnante d'informations que l'entreprise recueille grâce à elles, le manque de transparence quant à l'utilisation qui est faite de ces informations et l'impossibilité, pour le consommateur, de bénéficier des avantages que procure la carte tout en refusant de consentir à la cueillette, l'utilisation et la divulgation qui sont faites de ces renseignements ou d'une partie d'entre eux.

---

[207] Voir notamment : http://www.caspam.org/ ; http://eservice.free.fr/anti-spam.html (consulté le 7 mai 2007).

[208] Plusieurs Groupes de travail sur le pourriel ont été mis sur pied, notamment au Canada [En ligne] http://com-e.ic.gc.ca/epic/site/ecic-ceac.nsf/fr/h_gv00246f.html, à l'OCDE [En ligne] http://www.oecd-antispam.org/sommaire.fr.php3, et dans l'Union Européenne [En ligne] http://europa.eu/scadplus/leg/fr/lvb/l24189a.htm (consultés tous trois, le 7 mai 2007).

[209] O'HARROW, Robert Jr., *Op. cit.*, note 194.

[210] *Ibid*.

Durée de conservation et la sécurisation des données

Les lois relatives à la protection des renseignements personnels se penchent sur la sécurisation des données et la limitation de la collecte afin, notamment, de réduire au minimum les intrusions dans la vie privée et les risques associés au vol de renseignements personnels.

En effet, le vol d'identité et les fraudes informatiques sont de plus en plus courants et les pirates informatiques réussissent maintenant à déjouer les systèmes de protection les plus sophistiqués, comme, par exemple, ceux d'institutions financières. Le risque que ces intrusions représentent milite en faveur d'une restriction aussi bien de la nature et de la quantité des renseignements accumulés dans les banques de données que de la durée de leur conservation. En effet, plus un fraudeur aura accès à une quantité importante de renseignements personnels concernant un individu, renseignements qui pourraient de plus couvrir une longue période, plus la fraude subséquente pourra être importante. *Amazon.ca*, par exemple, mentionne dans sa politique de confidentialité que « *lorsque vous mettez vos renseignements à jour, nous conservons généralement dans nos dossiers une copie de la version antérieure*. » Le fraudeur qui réussit à obtenir ces renseignements aura donc accès à d'innombrables renseignements personnels, incluant les différentes adresses qu'un individu a pu avoir au fil des ans.

Ainsi, à la lumière de notre étude concernant la quantité de renseignements qui sont recueillis sur les consommateurs et le peu de mesures de sécurité mises en place, il nous apparaît clair que les pratiques actuelles concernant la durée de conservation et la sécurisation des données, non seulement ne bénéficient pas au consommateur, mais peuvent carrément lui être néfastes. En effet, la facilité avec laquelle des renseignements ont été illégalement achetés par les enquêteurs de *La facture*[211], les nombreuses intrusions qui ont eu lieu dans les différents systèmes informatiques d'entreprises et institutions financières, sans compter la consignation d'informations désuètes ou erronées, engendrent des risques pour la protection de la vie privée des individus qui sont exacerbés par une conservation prolongée et une mauvaise sécurisation de tous les renseignements le concernant.

Flux transfrontière de données

Du fait de l'absence de barrières géographiques concernant la transmission de l'information, le flux transfrontière de données à caractère personnel est appelé à devenir un phénomène de plus en plus répandu. En effet, non seulement une entreprise peut-elle entreposer les renseignements qu'elle recueille dans des bases de données situées à l'étranger, mais une entreprise étrangère – qui n'est pas soumise au droit canadien – peut également recueillir des renseignements personnels concernant des Canadiens. Le pays où les renseignements personnels des consommateurs sont entreposés peut avoir un impact considérable sur le traitement qui en sera fait, puisque les protections et les restrictions varieront d'un pays à l'autre. En vertu du principe de l'interdiction de l'extraterritorialité des lois, les entreprises étrangères ne sont pas soumises au droit canadien, mais à la législation nationale du territoire sur lequel elles se trouvent. Par ailleurs, puisqu'aucune obligation légale n'est imposée aux entreprises de conserver les renseignements personnels dans la province ou le pays où ils ont été recueillis, plusieurs entreprises envoient ces données à l'étranger. Par exemple, le Réseau Admission mentionne dans sa politique de confidentialité que :

[211] *Op. cit., 142.*

> *« Vos renseignements peuvent être transférés et conservés, en tout ou en partie, sur des réseaux informatiques situés à l'extérieur de la province, de l'état, du pays ou autre territoire que celui où vous habitez. Ils peuvent être sauvegardés sur du matériel informatique ou dans des établissements loués ou autorisés par des tierces parties. »*

De même, Air Canada précise dans sa politique :

> *« Sachez qu'à l'instar des autres compagnies aériennes, Air Canada est tenue de se plier aux nouvelles lois sur la sûreté édictées par les États-Unis et plusieurs autres pays l'obligeant à donner aux organes de contrôle frontalier accès aux données sur ses passagers. Ainsi les renseignements qui concernent votre personne ou votre voyage peuvent-ils devoir être communiqués aux autorités des douanes et de l'immigration des pays qui figurent sur votre itinéraire.*
>
> *De plus, les lois des États-Unis et de certains pays exigent qu'Air Canada et d'autres transporteurs aériens recueillent de l'INFORMATION PRÉALABLE SUR LES VOYAGEURS, qui comprend les données de passeport et des renseignements pertinents sur tous les passagers voyageant au départ ou à destination de ces pays.*
>
> *Air Canada est tenue de fournir ces renseignements aux autorités douanières et de l'Immigration officielles des pays en question. »*[212]

Ainsi, lorsque des renseignements personnels de Canadiens se retrouvent aux États-Unis ou dans un autre pays, il devient beaucoup plus difficile d'avoir un contrôle sur l'utilisation et/ou la divulgation qui seront faites de ces renseignements. Cette situation s'est présentée dans le cadre d'une plainte à l'encontre de l'entreprise *Abica.com,* qui offre différents services de recherche sur des individus et qui fait actuellement l'objet d'une enquête par la Commissaire. Les faits de cette affaire ont révélé que l'entreprise avait fourni divers renseignements personnels sur un individu qui avait fait l'objet d'une demande de recherche, incluant un profil psychologique qui s'est révélé être sans fondement. Outre l'absence de consentement à la cueillette, l'utilisation et la transmission d'informations, parfois fausses, les préoccupations soulevées dans cette affaire sont notamment que, bien que la Commissaire ait compétence pour enquêter, tel que l'a reconnu la Cour fédérale[213], son pouvoir s'avère dans les faits, limité, puisque l'entreprise située aux États-Unis n'est pas soumise aux lois canadiennes et ne peut donc être contrainte de témoigner ou de divulguer ses sources. Non seulement le consommateur n'a-t-il aucun contrôle sur la divulgation de ses renseignements personnels, mais il n'en possède pas non plus sur leur contenu, ce qui fait qu'il peut y avoir transmission de fausses informations, ce qui peut engendrer de fâcheuses conséquences, selon l'auteur de la demande (employeur, assureur, agence gouvernementale, individu mal intentionné, etc.).

La facilité de transmission que permettent les nouvelles technologies appellent à l'établissement de certaines règles relativement à la transmission des renseignements personnels des individus au-delà des frontières à l'intérieur desquelles ils ont été recueillis. Sans de telles règles, il serait facile pour l'entreprise qui désirerait se soustraire à une législation donnée de transmettre et stocker ses données dans un pays où la législation en matière de protection des renseignements personnels est inexistante ou laxiste[214]. Au-delà de ces considérations, les

---

[212] Air Canada, politique de confidentialité, [En ligne] http://www.aircanada.com/fr/about/legal/privacy/policy.html (consulté le 5 avril 2007).
[213] Lawson c. Accusearch inc. (abika.com), 2007 CF 125 (CanLII).
[214] BENYEKHLEF, Karim, « Les transactions dématérialisées » Montréal, 1994, [En ligne] http://www.lexum.com/conf/ae/fr/benyekhlef.html (consulté le 17 avril 2007).

entreprises sont de plus en plus souvent appelées à effectuer des transferts internationaux de renseignements personnels, aux fins de la réalisation d'une transaction ou du fait de leur fonctionnement interne. Au Canada, seule la loi québécoise traite expressément de cette problématique. Son article 17 stipule que :

> *« La personne qui exploite une entreprise au Québec et qui communique à l'extérieur du Québec des renseignements personnels ou qui confie à une personne à l'extérieur du Québec la tâche de détenir, d'utiliser ou de communiquer pour son compte de tels renseignements doit au préalable prendre tous les moyens raisonnables pour s'assurer:*
> *1° que les renseignements ne seront pas utilisés à des fins non pertinentes à l'objet du dossier ni communiqués à des tiers sans le consentement des personnes concernées sauf dans des cas similaires à ceux prévus par les articles 18 et 23*
> *(…)*
> *Si la personne qui exploite une entreprise estime que les renseignements visés au premier alinéa ne bénéficieront pas des conditions prévues aux paragraphes 1° et 2°, elle doit refuser de communiquer ces renseignements ou refuser de confier à une personne ou à un organisme à l'extérieur du Québec la tâche de les détenir, de les utiliser ou de les communiquer pour son compte.*[215] *»*

Une telle obligation s'impose également aux organismes publics en vertu de l'article 70,1 de la Loi sur l'accès aux documents des organismes publics :

> ***70.1.** Avant de communiquer à l'extérieur du Québec des renseignements personnels ou de confier à une personne ou à un organisme à l'extérieur du Québec la tâche de détenir, d'utiliser ou de communiquer pour son compte de tels renseignements, l'organisme public doit s'assurer qu'ils bénéficieront d'une protection équivalant à celle prévue à la présente loi.*
> *Si l'organisme public estime que les renseignements visés au premier alinéa ne bénéficieront pas d'une protection équivalant à celle prévue à la présente loi, il doit refuser de les communiquer ou refuser de confier à une personne ou à un organisme à l'extérieur du Québec la tâche de les détenir, de les utiliser ou de les communiquer pour son compte.* [216]

Cependant, tant la LPRPDÉ que la PIPA de la Colombie-Britannique et de l'Alberta sont silencieuses à ce sujet. Par ailleurs, les protections offertes par la loi provinciale québécoise restent défaillantes puisque la transmission transfrontière n'est ni prohibée ni soumise à des conditions d'équivalence de protection[217] contrairement à ce que prévoient la plupart des législations européennes.[218] Par conséquent, la transmission de renseignements personnels à l'étranger à partir du Canada, notamment vers les États-Unis, principal pays vers lequel les renseignements personnels des Canadiens sont exportés, permet aux entreprises de se soustraire aux normes canadiennes et de bénéficier de régimes dont les exigences de protection sont nettement moins contraignantes[219].

---

[215] LPRPSP art.17
[216] *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, LRQ ch. A-2.1, art. 70.1 .
[217] BENYEKHLEF, Karim, *Op. cit*., note 215.
[218] *Ibid.*
[219] *Ibid.*

CONCLUSION

Ce survol du commerce d'informations personnelles met en lumière la place prépondérante du marketing et les effets de l'utilisation sans cesse grandissante d'internet. Le développement des nouvelles technologies a en effet permis aux entreprises d'avoir accès à un plus grand nombre de renseignements personnels, souvent à l'insu des consommateurs, et d'en accroître et d'en optimiser la cueillette et l'utilisation grâce aux techniques informatiques.

L'analyse du cadre légal entourant ce commerce a laissé transparaître certaines lacunes quant à l'application des lois ainsi que des problèmes en ce qui a trait notamment à la définition de ce qui constitue un renseignement personnel ou à la détermination des entreprises ou des activités qui sont soumises à la loi.

Le manque d'harmonisation des lois provinciales et fédérale, notamment en ce qui a trait aux définitions et aux pouvoirs respectifs accordés aux organismes chargés de l'application de la loi, soulève des inquiétudes quant à la différence de protection qui pourra être accordée aux renseignements des consommateurs selon la loi applicable, soit selon la province dans laquelle ils habitent ou selon le type d'entreprise concernée. Le fait que seuls soient rendus publics des résumés des décisions des Commissaires plutôt que des décisions qui présenteraient de façon complète les motifs qui les fondent ne peut que contribuer au maintien de certaines ambiguïtés.

Bien que l'industrie prétende que la cueillette, l'utilisation et la communication des renseignements personnels servent le consommateur puisqu'elles lui permettent d'obtenir des rabais ou de recevoir des publicités et des offres personnalisées, elles peuvent également avoir d'autres finalités et entraîner des risques que le consommateur est en droit de connaître et qu'il doit avoir la possibilité d'accepter ou de refuser. Or, les pratiques de l'industrie, de plus en plus, passent outre ce consentement, qui constitue pourtant la pierre angulaire des lois qui visent à protéger les renseignements personnels des consommateurs. L'absence de divulgation expresse et l'absence de demande de consentement préalable à la cueillette, à l'utilisation et à la divulgation des renseignements personnels semblent malheureusement être devenues la norme, tout comme le manque de transparence des pratiques.

Le but premier des normes imposées aux entreprises était d'assurer la confiance des consommateurs, en vue de favoriser le commerce. Or, il appert de l'analyse effectuée que les principes de base sont en pratique largement bafoués. Les conséquences à moyen terme des pratiques cavalières des entreprises risquent d'être néfastes non seulement pour le consommateur, mais également pour l'industrie, les consommateurs risquant de devenir méfiants, voire réfractaires, face aux nouvelles technologies s'ils réalisent l'utilisation qui est ou qui peut être faite des renseignements personnels que recueillent les entreprises.

Alors que la collecte, la conservation et l'utilisation de certains renseignements peuvent en effet bénéficier au consommateur, lui évitant, par exemple, d'avoir à répéter inutilement certaines informations, permettant à une entreprise de lui offrir un service personnalisé et lui permettant des économies, la multiplication des pratiques de collecte, la large quantité de renseignements collectés et les utilisations en vue de marketing qui en sont faites suscitent bien des inquiétudes. Malgré que certaines des informations qui sont recueillies ne puissent, en soi, répondre à la définition de renseignements personnels, le fait que l'accumulation de ces renseignements puisse permettre d'établir un profil assez exact d'une personne ou que ces

informations puissent être éventuellement reliées à un individu identifiable laissent croire qu'il pourrait être nécessaire de songer à encadrer tous les types de renseignements qui peuvent être collectés par les entreprises et à soumettre toute cueillette à un consentement préalable.

Bien que la publicité ciblée envoyée au consommateur permette d'informer ce dernier des différents produits et services circulant sur le marché en fonction de ses goûts, il ne faut surtout pas perdre de vue que la publicité n'a pas pour but essentiel d'informer. Créée pour inciter, elle a pour but premier de séduire le consommateur en vue de l'amener à se procurer un bien ou un service, en le manipulant au besoin et en exploitant ses faiblesses, choses rendues maintenant beaucoup plus aisées grâce au profilage.

Peu importerait, ultimement, à qui profitent le plus ces collectes de renseignements personnels, pour autant que les collectes soient faites de façon transparente et qu'elles respectent le principe fondamental relatif à la collecte, l'utilisation et la divulgation des renseignements personnels, soit «le consentement éclairé du consommateur». Voilà le défi qui doit être relevé face aux nouvelles technologies et aux nouvelles pratiques.

RECOMMANDATIONS

Attendu que le gouvernement fédéral et les provinces ont choisi de confier à des organismes spécialisés l'application de leurs lois sur la protection des renseignements personnels ;

Attendu que les pouvoirs qu'accorde la Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDÉ) au Commissaire à la protection de la vie privée sont plus restreints que ceux qui sont conférés par les lois provinciales similaires aux organismes chargés de l'application de la loi;

Attendu que, du fait de ces différences, les consommateurs canadiens bénéficieront de protections différentes selon leur province de résidence ou selon l'entreprise visée ;

Attendu que la loi fédérale ne permet pas au Commissaire de mener de sa propre initiative des enquêtes de vérification ;

Attendu que les décisions de la Commissaire, contrairement à celles que peuvent rendre les organismes chargés de l'application des lois provinciales similaires, n'ont pas de force contraignante ;

Attendu que les lois provinciales prévoient l'imposition d'amendes et de pénalités aux entreprises qui contreviendraient aux règles relatives à la protection des renseignements personnels ou qui entraveraient le déroulement d'une enquête ;

Attendu que les entreprises, selon leur nature ou selon la province dans laquelle est logée la plainte, n'auront pas à assumer les mêmes conséquences en cas de contravention aux règles visant la protection des renseignements personnels ;

L'Union des consommateurs recommande au gouvernement fédéral de:

- modifier la LPRPDÉ en vue d'accorder au Commissaire un pouvoir de surveillance qui lui permette de mener de sa propre initiative des enquêtes de vérification ;

- modifier la LPRPDÉ en vue d'accorder au Commissaire tous les pouvoirs nécessaires à l'exercice de sa compétence, notamment celui de rendre toute ordonnance qu'il estimerait propre à sauvegarder les droits des parties;

- modifier la LPRPDÉ en vue prévoir que toute décision du Commissaire ayant pour effet d'ordonner à une partie d'accomplir un acte ou de cesser ou de s'abstenir d'accomplir un acte est exécutoire ;

- modifier la LPRPDÉ en vue de prévoir l'imposition de pénalités aux entreprises qui contreviendraient à la loi ou qui entraveraient le déroulement d'une enquête ;

Attendu que certaines différences entre les lois provinciales et la LPRPDÉ sont susceptibles de créer des incertitudes, notamment en ce qui a trait aux renseignements protégés et aux organisations qui sont soumises à ces lois ;

Attendu que, du fait de ces différences, les consommateurs canadiens pourraient bénéficier de protections différentes selon leur province de résidence ou selon la nature de l'entreprise visée ;

L'Union des consommateurs recommande :

- Que le gouvernement fédéral et les gouvernements du Québec, de l'Alberta et de la Colombie-Britannique veillent à harmoniser leurs lois sur la protection des renseignements personnels de façon à assurer que ces lois s'appliquent de façon uniforme aux organisations visées, indépendamment de leur nature ou de la province dans laquelle elles ont leur place d'affaires;

- Que le gouvernement fédéral et les gouvernements du Québec, de l'Alberta et de la Colombie-Britannique veillent à harmoniser leurs lois sur la protection des renseignements personnels en vue de dissiper les incertitudes qui peuvent exister quant au type de renseignements qui sont protégés par leurs lois, de façon à ce que ce qui est considéré comme un renseignement personnel soit protégé également, indépendamment de la nature de l'organisation visée ou de la province dans laquelle elle a sa place d'affaires ;

Attendu que les lois de protection des renseignements personnels ont été élaborées en vue de renforcer la confiance des consommateurs et de mettre en place des mécanismes susceptibles d'éviter les fraudes et abus qui peuvent résulter de la cueillette et de l'utilisation anarchique de ce type de renseignements ;

Attendu que le développement rapide des télécommunications a entraîné l'apparition ou l'amélioration de nombreuses techniques de cueillette, de stockage et de traitement des renseignements ;

Attendu la valeur commerciale qu'ont acquise les renseignements sur les consommateurs grâce, notamment, aux techniques de profilage ;

Attendu que l'un des principes essentiels qui régissent l'encadrement de la protection des renseignements personnels porte sur le consentement de l'individu à la collecte de ses renseignements de même qu'à l'usage qui en sera fait et à la communication à des tiers de ces renseignements ;

Attendu qu'un consentement ne sera éclairé pourvu que l'individu qui doit le donner ait en sa possession toutes les données pertinentes ;

Attendu que certains renseignements qui ne sont pas en soi des renseignements personnels au sens des lois peuvent être compilés et associés à des renseignements protégés, à l'insu des individus auxquels ils sont rattachés ;

Attendu que notre étude a permis de relever plusieurs manquements par les entreprises à leur devoir d'obtenir un consentement préalable à la collecte, à l'utilisation et à la communication de renseignements;

Attendu que les informations qui sont données ou qui sont mises à la disposition de l'individu dont l'entreprise doit obtenir le consentement se révèlent souvent incomplètes ou difficilement compréhensibles ;

Attendu que les politiques de confidentialité des entreprises ne sont que rarement portées expressément à la connaissance des consommateurs ;

L'Union des consommateurs recommande :

- Que le gouvernement fédéral élabore et mette en place une vaste campagne d'information en vue de renseigner les consommateurs sur :
  - Leurs droits en vertu de la LPRPDÉ ;
  - Les obligations des entreprises relativement à l'exigence d'un consentement préalable quant à la collecte, l'utilisation et la communication de renseignements personnels ;
  - Les pratiques des entreprises en matière de traitement des renseignements personnels par les entreprises, notamment en ce qui a trait au profilage ;

- Que cette campagne d'information soit élaborée et diffusée avec la collaboration des organismes de défense des droits des consommateurs et que des ressources suffisantes soient accordées à ces organismes en vue de garantir une participation adéquate ;

- Que les gouvernements provinciaux veillent, de concert avec les organismes de défense des droits des consommateurs, à la diffusion de l'information élaborée dans le cadre de cette campagne ;

- Que les gouvernements provinciaux veillent à ce que des ressources suffisantes soient accordées à ces organismes de défense des droits des consommateurs en vue de garantir une participation adéquate ;

L'Union des consommateurs recommande de plus:

- Que le gouvernement fédéral mette sur pied un groupe de travail qui serait chargé d'étudier l'encadrement qui devrait être prévu par les lois sur la protection des renseignements personnels relativement aux divers types de renseignements qui peuvent être collectés par les entreprises et qui, sans être au sens propre des renseignements personnels, sont susceptibles d'être assemblés en vue de dresser un profil des individus ;

- Que soient accordées aux organismes de défense des droits des consommateurs des ressources suffisantes pour leur permettre une participation adéquate à ce groupe de travail;

- Que les gouvernements fédéral et provinciaux mettent en place une vaste campagne d'information en vue de renseigner les entreprises sur les obligations qui leur reviennent en vertu des lois sur la protection des renseignements personnels ;

- Que les gouvernements fédéral et provinciaux, en collaboration avec les organismes de défense des droits des consommateurs, élaborent un modèle de politique de confidentialité complet, qui soit facile à comprendre et à utiliser, qui pourrait être mis à la disposition des entreprises en vue de faciliter le consentement adéquat des consommateurs à la collecte, l'utilisation et la communication des renseignements qui les concernent ;

L'Union des consommateurs recommande finalement:

- Que les organismes chargés de l'application des lois sur la protection des renseignements personnels utilisent les pouvoirs dont ils disposent pour s'assurer que les politiques de confidentialité des entreprises répondent aux critères nécessaires pour permettre de la part des consommateurs un consentement éclairé à la collecte, l'utilisation et la communication des renseignements qui les concernent ;

MEDIAGRAPHIE

Légalisation

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

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

Personal Information Protection Act, S.A. 2003, ch. P-6.5

Personal Information Protection Act, S.B.C. 2003, ch. 63

Agences gouvernementales

CANADA

Ministère de l'Industrie, « La société canadienne à l'ère de l'information : Pour entrer de plain-pied dans le XXIe siècle », Ottawa, 1996.

Groupe de travail sur le commerce électronique, Industrie Canada et Justice Canada « La protection des renseignements personnels : pour une économie et une société de l'information au Canada », Ottawa,1998.

Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique « La protection de la vie privée au Canada et l'examen de la LPRPDÉ », Ottawa, 2006.

COMMISSAIRE À LA PROTECTION DE LA VIE PRIVÉE DU CANADA

http://www.privcom.gc.ca/

« Rapport annuel 1984-1985 » Ottawa, Approvisionnements et Services Canada, 1985.

« Rapport annuel 1988-1989 » Ottawa, Approvisionnements et Services Canada, 1989.

« Rapport annuel 1989-1990 » Ottawa, Approvisionnements et Services Canada, 1990.

COMMISSION D'ACCÈS À L'INFORMATION, Montréal, Québec.
http://www.cai.gouv.qc.ca

Débat de la chambre des communes, volume 133, no.002, 1ere session, 35e Législature.

OCDE

« Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données à caractère personnel » C(80)58/Final, 23 septembre 1980, 72p.
http://www.oecd.org/document/53/0,2340,fr_2649_201185_15591797_1_1_1_1,00.html
« Déclaration relative à la protection de la vie privée sur les réseaux mondiaux » C(98)177, 8 octobre 1998.
http://webdomino1.oecd.org/horizontal/oecdacts.nsf/Display/DE3F18783E4829AAC125729B00515E52?OpenDocument
« Simplifier les notices d'information sur la protection de la vie privée : rapport et recommandation de l'OCDE » DSTI/ICCP/REG(2006)5/FINAL, 24 juillet 2006, 9p.
http://appli1.oecd.org/olis/2006doc.nsf/43bb6130e5e86e5fc12569fa005d004c/a56f6b2f04871d3fc12571b5003dac3f/$FILE/JT03212215.PDF

SMITH Margaret, « La protection des renseignements personnels et le commerce électronique : L'État de la question » Canada, Division du droit et du gouvernement, 31 mai 2000.
http://dsp-psd.tpsgc.gc.ca/Collection-R/LoPBdP/BP/prb0018-f.htm

UNION EUROPÉENNE, « Directive 95/46/EC du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques et à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données » Journal Officiel du Parlement européen, no. L.281, 23 novembre 1995. pp. 0031 – 0050.
http://europa.eu.int/eur-lex/lex/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:FR:HTML

UNITED STATES FEDERAL TRADE COMMISSION

« Privacy Online : A Report to Congress » États-Unis, 1998, 71 p.
http://www.ftc.gov/reports/privacy3/priv-23a.pdf
« *Self-Regulation and Online Privacy: A Report to Congress* », États-Unis, 1999, 26 p.
http://www.ftc.gov/os/1999/07/privacy99.pdf
« *Online Profiling: A Report to Congress* » États-Unis, 2000, 25 p.
http://www.ftc.gov/os/2000/06/onlineprofilingreportjune2000.pdf

Articles

Rédaction « Big Brother et les fichiers logs » Futura science
http://www.futura-sciences.com/news-big-brother-fichiers-log_9682.php

Rédaction « Les pourriels pullulent », Radio-Canada, Montréal, 20 mars 2007.
www.radio-Canada.ca/nouvelles/societe/2007/03/20/005-piratage-mardi.shtml

Rédaction « Les entreprises nonchalantes face aux courriels » La Presse Affaires, Montréal, 12 avril 2007.
http://technaute.lapresseaffaires.com/nouvelles/texte_complet.php?id=81,12399,0,042007,1345603.html&ref=nouvelles

Rédaction « L'adresse électronique professionnelle : renseignement personnel ou information à caractère public? » Centre de ressources Ogilvy Renaud, Montréal, 2005, 3 p.
http://www.ogilvyrenault.com/fr/ResourceCenter/ResourceCenterDetails.aspx?id=897&pId=43

Rédaction « les données personnelles de 59000 personnes exposées » Canoë cyberactualités, Montréal, 21 avril 2005.
http://souriez.info/article.php3?id_article=217

ADCOM INTERNET, « Les fichiers logs » Adcom referencement, Lyon, France, 2003
http://www.adcom.fr/expertise/fichier_log.htm

Atelier Groupe BNP Paribas « Les aspirateurs d'adresse mail dans la ligne de mire de la Cour de Cassation » Atelier juridique, France, 3 avril 2006
http://www.atelier.fr/juridique/aspirateurs,adresse,mail,ligne,mire,cour,cassation-31912-21.html

BARRIGAR J., BURKELL J., KERR I., « Let's Not Get Psyched Out of Privacy », ID Trail, Ottawa, Canada, 16 p.
http://www.idtrail.org/files/LETS_NOT_GET_PSYCHED_OUT_OF_PRIVACY%20final%5B1%5D.pdf

BENHAMOU Laurence, « La publicité de l'ère numérique traque les consommateurs » La Presse, cahier Actuel, Montréal, 28 mars 2007.
http://www.cyberpresse.ca/article/20070328/CPACTUEL/70328065/5320/CPACTUEL

BENZAKOUR Nadia, « La publicité sur internet et la nécessaire protection du consommateur » Université de Paris 2, Paris, 2004, 83 p.
http://www.u-paris2.fr/dess-dmi/rep_travaux/84_N.Benzakour_PSI.pdf

BOYER Joël, « La révolution d'internet » *Petites Affiches*, 10 novembre 1999, no 224, Université de Paris 2, Paris.

CANADIAN INTERNET POLICY AND PUBLIC INTEREST CLINIC (CIPPIC)

« Submission to the House of Commons Standing Committee on Access to Information, Privacy and Ethics on the *Personnal information Protection and Electronic Document Act* (PIPEDA), Ottawa, 28 novembre 2006, 27 p.
http://www.cippic.ca/en/projects-cases/privacy/submissions/CIPPIC_Submission_Nov06wFNs.pdf

« Compliance with Canadian Data Protection Laws : Are Retailers Measuring Up ? » Ottawa, avril 2006, 110 p.
http://www.cippic.ca/en/bulletin/compliance_report_06-07-06_(color)_(cover-english).pdf

CHASSIGNEUX, Cynthia,

« Aterritorialité des atteintes face aux logiques territoriales de protection juridique et problème de l'absence d'homogénéité des législations protectrices (quid des Safe Harbour Principles) » *Lex Electronica*, vol. 9, n°2, Numéro Spécial, hiver 2004, 23 p. Montréal, [En ligne] http://www.lex-electronica.org/articles/v9-2/chassigneux.htm

« La protection des informations à caractère personnel » dans le Guide juridique du commerçant électronique, sous la direction de LABBE E., POULIN D., JACQUOT F., BOURQUE J-F., Montréal, ed. Themis, 2003, 400 p.
http://www.jurisint.org/pub/05/fr/index.htm

COMMISSION NATIONALE INFORMATIQUE ET LIBERTÉ (CNIL),

« La radio-identification » Paris, 18 août 2006.
http://www.cnil.fr/index.php?id=1063

« Vos traces » Les cookies, Paris, 2004-2005

http://www.cnil.fr/index.php?id=170

CNIL, A. VITALIS, F. PAOLETTI, H. DELAHAIE. « *Dix ans d'informatique et de libertés* », Paris, Éd. Économica, 1988.

DELWAIDE Karl, AYLWIN Antoine, « Leçons tirées de dix ans d'expérience : La Loi sur la protection des renseignements personnels dans le secteur privé du Québec », Vancouver, 16 août 2005.
http://www.privcom.gc.ca/information/pub/dec_050816_f.asp

DILLON, Andrew « Reading from paper versus screens : a critical review of the empirical littérature » (1992) 35 Ergonomics, 1297-1326.

DINANT Jean-Marc, « les traitements invisibles sur internet » Université de Paris 1, Paris, 26 février 2006.
http://dess-droit-internet.univ-paris1.fr/bibliotheque/rubrique.php3?id_rubrique=242

DUMERAIN Emilie, ESTERELLAS A, IMANI E., « La répression pénale du spam » e-juristes.org, Université de Paris 10, Nanterre, 17 février 2005.
http://www.e-juristes.org/La-repression-penale-du-spam

ELECTRONIC PRIVACY INFORMATION CENTER (EPIC), « The Cookie Page », Washington DC, États-Unis, 5 novembre 2002.
http://www.epic.org/privacy/internet/cookies

FORTIER Caroline, « Les cookies, le profilage et les intrusions dans la vie privée », Université de Montréal, Montréal, 2000.
http://www.lexum.umontreal.ca/cours/internet2000/forc/forc.html

GAUTRAIS Vincent, « La couleur du consentement » Université de Montréal, Montréal, 2003 56 p.
http://www2.droit.umontreal.ca/cours/ecommerce/_textes/consentement2003CPI.pdf

GAUTRAIS, V. et MACKAAY E., « Les contrats informatiques » dans Denys-Claude LAMONTAGNE, *Contrats spéciaux*, Cowansville, Éditions Yvon Blais, 2001, p.279-317.

KERR Ian, « Submission to the House of Commons Standing Committee on Access to Information, Privacy and Ethics on the Personal Information Protection and Electronic Documents Acts (PIPEDA) », Ottawa, 11 décembre 2006, 15 p.
http://www.cippic.ca/en/projects-cases/privacy/submissions/IK_PIPEDA_Review_Submission_(final)_FORMATTED.pdf

KLEIMANN Communication Group Inc., « Evolution of a Prototype : Financial Privacy Notice », Washington DC, Etats-Unis, 28 février 2006.
http://www.ftc.gov/privacyinitiatives/ftcfinalreport060228.pdf

LAWFORD John, « Consumer Privacy Under PIPEDA : How Are We Doing ? » Public Interest Advocacy Center (PIAC), Ottawa, 2004, 55 p.
http://www.piac.ca/privacy/report_consumer_privacy_under_pipeda_how_are_we_doing+print

LAWSON Philippa et cons. « On the Data Trail : How Detailed Information About you Gets Into the Hands of Organizations With Whom you Have no Relationship » Canadian Internet Policy and Public Interest Clinic, Ottawa, avril 2006, 64 p.
http:// http://www.cippic.ca/en/news/documents/May1-06/DatabrokerReport.pdf

LEMARTELEUR Xavier, « Traçabilité contre vie privée : Les RFID » Juriscom, Asnières-sur-Seine, France, 22 octobre 2004.
http://www.juriscom.net/uni/visu.php?ID=587

MINTZ Jessica, « Microsoft Adds Behavioral Marketing » Associated Press, MSNBC, 27 décembre 2006.
http://www.msnbc.msn.com/id/16370058/

NANTEL Jacques, « La publicité web à la croisée des chemins » Montréal, 4p.
http://www.google.ca/search?hl=fr&ie=ISO-8859-1&q=nantel+publicit%E9+web&meta

NIELSON Jakob, « Writing for the Web » Sun microsystem, Etats-Unis,
http://www.sun.com/980713/webwriting/

O'HARROW Robert Jr., « Consumers Trade Privacy for Lower Prices » Washington Post, DC' États-unis, 31 décembre 1998, p. A- 1.

POELLHUBER David, « la sécurité du courriel ? perspective annuelle et solutions en entreprise », Zerospam, Montréal, 2006.
http://www.zerospam.ca/docu/le-contexte-de-la-securite-du-courriel.html

PONEMON INSTITUTE, « Online Advertising and Privacy Survey Shows Consumers Hold Strong Preference for Targeted Advertising », Revenue Science inc., Tucson, Arizona, États-Unis, 9 septembre 2004
http://www.revenuescience.com/site/media/press-releases/2004/20040909.asp

POULLET Yves,

« Report on the Application of Data Protection Principles to the Worldwide Telecommunication Networks » Consultative Committee of the Convention for the Protection of Individuals with Regars to Automatic Processing of Personnel Data, Conseil de l'Europe, Strasbourg, 2004, 64 p.
http://www.coe.int/t/e/legal_affairs/legal_co%2Doperation/data_protection/documents/reports_and_studies_by_experts/T-PD(2004)04_Poullet_report.pdf

« Les Safe Harbour Principles, une protection adéquate ? » Juriscom.net, Paris, 17 juin 2000, [En ligne] http://www.juriscom.net/uni/doc/20000617.htm#_ftn10

RISACHER Nancy, « Le procès de l'internet », Lamy, Droit de l'informatique et des réseaux, no.102, avril 1998.

RODGER Will, « Activists Charge DoubleClick Double Cross », USA Today, Etats-Unis, 7 juin 2000
http://www.usatoday.com/life/cyber/tech/cth211.htm

ROUILLÉ-Mirza, Ségolène « Les collectes de données personnelles à l'insu des internautes », Paris, 2001.
http://www.u-paris2.fr/dess-dmi/rep_travaux/19_segolenerouille.pdf

SHOLTZ Paul, « Economics of Personnal Information Exchange », First Monday, First Monday, volume 5, numéro 9, Université de l'Illinois à Chiago, États-Unis, septembre 2000.
http://www.firstmonday.org/issues/issue5_9/sholtz/index.html

SKOK Gavin, « Establishing a Legitimate Expectation of Privacy in Clickstream Data », 6 Michigan Telecommunications and Technology Law Review, no 61, Michigan, Etats-Unis, 2000.
http://www.mttlr.org/volsix/skok.html

SOLOVE Daniel, « The Digital Person : Technology and Privacy in the Information Age », New York University Press, New York, Etats-Unis, 2004, 202 p.
http://docs.law.gwu.edu/facweb/dsolove/Solove-Digital-Person.htm

TRUDEL Pierre, « Quel droit et quelle régulation dans le cyberespace ?» Sociologie et sociétés, vol. 32, no 2, Les Presses de l'Université de Montréal, Montréal, 2000, p. 189-209
https://papyrus.bib.umontreal.ca/dspace/bitstream/1866/57/1/0042.pdf

Reportage

La Facture

CRAIG Pierre « Hameçonnage, ne soyez pas le poisson » Montréal, émission du 29 novembre 2005.
http://www.radio-canada.ca/actualite/v2/lafacture/niveau2_14348.shtml

TASCHEREAU Jacques « Victime de vol d'identité » Montréal, émission du 13 février 2007.
http://www.radio-canada.ca/actualite/v2/lafacture/niveau2_14651.shtml