Université de Montréal

Analyse juridique des méthodes de protection des renseignements personnels sur Internet

par

Patrick GINGRAS

Faculté de droit

Mémoire présenté à la Faculté des études supérieures
en vue de l'obtention du grade de
Maître en droit (LL.M.)

Août, 2000

Université de Montréal
Faculté des études supérieures

Ce mémoire intitulé :

Analyse juridique des méthodes de protection des renseignements personnels sur Internet

présenté par :

Patrick GINGRAS

a été évalué par un jury composé des personnes suivantes :

Président-rapporteur: M. Pierre Trudel

Directeur de recherche: M. Karim Benyekhlef

Membre du jury: M. Daniel Poulin

Mémoire accepté le : 18 octobre 2000

SOMMAIRE

L'une des préoccupations majeures que suscitent les technologies de l'information est sans aucun doute la protection de la vie privée dans les environnements électroniques décentralisés et transfrontaliers. L'engouement de la population pour le réseau Internet a facilité les techniques de récolte de renseignements personnels et par le fait même, augmenté leur nombre de façon exponentielle.

Sur le réseau Internet, les nombreuses difficultés pratiques d'applications suscitées par la délocalisation et l'intangibilité de l'information sont à la base même des divers problèmes liés à la protection des renseignements personnels. Le présent mémoire se veut en premier lieu, une étude des différents mécanismes de protection des renseignements personnels qui existent actuellement sur le réseau Internet et en second lieu, une analyse ainsi qu'une réflexion sur le moyen le plus susceptible de faciliter la mise en œuvre des principes fondamentaux en matière de protection et de gestion des renseignements personnels, c'est-à-dire les méthodes de standardisation.

Le présent mémoire s'attardera à la protection de la vie privée et aux différents moyens présentement utilisés afin d'assurer les protections nécessaires dans un environnement qui dépasse les frontières territoriales et qui a de plus en plus vocation à devenir le lieu du déroulement de multitudes d'interactions. Malgré le fait que la « vie privée », notion floue par excellence, n'a jamais véritablement fait l'objet de définition précise, tant par les législateurs que par la doctrine, le présent mémoire tente de définir, en vertu du droit canadien et québécois, la notion de « vie privée » et de « renseignement personnel » afin de pouvoir mieux cibler les dimensions relatives à la protection de la vie privée et des renseignements personnels sur le réseau Internet. Les possibilités d'intrusions dans la vie privée donnent lieu à des préoccupations sans précédent quant aux moyens de protéger la zone d'intimité personnelle nécessaire à la vie humaine et à son développement dans la société. Ainsi, nous nous penchons aussi sur les moyens de protection présentement disponibles pour les internautes désireux de protéger leur vie privée lorsqu'ils naviguent sur le réseau Internet, soit l'anonymat et le droit de contrôle des usagers sur leurs renseignements personnels qui non sans le rappeler ont aussi leurs inconvénients.

Afin d'assurer une analyse globale, le mémoire s'attache de plus à énoncer les principes juridiques applicables aux collectes de renseignements personnels et à démystifier, d'un point de vue technique et juridique, diverses méthodes de collectes de renseignements personnels utilisées sur Internet.

En ce qui a trait aux approches pour améliorer la protection des renseignements personnels dans le contexte des inforoutes, nous analysons en tout premier lieu les diverses solutions présentement utilisées pour la protection des renseignements personnels dont, les solutions européennes, canadiennes et québécoises reposant principalement sur la législation, et la solution américaine utilisant les méthodes de standardisation en complémentarité de l'autoréglementation. Il va sans dire que les différences de point de vue découlant de l'utilisation de ces deux modes de protection ont causé bien de remous au courant des dernières années dont entre autres, depuis l'adoption de la *Directive* européenne *95/46/CE 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.* Le débat sur les moyens d'assurer une protection effective de la vie privée sur le réseau Internet illustre bien la nécessité d'y aborder la question de la protection de droits des usagers en se tenant loin du dogmatisme.

De plus en plus, les démarches de standardisation s'imposent comme l'un des principaux vecteurs de la régulation sur le réseau Internet. En raison de son caractère technique, la normalisation est une voie alternative ou complémentaire qui semble constituer une technique souple et adaptable de régulation d'un environnement électronique décentralisé tel le réseau Internet. En offrant ainsi de techniques performantes pour classifier et canaliser l'information, la technologie peut aider les internautes à exercer un contrôle approprié de la circulation de leurs renseignements personnels.

Une coopération internationale et une approche résultant de la technologie combinée à l'exercice d'un jugement éditorial s'avère un moyen efficace de répondre aux nouveaux défis posés par la révolution des communications électroniques. Pour ce faire, les méthodes de standardisation comme mode de protection des renseignements personnels sur Internet s'avèrent une solution intéressante.

TABLES DES MATIÈRES

LISTE DES SIGLES ET ABRÉVIATIONS

A.

ACLU	American Civil Liberties Union
AICPA	American Institute of Certified Public Accountants
Alberta L.R.	Alberta Law Review
AOL	America Online
ARMM	Automatic Retroactive Minimal Moderation

B.

Banking L.J.	Banking Law Journal
BBBOnLine	Better Business Bureau Online
BIOS	Basic Input Output System

C.

C.A.	Cour d'appel
Can. Bar Rev.	Canadian Bar Review
Cardozo Arts & Ent. L.J.	Cardozo Arts and Entertainment Law Journal
C.c.Q.	Code civil du Québec
CDT	Center for Democracy and Technology
CERN	Centre européen de recherche nucléaire
Computer L.J.	Computer Law Journal
C.S.	Cour supérieure
CSA	Association canadienne de normalisation (Canadian Standards Association)

D.

DES	Data Encryption Standard

E.

EFF	Electronic Frontier Foundation
EPIC	Electronic Privacy Information Center

F.

Fed. Comm. L.J.	Federal Communications Law Journal
Fordham Int'l L.J.	Fordham International Law Journal
FTC	Federal Trade Commission

H.

Harvard L.R.	Harvard Law Review
HTTP	Hypertext Transfer Protocol

I.

ICP	Infrastructure à clé publique
ICSA	International Computer Security Association
INRIA	Institut national de recherche en informatique et en automatique

J.

J. du B.	Journal du Barreau
J.E.	Jurisprudence Express
J. Marshall J. Computer & Info L.	John Marshall Journal of Computer and Information Law
J.O.C.E.	Journal officiel des communautés européennes
J. Online L.	Journal Online Law

L.

L.R.C.	Lois refondues du Canada
L.R.Q.	Lois refondues du Québec

M.

McGill L.J.	McGill Law Journal
MIT	Massachusetts Institute of Technology

N.

NSA	National Security Agency

O.

OCDE	Organisation de coopération et de développement économique

OCE	Organisations des consommateurs européens
OPS	Open Profiling Standard
Osgood Hall L.J.	Osgood Hall Law Journal
P.	
P3P	Platform for Privacy Preferences
PGP	Pretty Good Privacy
PICS	Platform for Internet Content Selection
PLPR	Privacy Law & Policy Reporter
R.	
R. du B.	Revue du Barreau
R.D.U.S.	Revue de droit de l'Université de Sherbrooke
R.G.D.	Revue générale de droit
Rich. J.L.. & Tech.	The Richmond Journal of Law & Technology
RSA	Rivest, Shamir et Adleman
S.	
San Diego L.R.	San Diego Law Review
Santa Clara Computer & High. Tech L.J.	Santa Clara Computer and High Technology Law Journal
S-HTTP	Secure Hypertext Transfer Protocol
SIMD	Single Instruction Multiple Data
U.	
U. of Pitt. J. of L. & C.	University of Pittsburgh Journal of Law and Commerce
U. of Pitt. L.R.	University of Pittsburgh Law Review
URL	Universal Resource Locater
W.	
W. Va. J. L. & Tech	West Virginia Journal Law and Technology
Wake Forest L.R.	Wake Forest Law Review
W3C	World Wide Web Consortium
Y.	
Yale L. J.	Yale Law Journal Fordham Int'l L.J.

REMERCIEMENTS

Québec, le 31 août 2000

« Ce n'est que dans l'accomplissement entier et absolu de chaque étape de la vie que l'étape suivante, supérieure, se développe ! »

Loi des Degrés provenant des douze lois de la vie, http://www.chez.com/12lois/presentation/degres.html

Finalement, après de longs mois ardus de recherches, de rédactions et de corrections parsemés de découragements, une étape se conclue.

Évidemment, celle-ci n'aurait pu se concrétiser sans les nombreux encouragements venus de toutes parts et en particulier, sans les appuis et les généreux coups de main de ma mère Lisette et de mon amie Véronique, sans les nombreux commentaires pertinents de mon directeur Me Karim Benyekhlef et surtout, sans ma volonté et ma persévérance de voir un jour, cette étape accomplie.

Je tiens aussi à remercier les différentes fondations qui m'ont octroyé de généreuses bourses d'études durant mes études, dont la Bourse Louis-Philippe Taschereau reçue en 1999, la Bourse de Maîtrise de la Faculté de Droit de l'Université de Montréal reçue en 1999 et la Bourse d'étude Marguerite-Bourgeoys reçue de 1995 à 2000.

Enfin, merci aussi au réseau Internet pour l'ampleur et l'engouement qu'il connaît actuellement. Sans ce nouveau médium, le droit ne serait pas ce qu'il est pour moi aujourd'hui. Grâce à lui, je peux maintenant faire face à cette nouvelle étape ; supérieure.

[redacted]

Patrick Gingras, avocat

« Le virage juridique aura t'il lieu ? Le droit ne pourra-t-il jamais s'adapter aux changements rapides provoqués par les progrès de la science ? »

H. Patrick GLENN, « Le droit en l'an 2000 : L'envahissement des contrôles gouvernementaux et des technologies nouvelles dans la vie privée des citoyens », (1987) 18 *R.G.D.* 705, 711.

« Il est peut-être vrai qu'au fond, rien n'est privé puisque tout se dit ou finit, un jour ou l'autre, par se savoir; que les secrets finissent toujours par franchir les arcanes de sa propre pensée. Cependant, il reste au moins, l'illusion de contrôler, tant bien que mal, sa propre vie. Hors cette illusion, que reste-t-il ? »

Karim BENYEKHLEF, « Les dimensions constitutionnelles du droit à la vie privée » dans *Droit du public à l'information et vie privée : Deux droits irréconciliables*, Actes du colloque tenu à Montréal les 9 et 10 mai 1999, Montréal, Éditons Thémis, 1991, p.43.

INTRODUCTION

> *« Les renseignements personnels coulent sur l'autoroute de l'information comme l'eau qui se déverse des ruisseaux dans les rivières, les lacs, puis les océans. Comme l'eau, l'information provient d'une multitude de sources et sert à des activités d'affaires sans nombre. Une fois puisés à une source, les renseignements personnels se mêlent à d'autres courants d'information où ils sont traités, modifiés, vendus, utilisés dans la production industrielle, d'où il leur est ensuite permis de se déverser, souvent dans un état pollué, méconnaissable*[1]. »

L'avènement des environnements électroniques décentralisés a créé plusieurs défis concernant la protection et la gestion des renseignements personnels. En raison de l'anonymat rendu possible par les concentrations urbaines, les individus sont en droit de s'attendre à un degré élevé d'intimité dans la société actuelle[2]. Néanmoins, l'utilisation généralisée des ordinateurs et des réseaux informatiques affecte la portée de cette sphère d'intimité propre à chaque individu.

Notre siècle est avant tout un siècle tourné vers la technique et l'information. L'information que Littré définissait comme un renseignement[3], naguère considérée comme un bien culturel, est devenue cruciale au point d'être aujourd'hui une véritable entité économique, objet de vente et d'échange. Ces informations sur les personnes permettent directement ou non, d'identifier ou d'être associées à une personne physique. Indirectement, les informations peuvent être considérées nominatives dès que leur nombre ou leur nature permettent de distinguer un individu précis. Ainsi, à l'aide de l'informatique, l'information est devenue plus précise, plus nombreuse, plus envahissante[4]. Dans une société où l'information ne connaît ni frontière, ni dimension, la protection des renseignements personnels constitue donc une condition fondamentale

---

1 INDUSTRIE CANADA, *Protection de la vie privée et autoroute de l'information : Les options du Canada en matière de réglementation*, Ottawa, 1996, http://strategis.ic.gc.ca/SSGF/ca00259f.html

2 CONSEIL DES SCIENCES DU CANADA, *Atelier sur les technologies de l'information et la protection de la vie privée au Canada*, 1985, p.9.

3 LITTRÉ, Dictionnaire, V° Information.

4 Jean PRADEL, « L'information personnelle : entre le commerce et les libertés » dans *Le droit de la communicatique, Actes du colloque conjoint des Facultés de droit de l'Université de Poitiers et de l'Université de Montréal*, Montréal, Éditions Thémis, 1992, p. 23.

à la préservation de la vie privée ; elles se situent « au cœur du droit des personnes et des libertés[5] ».

Considéré comme un droit de la personnalité, le droit à la vie privée sert de plus en plus de bouclier à ceux qui estiment envahissante la présence de l'État, des employeurs, des entreprises financières et du marketing direct[6]. La protection des renseignements personnels existe depuis fort longtemps : des réglementations anciennes visaient le secret professionnel, le secret des affaires ou encore le secret médical[7]. Toutefois, dans la grande majorité des cas, l'informatisation des sociétés a fait tomber les barrières traditionnelles entre l'information personnelle et publique.

Sur le réseau Internet, le respect de la vie privée a prit une toute autre signification en raison de la collecte généralisée de renseignements personnels et de l'utilisation qui en est faite. La multiplication des banques de renseignements découlant de ces collectes devient un fléau. « The Net increases the ease and economic value of the mass collection of personal information[8]. » À cet effet, un grand nombre d'entreprises qui récoltent des renseignements sur le réseau Internet ne se soucient peu ou presque pas de la protection de la vie privée des internautes. Sans trop de mal, ces entreprises réussissent à connaître les habitudes, les convictions et les valeurs de leurs visiteurs. « To businesses, information is extraordinary valuable. Before long, companies won't be able to survive without detailed customer profiles that make it possible to tailor content and ads to suit visitors' tastes[9]. » Les conséquences résultant de ces récoltes sont importantes ; les internautes perdent le contrôle de leurs informations.

À l'heure actuelle, les sociétés industrialisées mettent en place divers instruments visant à protéger les internautes des collectes abusives de renseignements personnels et à en contrôler les flux transfrontaliers. La plupart des pays occidentaux ont choisi de légiférer en normalisant la collecte, l'utilisation, la divulgation, la sécurité et la qualité des renseignements personnels, et ce, de manière à assurer « la vie privée

---

5 C.N.I.L., *10 ans d'informatique et libertés*, Paris, Economica, 1988, P.41.

6 Danielle PARENT, « La reconnaissance et les limites du droit à la vie privée en droit québécois », *dans Développements récents en droit administratif (1994), Service de la formation permanente, Barreau du Québec*, Cowansville, Éditions Yvon Blais Inc., 1994, p. 219.

7 Yves POULET, « La protection des données : normes et principes », (1981) 124 *Informatique et gestion*, 25.

8 Joel R. REIDENBERG, « The Use of Technology to Assure Internet Privacy : Adapting Labels and Filters to Data Protection », *Lex Electronica*, Volume 3, Numéro 2, http://www.lex-electronica.org/reidenbe.html

9 Leslie MILLER et Elizabeth WEISE, « Keeping 'pry' out of the privacy debate », 31 mars 1999, *USA Today*, http://www.usatoday.com/life/cyber/tech/cte755.htm.

informationnelle[10] » des individus. Le mouvement a été amplifié par l'intervention des institutions internationales, notamment en raison du développement des échanges transfrontaliers d'informations. Le Conseil de l'Europe a adopté très tôt deux résolutions et l'Union européenne a elle aussi, adoptée en 1995, la *Directive 95/46/CE relative à la protection des personnes physique à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.* Au Canada, les législateurs québécois et canadien ont aussi suivi cette même voie en adoptant des législations semblables.

En contrepartie, les Américains ont plutôt opté pour une position différente, c'est-à-dire qui repose non pas sur une législation, mais sur des principes ultralibéraux[11] mis en place par des méthodes de standardisation[12]. Aux dires des Américains, ce sont les entreprises qui connaissent le mieux le fonctionnement des nouveaux environnements. Ainsi, celles-ci se doivent de s'associer dans des organisations professionnelles, de rédiger des codes de conduites, voire de concevoir des labels de qualité et de proposer ces méthodes de standardisation aux internautes.

Dans l'optique où les États-Unis est le seul pays à mettre l'emphase sur le développement et l'instauration de méthodes de standardisation et où la plupart des pays occidentaux critiquent ouvertement ces méthodes, il importe de se questionner sur le rôle et les avantages que les méthodes de standardisation peuvent apporter comme méthode de protection des renseignements personnels sur le réseau Internet. À cet effet, l'objectif principal de cette étude est d'analyser les méthodes de standardisation pour la protection des renseignements personnels sur le réseau Internet. Plus particulièrement, nous comparerons les différentes méthodes présentement utilisées par les Américains et nous nous interrogeons sur la notion de standardisation comme source de normativité et de complémentarité à la législation.

---

[10] Voir Karim BENYEKHLEF, *La protection de la vie privée dans les échanges internationaux d'informations*, Montréal, Thémis, 1992, p.3.

[11] Communément appelé l'autoréglementation.

[12] Dans le cours de la présente étude, nous définissons les méthodes de standardisation comme étant l'établissement et la mise en application, par voie consensuelle, d'un ensemble de standards et de spécifications par un organisme et ayant pour objet de simplifier, d'unifier et de rationaliser la protection des renseignements personnels sur le réseau Internet. Nous y reviendrons.

Ainsi, la présente étude se compose de deux (2) parties. La première, intitulée « Internet & les renseignements personnels », comporte deux chapitres traitant respectivement de la protection de la vie privée et des collectes de renseignements personnels sur Internet. La seconde partie intitulée « La protection des renseignements personnels sur Internet », compte quant à elle deux chapitres traitant, d'une part, des diverses solutions préconisées pour la protection des renseignements personnels en Europe, au Canada, au Québec et aux États-Unis, et d'autre part, de la standardisation comme méthode de protection des renseignements personnels sur Internet. Du fait de leur spécificité et de leur importance en ce qui a trait à la protection des renseignements personnels sur le réseau Internet, les questions et réflexions relatives à la notion de standardisation comme méthode de protection des renseignements personnels sont abordées dans le dernier chapitre.

PREMIÈRE PARTIE
INTERNET & LES RENSEIGNEMENTS PERSONNELS

Chapitre 1
La protection de la vie privée sur Internet

À l'ère de l'information, les sondages révèlent que la protection de la vie privée est au cœur des préoccupations de la population[13]. En tant qu'élément essentiel de la liberté et de la dignité humaine, le droit au respect de la vie privée revêt une importance primordiale[14]. Ce premier chapitre s'intéressera à la protection de la vie privée dans les environnements électroniques décentralisés[15]. Dans un premier temps, nous nous attarderons à la notion de renseignement personnel à l'intérieur de la sphère du droit à la vie privée (A) et, en second lieu, aux moyens généralement utilisés par les internautes pour protéger leur vie privée et leurs renseignements personnels lorsqu'ils naviguent sur la toile[16] (B).

A. Vie privée et Internet

L'une des préoccupations majeures que suscitent les technologies de l'information est sans aucun doute la protection de la vie privée dans les environnements électroniques. Le mythe du Big Brother où l'État maintient une surveillance constante des

---

[13] INDUSTRIE CANADA, *La protection de la vie privée et l'autoroute canadienne de l'information*, Ottawa, Ministère des Approvisionnements et Services Canada, 1994, p.3.

[14] « Dans la société contemporaine, la conservation de renseignements à notre sujet revêt une importance accrue. Il peut arriver, pour une raison ou pour une autre, que nous voulions divulguer ces renseignements ou que nous soyons forcés de le faire, mais les cas abondent où on se doit de protéger les attentes raisonnables de l'individu que ces renseignements seront gardés confidentiels par ceux à qui ils sont divulgués et qu'ils ne seront utilisés que pour les fins pour lesquelles ils ont été divulgués. » *R.* c. *Dyment*, [1988] 2 R.C.S. 417.

[15] « Les environnements électroniques décentralisés se caractérisent par l'absence d'un lieu centralisé susceptible d'exercer un contrôle sur les contenus véhiculés dans ces environnements. La plupart de ces environnements fonctionnent de manière à constituer à la fois un mode de diffusion, de distribution et d'échange d'information. C'est ainsi qu'ils offrent la possibilité de communiquer avec un seul correspondant ou une multitude d'entre eux, celle de mettre des informations à la disposition d'un ou d'une multitude d'usagers [...]. » Dans ce contexte, « les possibilités effectives de contrôle sont aux mains de ceux qui administrent les différents sites entre lesquels des interconnections existent ou sont possibles. » Pierre TRUDEL (avec la collaboration de R. GÉRIN-LAJOIE), « La protection des droits et valeurs dans la gestion des réseaux ouverts », dans Daniel POULIN, Pierre TRUDEL et Ejan MACKAAY (dir.), *Les autoroutes électroniques : usages, droit et promesses*, Cowansville, Éditions Yvon Blais Inc., 1995, p.302.

[16] Outre le terme Web, on trouve également en français les termes toile d'araignée mondiale, toile mondiale et toile. PUBLICATIONS DU QUÉBEC, *Terminologie d'Internet*, http://www.olf.gouv.qc.ca/ressources/internet/fiches/2075076.htm

communications effectuées à partir des ordinateurs, hante toujours les usagers de ces environnements[17].

Une étude datant du mois de juin 1997 démontre que parmi les 100 sites Web[18] les plus populaires du World Wide Web[19], seulement 17 d'entre eux avaient adopté une politique en matière de vie privée[20]. De plus, il appert qu'aucun d'entre eux ne répondait aux normes de protection de la vie privée internationalement reconnues[21].

À la lecture de ces résultats, nous constatons que les internautes sont en droit de se questionner :

- Sur le niveau de protection qui leur est accordé lorsqu'ils naviguent sur la toile et,
- Sur la possibilité d'appliquer concrètement et valablement les normes internationales visant la protection de leur vie privée et de leurs renseignements personnels.

Depuis quelques années, la conscientisation des internautes et la création de divers organismes[22] de protection ont tenté de régulariser la situation. Une étude datant du mois de juin 1999 effectuée par le Georgetown Internet Privacy Policy Study illustre bien cette situation[23]. Parmi les 361 sites Web visités, près de 93 % de ceux-ci récoltaient des renseignements personnels sur leurs visiteurs. De ce nombre, seulement 66 %

---

17 Ce mythe joue pour beaucoup dans la place parfois démesurée que prennent les préoccupations au sujet de la vie privée. Pierre TRUDEL, France ABRAN, Karim BENYEKHLEF et Sophie HEIN, *Droit du cyberespace*, Montréal, Éditions Thémis, 1996, p. 1-19.

Pour une vision romancée de ce sujet, lire George ORWELL, *1984*, Mass Market Paperback, Reissue edition (May 1990), 268 pages et visionner : *Ennemy of the State* du réalisateur Tony Scott, mettant en vedette Will Smith, Gene Hackman et Jon Voight, 1998, http://www.movies.go.com/eos/

18 L'adresse Web ou l'Universal Resource Locater (URL), est un ensemble de données permettant d'avoir accès à l'information d'Internet quand on utilise un navigateur Web et qui contient une méthode d'accès au document recherché, le nom du serveur et le chemin d'accès au document. PUBLICATIONS DU QUÉBEC, *Terminologie d'Internet*, http://www.olf.gouv.qc.ca/ressources/internet/fiches/2075082.htm

19 Mieux connus sous le terme Web ou son abréviation WWW, le World Wide Web est un système basé sur l'utilisation de l'hypertexte, qui permet la recherche d'information dans Internet, l'accès à cette information et sa visualisation. PUBLICATIONS DU QUÉBEC, *Terminologie d'Internet*, http://www.olf.gouv.qc.ca/ressources/internet/fiches/2075076.htm

20 Communément appelé « privacy policies » en anglais.

21 EPIC, *Surfer bewares: Personal privacy and the Internet*, Juin 1997, http://www.epic.org/reports/surfer-beware.html

22 PANORANET, *Organismes impliqués dans la protection de la vie privée*, 1999, http://www.canalnet.net/vvp/ressources/veilleur/orgen.htm

23 GEORGETOWN INTERNET PRIVACY POLICY STUDY, *Georgetown Internet Privacy Policy Survey*, 21 juin 1999, http://www.msb.edu/faculty/culnanm/gippshome.html

affichaient une politique en matière de vie privée[24]. En conséquence, il subsiste toujours, au fil des ans, un grand nombre de sites qui n'adoptent et/ou n'appliquent pas de politiques en matière de vie privée.

Les législations nationales et internationales visant à protéger les renseignements personnels sont extrêmement difficiles à appliquer vu le caractère transfrontalier du réseau et le développement de plus en plus sophistiqué des techniques de collectes. Néanmoins, des organismes, tels que TRUSTe aux États-Unis et VVP[25] en France, tentent de renverser la vapeur en misant sur l'éveil des internautes. En éduquant les usagers au respect de leur vie privée, ils espèrent diminuer les collectes illicites et inciter les usagers à visiter seulement les sites qui énoncent et maintiennent des politiques en matière de vie privée. Comme l'espérait Alan F.Westin en 1970, la société a fini par se rendre compte que la notion de vie privée est au cœur de celle de la liberté dans un État moderne[26].

1) La sphère de la vie privée

La vie privée, notion floue par excellence, n'a jamais véritablement fait l'objet de définition précise, tant par les législateurs que par la doctrine[27]. L'une des difficultés

---

[24] Toutefois, il importe de souligner que dans la grande majorité des cas, ces politiques sont souvent de simples pétitions de principes ou de vœux pieux. «Very few Web sites have strong privacy policies-and a surprising number don't even have any policy. Only 3.5% of the 30,000 Web sites reviewed by Enonymous.com were judged to have a four-star privacy rating, the top mark given by the survey-and 77.2% had no privacy policy. » En consequence, selon l'EPIC, une politique adéquate en matière de vie privée devrait comporter : « There are many different privacy policies, but all good policies share certain characteristics: they explain the responsibilities of the organization that is collecting personal information and the rights of the individual who provided the personal information. Typically, this means that an organization will explain why information is being collected, how it will be used, and what steps will be taken to limit improper disclosure. It also means that individuals will be able to obtain their own data and make corrections if necessary. » EPIC, *Surfer Beware: Personal Privacy and the Internet*, Juin 1997, http://www.epic.org/reports/surfer-beware.html, Matthew G. NELSON, « Majority Of Web Sites Lack Privacy Policies », 17 avril 2000, *TechWeb*, http://www.techweb.com/se/directlink.cgi?IWK20000417S0076 et Kristen GERENCHER, « Web site privacy policies unclear, survey finds less than 4% of 30,000 sites reviewed get top grade » , 11 avril 2000, *CBS – Marketwatch*, http://cbs.marketwatch.com/archive/20000411/news/current/pf.htx?source=htx/http2_mw

[25] Votre Vie Privée. Nous y reviendrons dans le second titre.

[26] Alan F. WESTIN, *Privacy and Freedom*, New York, Atheneum, 1970, p.350.

[27] Le professeur de sciences politiques Alan F. Westin, reconnu pour son expertise dans le domaine de la vie privée et des renseignements personnels, a donné l'une définition de la vie privée les plus lucides et les plus fouillées qui soient jusqu'à aujourd'hui. Elle s'énonce ainsi :

« La vie privée est le droit des particuliers, des groupes ou des établissements à déterminer eux-mêmes quand, comment et dans quelle mesure des renseignements à leur sujet peuvent être communiqués à d'autres. Dans le contexte des relations sociales, la vie privée consiste, pour un individu, à se retirer volontairement et temporairement de la société, qu'il s'agisse d'un retrait physique ou psychologique, pour trouver la solitude, l'intimité d'un petit groupe ou l'anonymat et la réserve au sein de groupes plus importants. Le désir de la vie privée d'un particulier n'est jamais absolu, puisqu'il est contrebalancé par son désir de participation à la société. Ainsi, chaque particulier cherche constamment, dans un processus d'ajustement personnel, à équilibrer son désir de solitude avec son désir de s'ouvrir et de se confier aux autres, en se

d'appréhension de cette notion réside dans le fait que de tenter de « définir ce droit, en ferait un instrument sclérosé dépourvu de toute efficience et en restreindrait sa portée pour l'avenir[28]. »

Fondée sur l'autonomie morale et physique de l'individu, la notion de vie privée est essentielle à son bien-être[29]. Elle est la vie elle-même : une qualité, un état d'être que l'on ne peut saisir par des techniques de mesure et de catégorisation. L'une des principales difficultés dans l'établissement d'une définition précise réside dans le fait que la vie privée est une notion qui varie selon les époques, les contextes, les mœurs et les individus[30]. Elle ne peut se définir à l'intérieur d'une définition fixe ; elle doit nécessairement participer aux principes d'autonomie des individus[31] et évoluer au fil du temps.

Le droit au respect de la vie privée est un droit fondamental de la personne dont les Chartes ne sont que déclaratoires[32]. L'objet du droit étant, dans une certaine mesure indéterminé, le droit à la vie privée est un ensemble de droits[33]. Ainsi, la doctrine

---

laissant guider par les conditions du milieu et les normes sociales dictées par la société dans laquelle il vit. En agissant de la sorte, l'individu est soumis à certaines pressions : la curiosité des autres et les méthodes de surveillance dont se dote toute société pour imposer le respect de ses normes sociales. » Alan F. WESTIN cité dans CONSEIL DES SCIENCES DU CANADA, *Atelier sur les technologies de l'information et la protection de la vie privée au Canada*, 1985, p.10.

28 Raymond LINDON, « La protection de la vie privée: champ d'application », (1971) *J.T.* 713, Peter BURNS, « The law and Privacy : the Canadian Experience », (1976) 54 *Can. Bar Rev.* 1 et Geoffrey MARSHALL, « The Right to Privacy : A Sceptical View », (1975) 21 *McGill L. J.* 242.

29 Alan F. WESTIN, *Privacy and Freedom*, New York, Atheneum, 1970, p. 349.

30 Selon le professeur Trudel, la vie privée est une notion qui n'a pas à être déterminée de façon définitive ; ce qui ne l'empêche pas d'être une notion déterminable dans chaque situation concrète. Une détermination ayant été faite à une occasion, ne constitue pas nécessairement un précédent dans d'autres circonstances. Pierre TRUDEL, « Le rôle de la loi, de la déontologie et des décisions judiciaires dans l'articulation du droit à la vie privée et de la liberté de presse », dans Pierre TRUDEL et France ABRAN, *Droit du public à l'information et vie privée : Deux droits irréconciliables ?*, Montréal, Éditions Thémis, 1992, p.181.

Voir Karim BENYEKHLEF qui traite de l'inutilité d'une définition du droit à la vie privée dans « Les dimensions constitutionnelles du droit à la vie privée » dans *Droit du public à l'information et vie privée : Deux droits irréconciliables*, Actes du colloque tenu à Montréal les 9 et 10 mai 1999, Montréal, Éditons Thémis, 1991, p.17.

31 Pierre TRUDEL, France ABRAN, Karim BENYEKHLEF et Sophie HEIN, *Droit du cyberespace*, Montréal, Éditions Thémis, 1996, p. 11-25.

32 Le droit à la vie privée n'est pas un droit absolu malgré que son existence implique nécessairement une obligation corrélative de respecter la vie privée d'autrui. H. Patrick. GLENN, « Le droit au respect de la vie privée », (1979) 39 *R. du B.* 879, p. 879, 892.

De plus, la Cour suprême du Canada a rappelé qu'il est possible de renoncer à la protection de sa vie privée. *Frenette* c. *Metropolitan Life Insurance Co.*, [1992] 1 R.C.S. 647.

33 H. Patrick. GLENN, « Le droit au respect de la vie privée », (1979) 39 *R. du B.* 879, p. 880.

juridique a défini la vie privée comme étant « le droit de vivre en paix, sans intrusion ni interruption[34], et le droit de contrôler les renseignements qui touchent sa personne[35]. »

Le droit de vivre en paix correspond concrètement à deux intérêts, soit l'intrusion injustifiée et l'anonymat[36]. L'intrusion injustifiée est une sorte d'intégrité mentale ou spirituelle ; c'est une condition dans laquelle un individu est libre de toute entrave injustifiable à son état d'esprit. C'est la solitude de la victime qui est atteinte par cette intrusion[37]. Le second intérêt, l'anonymat, provient en l'absence de faits justificatifs, de l'investigation ou l'intrusion dans le secret de la vie privée et de la divulgation ou la diffusion non autorisée de renseignements ou d'images[38]. C'est le droit d'un individu de mener sa vie comme il l'entend, avec un minimum d'ingérence de la part d'autrui.

La *Charte canadienne des droits et libertés*[39], dont l'application est limitée aux actions de l'État[40], édicte une protection constitutionnelle contre les fouilles, les perquisitions et les saisies abusives.[41] À première vue, l'article 8 de la *Charte canadienne* ne garantit pas

---

[34] La protection juridique contemporaine quant au droit du citoyen d'être laissé tranquille s'est manifestée d'abord aux États-Unis en 1888, lorsque l'Américain Thomas Cooley référait au droit d'être laissé seul : « The right to be let alone. » Deux ans plus tard, Warren et Brandeis reprenait à leur compte l'argumentation de leur collègue et s'inspiraient de cette dernière pour conclure à l'existence légale d'un droit à la vie privée. Thomas M. COOLEY, *A Treatise on the Law of Torts or the Wrongs which Arise Independents of Contract*, 2d. ed., Chicago, Callaghan & Co., 1888, p.29 et WARREN & BRANDEIS, « The Right to Privacy », (1890) 4 *Harvard L.R.* 193.

[35] Ce droit de contrôle sera plus amplement analysé à la fin du présent chapitre. Néanmoins, au sujet de l'importance de ce droit, le Commissaire à la protection de la vie privée du Canada affirma : « La vie privée est protégée dans la mesure où nous possédons une emprise sur ce que les autres savent à notre sujet. » COMMISSAIRE À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Le dépistage génétique et la vie privée, ministre des Approvisionnements et Services Canada*, Ottawa, Ontario, 1992, p2.

[36] H. Patrick. GLENN, « Le droit au respect de la vie privée », (1979) 39 *R. du B.* 879, p. 884 et voir *Valiquette* c. *The Gazette* où le juge Viau déclara que le droit à la vie privée est un droit fondamental qui comporte celui de vivre de façon retirée [droit à la solitude] et anonyme. *Valiquette* c. *The Gazette* J.E. 97-133 (C.A.).

[37] Le droit à la solitude qui fut expressément reconnu par la jurisprudence pourrait être protégé en fonction d'une sphère d'autonomie personnelle propre à l'individu, à l'intérieur de laquelle il peut prendre des décisions fondamentales relatives à sa propre personne. Voir Isabelle HARNOIS, « La protection constitutionnelle et quasi constitutionnelle du droit au respect de la vie privée et les banques de données informatisées », dans *Congrès annuel du Barreau du Québec (1997)*, Service de la formation permanente, Barreau du Québec 1997, p.676.

Au sujet du droit à la solitude, le professeur Glenn écrit : « Le droit au respect de la vie privée est protecteur d'un intérêt distinct de celui de la jouissance des choses matérielles. Il s'agit d'un intérêt qui ne peut être défini qu'en fonction de la solitude de l'individu, et cette notion de solitude doit signifier une sorte d'intégrité mentale ou spirituelle, une condition dans laquelle l'individu est libre de toute entrave injustifiable à son état d'esprit. [...] Il existe ainsi un droit d'être seule dans la foule. » H. Patrick. GLENN, « Le droit au respect de la vie privée », (1979) 39 *R. du B.* 879, p. 884 et *Valiquette* c. *The Gazette*, [1991] R.J.Q. 1075 (C.S.).

[38] Le droit à l'anonymat sera plus amplement analysé dans la seconde partie de ce chapitre.

[39] 1982, ch. 11 (R.U.) dans L.R.C. (1985), App. II, no. 44.

[40] Ce qui implique qu'elle ne peut être invoquée dans le cadre d'un litige privé n'ayant aucun lien avec les gouvernements fédéral ou provincial. Voir l'article 32 de la *Charte canadienne* et *S.D.G.M.R.* c. *Dolphin Delivery Ltd.*, [1986] 2 R.C.S. 573.

[41] La *Charte canadienne* ne garantit pas expressément le droit à la vie privée de façon automne. Quoique les tribunaux n'aient pas encore clairement établi de liens entre l'article 7 de la Charte canadienne [« Chacun a

expressément le droit au respect ou à la protection de la vie privée[42]. Cependant, la Cour suprême du Canada lui a accordé un sens plus large en étendant sa portée à la protection de l'expectative raisonnable des citoyens en matière de vie privée. Selon le juge La Forest, l'essence de la garantie offerte par l'article 8 vise ce qui suit :

> « *Selon ce que nous dit Westin, la société a fini par se rendre compte que la notion de vie privée est au cœur de celle de la liberté dans un état moderne [...] Fondée sur l'autonomie morale et physique de la personne, la notion de vie privée est essentielle à son bien-être. Ne serait-ce que pour cette raison, elle mériterait une protection constitutionnelle, mais elle revêt aussi une importance capitale sur le plan de l'ordre public. L'interdiction qui est faite au gouvernement de s'intéresser de trop près à la vie des citoyens touche à l'essence même de l'état démocratique*[43]. »

En interprétant l'article 8, la Cour suprême a certes reconnu que le droit à la vie privée ne donnait naissance qu'à une attente raisonnable en la matière[44]. Les règles et l'étendue de la protection du droit à la vie privée varient notamment, selon qu'il s'agit d'un lieu public ou privé[45]. Un juste équilibre doit être atteint entre le droit au respect de la vie privée et les autres droits avec lesquels il peut entrer en conflit.

---

droit à la vie, à la liberté et à la sécurité de sa personne; il ne peut être porté atteinte à ce droit qu'en conformité avec les principes de justice fondamentale. »] et la vie privée, le juge Wilson dans *Morgentaler*, semble laisser entendre que l'article 7 garantit à chaque individu une marge d'autonomie personnelle sur ses décisions importantes touchant intimement à sa vie privée (ou à tout le moins, une autonomie décisionnelle). Voir *Morgentaler* c. *La Reine,* [1988] 1 R.C.S. 30. p. 171, Karim BENYEKHLEF, *La protection de la vie privée dans les échanges internationaux d'information*, Montréal, Éditions Thémis, 1992, p. 31 et Danielle PARENT, « La reconnaissance et les limites du droit à la vie privée en droit québécois » dans *Développements récents en droit administratif (1994)*, 1994, Cowansville, Éditions Yvon Blais Inc., 215, p. 215 et *R.* c. *Beare*, [1988] 2 R.C.S. 387.

[42] Article 8 : Chacun a droit à la protection contre les fouilles, les perquisitions ou les saisies abusives.

[43] *R.* c. *Dyment*, [1988] 2 R.C.S. 417, 441. Voir *Thomson Newspaper* c. *Directeur des enquêtes et recherches*, [1990] 1 R.C.S. 153, où la Cour suprême circonscrit la notion de droit à la vie privée.

[44] Il faut apprécier si, dans une situation donnée, le droit du public de ne pas être importuné par le gouvernement doit céder les pas au droit du gouvernement de s'immiscer dans la vie privée des particuliers afin de réaliser ses fins et, notamment, d'assurer l'application de la loi. *Hunter* c. *Southam Inc.* [1984] 2 R.C.S. 145, 159-160.

Pour une analyse détaillée de l'état du droit constitutionnel en vertu de l'article 8 de la Charte canadienne, lire Karim BENYEKHLEF, « Les dimensions constitutionnelles du droit à la vie privée » dans *Droit du public à l'information et vie privée : Deux droits irréconciliables*, Actes du colloque tenu à Montréal les 9 et 10 mai 1999, Montréal, Éditons Thémis, 1991, p.25, *R.* c. *Duarte*, [1990] 1 R.C.S. 30,46 et *R.* c. *Beare*, [1988] 2 R.C.S. 387,412.

[45] Le principe de base demeure toutefois le même : existe-t-il ou non, dans chaque cas précis, une attente raisonnable en matière de respect de la vie privée.

Afin de mieux saisir l'essence du droit à la vie privée, la Cour décompose cette notion en trois sphères de revendications distinctes[46] :

- Celles qui comportent des aspects territoriaux ou spatiaux ;
- Celles qui ont trait à la personne ;
- Celles qui sont faites dans un contexte informationnel.

L'aspect informationnel de la vie privé découle du postulat selon lequel l'information de caractère personnel est propre à l'intéressé qui est libre de la communiquer ou de la taire comme il l'entend[47]. Selon Rankin, l'essence du droit à la vie privée informationnelle se résume comme suit : « The claim of information privacy assumes that all information about an individual is fundamentally the property of the individual : for him to communicate or withhold as he determines[48]. »

Dans *Dyment*, la Cour suprême a défini le droit à la vie privée en matière d'information :

> « *Cet aspect [...] est fondé sur la notion de dignité et d'intégrité de la personne. Comme l'affirme le groupe d'étude [...] : « Cette conception de la vie privée découle du postulat selon lequel l'information de caractère personnel est propre à l'intéressé, qui est libre de la communiquer ou de la taire comme il l'entend. » Dans la société contemporaine tout spécialement, la conservation de renseignements à notre sujet revêt une importance accrue. Il peut arriver, pour une raison ou pour une autre, que nous voulions divulguer ces renseignements ou que nous soyons forcés de le faire, mais les cas abondent où on se doit de protéger les attentes raisonnables des individus que ces renseignements ou que nous soyons forcés de le faire, mais les cas abondent où on se doit de protéger les attentes raisonnables de l'individu que ces renseignements seront gardés confidentiellement par ceux à qui ils sont divulgués, et qu'ils ne seront pas utilisés que pour les fins pour lesquelles ils ont été divulgués [principes des finalités]*[49].»

Au Québec, les articles 3 et 35 du *Code civil du Québec*[50] et l'article 5 de la *Charte des droits et libertés de la personne*[51] garantit expressément à toute personne le droit au respect de sa vie privée. En tant que loi quasi constitutionnelle, la *Charte québécoise* octroie aux droits qu'elle consacre une très haute place dans la hiérarchie juridique[52].

---

[46] Pour une étude détaillée des aspects, lire Karim BENYEKHLEF, « Les dimensions constitutionnelles du droit à la vie privée » dans *Droit du public à l'information et vie privée : Deux droits irréconciliables*, Actes du colloque tenu à Montréal les 9 et 10 mai 1999, Montréal, Éditons Thémis, 1991, p. 26.

Néanmoins, il existe des conséquences pratiques de la consécration du respect de la vie privée par la *Charte québécoise* :

> « *Cette inclusion du droit à l'intimité dans une charte implique que le législateur lui reconnaît la valeur d'un droit fondamental, ce qui peut avoir plusieurs conséquences pratiques : premièrement, l'atteinte sera considérée dommageable in se. [...] La preuve du préjudice est rendue beaucoup plus facile – dès l'atteinte commise, le préjudice existe. Deuxièmement, il en est de même pour la preuve de la faute [...]*[53]. »

Concrètement, la notion de vie privée réfère à deux volets : le volet identificateur et le volet contextuel[54]. Le volet identificateur se rapporte aux aspects et aux faits de la vie d'une personne. Il permet d'identifier objectivement les éléments traditionnellement reconnus comme faisant partie de la vie privée à une époque donnée. Le volet subjectif pour sa part, prend en considération les personnes visées et varie selon les individus, les époques, les contextes et les mœurs.

Pour établir une atteinte à la vie privée, il est primordial de déterminer si l'information obtenue lors de cette récolte porte sur un élément de la vie privée de l'usager. Un usager peut prétendre au respect de sa vie privée, seulement lorsqu'il se trouve dans un contexte où il a une expectative légitime de vie privée. L'évaluation du contexte doit tenir compte de la dichotomie entre ce qui est privé et ce qui est public, de l'identité de la

---

47 Pour une étude détaillée du droit à la vie privée informationnelle, lire Karim BENYEKHLEF, *La protection de la vie privée dans les échanges internationaux d'information*, Montréal, Éditions Thémis, 1992, p. 49 et suivantes.

48 Murray RANKIN, « Privacy & Technology: A Canadian Perspective », [1984] 22 *Alberta L.R.* 323, p. 325.

49 *R.* c. *Dyment*, [1988] 2 R.C.S. 417, 429-430.

50 L.Q. 1991, c.64.

L'article 3 C.c.Q. édicte que toute personne est titulaire de droits de la personnalité, tel le droit à la vie, à l'inviolabilité et à l'intégrité de sa personne, au respect de son nom, de sa réputation et de sa vie privée. L'article 35 pour sa part, énonce que toute personne a droit au respect de sa réputation et de sa vie privée et que nulle atteinte ne peut être portée à la vie privée d'une personne sans que celle-ci ou ses héritiers y consentent ou sans que la loi l'autorise.

51 L.R.Q., c. C-12.

L'article 5 de la Charte québécoise énonce que toute personne a droit au respect de sa vie privée. De plus, l'article 44 reconnaît le droit à l'information, dans la mesure prévue par la loi.

52 L'article 52 de la Charte québécoise établit le caractère prépondérant des articles 1 à 38 et stipule que l'on ne peut déroger à ces articles, sauf dans la mesure prévue par ces articles et à moins que la loi n'énonce expressément que la disposition s'applique malgré la Charte. Les garanties offertes s'étendent non seulement au rapports entre l'administration publique québécoise et ses administrés, mais aussi aux rapports privés. F. CHEVRETTE et H. MARX, *Droit constitutionnel : notes et jurisprudences*, Montréal, P.U.M. 1982, p.19.

53 Pierre PATENAUDE, *La preuve, les techniques modernes et le respect des valeurs fondamentales : enquête, surveillance et conservation des données*, Sherbrooke, Éditions R.D.U.S., 1990, p. 23-24.

54 Patrick A. Molinari et Pierre TRUDEL, « Le droit au respect de l'honneur, de la réputation et de la vie privée : Aspects généraux et applications », dans *Application des chartes des droits et libertés en matière civile*, Service de la Formation permanente, Barreau du Québec Cowansville, Éditions Yvon Blais, 1988, 197, p.211.

personne, de son rôle social, de la nature des actes qu'elle accomplit et des attentes raisonnables qu'une personne a de se protéger des ingérences d'autrui.

a) Le volet identificateur

Le volet identificateur réfère aux faits et aux aspects de la vie d'une personne qui sont inclus dans un domaine protégé. Au Québec, les tribunaux ont statué à plusieurs reprises pour déterminer ce qui est inclus dans la vie privée des personnes publiques. Rare sont les décisions qui ont traité de cette question pour les simples particuliers[55]. Toutefois, lorsqu'il fut jugé qu'une divulgation ou une recherche d'information est illicite parce qu'elle a pour objet un élément de la vie privée, fut-ce d'une vedette, il en découle à plus forte raison que ce type d'information fait partie de la vie privée des simples particuliers[56].

L'article 36 *C.c.Q* énonce certains actes qui peuvent être considérés comme des atteintes à la vie privée. La jurisprudence énonce aussi certains éléments de la vie privée rattachés à l'intimité d'un individu. Parmi ceux-ci, on retrouve l'intimité de son foyer, ses origines, son état de santé, son anatomie, sa vie conjugale, familiale et amoureuse, ses opinions politiques, philosophiques ou religieuses, sa vie professionnelle et son orientation sexuelle[57]. En conséquence, à chaque fois où une information se rapportant au volet identificateur d'un individu est soit récoltée et/ou dévoilée sans son approbation, il peut y avoir une atteinte à la vie privée de cet individu.

---

[55] Selon le professeur Kayser, les éléments de la vie privée des simples particuliers sont rarement l'objet de décision de justice, parce qu'ils ne sont pas souvent l'objet d'investigations ni de divulgations. Pierre KAYSER, *La protection de la vie privée : Protection du secret de la vie privée*, 2e éd., Paris Aix-en-Provence, Économica, Presse Universitaires d'Aix Marseille, 1990, p.174.

[56] Pierre KAYSER, *La protection de la vie privée : Protection du secret de la vie privée*, 2e éd., Paris Aix-en-Provence, Économica, Presse Universitaires d'Aix Marseille, 1990, p.174.

[57] Karim BENYEKHLEF et Pierre TRUDEL, *Approches et stratégies pour améliorer la protection de la vie privée dans le contexte des inforoutes*, Mémoire présenté à la Commission de la culture de l'Assemblée nationale dans le cadre de son mandat sur l'étude du Rapport quinquennal de la Commission d'accès à l'information, septembre 1997, p. 6.

b) Le volet contextuel

Le volet contextuel de la vie privée s'évalue en fonction de chaque individu. Il est fort probable que ce qui est présentement inclus dans ce volet, devienne au fil des ans, une information d'intérêt public[58].

Le volet contextuel se détermine en tenant compte des nécessités de l'information publique et des autres valeurs qui sont en cause dans la délimitation du droit à la vie privée. La définition de ce volet repose sur le rôle de l'individu dans la société. Le droit au respect de sa vie privée trouve ses limites dans l'intérêt du public à prendre connaissance de certains aspects de sa personnalité.

À l'intérieur de ce volet, l'intérêt du public à être informé devient une notion de référence pour déterminer si le comportement attaqué est une entrave au droit à la vie privée[59]. L'état de santé d'un simple individu ne possède pas le même intérêt aux yeux du public que celui d'une personne publique par exemple[60].

Les environnements électroniques décentralisés offrent une multitude de situations particulières qui peuvent donner ouverture à une intrusion dans la vie privée des usagers. La simple visite d'un site Web ou la participation à un groupe de discussion laissent des traces qui, suite aux cumuls de ces informations, peuvent équivaloir à une intrusion dans la vie privée d'un usager.

À l'intérieur des réseaux informatiques, la vie privée doit être protégée en fonction des expectatives légitimes des utilisateurs qui, étant impliqués à divers degrés dans la vie sur ces réseaux, ont une vie privée et publique. Néanmoins, cette expectative légitime de vie privée varie en fonction du lieu où ils se trouvent[61].

---

[58] « Vu que les individus n'ont pas tout le même rôle dans la société, il est fort probable que ce qui est assimilable à un aspect de la vie privée pour l'un ne le soit pas pour l'autre. » Martin MICHAUD, *Le droit au respect de la vie privée dans le contexte médiatique : de Warren et Brandeis à l'inforoute*, Montréal, Wilson & Lafleur, 1996, p.45 et ss.

[59] Martin MICHAUD, *Le droit au respect de la vie privée dans le contexte médiatique : de Warren et Brandeis à l'inforoute*, Montréal, Wilson & Lafleur, 1996, p.31.

[60] *Valiquette* c. *The Gazette*, (1991) R.J.Q. 1075 (C.S.).

[61] Anne Wells BRANSCOMB, « Anonymity, Autonomy and Accountability : Challenge to the First Amendment in Cyberspaces », (1995) 104 *Yale L.J.* 1639, p. 1655.

2) *Les renseignements personnels*

Le développement des réseaux informatiques a grandement contribué à augmenter le volume de renseignements personnels disponibles et à remplacer les méthodes désuètes de collecte de renseignements par des méthodes plus efficaces et plus rapides[62]. À ce sujet, le professeur Kayser écrit :

> « *Les progrès récents des sciences et des techniques ont suscité des procédés d'investigation dans la vie privée et des procédés de divulgation de celle-ci sans commune mesure avec ceux qui existaient jusqu'alors. [...] La protection du secret de la vie privée est ainsi devenue dans les sociétés industrielles un des problèmes les plus urgents et les plus difficiles à résoudre, parce que ces modes de protection ne se sont pas développés en proportion des menaces nouvelles qui pèsent sur elle*[63]. »

Sur la toile, la préoccupation principale des usagers à l'égard du respect de leur vie privée a trait à leur vie privée informationnelle, soit l'intérêt des personnes à l'égard des informations qui les concernent ou qui sont susceptibles d'être divulguées. Cette problématique qui ne constitue pas en elle-même un phénomène exclusif aux environnements électroniques, semble toutefois indubitablement liée au développement des technologies de l'information[64].

Les principes fondamentaux en matière de protection des renseignements personnels n'ont pas vocation à régir toutes les situations mettant en cause la vie privée des usagers des environnements électroniques décentralisés[65]. Il va de soi que la protection des renseignements personnels n'est qu'un sous-ensemble ; qu'une facette du droit à la vie privée représentant l'aspect informationnel de ce droit[66].

---

62 Joel REIDENBERG, « Privacy in the Information Economy: A Fortress or Frontier for Individual Rights » (1992) 44 *Fed. Comm. L.J.* 195.

63 Pierre KAYSER, *La protection de la vie privée par le droit, protection du secret de la vie privée*, 3e éd., Paris, Économica-Presses Universitaires d'Aix-Marseille, 1995, p.12.

64 L'évolution de l'un entraîne nécessairement une mouvance de l'autre. Pierre TRUDEL, France ABRAN, Karim BENYEKHLEF et Sophie HEIN, *Droit du cyberespace*, Montréal, Éditions Thémis, 1996, p. 11-32.

Pour plus d'informations au sujet de l'antériorité du phénomène, lire : G.R. SEGAL, « The Threat From Within: Cable Television and the Invasion of Privacy », (1986) 7 *Computer L.J.* 89, 91.

65 Karim BENYEKHLEF et Pierre TRUDEL, *Approches et stratégies pour améliorer la protection de la vie privée dans le contexte des inforoutes*, Mémoire présenté à la Commission de la culture de l'Assemblée nationale dans le cadre de son mandat sur l'étude du Rapport quinquennal de la Commission d'accès à l'information, septembre 1997, p. 14 et Karim BENYEKHLEF, « Les normes internationales de protection des données personnelles et l'autoroute de l'information », dans *Le respect de la vie privée dans l'entreprise*, Actes des Journées Maximilien Caron, Montréal, Éditions Thémis, 1996, p. 91.

66 Karim BENYEKHLEF, « Réflexions sur le droit de la protection des données personnelles à la lumière des propositions de la Commissions des Communautés européennes », (1992) 2 *M.C.L.R.* 149. Pour plus

Au Québec, le *Code civil du Québec* ne définit pas la notion de renseignement personnel. Pour obtenir une telle définition applicable aux dispositions du *Code civil du Québec*, on doit se référer à la *Loi sur la protection des renseignements dans le secteur privé*[67] qui édicte à son article 2 une définition en tout point semblable, mot pour mot, à celle offerte par la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*[68] : « Est un renseignement personnel, tout renseignement qui concerne une personne physique et permet de l'identifier. »

Par l'entremise de la *Loi sur la protection des renseignements personnels et les documents électroniques*[69], le gouvernement fédéral énonce sa propre définition de la notion de renseignement personnel. Semblable à celle contenue dans les lois québécoises, elle exclut toutefois spécifiquement certaines informations de la notion de renseignement personnel. À cet effet, l'article 2 de la loi définit le renseignement

---

d'informations au sujet des conséquences découlant de cette distinction, lire Karim BENYEKHLEF, *La protection de la vie privée dans les échanges internationaux d'information*, Montréal, Éditions Thémis, 1992, à la page 91

67 L.R.Q., c. P-39.1.

68 L.R.Q., c. A-2.1.

De plus, voir l'article 54 et l'article 55 qui établissent une distinction entre un renseignement personnel à caractère public en vertu de la loi et un renseignement nominatif.

69 La *Loi sur la protection des renseignements personnels et les documents électroniques* a reçu la sanction royale le 13 avril 2000 (Projet de loi C-6 - Deuxième session, trente-sixième législature, 48-49 Elizabeth II, 1999-2000). Son application est rétroactive au 15 octobre 1999.

Les nouvelles technologies, la collecte croissante de données dans le secteur privé, l'évolution des tendances du marché et le nouveau marché mondial qui s'ouvre au commerce électronique, sont autant d'éléments qui contribuent au rôle de plus en plus important de l'information dans l'économie mondiale. Puisque plus de la moitié des Canadiens sont d'avis que l'inforoute réduit la vie privée au Canada, il était essentiel à la croissance de l'économie de l'information canadienne que les consommateurs aient confiance dans le système. 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 de renseignements personnels ne pourra conférer un avantage concurrentiel.

Par ailleurs, la législation visant l'information détenue par le secteur public ne tient pas compte du fait qu'aujourd'hui, le secteur privé recueille et utilise beaucoup de renseignements personnels. À ce jour, seul le Québec a adopté une loi d'ensemble sur la protection des renseignements personnels visant le secteur privé. La *Loi sur la protection des renseignements personnels dans le secteur privé* fournit un cadre détaillé en ce qui concerne la collecte, l'utilisation et la divulgation de renseignements personnels. Dans le reste du pays, la protection est sporadique et inégale, ce qui suscite l'incertitude chez les entreprises et assure une protection peu uniforme aux consommateurs. Nombre de secteurs ne sont soumis à aucune règle en ce qui concerne la collecte, l'utilisation et la divulgation de renseignements personnels, mais quelques-uns sont couverts par ce que le Commissariat à la protection de la vie privée du Canada décrit comme un « ensemble disparate » de lois, de règlements et de codes. Cet ensemble se compose de diverses lois fédérales et provinciales, d'où une protection incomplète, voire incohérente. Même s'il donne des résultats dans certains secteurs, il n'établit pas de principes communs pour tous et tous ne sont pas visés. Ce côté incomplet de la législation explique l'incertitude des entreprises et l'absence de protection uniforme des consommateurs. Et si l'ensemble de lois disparates a une utilité relative, il n'en est pas moins inadéquat face à l'évolution du monde.

« Assurer la protection efficace des renseignements personnels s'avère essentiel pour que le Canada reste concurrentiel à l'échelle internationale dans l'économie de l'information mondiale. En adoptant la *Loi sur la protection des renseignements personnels et les documents électroniques*, le Canada a maintenant décidé de protéger les renseignements personnels. » Colin BENNETT, *Réflexions sur une norme internationale de*

personnel comme étant : « Tout renseignement concernant un individu identifiable, à l'exclusion du nom et du titre d'un employé d'une organisation et des adresses et numéros de téléphone de son lieu de travail. »

En somme, est personnel aux yeux de la loi, un renseignement qui désigne tout moyen d'identification d'une personne et englobe tout autant des caractéristiques objectives que des symboles mathématiques[70]. Dès qu'elle permet d'identifier une personne, d'isoler un individu, l'information se range sous la rubrique des renseignements personnels[71].

Cette définition soulève toutefois des débats dans les environnements électroniques. Entre autres, selon les professeurs Benyekhlef et Trudel, la définition de renseignement personnel fournit par les lois actuelles est beaucoup trop large et englobante[72]. En tenant compte spécifiquement du contexte de communication dans lequel un usager se trouve, soit le courriel[73], les groupes de discussions, les banques de données ou les sites Web, ils sont d'avis qu'il faut délimiter la définition de renseignements personnels afin de ne viser que les renseignements qui ont réellement trait à la vie privée des usagers, soit ceux se rapportant à leur vie privée informationnelle. Ainsi, à l'aide de ces balises et en tenant compte du contexte électronique, il n'y aurait plus lieu d'interdire toute circulation de renseignements personnels du seul fait qu'elles pourraient éventuellement constituer une atteinte à la vie privée des usagers. Cette réflexion

---

protection des renseignements personnels, Groupe de travail sur le commerce électronique d'Industrie Canada, http://e-com.ic.gc.ca/francais/privee/632d29.html

[70] Paul-André COMEAU, « La vie privée : droit et culture » dans *Le respect de la vie privée dans l'entreprise : de l'affirmation à l'exercice d'un droit*, Les journées Maximilien-Caron 1995, Montréal, Éditions Thémis, 1995, p.3.

[71] *Chambre des notaires* c. *Hydro-Québec*, (1984-86) 1 C.A.I. 306, *Segal* c. *Centre de services sociaux de Québec*, [1988] C.A.I. 315 et *Direction Média Inc.* c. *Inspecteur général des institutions financières*, [1990] C.A.I. 171.

[72] Karim BENYEKHLEF et Pierre TRUDEL, *Approches et stratégies pour améliorer la protection de la vie privée dans le contexte des inforoutes*, Mémoire présenté à la Commission de la culture de l'Assemblée nationale dans le cadre de son mandat sur l'étude du Rapport quinquennal de la Commission d'accès à l'information, septembre 1997, p. 2.

Raymond Doray va aussi dans la même lignée en traitant des notions de dossier et d'objet énoncées dans le Code civil du Québec et dans la *Loi sur la protection des renseignements personnels dans le secteur privé.* « L'exégèse des décisions de la Commission d'accès à l'information et de ses rapports d'enquête nous permet de constater que celle-ci a pratiquement ignoré la notion de dossier. [...] En mettant de côté la notion de dossier, la Commission donne une portée insoupçonnée à la Loi dans le secteur privé, au point même d'englober dans son champ d'application des renseignements qui n'ont qu'un lien éloigné avec des personnes physiques. » Raymond DORAY, « Mise à jour, mise au point et mise en garde au sujet de la protection des renseignements personnels dans le secteur privé », dans *Développements récents en droit administratif (1998)*, Service de la formation permanente, Barreau du Québec, Montréal, Éditions Yvon Blais Inc., 1998, 135, p. 145.

[73] « Service de correspondance sous forme d'échange de messages électroniques, à travers un réseau informatique. Par extension, on utilise aussi les termes courrier électronique et courriel pour désigner le message lui-même. » PUBLICATIONS DU QUÉBEC, *Terminologie d'Internet*, http://www.olf.gouv.qc.ca/ressources/internet/fiches/2075076.htm

apparaît donc très intéressante. La notion de renseignement personnel étant définie de façon large, elle englobe par conséquent une multitude d'informations qui devraient pouvoir circuler librement sur les réseaux informatiques[74].

Les lois québécoises et la *Loi sur la protection des renseignements personnels et les documents électroniques* visent tous les renseignements personnels, peu importe la nature du support ou la forme sous laquelle ils sont accessibles[75]. Pour qu'une information soit qualifiée de renseignement personnel, celle-ci doit répondre à deux critères, soit :

1. Concerner une personne physique, et
2. Permettre de l'identifier.

L'information qui concerne une personne physique doit de plus, être relative et rattachée d'une façon ou d'une autre à la personne physique. Elle doit permettre de l'identifier.

Ces deux critères ont aussi été retenus pour définir les données à caractère personnel selon la *Directive 95/46/CE relative à la protection des personnes physique à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données* (ci-après nommé la *Directive*)[76]. L'article 2 de la *Directive* définit les données à caractère personnel comme toutes informations concernant une personne physique identifiée ou identifiable.

La *Directive* édicte entre autres des exemples de données à caractère personnel. Elle énonce : « est réputée identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale »[77].

---

[74] À ce sujet, les professeurs Benyekhlef et Trudel tiennent à préciser que les règles relatives au traitement de tous les renseignements concernant un usager devraient être ajustés de manière à éviter que des informations à caractère public soient accumulées et traitées de manière à constituer une atteinte à la vie privée.

[75] Voir les articles 1(2) de la *Loi sur la protection des renseignements personnels dans le secteur privé*, l'article 1(2) de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* et l'article 2(1) de la *Loi sur la protection des renseignements personnels et les documents électroniques*.

[76] *Directive 95/46/CE* du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physique à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, J.O.C.E, 23 novembre 1995, No. L. 281, p. 31.

[77] Article 2 a) de la *Directive*.

Au Québec, les lois ne fournissent pas de tels exemples. La Commission d'accès à l'information et les tribunaux québécois ont toutefois statué de manière constante à l'effet que les renseignements personnels sont définis comme des renseignements qui sont directement ou indirectement rattachés à un individu identifié ou identifiable. Il fut notamment décidé que le nom, un numéro d'identification, le numéro d'assurance-sociale, le numéro d'assurance-maladie, le numéro de permis de conduire, l'adresse du domicile, le numéro de téléphone au domicile, le sexe et l'âge sont des renseignements personnels.

Outre les renseignements personnels énoncés précédemment, on considère comme tels, les informations concernant le revenu d'une personne, son statut de propriétaire ou de locataire, ses résultats académiques, ses diplômes, sa race, son statut social, sa condition économique, son comportement disciplinaire, ses actifs et passifs économiques, son état de santé, sa réputation, son comportement, ses déplacements ainsi que sa présence dans un lieu. En tenant compte de ces exemples, on vient à la conclusion que les fichiers de témoins[78] et le numéro de série du Pentium III[79] peuvent être considérés comme des atteintes à la vie privée[80]. Nous y reviendrons.

B. Les moyens de protection de la vie privée

Les possibilités d'intrusions dans la vie privée donnent lieu à des préoccupations sans précédent quant aux moyens de protéger la zone d'intimité personnelle nécessaire à la vie humaine et à son développement dans la société[81]. La protection de la vie privée dans les environnements électroniques décentralisés se concrétise généralement à l'aide de deux moyens : l'anonymat et le droit de contrôle des usagers sur leurs renseignements personnels.

---

[78] Les fichiers de témoins sont des fichiers créés dans les serveurs gérant les sites Web et rassemblant les témoins persistants issus des sites Web visités par les utilisateurs. PUBLICATIONS DU QUÉBEC, *Terminologie d'Internet*, http://www.olf.gouv.qc.ca/ressources/internet/fiches/2075187.htm.

[79] Dans le deuxième chapitre de cette étude, une section entière est réservée à la problématique du numéro de série de la puce du Pentium III.

[80] « In addition to the generally accepted definition of privacy as « the right to be left alone », privacy has become a broad, all-encompassing concept that envelops a whole host of human concerns about various forms of intrusive behaviour [...]. In recent years, these claims have expanded to include the right to keep one's trail of sites visited on the World Wide Web confidential. » Lance J. HOFFMAN et Karen A. METIVIER CARREIRO, « Computer Technology to Balance Accountability and Anonymity in Self-regulatory Privacy Regimes » dans *Privacy and Self-Regulation in the Information Age, Chapter 5: Technology and Privacy Policy*, National Telecommunications and Information Administration, Juin 1997, http://www.ntia.doc.gov/reports/privacy/selfreg5.htm#5A

[81] Pierre KAYSER, *La protection de la vie privée par le droit, protection du secret de la vie privée*, 3e éd. Économica-Presses Universitaires d'Aix-Marseille, Paris, 1995, p.15.

1) L'anonymat

Dans certaines circonstances, le simple fait d'identifier un individu lors d'une communication est aussi important, sinon plus préjudiciable, que de prendre connaissance du message lui-même[82]. Un exemple frappant d'un méfait de l'anonymat qui a choqué l'Amérique au cours des dernières années est celui du message anonyme posté sur Internet peu de temps après l'attentat terroriste d'Oklahoma City. Ce courriel contenait les composants et les matériaux nécessaires à la construction d'une bombe identique.

> « [Traduction] *L'information contenait des détails spécifiquement à la construction, le déploiement et la détonation d'engins à haut pouvoir explosif. Elle incluait également des détails complets de la bombe utilisée à Oklahoma, comment elle a été utilisée et comment cela aurait pu être mieux*[83]. »

Utilisé dans un tel contexte, l'anonymat facilite les activités illicites en rendant difficile, voire même impossible, l'obtention d'informations sur l'auteur du message. En contrepartie, l'anonymat s'avère aussi, dans certaines situations, un excellent moyen de protection de la vie privée[84]. Il permet, entre autres, à des personnes de participer à des discussions consacrées à des questions médicales ou psychologiques tout en restant anonymes pour des raisons d'ordre personnel. De plus, en sachant préalablement que les contributions faites dans les groupes de discussions sont archivées sur des sites Web en libre accès, l'utilisation de l'anonymat dans ces forums permet aux usagers de s'assurer d'une certaine protection de leur vie privée[85].

Au Québec, le professeur Glenn définit l'anonymat comme une faculté qui protège les renseignements personnels[86]. Le professeur Baudouin abonde en ce sens en ajoutant

---

[82] L'exemple le plus marquant de ces dernières années et sans doute la poursuite automobile de O.J. Simpson. « The O.J. Simpson freeway chase and capture resulted from tracking the ID signal of his cellular phone, which routinely reported its location to the nearest cell. » Jonathan ROSENOER, *CyberLaw, The Law of the Internet*, New York, Springer-Verlag, 1996, p. 139.

[83] Déclaration d'un sénateur américain cité par David POST dans « Thoughts on Anonymity, Pseudonymity and Limited Liability in Cyberspace », présenté à la conférence des 3 et 4 novembre 1996 à la faculté de droit de l'Université de Chicago. http://www-law.lib.uchicago.edu/forum/96vol.html

[84] Jay KRASOVEC, « Cyberspace : The Final Frontier, For Regulation? », *Akron Law Review*, Volume 31, Numéro 1 (1997-1998), http://www.uakron.edu/lawrev/krasovec.html.

De plus, il importe de préciser qu'il existe différents degrés d'anonymat sur Internet : l'anonymat relatif ou traçable, l'anonymat intraçable et l'anonymat absolu. Michael FROOMKIN, « Anonymity and its Enmities », (1995) *J. Online L.*, art. 4., http://warthog.cc.wm.edu/law/publications/jol/fromkin.html.

[85] Pour plus d'informations au sujet du site Web Deja News, lire le second chapitre du premier titre.

[86] H. Patrick. GLENN, « Le droit au respect de la vie privée », (1979) 39 *R. du B.* 879, p. 884

que toute diffusion non normalisée d'informations personnelles est protégée sous le couvert du droit à l'intimité[87]. Ainsi, l'anonymat se conçoit au regard de la divulgation ou de la diffusion d'éléments de la vie privée d'un individu.

Étant une préoccupation majeure rattachée d'emblée à la protection de la vie privée, l'anonymat est devenu, au fils des ans, un mode de protection reconnu par les tribunaux américains[88]. Plus particulièrement, ces tribunaux ont reconnu un droit à la vie privée informationnelle fondé sur l'intérêt d'un individu d'éviter la divulgation de ses renseignements personnels[89]. « Si l'anonymat était prohibé sur Internet, la divulgation d'informations importantes pourrait être compromise »[90].

En tenant compte des critères développés par la Cour suprême des États-Unis, le professeur Long vient à la conclusion qu'à l'intérieur des groupes de discussion, l'anonymat des participants est protégé par le droit à la vie privée[91]. Pour ce qui est des

---

87 Jean-Louis BAUDOUIN, *La responsabilité civile*, 4e édition, Cowansville, Éditions Yvon Blais Inc., p. 227.

88 La Constitution des États-Unis ne garantie pas expressément un droit à l'anonymat. « The First Amendment's guarantees of free speech and freedom of assembly have, however, been understood for many years to provide protections for at least some, and possibly a great deal of, anonymous speech and secret association. » Jay KRASOVEC, « Cyberspace: The Final Frontier, For Regulation? », *Akron Law Review*, Volume 31, Numéro 1 (1997-1998), http://www.uakron.edu/lawrev/krasovec.html.

Néanmoins, la Cour suprême des États-Unis a reconnu un droit à l'anonymat dans certaines situations où la divulgation de l'identité pourrait embarrasser ou stigmatiser une personne. Par exemple, les tribunaux américains ont jugé que l'utilisation des services d'affichage téléphonique automatique du nom de l'appelant lors d'une conversation téléphonique n'était pas dans l'intérêt public, à moins qu'une commande de blocage gratuite ne soit mise à la disposition des consommateurs. George P. LONG, « Who are You: Identity and Anonymity in Cyberspace », (1994) 55 *U. of Pitt.* L.R. 1177, 1183.

89 La Cour suprême des États-Unis a retenu trois critères qui permettent d'analyser si dans une circonstance précise, un individu dispose d'un droit à la vie privée informationnelle, permettant ainsi d'éviter la divulgation d'information personnelle. Le premier critère à examiner est de se demander si par la divulgation de l'information, il existe un risque de porter atteinte à la vie privée ou d'embarrasser la personne concernée par cette information. Deuxièmement, il faut vérifier si la divulgation de l'information risque de mener à du harcèlement ou à une intrusion dans la vie privée de la personne concernée. Finalement, il importe de vérifier avant de procéder à la divulgation si la personne concernée bénéficiait d'une expectative raisonnable de vie privée au moment où elle a prononcé cette information. George P. LONG, « Who are You : Identity and Anonymity in Cyberspace », (1994) 55 *U. of Pitt.* L.R. 1177, 1192.

90 Pierre TRUDEL, France ABRAN, Karim BENYEKHLEF et Sophie HEIN, *Droit du cyberespace*, Montréal, Éditions Thémis, 1996, p. 11-62.

Pour certains individus, l'utilisation de l'anonymat sur Internet permet de dénoncer certaines activités illégales et de communiquer en toute sécurité, sans être identifié.

91 Toutefois, un récent jugement de l'état de la Californie a rejeté le droit à l'anonymat d'un usager en cas de diffamation dans un forum de discussion. Le juge à rejeté l'allégation du défendeur en énonçant : « there is no right to free speech to defame. » (Aucun jugement écrit et aucun appel ne fut porté dans cette affaire) Rebecca FAIRLEY RANEY, « Judge Rejects Online Critic's Efforts to Remain Anonymous », *New York Times*, 15 juin 1999. http://www.nytimes.com/library/tech/99/06/cyber/articles/15identity.html. Voir George P. LONG, « Who are You : Identity and Anonymity in Cyberspace », (1994) 55 *U. of Pitt. L.R.* 1177, 1193 et Declan MCCULLAGH, « Miffed Judge Subpoenas AOL », 9 avril 1999, *Wired*, http://www.wired.com/news/news/politics/story/19044.html, où AOL et ACLU ont refusé de livrer à la justice un de leurs abonnés au nom de la liberté d'expression et du droit à l'anonymat.

autres situations électroniques, il appert qu'il faudrait tenter d'appliquer ces critères pour préserver son anonymat.

Ces critères énoncés par les tribunaux américains démontrent bien l'importance des enjeux liés à l'utilisation de l'anonymat dans les environnements électroniques décentralisés. L'anonymat a une double facette à l'opposé l'une de l'autre. L'une représente un moyen efficace pour la protection de la vie privée, et l'autre « is a great tool for evading detection of illegal and immoral activity[92]. » De cette seconde facette, il en découle évidemment des problèmes d'application et de maintien de la loi.

a) L'articulation technique de l'anonymat

On retrouve sur Internet une multitude de programmes et de techniques permettant aux internautes de restreindre l'accès à leur identité au point de devenir anonyme sur la toile[93]. L'anonymat étant une notion faisant référence à l'absence d'éléments identifiants, ces moyens offrent la possibilité aux internautes de naviguer de façon anonyme et de protéger leur vie privée des dangers et des embarras qu'une divulgation peut susciter.

Les divers moyens proposés aux internautes pour articuler techniquement l'anonymat découlent de deux grandes approches, soit : les serveurs anonymisateurs et la cryptographie. La présente partie de l'étude présentera un survol de ces deux grandes approches et des moyens techniques qu'elles proposent[94].

---

[92] « Conspiracy, electronic hate-mail and hate-speech in general, electronic stalking, libel, general nastiness, disclosure of trade secrets and other valuable intellectual property, all become lower-risk activities if conducted via anonymous communications. » Michael FROOMKIN, « Flood Control on the Information Ocean: Living With Anonymity, Digital Cash, and Distributed Databases », 15 *U. of Pitt. J. of L. & C.* 395 (1996).

[93] À ce sujet, l'entreprise montréalaise Zero Knowledge Systems a créé le logiciel Freedom qui permet aux internautes de naviguer sur la toile en toute intimité. Freedom offre aux internautes d'utiliser les techniques les plus avancées de cryptographie afin de préserver leur identité et d'empêcher toute collecte non autorisée de renseignements personnels.

D'un point de vue technique, Freedom permet à un usagé d'utiliser jusqu'à cinq pseudonymes avec des courriels anonymes, des adresses IP dissimulées ainsi que des noms secrets afin que seuls les gens qui ont obtenu préalablement une autorisation explicite de l'usager puissent savoir qui il est.

Les informations envoyées à l'aide du logiciel sur l'Internet par l'entremise des serveurs de l'entreprise et des fournisseurs d'accès partenaires, sont encodées à quatre niveaux et chacun des serveurs ne possède qu'une clé de décryptage. Ainsi, le contenu des transmissions est crypté à l'aide d'une clé d'une longueur minimal de 128 bits jusqu'à sa destination finale. En d'autres mots, on pourrait comparer le cheminement à un colis postal barré par trois serrures détenues par trois personnes différentes qui ne font que re-poster le colis. ZERO KNOWLEDGE, http://www.zeroknowledge.com.

[94] Pour une étude approfondie des questions relatives à l'anonymat sur les réseaux décentralisés, lire Michael FROOMKIN, « Anonymity and its Enmities », (1995) *J. Online L.* art. 4, http://warthog.cc.wm.edu/law/publications/jol/fromkin.html

- **Les services anonymisateurs**

Les internautes en quête d'anonymat pour envoyer des courriels connaissent bien les services anonymisateurs, dont le service anonymisateur Nym.alias.net[95].

De façon usuelle, l'en-tête d'un courriel peut révéler beaucoup de choses sur l'expéditeur et le parcours de celui-ci sur le réseau. En principe, l'en-tête d'un message électronique contient[96] :

- L'adresse de l'expéditeur saisie par l'auteur du message. Toutefois, il se peut qu'elle ne corresponde pas à l'adresse réelle de l'expéditeur. En effet, si celui-ci a décidé d'écrire une fausse adresse lors de la configuration de son logiciel de courriel, c'est cette adresse qui apparaîtra.
- L'adresse du destinataire du message.
- L'objet ou le sujet du message.
- La date et l'heure de l'envoi du message à partir du serveur de l'expéditeur.
- Le tampon postal de chaque serveur ayant participé à l'acheminement du message. En pratique, chaque serveur laisse son tampon postal dans l'en-tête du message en y déposant son nom, le nom de l'autre serveur participant et la date de transaction.

De plus, on peut retrouver d'autres informations, telles :

- Le nom du programme de messagerie utilisé pour expédier le message, et/ou
- L'adresse de l'expéditeur saisie par le serveur de courriels de l'expéditeur. Celle-ci sera beaucoup plus fiable que l'adresse de l'expéditeur saisie par l'auteur, étant donné qu'il est pratiquement impossible de la modifier.

---

[95] Mis au point par David Mazières, étudiant au Laboratory for Computer Science du Massachusset Institute of Technology, Nym.alias.net est à l'heure actuelle l'un des remailers les plus performants au monde. Sa fonction principale consiste à effacer tous les éléments d'un courriel permettant d'identifier l'auteur avant de le transmettre à destination. Outre le recours classique à l'encodage, il fait transiter les courriels par l'intermédiaire de nombreux autres remailers indépendants les uns des autres et achève de brouiller les pistes en effaçant à nouveau les indications permettant de retracer le chemin parcouru par le courriel.

Ainsi, les transitaires du message ne peuvent se voir contraints de remettre à la justice ou à la police des éléments permettant d'identifier les auteurs des courriels, car les gestionnaires du serveur eux-mêmes n'ont pas accès à cette information à la différence de fournisseurs Internet, tel AOL ou Compuserve, dont les ordinateurs peuvent identifier les abonnés. Luc LAMPRIÈRE, « Quand l'e-mail garde l'incognito », 16 avril 1999, *Libération*, http://www.liberation.com/multi/cahier/articles/sem99.16/cah990416d.html

En ce qui a trait à la navigation sur le réseau Internet, le site Anonymizer.com permet aux Internautes de naviguer sur Internet en tout anonymat. http://www.anonymizer.com

[96] Wolfram GIESEKE, *PC 100 % Pratique, Sécurité et Protection*, traduction de C. STOLL, H. BERTRAND et P. M. WOLF, Paris, Micro Application, 1998, p. 310.

En théorie, il est possible de relier un message électronique à son auteur grâce aux informations contenues dans l'en-tête. En pratique, le tout peut s'avérer fort différent si l'expéditeur a utilisé un service anonymisateur lors de l'envoi de son courriel.

Les services anonymisateurs offrent la possibilité d'envoyer aisément des messages anonymes en usurpant l'en-tête usuel d'un message expédié et en le remplaçant par un nouveau, souvent farfelu[97].

Ces services ont leurs bons côtés. Ils offrent par exemple, aux internautes vivant dans des pays où la liberté d'expression est restreinte par la crainte de représailles, de communiquer leurs idées de façon sécuritaire sans être identifiés[98]. Néanmoins, la double facette de l'anonymat fait que ces services sont aussi utilisés pour commettre des actes illicites.

Pour contrer l'utilisation de ces services, il existe des logiciels, tel le Automatic Retroactive Minimal Moderation (ARMM)[99], qui permettent d'éliminer ces messages anonymes. Toutefois, ces logiciels peuvent causer des dommages vu qu'ils sont incapables de distinguer les messages licites des messages illicites[100]. On imagine facilement les conséquences de l'usage de tels logiciels sur une valeur aussi fondamentale que la liberté d'expression. En éliminant les courriels qui transigent par les services anonymisateurs, ils briment la liberté d'expression des internautes désireux de participer à des groupes de discussions sous le couvert de l'anonymat[101].

---

97 George P. LONG, « Who are You : Identity and Anonymity in Cyberspace », (1994) 55 *U. of Pitt. L.R.* 1177 et L. DETWEILER, « Identity, Privacy, And Anonymity on the Internet », http://www.csis.ohio-state.edu/hypertext/faq/usenet/net-privacy/part1/faq.html

98 Citant *McIntyre* c. *Ohio Elections Comm'n*, _ U.S. _, 131 L.Ed2d 426, 115 S.Ct. 1511, 1516 (1995), Jonathan ROSENOER écrit : « [Anonymity] provides a way for writer who may be personally unpopular to ensure that readers will not prejudge her message simply because they do not like its proponent. » *Cyber Law, The Law of the Internet*, New York, Springer-Verlag, 1996, p. 141.

99 « A Usenet robot created by Dick Depew of Munroe Falls, Ohio. ARMM was intended to automatically cancel posts from anonymous-posting sites. » Eric S. RAYMOND, *The New Hacker's Dictionary*, 1 novembre 1996, http://www.elsewhere.org/jargon_search/TAG38.html et Hans DE WOLF, *The Jargon File: The World Wide Web version*, http://yardim.bilkent.edu.tr/Online/Jargon30/JARGON_A/ARMM.HTML

100 George P. LONG, « Who are You : Identity and Anonymity in Cyberspace", (1994) *55 U. of Pitt. L.R.*, 1177, A. Michael FROOMKIN, « The Internet As A Source Of Regulatory Arbitrage », 1996, http://www.law.miami.edu/~froomkin/articles/arbitr.htm#xtocid158346.

101 « The decision to remain anonymous, says the U.S. Supreme Court, is an aspect of the freedom of speech protected by the First Amendment. The decision in favor of anonymity may be motivated by fear of economic or official retaliation, by concern about social ostracism, or merely by a desire to preserve as much of one's privacy as possible. » *McIntyre* c. *Ohio Elections Comm'n*, _ U.S. _, 131 L.Ed2d 426, 115 S.Ct. 1511, 1516 (1995) cité dans Jonathan ROSENOER, *Cyber Law, The Law of the Internet*, New York, Springer-Verlag, 1996, p. 141.

- **La cryptographie**

La cryptographie est la seconde articulation technique de l'anonymat. La cryptographie est un processus de transcription d'une information intelligible en une information inintelligible par l'application de conventions secrètes dont l'effet est réversible[102].

L'utilisation de la cryptographie n'est pas récente. Elle existe déjà depuis fort longtemps. Très tôt, les forces militaires romaines ont eu recours à certaines techniques d'écritures afin d'échanger des messages codés incompréhensibles pour l'ennemi[103]. En constante évolution depuis l'antiquité, la cryptographie est devenue aujourd'hui une véritable science. Employée pour la protection des secrets militaires et diplomatiques, la cryptographie est longtemps restée l'apanage des gouvernements. À l'ère des réseaux numériques, elle est devenue un outil indispensable au service des entreprises et des particuliers, notamment au niveau de la protection de la vie privée et du commerce électronique.

La signature numérique et le chiffrement constituent deux applications importantes de la cryptographie. La signature numérique permet de prouver l'origine des données, c'est-à-dire l'authentification, et de vérifier si les données ont été altérées[104]. Le chiffrement quant à lui, maintient la confidentialité des données et des communications en rendant illisible le message envoyé. La cryptographie permet ainsi d'effectuer des transactions en toute sécurité et confidentialité.

D'un point de vue technique, il existe deux types distincts de techniques cryptographiques : la cryptographie symétrique qui utilise seulement une clé privée, et la cryptographie asymétrique qui utilise une clé privée et publique.

---

[102] Valérie SÉDALLIAN, « Les problèmes posés par la législation française en matière de chiffrement », octobre 1998, http://62.161.196.163/lij/cryptoTC.html, à paraître dans la revue *Droit de l'Informatique et des télécommunications*.

[103] Claude CRÉPEAU, « La Cryptographie : pour que les secrets le restent », 8 juin 1997, *Québec - Science*, http://www.cybersciences.com/cyber/4.0/dec_jan98/net.htm.

[104] La signature numérique est seulement possible lorsqu'un utilisateur utilise la cryptographie à clé publique. À ce sujet, l'office de la langue française définit la signature numérique comme suit : Sceau électronique produit généralement par un algorithme à clé publique, qui garantit à la fois l'origine et l'intégrité du message transmis, rendant ainsi impossible son éventuelle répudiation après émission par l'expéditeur ou sa contrefaçon à la réception par le destinataire ou au cours de la transmission par un tiers. PUBLICATIONS DU QUÉBEC, *Terminologie d'Internet*, http://www.olf.gouv.qc.ca/ressources/internet/fiches/8384641.htm

Le système de cryptographie à clé privée Date Encryption Standard (DES)[105] fut développé par le gouvernement américain. Il fonctionne à partir d'une même clé dite privée, possédée par l'émetteur et le récepteur d'un message. Cette clé privée utilise un algorithme qui sert à la fois au chiffrement et au déchiffrement du message[106].

Le principal inconvénient lié à l'utilisation de cette technique résulte dans le fait que les correspondants doivent s'échanger la clé avant l'envoi du premier message pour que le destinataire puisse déchiffrer ledit message. De plus, l'échange de la clé doit se dérouler en texte clair, c'est-à-dire non chiffré, étant donné que les correspondants ne détiennent pas encore de clé commune. L'échange de cette clé doit ainsi se faire de manière extrêmement sécuritaire, car prendre la décision de faire parvenir la clé par courriel équivaudrait à donner, au sens propre et au sens figuré, la clé de sa propre sécurité à ceux dont on désire se protéger.

Pour contourner les problèmes découlant de l'utilisation de la cryptographie symétrique, un système de cryptographie à clés non identiques a été développé. La cryptographie asymétrique ou communément appelée à clé publique, s'est concrétisée en 1977 sous le nom de RSA[107]. L'utilisation de la cryptographie à clé publique nécessite l'utilisation de deux clés, l'une privée et l'autre publique. Ces clés sont intimement liées ; la clé publique constitue la clé de chiffrement qui doit être dévoilée, alors que la clé privée constitue la clé de déchiffrement que seul le destinataire du message doit avoir sous sa garde. Seule la clé privée permet de déchiffrer un message chiffré avec la clé publique complémentaire.

Par l'ajout de la signature numérique, la technique de cryptographie asymétrique présente un avantage indéniable pour la sécurité. Le signataire d'un message peut utiliser sa clé privée pour chiffrer sa signature et ainsi transmettre le message. Le destinataire du message pourra alors utiliser la clé publique du signataire pour déchiffrer la signature du message et authentifier l'expéditeur. Toutefois, utilisée seule, la

---

[105] Le DES a été développé dès le début des années 70 conjointement par l'entreprise IBM et la NSA. Le fait qu'il soit encore d'actualité aujourd'hui en dit long sur son efficacité en matière de sécurité. Aujourd'hui, il est très répandu dans divers secteurs de l'Internet. Par exemple, les protocoles Web sécurisés SHTTP et SSL, ainsi que le standard HBCI de banque en ligne y recourent. NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, *FIPS Publication 46-1 : Data Encryption Standard*, 22 janvier 1988.

[106] Au sujet de la cryptographie symétrique, voir Douglas R. STINSON, Cryptography : Theory and Practice, Londres, CRC Press, 1995, Simon GARFINKEL et Gene SPAFFORD, « Chapter IV - Cryptography », dans *Web Security & Commerce*, O'Reilly & Associates Inc., 1997, Sebastopol CA, p, 168 - 208.

[107] L'acronyme RSA représente les initiales des inventeurs de la principale application commerciale, soit Rivest, Shamir et Adleman. RSA, *RSA*, http://www.rsa.com/rsalabs/faq/faq_rsa.html

signature numérique ne permet pas d'assurer la confidentialité des messages puisque la clé de déchiffrement est publique. Afin de combiner dans un seul échange la signature numérique et la confidentialité d'un message, celui-ci devra être chiffré deux fois plutôt qu'une. L'émetteur signataire d'un message devra chiffrer le message à l'aide de la clé publique du destinataire et, en deuxième temps, chiffrer sa signature au moyen de sa clé privée[108].

Outre les avantages que présente la cryptographie à clé publique, son principal inconvénient se situe au niveau de sa vitesse d'exécution des fonctions de chiffrement et de déchiffrement. Le DES qui utilise la cryptographie à clé privée est de 100 fois à 10 000 fois plus rapide que le RSA qui utilise la cryptographie à clé publique[109]. De plus, il est très peu probable que la cryptographie à clé publique parvienne un jour à égaler les performances du DES en matière de chiffrement[110].

Utilisée avec la complicité des services anonymisateurs ou à l'aide d'une adresse de courriel fantaisiste offerte par le fournisseur d'adresse de courriel gratuite Hushmail[111], la cryptographie permet l'envoi de messages anonymes sur les réseaux informatiques.

En Amérique du Nord, l'utilisation de la cryptographie est permise à l'intérieur même des frontières[112]. Toutefois, l'exportation des logiciels de cryptographie et des données

---

[108] Au sujet de la signature numérique et des autorités de certification, voir RSA, *RSA's FAQ Today's Cryptography*, http://www.rsa.com/rsalabs/faq/faq_rsa.html, Pierre TRUDEL, Guy LEFEBVRE et Serge PARISIEN, *La preuve et la signature dans l'échange de documents informatisés au Québec*, Québec, Publications du Québec, 1993, et Serge PARISIEN et Pierre TRUDEL, *L'identification et la certification dans le commerce électronique*, Québec, Publications du Québec, 1996.

[109] RSA, RSA, http://www.rsa.com/rsalabs/faq/faq_rsa.html.

[110] À cet effet, à l'heure actuelle, sous forme de logiciel, le DES permet de réaliser ces fonctions 100 fois plus rapide que le RSA et sous forme de « hardware », le DES est près de 1000 à 10000 fois plus rapide. RSA, http://www.rsa.com/rsalabs/faq/faq_rsa.html.

[111] Fondée en 1998, « Hush Mail is the world's first, fully encrypted, free Web-based email service. Our patent pending, state-of-the-art technology keeps private communication private. Free and easy to use, HushMail works just like other Web-based email providers, except HushMail offers the security of 1024-bit encryption between users. HushMail implements patent-pending technology known as a "Public Key Cryptosystem with Roaming User Capability." That means that the only people who can read your HushMail are the people that you send it to. It also means that you can access your account from any computer that has a Web browser and Internet access, anywhere in the world! Remember that you can use your HushMail account to send email to anyone on the planet, but to take advantage of our 1024-bit encryption, all parties sending and receiving email must be using HushMail. » HUSHMAIL, *Frequently asked question*, http://www.hushmail.com/faq.htm. De plus, voir Marcia STEPANEK, « Getting Doctors and Lawyers to Pay HushMail », 10 août 1999, *Business Week Online*, http://www.businessweek.com/cgi-bin/ebiz/ebiz_frame.pl?url=/ebiz/9908/ec0810.htm, « Bulletproof Email for the Masses », 21 mai 1999 *Wired*, http://www.wired.com/news/print_version/technology/story/19804.html, Stan MIASTKOWSKI, « Hushmail Offers E-Mail Encryption », 28 mai 1999, *PC World*, http://www.pcworld.com/shared/printable_articles/0,1440,11189,00.html.

[112] Susan E. GINDIN, « Lost and found in cyberspace: Information privacy in the age of the Internet », 1997 *San Diego Law Review*, http://www.info-law.com/lost.html.

chiffrées est réglementée par les droits nationaux en vertu de l'Arrangement de Wassenaar[113] sur les contrôles à l'exportation pour les armes conventionnelles et les biens et technologies à double usage[114]. De plus, la plupart des États membres de l'Union européenne réglementent l'exportation des programmes de chiffrement considérés comme du matériel militaire[115]. Néanmoins, malgré les restrictions qui existent en vertu des législations, la cryptographie est de plus en plus présente sur la toile. Que ce soit par l'utilisation du logiciel PGP[116] ou ICQ[117], la cryptographie permet aux internautes de s'assurer d'un certain niveau d'anonymat et de sécurité sur le réseau.

2) Le droit de contrôle des usagers sur leurs renseignements personnels

Outre l'anonymat, les internautes disposent aussi d'un droit de contrôle sur leurs renseignements personnels recueillis sur le réseau Internet. Au Canada et dans la province de Québec, les lois concernant la protection des renseignements personnels reconnaissent aux individus un certain droit d'accès aux informations les concernant.

Les articles 38 à 40 *C.c.Q.* et l'article 4.9 de l'annexe 1 de la *Loi sur la protection des renseignements personnels et les documents électroniques* énoncent que la personne physique et/ou morale qui détient un dossier sur autrui, ne peut lui refuser l'accès aux renseignements qui y sont contenus, à moins qu'elle ne justifie son refus par un intérêt sérieux et légitime[118] ou que la divulgation de ces renseignements soit susceptible de nuire sérieusement à un tiers. Pour ce qui est des dossiers détenus par les entreprises privées, l'article 27 de la *Loi sur la protection des renseignements dans le secteur privé*

---

[113] http://www.wassenaar.org

[114] MINISTÈRE DES AFFAIRES ÉTRANGÈRES ET DU COMMERCE INTERNATIONAL, « Contrôle à l'exportation sur les produits de la cryptographie », 23 décembre 1998, http://www.dfait-maeci.gc.ca/~eicb/notices/ser113-f.htm et INDUSTRIE CANADA, « Résumé de la politique du Canada en matière de cryptographie », http://strategis.ic.gc.ca/virtual_hosts/e-com/francais/fastfacts/43d7.html.

Pour une excellente analyse des législations internationales à ce sujet, voir : Valérie SÉDALLIAN, « Les problèmes posés par la législation française en matière de chiffrement », octobre 1998, http://62.161.196.163/lij/cryptoTC.html à paraître dans la revue *Droit de l'Informatique et des télécommunications.*

[115] Pour ce qui a trait au droit français, voir : Éric A. CAPRIOLI, « Sécurité technique et cryptologie dans le commerce électronique en droit français », *Lex Electronica*, Volume 3, Numéro 1 (hiver 1997), http://www.lex-electronica.org/articles/v3-1/caprio.html.

[116] PRETTY GOOD PRIVACY INC., http://www.pgp.com:8001/freeware/PGPfreeware6.0.2.zip.

[117] Depuis le mois de mai 1999, le logiciel ICQ a pris une autre longueur d'avance sur le courriel. L'entreprise Encryption Software, a lancé sur le marché un partagiciel, le Top Secret Messenger, qui permet de chiffrer les messages ICQ avec un chiffrement pouvant aller jusqu'à 464 bits. MIRABILIS, http://www.mirabilis.com/ et ENCRYPTION SOFTWARE, http://www.encrsoft.com/

[118] Contrairement à l'article 6 de la *Loi sur la protection des renseignements dans le secteur privé* où il est prévu des restrictions spécifiques, le législateur n'a pas identifié quels étaient les intérêts légitimes que peut invoquer le détenteur d'un dossier pour s'opposer à cette divulgation.

prévoit que toute personne a le droit d'obtenir la communication des renseignements personnels la concernant et contenus dans un dossier détenu par une entreprise assujettie à cette loi[119].

Le droit d'un individu d'accéder aux informations le concernant constitue un des éléments les plus fondamentaux du dispositif général instauré par les lois de protection des renseignements. De ce droit d'accès prévu par le législateur, il découle un droit de contrôle et de rectification des informations contenues dans ces dossiers. L'individu concerné par des informations emmagasinées dans un dossier peut le consulter et y contrôler ses informations. Ce droit d'accès non absolu, obéit toutefois à une certaine procédure qui peut faire l'objet d'un recours judiciaire en cas de malentendu[120].

Ce bref survol des dispositions législatives québécoises et canadiennes démontrent bien l'un des problèmes auxquels les usagés des réseaux informatiques décentralisés sont confrontés : la difficulté de s'assurer que les mécanismes propres à éviter l'exportation indue de renseignements personnels en dehors du territoire demeurent opérants en tout temps.

Ce problème de la délocalisation et de l'intangibilité de l'information n'est pas vraiment nouveau.

> « *[...] Une lecture attentive des lois de protection des données personnelles, élaborées dans les années soixante-dix, permet de constater que les législateurs européens étaient conscients du fait que le mariage de l'informatique et des télécommunications (télématique) pouvait faciliter le contournement de leurs législations. Il existe donc des dispositions législatives qui prohibent la transmission de données personnelles, à partir du territoire national, vers les pays dont le droit interne ne leur assure pas une protection satisfaisante*[121]. »

La décentralisation des réseaux se caractérise par l'absence d'un lieu centralisé susceptible d'exercer un contrôle sur les contenus véhiculés dans le réseau ou plus

---

[119] Voir les articles 9 et suivants de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels.*

[120] À ce sujet, l'article 41 (2) *C.c.Q.* édicte que s'il survient une difficulté dans l'exercice de ces droits [soit le droit de consultation et de rectification d'un dossier], le tribunal la tranche sur demande.

[121] Karim BENYEKHLEF et Pierre TRUDEL, *Approches et stratégies pour améliorer la protection de la vie privée dans le contexte des inforoutes*, Mémoire présenté à la Commission de la culture de l'Assemblée nationale dans le cadre de son mandat sur l'étude du Rapport quinquennal de la Commission d'accès à l'information, septembre 1997, p. 16.

exactement dans les réseaux interconnectés[122] et entraîne une augmentation des usagers et des acteurs. Cette multiplicité rend illusoire le respect et la conformité à chacune des législations adoptées[123]. En contrepartie, l'adoption de dispositions législatives prohibant toute transmission de renseignements personnels vers un pays dont le droit interne n'assure pas une protection satisfaisante des renseignements personnels met en opposition deux principes fondamentaux : le droit au respect de la vie privée versus la libre circulation de l'information consacré par le droit international.

Dans le but d'harmoniser les législations traitant de la protection des renseignements personnels, l'OCDE a adopté en 1981 les *Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel*[124], et le Conseil de l'Europe a adopté la *Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel*[125]. Dû en partie à l'échec de la *Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel*, l'Union européenne a adopté en 1995 la *Directive*[126].

---

[122] Pierre TRUDEL (avec la collaboration de R. GÉRIN-LAJOIE), « La protection des droits et valeurs dans la gestion des réseaux ouverts », dans Daniel POULIN, Pierre TRUDEL et Ejan MACKAYY (dir.), *Les autoroutes électroniques : usages, droit et promesses*, Cowansville, Éditions Yvon Blais Inc, 1995, p. 299.

[123] « L'architecture de l'Internet, le nombre croissant d'usagers et le recours aux réseaux pour transiger et conclure tout type de transactions constituent autant de facteurs expliquant les difficultés d'appliquer les normes relatives au contrôle des transmissions d'informations personnelles. » Karim BENYEKHLEF et Pierre TRUDEL, *Approches et stratégies pour améliorer la protection de la vie privée dans le contexte des inforoutes*, Mémoire présenté à la Commission de la culture de l'Assemblée nationale dans le cadre de son mandat sur l'étude du Rapport quinquennal de la Commission d'accès à l'information, septembre 1997, p. 16.

[124] « La négociation des lignes directrices de 1982 s'est faite dans une certaine atmosphère de suspicion de part et d'autre de l'Atlantique. Il n'en demeure pas moins que le document sur lequel on s'est entendu représentait à l'époque un important consensus international sur les principes de la protection de la vie privée.

Les Lignes directrices n'offrent qu'un moyen bien faible d'assurer la protection des renseignements personnels dans les transferts internationaux de données. Premièrement, elles sont rédigées dans l'esprit de la libre circulation, qui témoigne de la volonté des États-Unis de faire en sorte que les pays membres évitent d'élaborer des lois, des politiques et des procédures qui, sous couvert de la protection de la vie privée et des libertés individuelles, créeraient des obstacles à la circulation transfrontière des données de caractère personnel qui iraient au-delà des exigences propres à cette protection. Deuxièmement, le respect des Lignes directrices est entièrement volontaire, et l'on n'a jamais su au juste la différence qu'il y a entre le fait de les « adopter » ou celui d'y adhérer. » Colin BENNETT, *Réflexions sur une norme internationale de protection des renseignements personnels, Chapitre 3 - Instruments de réglementation des flux de données transfrontières*, Groupe de travail sur le commerce électronique d'Industrie Canada, http://e-com.ic.gc.ca/francais/privee/632d29.html

[125] « Contrairement aux Lignes directrices de l'OCDE, la Convention est un instrument juridique international en vertu duquel les pays signataires doivent adopter une législation nationale de protection des données pour donner concrètement effet aux principes de la Convention

La Convention du Conseil de l'Europe a davantage servi de point de référence commun et de stimulant à l'adoption de législations nationales que d'instrument de régulation des échanges internationaux de données personnelles. Il n'a pas été prévu de mécanisme commun de conciliation des divergences d'interprétation. » Colin BENNETT, *Réflexions sur une norme internationale de protection des renseignements personnels, Chapitre 3 - Instruments de réglementation des flux de données transfrontières*, Groupe de travail sur le commerce électronique d'Industrie Canada, http://e-com.ic.gc.ca/francais/privee/632d29.html

[126] « Cette directive a pour objectif, à l'instar des autres instruments, de concilier à l'intérieure d'une zone européenne, le principe de la libre circulation de l'information et de la protection des données personnelles.

« Ces instruments consacrent les principes fondamentaux en matière de gestion des renseignements personnels instaurés dans les lois nationales et internationales[127]. » Ils traduisent en termes pratiques les préoccupations afférentes aux dimensions informationnelles du droit à la vie privée. « Les principes fondamentaux constituent finalement des énoncés généraux qui identifient les enjeux en imposant des limitations. À l'instar des garanties constitutionnelles, ils seront appelés à s'adapter aux nouvelles circonstances[128]. »

La *Directive* s'applique, en principe, à toutes personnes physiques et morales[129] et établit des procédures et des pratiques dans le but d'assurer aux individus concernés, un droit de contrôle sur leurs renseignements personnels[130]. Elle énonce à son article 25(1) un standard pour le transfert de données personnelles d'un état membre vers un pays tiers.[131]

Les pays membres ayant traduit la directive dans leur droit interne, il ne devrait a priori plus y avoir de restrictions législatives à la circulation des données personnelles. » *Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractères personnels et à la libre circulation de ces données*, http://www2.echo.lu/legal/fr/dataprot/directiv/direct.html. Voir aussi Colin BENNETT, *Réflexions sur une norme internationale de protection des renseignements personnels, Chapitre 3 - Instruments de réglementation des flux de données transfrontières*, Groupe de travail sur le commerce électronique d'Industrie Canada, http://e-com.ic.gc.ca/francais/privee/632d29.html.

[127] Karim BENYEKHLEF et Pierre TRUDEL, *Approches et stratégies pour améliorer la protection de la vie privée dans le contexte des inforoutes*, Mémoire présenté à la Commission de la culture de l'Assemblée nationale dans le cadre de son mandat sur l'étude du Rapport quinquennal de la Commission d'accès à l'information, septembre 1997, p. 18.

[128] Karim BENYEKHLEF et Pierre TRUDEL, *Approches et stratégies pour améliorer la protection de la vie privée dans le contexte des inforoutes*, Mémoire présenté à la Commission de la culture de l'Assemblée nationale dans le cadre de son mandat sur l'étude du Rapport quinquennal de la Commission d'accès à l'information, septembre 1997, p. 18.

[129] L'article 3 (2) énonce deux exceptions au champ d'application de la *Directive*. Il se lit comme suit :

La présente directive ne s'applique pas aux traitements de données à caractère personnel :

- Mis en œuvre pour l'exercice d'activités qui ne relèvent pas du champ d'application du droit communautaire, telles que celles prévues aux titres V et VI du traité sur l'Union européenne et, en tout état de cause, aux traitements ayant pour objet la sécurité publique, la défense, la sûreté de l'État (y compris le bien-être économique de l'État lorsque ces traitements sont liés à des questions de sûreté de l'État) et les activités de l'État relatives à des domaines du droit pénal ;
- Effectué par une personne physique pour l'exercice d'activités exclusivement personnelles ou domestiques.

[130] Entre autre, l'article 12 de la *Directive* octroie un droit d'accès à toute personne concernée et l'article 14 énonce le droit d'opposition de la personne concernée.

[131] L'article 26 de la *Directive* prévoit une série de dérogations à l'article 25 et sous réserve de dispositions contraires du droit national régissant des cas particuliers.

CHAPITRE IV –

TRANSFERT DE DONNÉES À CARACTÈRE PERSONNEL VERS DES PAYS TIERS

Article 25 - Principes

1. *Les États membres prévoient que le transfert vers un pays tiers de données à caractère personnel faisant l'objet d'un traitement, ou destinées à faire l'objet d'un traitement après leur transfert, ne peut avoir lieu que si, sous réserve du respect des dispositions nationales prises en application des autres dispositions de la présente directive, le pays tiers en question assure un niveau de protection adéquat.*

Bien qu'ils soient rassurants, ces instruments ne règlent pas les difficultés pratiques d'applications suscitées par la délocalisation et l'intangibilité de l'information[132]. L'existence de ces instruments ne vient pas régler les questions d'autorités compétentes, de conflits de lois et de plus, ne permettent pas de déterminer l'existence ou non d'un traitement de renseignements personnels[133]. Ils établissent les principes fondamentaux de la protection des renseignements personnels sans être en mesure de les mettre pleinement en application dans les environnements électroniques décentralisés.

En pratique, l'application de ces instruments et des législations nationales peut avoir lieu sans trop de difficultés lorsqu'il s'agit de policer l'État et ses composantes, ou des groupes industriels importants qui ont pignon sur rue dans les divers ressorts nationaux[134]. Toutefois, lorsque vient le moment d'appliquer ces instruments sur Internet, la situation se corse et devient impossible à gérer. Il est beaucoup plus simple de surveiller un nombre restreint d'acteurs dans un territoire donné, que de tenter de surveiller tous les acteurs d'un réseau décentralisé. La caractéristique première des réseaux décentralisés, soit l'absence d'un lieu centralisé où il est possible d'exercer un certain contrôle, génère les plus grandes complications pour le contrôle et la protection des renseignements personnels. La difficulté de mettre en pratique les législations

---

[132] Karim BENYEKHLEF et Pierre TRUDEL, *Approches et stratégies pour améliorer la protection de la vie privée dans le contexte des inforoutes*, Mémoire présenté à la Commission de la culture de l'Assemblée nationale dans le cadre de son mandat sur l'étude du Rapport quinquennal de la Commission d'accès à l'information, septembre 1997, p. 18.

[133] Karim BENYEKHLEF, « L'Internet : un reflet de la concurrence des souverainetés », dans *Réglementer les inforoutes* (Actes du colloque d'octobre 1996).

[134] Karim BENYEKHLEF et Pierre TRUDEL, *Approches et stratégies pour améliorer la protection de la vie privée dans le contexte des inforoutes*, Mémoire présenté à la Commission de la culture de l'Assemblée nationale dans le cadre de son mandat sur l'étude du Rapport quinquennal de la Commission d'accès à l'information, septembre 1997, p. 18.

relatives à la protection des renseignements personnels a généré d'autres moyens pour répondre aux défis de la numérisation de l'information et de l'architecture éclatée des réseaux. Nous y reviendrons.

Les défis que posent les environnements électroniques décentralisés en ce qui a trait à la protection des renseignements personnels sont considérables. À l'heure actuelle, grâce aux divers moyens techniques disponibles, une récolte de renseignements personnels peut s'exécuter très rapidement et à l'insu des internautes. Comme nous le constaterons dans le prochain chapitre, ces récoltes, omniprésentes sur Internet, deviennent un fléau pour la protection de la vie privée.

Chapitre 2

Les collectes de renseignements personnels sur Internet

Le temps passe, les moyens changent, mais les objectifs restent toujours les mêmes. Elles sont terminées les années où, pour obtenir des renseignements personnels, les entreprises effectuaient des sondages téléphoniques et envoyaient des questionnaires via la poste. Depuis quelques années, l'engouement de la population pour le réseau Internet est venu faciliter les techniques de récolte de renseignements personnels. Le présent chapitre traitera spécifiquement des principes juridiques (A) et des enjeux liés aux récoltes de renseignements (B). De plus, les techniques les plus fréquemment utilisées pour effectuer des collectes à l'insu des internautes y seront abordées (C).

A. Les principes juridiques en matières de collectes

Tant qu'ils sont tenus au courant et qu'ils peuvent y mettre fin, 79% de la population canadienne n'est pas dérangée par l'utilisation de leurs renseignements personnels[135]. Néanmoins, ces deux conditions sont pratiquement impossibles à réunir dans les environnements électroniques. Ainsi, il n'est donc pas rare de constater que les internautes sont victimes de récoltes de renseignements personnels à leur insu !

Un grand nombre de pays occidentaux possèdent leurs propres législations concernant la protection de la vie privée et des renseignements personnels. Toutefois, l'application de ces législations est un tour de force dans les environnements électroniques décentralisés et transfrontaliers.

Au Québec, les législations sur la protection des renseignements personnels accordent une priorité aux valeurs individuelles et au statut des individus. « L'expression « renseignement personnel » recouvre et concrétise à la fois une dimension de la vie privée ; la zone d'exclusivité où toute personne s'assume et se prémunit du regard, de l'intrusion d'autrui, y compris de la société[136]. »

La *Loi sur la protection des renseignements dans le secteur privé*, la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*

---

[135] Philippa LAWSON et Marie VALLÉE, « Canadians Take their Information Personal », (octobre 1995), *1 Privacy Files 4* cité dans Pierre TRUDEL, France ABRAN, Karim BENYEKHLEF et Sophie HEIN, *Droit du cyberespace*, Montréal, Éditions Thémis, 1996, p. 11-33.

[136] Paul-André COMEAU, « La vie privée : droit et culture » dans *Le respect de la vie privée dans l'entreprise : de l'affirmation à l'exercice d'un droit*, Les journées Maximilien-Caron 1995, Montréal, Éditions Thémis, 1995, p.3.

et le *Code civil du Québec* offrent une protection globale de cet aspect important de la vie privée[137]. Au Canada, la protection des renseignements personnels est assurée par la *Charte canadienne*, les codes autoréglementaires adoptés par les différents secteurs industriels et la *Loi sur la protection des renseignements personnels et les documents électroniques*[138].

Le droit à la vie privée jouit ainsi d'une protection particulière en ce qui concerne le contrôle des renseignements personnels. Chaque individu a le droit de déterminer quand, comment, et dans quelle mesure les renseignements personnels qui le concerne seront recueillis, utilisés et conservés.

La collecte et l'utilisation des renseignements

Le principe de base en matière de collecte de renseignements personnels est l'obligation d'obtenir le consentement de l'individu concerné avant de recueillir des renseignements personnels à son sujet et d'utiliser ou de communiquer les dits renseignements. En outre, une personne[139] ne peut, pour le motif qu'il fournit un bien ou un service, exiger d'un individu qu'il consente à la collecte, l'utilisation ou la communication de renseignements qui ne sont pas nécessaires à la réalisation des fins légitimes et explicitement indiquées.

La renonciation au droit à la vie privée par consentement laisse ainsi ouverte toute l'épineuse question de la qualité de ce consentement. L'article 14 de la *Loi sur la protection des renseignements dans le secteur privé* fournit un indice sur la valeur de ce consentement. « Le consentement à la communication ou à l'utilisation d'un renseignement personnel doit être manifeste, libre, éclairé et être donné à des fins spécifiques. Ce consentement ne vaut que pour la durée nécessaire à la réalisation des fins pour lesquelles il a été demandé. »

La façon dont une personne obtient un consentement varie selon les circonstances et la nature des renseignements recueillis. De façon générale, il faut obtenir un consentement explicite si les renseignements demandés sont susceptibles d'être

---

[137] Tout comme la Charte québécoise, les lois du secteur public et privé possèdent un attribut exceptionnel : leur prépondérance sur l'ensemble des lois québécoises.

[138] Voir le *Code type sur la protection des renseignements personnels de l'Association canadienne de normalisation*, le *Model Privacy Code for Individual Customers de l'Association des banquiers canadiens* (1989) et le *Code de déontologie et de normes de pratique de l'Association canadienne de marketing direct* qui contient, depuis 1993, des mesures relatives à la vie privée.

[139] Pour la présente section, le terme personne inclus les personnes physiques, morales et les organismes.

considérés sensibles. Lorsque les renseignements sont moins sensibles, un consentement implicite est normalement jugé suffisant[140].

La personne qui constitue un dossier sur un individu doit aussi avoir un intérêt sérieux et légitime de le faire. Actuellement, il n'existe aucune disposition législative qui définit la notion de dossier. Néanmoins, il appert que dans le présent contexte, un dossier sera constitué de l'ensemble des pièces relatives à une personne physique et regroupées en fonction d'un objet ou d'une finalité donnée[141]. En conséquence, il appert que le profil de consommation d'un internaute peut être qualifié de dossier, vu que les informations qu'il contient sont regroupées ou susceptibles d'être regroupées de manière à prendre une décision au sujet de l'individu concerné ou d'informer un tiers à son égard.

La condition principale à la constitution d'un dossier est l'intérêt sérieux et légitime à le faire. Cet intérêt sérieux et légitime n'est pas défini dans le *Code civil du Québec* et dans les législations traitant de la protection des renseignements personnels. Il appartient aux tribunaux d'identifier les cas où il est acceptable qu'une personne physique ou morale constitue un dossier au sujet d'un internaute.

La personne qui constitue un dossier doit faire la mention de son objet à l'internaute avant ou au moment de la collecte et lui indiquer clairement les raisons qui justifient la cueillette de ces renseignements[142]. Malgré le fait que cette notion ne soit pas tout à fait définie, elle semble référer à la raison d'être, à la finalité du dossier. En conséquence, toute personne qui constitue un dossier sur autrui doit, au moment de la constitution de ce dossier, se demander dans quel but elle cherche à recueillir des renseignements au sujet de cet individu. L'objet doit être assez spécifique pour permettre de vérifier le caractère sérieux et légitime de l'intérêt du détenteur du dossier ainsi que pour circonscrire la nature des informations qui y seront versées. Il doit exister un lien rationnel entre les renseignements personnels et l'objet du dossier.

---

[140] Le nom et l'adresse des abonnés d'une revue d'information ne seront généralement pas considérés comme des renseignements sensibles. Par contre, les noms et adresse des abonnés de certains périodiques spécialisés pourraient l'être.

[141] Raymond DORAY, « Mise à jour, mise au point et mise en garde au sujet de la protection des renseignements personnels dans le secteur privé », dans *Développements récents en droit administratif (1998)*, Service de la formation permanente, Barreau du Québec, Montréal, Éditions Yvon Blais Inc., 1998, 135, p. 146.

[142] La personne doit être en mesure de justifier les raisons qui ont donné lieu à la collecte d'un renseignement. À l'inverse, elle ne peut recueillir des renseignements dont elle ne peut justifier un usage qu'une personne raisonnable estimerait acceptable dans les circonstances.

De plus, le dossier doit seulement être utilisé à des fins compatibles avec son objet. Les informations contenues ne peuvent être communiquées à des tiers sans le consentement de l'intéressé ou l'autorisation de la loi. En conséquence, toute utilisation primaire ou secondaire de ces renseignements personnels doit être portée à la connaissance de l'internaute, qu'il acquière ou non des biens ou des services d'un site Web. De plus, toutes communications de renseignements personnels à des tiers doivent être divulguées et l'internaute doit y consentir en tout état de cause.

En conséquence, la personne qui constitue un dossier ne peut recueillir que les renseignements nécessaires aux fins déterminées et doit procéder de façon honnête lorsqu'elle recueille les renseignements[143]. Chaque personne doit ainsi rédiger à l'attention du public des documents explicatifs concernant ses politiques et procédures relatives à la protection des renseignements personnels. Dans le cadre des activités commerciales d'une entreprise sur le réseau Internet, cela signifie que le consommateur doit être en mesure, lorsqu'il accède au site Web, de prendre connaissance des politiques et des procédures de plaintes.

Les personnes doivent de plus protéger les renseignements personnels au moyen de mesures de sécurité correspondant à leur degré de sensibilité. Chaque personne est responsable des renseignements personnels qu'il a en sa possession ou sous sa garde, y compris les renseignements confiés à une tierce partie aux fins de traitement. Aucune loi ou règlement ne précise cependant la forme que doivent revêtir ces mesures de sécurité, laissant ainsi entière liberté à l'entreprise d'agir à sa guise.

Les renseignements doivent de plus être à jour et exacts au moment où l'entreprise les utilise pour prendre une décision relative à l'individu concerné. Le degré d'exactitude et de mise à jour dépend de l'usage auquel ils sont destinés, compte tenu des intérêts de l'individu.

Le droit d'accès et de rectification

La personne qui collige de l'information doit informer l'individu concerné de l'endroit où sera détenu son dossier et pendant combien de temps les renseignements y seront conservés. Chaque personne doit prendre les mesures nécessaires pour assurer

---

[143] À cet égard, il est intéressant de souligner que l'article 37 *C.c.Q.* utilise plutôt la notion de renseignement pertinent contrairement aux lois traitant de la protection des renseignements personnels qui utilise la notion de renseignement nécessaire.

l'exercice du droit d'accès et faire en sorte que des informations précises sur ses politiques et ses pratiques soient facilement accessibles à tous les internautes[144].

Une personne doit aussi informer tout individu qui en fait la demande de l'existence de renseignements personnels qui la concerne, de l'usage et de la communication qui en est fait, et de lui permettre de les consulter. En conséquence, celui qui détient un dossier sur autrui ne peut lui refuser l'accès, à moins qu'il ne justifie son refus par un intérêt sérieux et légitime ou que la divulgation de ces renseignements soit susceptible de nuire sérieusement à un tiers. Advenant le cas où des renseignements sont faux ou inexacts, l'individu dispose d'un droit de rectification qui lui permet de corriger un renseignement inexact, incomplet ou équivoque, et de supprimer un renseignement périmé ou non justifié par l'objet du dossier[145].

En résumé, une personne qui récolte des renseignements personnels doit[146] :

- Obtenir le consentement de l'individu concerné ;
- Renseigner l'individu concerné avant la collecte ou lors de celle-ci, sur les fins pour lesquelles ces renseignements personnels sont recueillis ;
- Limiter la collecte d'information en ne recueillant que les renseignements personnels nécessaires aux fins déterminées ;
- Limiter l'utilisation et la conservation des renseignements personnels. Ceux-ci ne doivent pas être utilisés ou communiqués pour des fins autres que celles pour lesquelles ils ont été recueillis à moins que l'individu concerné n'y consente ou que la loi l'exige ;
- Établir des mesures pour protéger les renseignements personnels en sa possession ou sous sa garde ;
- Désigner une ou des personnes qui doivent s'assurer du respect de ces principes et recevoir les plaintes des usagers s'il y a lieu.

---

[144] Voir à ce sujet, une enquête effectuée par la CNIL sur les sites de commerce en ligne. Florent LATRIVE, « Pouvez-vous me rayer de vos fichiers ? », 14 avril 2000, *Libération*, http://www.liberation.fr/multi/actu/20001004/20000414venzc.html

[145] À ce sujet, il s'avère, en pratique, extrêmement difficile de faire rectifier ou enlever des renseignements personnels. David LAZARUS, « Fan Spam Is Hard To Shake subscribing from e-mail lists nearly impossible », 7 février 2000, *San Francisco Chronicle*, http://www.sfgate.com/cgi-bin/article.cgi?file=/chronicle/archive/2000/02/07/BU44258.DTL&type=tech_article.

[146] André OUIMET, « Vers un régime de protection des renseignements personnels dans le secteur privé » *Développements récents en droit de l'accès à l'information (1991)*, Service de la formation permanente, Barreau du Québec, Cowansville, Éditions Yvon Blais, 1991, p.183 et Raymond DORAY, « La protection de la vie privée », *Développements récents en droit administratif (1995)*, Service de la formation permanente, Barreau du Québec, Cowansville, Éditions Yvon Blais, 1995, p.121.

Ces principes constituent les fondements juridiques des récoltes de renseignements personnels. Malgré le fait qu'ils se retrouvent généralement dans toutes les lois visant la protection des renseignements personnels, plusieurs personnes outrepassent ces principes et, à l'insu des internautes, récoltent des renseignements personnels.

B. Les enjeux liés à la récolte de renseignements personnels

Sur le réseau Internet, les renseignements personnels sont des informations précieuses que les internautes désirent protéger et que, par ailleurs, les entreprises recherchent à tout prix[147].

Le nombre grandissant d'internautes a créé un tout nouveau marché depuis quelques années. La récolte et la vente de renseignements personnels sont devenues chose courante.

> « *Unfortunately, there is such a large black market industry right now of [people] -- by hook or by crook -- getting a hold of names, of emails. There are an awful lot of people who're collecting information without the knowledge of other consumer, selling it, stealing it, and it finding its way around*[148]. »

Étant donné que tout est à vendre, même la vie privée, le désir naturel d'être laissé en paix peut rapporter beaucoup d'argent[149].

Au contraire des pays occidentaux qui ont élaboré des législations de protection des renseignements personnels, les États-Unis, terre promise des pratiques de « data profiling »[150], font présentement bande à part en laissant le marché autoréglementer la

---

147 « Dans la société contemporaine tout spécialement, la conservation de renseignements à notre sujet, revêt une importance accrue. » *R.* c. *Dyment*, [1988] 2 R.C.S. 417, p. 428-429.

148 Jennifer SULLIVAN, « Your Data on the Black Market », 12 janvier 1999, *Wired*, http://www.wirednews.com/print_version/email/explode-infobeat/story/17297.html?wnpg=all.

149 « The marketplace of personal information is big business in the United States. By 1998, the gross annual revenue of companies selling personal information and profiles, largely without the knowledge or consent of the individuals concerned, was reportedly $1.5 billion. » Joel REIDENBERG, « Restoring Americans' Privacy in Electronic Commerce », *Berkeley Technology Law Journal*, Volume 14-2, http://www.law.berkeley.edu/journals/btlj/articles/14_2/Reidenberg/html/reader.html et FTC, *In re Trans Union*, Docket No. 9255, 31 juillet 1998, http://www.ftc.gov/os/1998/9808/d9255pub.id.pdf.

150 Les pratiques de « data profiling » permettent de construire des schémas comportementaux d'achat des internautes. Notamment, c'est le cas lorsqu'une entreprise utilise ou vend de l'information qu'elle accumule, licitement ou illicitement, aux fins de dresser un profil de consommation ou lorsqu'elle utilise des renseignements personnels obtenus lors d'une transaction pour des fins autres que celles rendues nécessaires pour l'exécution de la transaction. Pierre TRUDEL, France ABRAN, Karim BENYEKHLEF et Sophie HEIN, *Droit du cyberespace*, Montréal, Éditions Thémis, 1996, p. 11-42.

protection des renseignements personnels[151]. Mieux cibler les goûts et les opinions des consommateurs pour ainsi leur faire des offres alléchantes rapporte gros aux commerçants américains.

Les enjeux découlant de la récolte, l'utilisation, la conservation et la transmission des renseignements personnels sont considérables. Le détournement des renseignements personnels résultant d'utilisations illégitimes donne lieu à des abus, telles des catégorisations discriminatoires d'individus en fonction de leur état de santé, de leur orientation sexuelle, de leurs convictions politiques ou religieuses, de leur sexe ou, de leur condition sociale[152].

Andrew Shapiro, journaliste à l'hebdomadaire américain « The Nation », met en garde contre la suite logique du raisonnement : l'avènement d'un marché de la vie privée, où les internautes en mal de discrétion paieront au prix fort la sécurité de leurs données, alors que les autres verront leur intimité offerte au tout-venant. Assurément, ce système comportera quelques inconvénients, et non des moindres[153]. L'anonymat qui fait les délices des surfeurs disparaîtra : il sera difficile de se protéger en donnant de fausses informations. Les moins riches, détenteurs d'informations confidentielles de « deuxième classe », seront naturellement pauvres en intimité.

1) L'élaboration de profils

Depuis l'avènement de l'informatisation, les collectes de renseignements personnels s'effectuent plus aisément. En 1994, Industrie Canada rappelait que :

> *« Les grands projets réalisés quant à la capacité des ordinateurs, la liaison d'un grand nombre d'entreprises par des systèmes de paiement électronique, et le maillage complet des bases de données sur les ventes et les commandes ont révolutionné la relation entre les consommateurs et les producteurs de biens et de services*[154]. »

---

[151] CNIL, *Informatique et libertés dans le monde*, 1999, http://www.cnil.fr/thematic/tdoss3.htm

[152] Isabelle HARNOIS, « La protection constitutionnelle et quasi constitutionnelle du droit au respect de la vie privée et les banques de données informatisées », dans *Congrès annuel du Barreau du Québec (1997)*, Service de la formation permanente, Barreau du Québec, 1997, p.673.

[153] Andrew L. SHAPIRO, « Privacy for Sale : Peddling Data on the Internet », juin 1997, *The Nation*.

[154] INDUSTRIE Canada, *La protection de la vie privée et l'autoroute canadienne de l'information : une nouvelle infrastructure de l'information et des télécommunications*, Ottawa, 1994, p.6.

Dans le monde industrialisé « les lois de protection des renseignements personnels doivent leur existence à une conscientisation de l'importance de l'information en tant qu'instrument de pouvoir et d'influence. » Le consommateur est maintenant considéré comme un maillon très important dans la chaîne qui facilite l'analyse du marché à conquérir et la commercialisation directe. L'information *per se* n'a aucune valeur, c'est l'utilisation que l'on en fait qui lui confère de l'importance[155].

Auparavant, lorsqu'il n'y avait pas de législations protégeant les renseignements personnels, une majorité de la population savait qu'un établissement émetteur de cartes de crédit pouvait vendre à des fournisseurs de produits les données transactionnelles qui les concernaient[156]. Certains d'entre eux considéraient ce risque comme un inconvénient raisonnable compensé par l'avantage du recours à un établissement de crédit important et fiable. Aujourd'hui, à l'heure où le commerce électronique prend une ampleur phénoménale, il est primordial de se questionner sur le renouveau sur ce phénomène. Est-ce qu'une diminution de la protection de la vie privée, c'est-à-dire une certaine renonciation à la protection accordée, est le prix à payer pour obtenir une personnalisation des services sur le réseau Internet[157] ? La journaliste Courtney Macavinta écrivait à ce sujet :

---

[155] Karim BENYEKHLEF, « Les libertés : voie médiatrice de la protection des données personnelles » dans *Le droit de la communicatique*, Actes du colloque conjoint des Facultés de droit de l'Université de Poitiers et de l'Université de Montréal, Montréal, Éditions Thémis, 1992, p. 45.

[156] INDUSTRIE Canada, *La protection de la vie privée et l'autoroute canadienne de l'information : une nouvelle infrastructure de l'information et des télécommunications*, Ottawa, 1994, p.6.

[157] Selon le Privacy & American Business and Opinion Research, 86 % des internautes américains ne se déclarent pas choqués par l'échange de renseignements personnels contre des biens et services. BLOOMBERG NEWS, « Survey : Personal data flows for freebies », 14 juillet 1999, *CNET*, http://www.news.com/News/Item/0,4,39156,00.html?pfv. Voir Bob TEDESCHI, « Targeted Marketing Confronts Privacy Concerns », 10 mai 1999, *New York Times - E Commerce Report*, http://search.nytimes.com/search/daily/bin/fastweb?getdoc+site+site+78182+0+wAAA+tedeschi%7Etargeted%7Emarketing%7Econfronts.

> « *The buzzword of the day seems to be "personalization" ; from the portals to financial services firms and special-interest sites such as those for sports fans, users are often given the opportunity to trade personal data for a page built just for them. The idea is that everybody wins--users get exactly what they want, so in theory they will come back often and stay a while, and the site gets a loyal audience and a wealth of demographic data it can use to sell advertising at a premium*[158]. »

Cependant, l'échange n'est pas aussi simple en réalité. Grâce à cette personnalisation, les commerçants collectent plus de renseignements personnels pour élaborer des profils de consommation[159]. Depuis l'achat de l'entreprise Abacus par DoubleClick,[160] le débat se déplace maintenant des sites Web individuels aux serveurs qui collectent des renseignements personnels en traquant les internautes de site en site. Comme le souligne Alan F. Westin :

> « *[...] Electronic networks can place unique pressures on privacy in that electronic networks may be able to compile a "richer, more detailed profile" of a user that can individual companies preparing one-dimensional list of their customers*[161]. »

L'archivage, le rapprochement et l'élaboration de profils en fonction d'informations collectées lors de transactions électroniques permettent aux commerçants de mieux cibler leur clientèle en tenant compte de leurs besoins et de leur style de vie[162]. Une fois

---

[158] Courtney MACAVINTA, « Is no privacy the price of personalization? », 10 mars 1999, *CNET*, http://www.news.com/News/Item/0,4,33560,00.html

[159] À ce sujet, le professeur Froomkin écrit : « It is now possible to construct a consumer profile based on widely divergent types of data, to correlate and re-correlate information as never before. [...] Data collection will grow in at least five areas: medical history, government records, personal movements, transactions, and reading and viewing habits between them these five areas cover most of modern life. » Michael FROOMKIN, « Flood Control on the Information Ocean : Living With Anonymity, Digital Cash and Distributed Databases », 15 *U. of Pitt. J. of L. & C.* 395 (1996), http://www.law.miami.edu/[froomkin/articles/ocean1.htm.

[160] Le 24 novembre 1999, l'entreprise de publicité sur Internet DoubleClick a acquis la société d'analyse de comportement d'achat Abacus Direct, malgré l'opposition des groupes de défense de la vie privée. Pour ces groupes, la fusion entre la publicité et les renseignements représente une menace à la vie privée des internautes. Plus précisément, c'est la capacité de DoubleClick à utiliser ses cinq milliards de bannières vues par semaine pour identifier des habitudes de navigation, jumelée aux deux milliards de transactions par catalogue effectuées par des individus identifiables enregistrées chez Abacus que craignent les défendeurs des consommateurs. Steve GELSI, « DoubleClick buying Abacus Direct », 14 juin 1999, *CBC Market Watch*, http://cbs.marketwatch.com/archive/19990614/news/current/dclk.htx?source=blq/yhoo&dist=yhoo et Courtney MACAVINTA, « DoubleClik, Abacus merge in $1.7 billion deal », 24 novembre 1999, *CNET*, http://news.cnet.com/news/0-1005-202-1463444.html

[161] Propos tenus par Alan F. Westin dans Dorothy E. DENNING et Herbert S. LIN (dir.), *Rights and Responsibilities of participants in Networked Communities*, Washington, National Academy Press, 1994, p.106.

[162] Segal souligne que la problématique entourant la compilation d'informations et la création de profils de consommation n'est pas nouvelle. Les entreprises de câblodistribution ont depuis déjà fort longtemps acquis cette possibilité de développer et de maintenir un portrait à jour des activités et des préoccupations politiques, économiques et sociales des usagers de leur service. G. R. SEGAL, « The Threat From Within: Cable

établi, ce profil devient une source précieuse d'informations qui, vendues à d'autres entreprises, entraînent souvent un détournement des finalités premières de la collecte[163].

En vérité, ce n'est pas tant la transaction électronique prise isolément qui constitue le danger pour la vie privée ; mais plutôt la possibilité pour les serveurs commerciaux de dresser des profils des habitudes de consommation des usagers[164]. Les coûts reliés au développement et à l'exploitation des services électroniques interactifs ont incité les commerçants à compiler des informations sur les consommateurs pour leur offrir de meilleures offres commerciales[165]. Chaque contact personnalisé permet à un site Web de collecter plus d'informations que tout autre acteur traditionnel de la vente par correspondance.

Les acteurs du réseau étant des adeptes du marketing personnalisé[166], ils rivalisent d'imagination pour constituer des gisements de renseignements personnels, allant même jusqu'à offrir des lots ou une rémunération en contrepartie d'un questionnaire bien rempli. Mieux encore, connaissant le nom et l'adresse électronique du consommateur, ils ne se gênent pas pour lui faire parvenir diverses publicités alléchantes tenant compte de son profil. Les campagnes de marketing sont dès lors plus précises et rapportent

---

Television and the Invasion of Privacy », (1986) 7 *Computer L.J.* 89, P. WASHBURN, « Electronic Journalism, Computers and Privacy » (1982) 3 *Computer L.J.* 189 et Joel REIDENBERG, « Privacy in the Information Economy: A Fortress or Frontier for Individual Rights », (1992) 44 *Fed. Comm. L.J.* 195.

[163] Karim BENYEKHLEF, « Les normes internationales de protection des données personnelles et l'autoroute de l'information », dans *Le respect de la vie privée dans l'entreprise*, Actes des Journées Maximilien Caron, Montréal, Éditions Thémis, 1996, 65, p.90 et Michael FROOMKIN, « Flood Control on the Information Ocean: Living With Anonymity, Digital Cash and Distributed Databases », 15 *U. of Pitt. J. of L. & C.* 395 (1996), http://www.law.miami.edu/~froomkin/articles/ocean1.htm

[164] A ce sujet, Jeff Chester du Center for Media Education énonce : « Millions and millions of online profiles of you and me have been created. They don't have to know your name, but they know you. » Jeri CLAUSING, « FTC Asked To Examine Data Profiling Practices », 9 novembre 1999, *New York Times*, http:///www.nytimes.com/library/tech/99/11/cyber/capital/09capital.html.

[165] Louis HARRIS et Alan F. WESTIN, « Privacy of Consumer Transaction Records in Future Home Interactive Services: What the Public Says - What the Public Wants (Reports from and Commentaires on a National Survey of Consumers, Interactive Services, and Privacy) », présenté dans le cadre du *Fifth Conference on Computer, Freedom and Privacy*, Conférence organisée par le Board of Trustees de l'Université Leland Stanford, juin-juillet 1994, http://www.techlaw.stanford.edu/CFP95.Program.html

[166] Communément appelé le marketing « one to one », il implique une parfaite connaissance des goûts et des comportements des consommateurs potentiels.

beaucoup plus d'argent qu'auparavant[167]. Déshabiller un internaute est maintenant à la portée des commerçants[168].

L'enjeu est grand ! La réalisation de profils commercialisés et le caractère problématique de l'élaboration et de la manipulation de ces profils sont accentués par leur clandestinité. Dans la grande majorité des cas, il est quasiment impossible de savoir quand, comment, et par quelles entreprises sont traitées ces informations. Des commerçants et des organismes peuvent ainsi décortiquer les goûts et le comportement de tous et chacun sans que les usagés n'en soient informés ou qu'ils n'aient donné leur consentement. De plus, lorsque ces manipulations causent un préjudice, les usagers l'ignorent et lorsque par chance ils l'apprennent, il devient extrêmement difficile de tenter de prouver quoi que ce soit.

2) La sécurité transactionnelle

Au-delà de l'utilisation des renseignements personnels et des données transactionnelles pour établir des profils, il importe de souligner l'importance de la sécurité transactionnelle et de l'identification individuelle sur Internet[169].

Bien qu'il soit possible de protéger le contenu d'un message électronique, la vérification de l'identité de l'expéditeur et du destinataire constitue un élément critique de la protection de la vie privée. Les usagers effectuant des transactions via le réseau Internet sont appelés à s'identifier et à fournir une multitude de renseignements personnels, tels un numéro de carte de crédit, un numéro du permis de conduire ou le nom de jeune fille de leur mère.

---

[167] Craig BICKNELL, « Database Marketing on the Web », 7 octobre 1999, *Wired*, http://www.wired.com/news/news/business/story/15456.html et Susan E. GINDIN, « Lost and Found in Cyberspace, Informational Privacy in the Age of the Internet », 34 *San Diego Law Review* 1153 (1997), http://www.info-law.com/lost.htm

[168] Des profils d'identités uniformes, prêts à être partagés ! Voilà l'idée derrière le Customer Profile Exchange (CPEX), une norme que veut établir un consortium de firmes de marketing direct. Le CPEX regrouperait toute l'information à propos d'un consommateur, tant l'information recueillie en ligne que celle obtenue par les marchands traditionnels. « Mass marketing is dead. New marketing is serving the needs of each customer as an individual. » Stacy COLLETT & Julekha DASH, « Internet advertiser to develop standard for exchanging customer profiles », 15 novembre 1999, *Online News*, http://www.computerw...m/home/news.nsf/all/9911151privacy et Leslie MILLER & Elizabeth WEISE, « FTC studies Web site profiling », 23 novembre 1999, *USA Today*, http://www.usatoday.com/life/cyber/tech/review/crg570.htm

[169] Les données transactionnelles sont aussi, sinon plus importantes que les profils, étant donné qu'elles offrent des informations pertinentes, telle l'adresse de courriel, qui permet de rejoindre directement les usagers. Pierre TRUDEL, France ABRAN, Karim BENYEKHLEF et Sophie HEIN, *Droit du cyberespace*, Montréal, Éditions Thémis, 1996, p. 11-46.

Dans une ère où le montant total des transactions électroniques s'accroît d'année en année, il importe de porter une attention particulière à la sécurité transactionnelle. Dans ces situations, l'utilisation de l'anonymat, des services anonymisateurs, de la cryptographie et de la signature électronique sont des solutions à préconiser.

C. Les moyens utilisés

Le respect de la vie privée est menacé par « les investigations que rendent possibles les progrès des sciences et des techniques, et par les divulgations que permettent les nouveaux moyens de communication de masse[170]. » De jour en jour, de nouveaux logiciels et plugiciels font leur apparition en ayant comme objectif principal de récolter des renseignements personnels et ce, à l'insu de leurs utilisateurs. La présente section traitera de cinq moyens utilisés pour récolter des renseignements personnels sur Internet.

1. L'éternel problématique des « cookies »

Au début de l'année 1999, l'éternel problématique des fichiers de témoins[171] a refait surface. Après que le géant Microsoft ait admis avoir codé par inadvertance la procédure d'enregistrement du système d'exploitation Windows 98[172], ce fut au tour de l'entreprise californienne Macromedia d'être prise au piège au courant du mois de mars 1999. Comme Microsoft, Macromedia a admis que la procédure automatique de mise à jour de son plugiciel[173] Shockwave[174] lui faisait parvenir des fichiers de témoins

---

[170] Pierre Kayser, *La protection de la vie privée par le droit : protection du secret de la vie privée*, 3e éd., Paris, Les presses universitaires d'Aix-Marseille, 1995, p.18.

[171] Mieux connu sous ses expressions anglaises « cookies » et « cookie file ». PUBLICATIONS DU QUÉBEC, *Terminologie d'Internet*, http://www.olf.gouv.qc.ca/ressources/internet/fiches/2075187.htm.

[172] À cet effet, Rob Bennet de Microsoft énoncait : « Microsoft has acknowledged that a feature in its Windows 98 operating system can be used to collect information on authors of electronic documents without their knowledge. Microsoft software applications such as Word and Excel, generate unique identification numbers that include information about users' personal computers that are then transmitted during the Windows 98 registration process. » Mike RUCCIUTI, « Microsoft admits privacy problem, plans fix », 7 mars 1999, *CNET*, http://www.news.com/News/Item/0,4,334413,00.html

[173] Logiciel d'application complémentaire qui, associé à un navigateur Web, entre automatiquement en action en présence d'un objet multimédia, et ce, sans que l'utilisateur ait à intervenir. PUBLICATIONS DU QUÉBEC, *Terminologie d'Internet*, http://www.olf.gouv.qc.ca/ressources/internet/fiches/2075236.htm

[174] Plugiciel conçu par Macromedia, qui, associé à un navigateur Web, permet de visualiser des fichiers de type Director, comprenant du son et des animations, en créant un environnement interactif et sonore d'une qualité comparable à celle d'un CD-ROM. PUBLICATIONS DU QUÉBEC, *Terminologie d'Internet*, http://www.olf.gouv.qc.ca/ressources/internet/fiches/8394306.htm

contenant les adresses des sites Web visités par les utilisateurs du plugiciel Shockwave[175].

Un fichier de témoins désigne un fichier créé par le navigateur[176] de l'utilisateur et enregistré dans son ordinateur rassemblant les témoins[177] issus de sa navigation sur Internet. Ce petit fichier contient seulement les informations que l'utilisateur a bien voulu donner. En principe, jamais un fichier de témoins ne pourra récupérer à l'insu de l'internaute son adresse de courriel, à moins que l'utilisateur l'ait expressément inscrite sur un formulaire[178]. En contrepartie, les autres renseignements tels l'adresse IP[179] de l'ordinateur et le type de navigateur utilisé, sont généralement connus indépendamment de l'utilisation d'un fichier de témoins.

Un fichier de témoins peut contenir tout au plus 300 témoins à la fois, d'une grosseur maximale de 4 Kilo-octets chacun[180]. Chaque témoin occupe spécifiquement une ligne du fichier. Lorsque le fichier compte 300 témoins, les nouveaux témoins prennent la place de ceux dont la date de création est la plus ancienne. Dépendant de l'environnement dans lequel l'utilisateur se trouve, le fichier de témoins porte différents noms. Dans un environnement Windows, il se nomme cookies.txt. Pour les ordinateurs

---

[175] Techniquement, à chaque fois qu'un utilisateur naviguait sur un site Web utilisant la technologie Shockwave, l'adresse Web du site était emmagasinée dans un fichier semblable aux fichiers de témoins. De plus, un nombre important de sites incluent des données personnelles, tel le nom d'utilisateur ou le mot de passe dans leurs adresses Web, afin de permettre à leurs visiteurs de naviguer de façon personnalisée sans pour autant avoir recours aux témoins. Ainsi, lorsque l'utilisateur se faisait offrir par Macromedia une mise à jour de son plugiciel Shockwave, le fichier contenant les adresses Web et les noms d'utilisateurs et mots de passe étaient automatiquement envoyés à l'entreprise et ce, à l'insu de l'utilisateur.

Aux dires de Macromedia, celle-ci ne voulait que conserver ces données pour fins de statistiques afin d'aider les webmestres des sites visités à les rendre plus conviviaux. Néanmoins, l'entreprise assure que dans la nouvelle version du plugiciel le problème est réglé et qu'il fut codé pour éliminer tous renseignements personnels des adresses Web transmises. Paul FESTA, « Macromedia patching Shockwave privacy hole », March 11, 1999, *CNET*, http://www.news.com/News/Item/0,4,33648,00.html.

[176] Logiciel client capable d'exploiter les ressources hypertextes et hypermédias du Web ainsi que les ressources d'Internet dans son ensemble, qui permet donc la recherche d'information et l'accès à cette information. PUBLICATIONS DU QUÉBEC, *Terminologie d'Internet*, http://www.olf.gouv.qc.ca/ressources/internet/fiches/1299148.htm

[177] Élément d'information transmis par le serveur au navigateur lorsque l'internaute visite un site Web, et qui peut être récupéré par le serveur lors de visites subséquentes. PUBLICATIONS DU QUÉBEC, *Terminologie d'Internet*, http://www.olf.gouv.qc.ca/ressources/internet/fiches/2075187.htm

[178] Il fut un temps où il était possible de faire un formulaire à l'aide du Javascript qui transmettait à l'insu de l'utilisateur, son adresse de courriel. Dès lors, il était possible de lier un témoin à l'adresse de courriel de l'utilisateur. Toutefois, cette faille est supposée avoir été corrigé dans les versions récentes des logiciels de programmation Java. Clément GAGNON, *Les « cookies » démystifiés*, 23 mars 1999, http://www.tactika.com/cookie/.

[179] Du terme anglais Internet Protocol, c'est le protocole de base du réseau Internet qui régit l'expédition et la circulation des paquets de données à travers des réseaux hétérogènes. PUBLICATIONS DU QUÉBEC, *Terminologie d'Internet*, http://www.olf.gouv.qc.ca/ressources/internet/fiches/2076487.htm

[180] De plus, seul vingt témoins par serveur ou domaine pourront être enregistrés par fichier de témoins.

Macintosh, c'est MagicCookie, et pour les ordinateurs utilisant Unix, c'est cookies. De plus, il importe de signaler qu'un navigateur ne peut utiliser le fichier de témoins créé par un autre navigateur. En conséquence, il existe autant de fichiers de témoins sur un ordinateur qu'il y a de navigateurs utilisés par l'internaute.

Chaque témoin contenu dans un fichier de témoins contient nécessairement un nom auquel il peut s'ajouter des paramètres facultatifs, tels[181] :

- Une date d'expiration indiquant jusqu'à quelle date le témoin peut être utilisé. Si aucune date d'expiration n'est indiquée, le témoin expire à la fin de la présente session.
- Un chemin indiquant sur quelles pages du site Web le témoin sera visible. Si aucune précision n'est faite à ce sujet, le témoin est visible sur le site en entier.
- Un domaine[182] indiquant le nom de domaine pour lequel le témoin sera valable. Malgré l'application restreinte qu'il pourrait en résulter, il est possible de créer un témoin qui pourrait être lu par un autre serveur. Néanmoins, si on ne définit pas le domaine lors de la création du témoin, seul le serveur créant le témoin pourra y avoir accès.
- Un attribut de sécurité indiquant que le témoin n'est transmis que si la connexion vers le serveur est une connexion sécurisée, tel le protocole S-HTTP[183] par exemple.

Concrètement, un extrait d'un fichier de témoins confectionné par un navigateur Netscape ressemble à ceci :

 # Netscape HTTP Cookie File
 # http://www.netscape.com/newsref/std/cookie_spec.html
 # This is a generated file! Do not edit.
.disney.com TRUE / FALSE 942189160 DOL 142169905648619
altavista.digital.com TRUE /FALSE 946641593 AV_UID d3060caa39584f
www.bell.ca FALSE / FALSE 944028198 LanguagePreference EN

---

[181] D. KRISTOL & L. MONTULLI, *HTTP State Management Mechanism*, Février 1997, http://www.cis.ohio-state.edu/htbin/rfc/rfc2109.html et NETSCAPE, *Persistent Client State HTTP Cookies*, 1999, http://www.netscape.com/newsref/std/cookie_spec.html.

[182] Partie d'un nom Internet qui identifie une organisation membre du réseau et qui précise le niveau hiérarchique de cette organisation dans le réseau Internet. PUBLICATIONS DU QUÉBEC, *Terminologie d'Internet*, http://www.olf.gouv.qc.ca/ressources/internet/fiches/2076505.htm.

[183] Le protocole S-HTTP est une extension du protocole HTTP qui est le protocole principal du World Wide Web. La lettre S signifie Sécurisé, et ajoute les fonctions nécessaires pour assurer la confidentialité, l'intégrité, l'opposabilité et l'authenticité. Ce protocole apporte une grande flexibilité dans la sélection des algorithmes de cryptage. Wolfram GIESEKE, *PC 100 % Pratique, Sécurité et Protection*, traduction de C. STOLL, H. BERTRAND et P. M. WOLF, Paris, Micro Application, 1998, p. 409 et ss.

L'utilisation des témoins et des fichiers de témoins donne aux sites Web, le pouvoir de déposer et de récupérer à tout moment, une information très courte et très importante enregistrée sur le disque dur d'un internaute, habituellement à son insu[184].

Le dépouillement des données rapportées par les témoins peut fournir des informations relativement pertinentes à propos des utilisateurs du site et du site en lui-même. En effet, les éditeurs peuvent quantifier, avec une faible marge d'erreur, le trafic du site, le nombre d'utilisateurs isolés, la fréquence et la durée moyenne d'une visite, le nombre moyen de pages visitées, les types de bandeaux publicitaires qui attirent l'attention et les pages ou les zones de chaque page qui suscitent le plus d'intérêt. Concernant chacun de ces utilisateurs isolés, les éditeurs disposent d'une masse d'information permettant de reconstituer les scénarios de navigation et les préférences individuelles. Le niveau de profondeur et le champ de diversification de l'information contenue dans le site influencent l'exactitude du profil que l'on peut dresser. Plus le site est complet et diversifié, plus les utilisateurs opèrent eux-mêmes une sélection en fonction de leurs préférences. Ceci permet donc d'augmenter le raffinement des renseignements sur les centres d'intérêt de l'utilisateur.

Le but premier de ces témoins est de permettre aux éditeurs des sites Web de reconnaître leurs visiteurs[185]. En octroyant un numéro d'identification à chaque nouvel internaute lors de leur première visite, ils peuvent, à chacune de leurs visites ultérieures, les identifier et enregistrer les pages qu'ils ont visitées pour ainsi personnaliser leurs prochaines visites. Les fichiers de témoins ont leurs avantages et leurs inconvénients.

---

[184] « Cookies are based on a two-stage process. First the cookie is stored in the user's computer without her consent or knowledge [à cet effet, il convient de mettre un bémol dû aux changements technologiques. Tel qu'il en sera amplement discuté ci-dessous, les versions 4 des navigateurs Netscape et Microsoft offrent la possibilité d'avertir l'internaute lorsqu'un site Web désire installer un témoin].

During the second stage, the cookie is clandestinely and automatically transferred from the user's machine to a Web server. Whenever a user directs her Web browser to display a certain Web page from the server, the browser will, without the user's knowledge, transmit the cookie containing personal information to the Web server. » Viktor MAYER-SCHÖNBERGER, « The Internet and Privacy Legislation: Cookies for a Treat ? », 1 *W. Va. J. L. & Tech.* 1 (1997) http://www.wvjolt.wvu.edu/wvjolt/current/issue1/articles/mayer/mayer.htm

[185] « Under the law of Texas, a person who follows another person around repeatedly in a way that is calculated to cause the victim to fear for his safety or the safety of his family or property is guilty of the crime of stalking. Obviously, the law would apply to a crazed fan who shows up with a baseball bat at a movie starlet's home every Saturday night. But in the Internet age, can the Texas law be applied to a Web site owner that is accused of electronically monitoring the browsing habits of its customers?

That is the novel theory put forward in a suit filed last week in Dallas County District Court by a big-thinking Texas lawyer. The case, filed against Yahoo! Inc. and another company it owns, Broadcast.com, seeks class-action status on behalf of 50 million Yahoo users in the United States and seeks economic damages of more than $50 billion for violation of the state's anti-stalking law, as well as other wrongs. » Carl S. KAPLAN, « Lawsuit Says Web Cookies Allow Illegal Stalking », 18 février 2000, *New York Times – Cyber Law Journal*, http://www.nytimes.com/library/tech/00/02/cyber/cyberlaw/18law.html.

Par exemple, si un internaute s'intéresse à la musique, le serveur Web pourra choisir la bannière publicitaire d'une société de vente par correspondance de disques compacts. En outre, si l'internaute a donné son adresse de courriel, il ne serait pas surprenant qu'ils reçoivent des messages publicitaires tenant compte des sites qu'il a visités[186]. En contrepartie, les commerçants considèrent cette technique comme un outil intéressant et l'utilisent de plus en plus[187] en affirmant exploiter ces renseignements de manière rigoureuse et en ne les transmettant pas à d'autres opérateurs. Toutefois, il y a fort à parier que l'on ne peut totalement faire confiance aux opérateurs sur ce point.

Le danger que représentent les témoins se situe à un niveau différent ; ils donnent des informations sur les sites Web visités par un internaute. En outre, les commerçants virtuels ne sont pas les seuls à utiliser les témoins. Plusieurs sites pornographiques utilisent cette technique pour reconnaître leurs visiteurs. En principe, toute personne qui peut accéder au disque dur d'un ordinateur peut y lire les informations enregistrées sous la forme des fichiers de témoins et ainsi, se faire une bonne idée des habitudes de navigation de l'utilisateur de l'ordinateur. De plus, il existe à l'heure actuelle certaines techniques comme « ActiveX »[188] qui permettent de lire ces informations à l'insu de l'utilisateur.

Depuis le lancement de version 4 des navigateurs Netscape et Microsoft, ceux-ci offrent la possibilité d'aviser l'internaute de tout nouveau témoin[189]. La protection qu'ils offrent

---

[186] Wolfram GIESEKE, *PC 100 % Pratique, Sécurité et Protection*, traduction de C. STOLL, H. BERTRAND et P. M. WOLF, Paris, Micro Application, 1998, p. 409 et ss.

[187] Un des géants de ce domaine est l'entreprise DoubleClick. Celle-ci, grâce à des bannières sur les sites Web, suit le cheminement des Internautes. À l'heure actuelle, DoubleClick n'est pas en mesure d'identifier spécifiquement un individu, mais elle peut déterminer que parmi les visiteurs d'un site Web spécifique, 60% ont visité le site de l'entreprise A, 15 % le site de l'entreprise B et 30 % le site de l'entreprise C. Ainsi, Doubleclick est en mesure de dresser un profil du consommateur potentiel.

[188] La technologie ActiveX a été développée par Microsoft comme une alternative à Java, cette technologie permet d'inclure des programmes exécutables sous forme de contrôles ActiveX dans des pages Web. Les contrôles ActiveX apparaissent dans les navigateurs sous forme d'images interactives permettant aux utilisateurs d'exécuter certaines fonctions.

Les contrôles ActiveX sont des fichiers binaires directement exécutables. La technologie ActiveX ne répond pas à l'impératif d'indépendance par rapport aux plates-formes, qui est la caractéristique principale de Java. Les contrôles ActiveX doivent être implémentés et compilés spécialement pour chaque plate-forme.

Côté sécurité, les contrôles ActiveX étant des fichiers binaires directement exécutés par le processeur, il est pratiquement impossible de réglementer les accès qu'ils effectuent. Un contrôle ActiveX qui fonctionne sur un ordinateur dispose d'un accès pratiquement illimité au processeur, à l'ensemble des fichiers du poste de travail et à toutes ses ressources. Ainsi, le niveau d'insécurité d'ActiveX est très élevé. Wolfram GIESEKE, *PC 100 % Pratique, Sécurité et Protection*, traduction de C. STOLL, H. BERTRAND et P. M. WOLF, Paris, Micro Application, 1998, p. 369 et ss. et PUBLICATIONS DU QUÉBEC, *Terminologie d'Internet*, http://www.olf.gouv.qc.ca/ressources/internet/fiches/2075162.htm

[189] Wolfram GIESEKE, *PC 100 % Pratique, Sécurité et Protection*, traduction de C. STOLL, H. BERTRAND et P. M. WOLF, Paris, Micro Application, 1998, p. 412.

est toutefois limitée. Un internaute pourra soit demander d'être avisé, d'accepter ou de refuser tous les témoins. Néanmoins, demander à être avisé de tous les témoins pourra importuner excessivement étant donné que l'on compte généralement plusieurs témoins par site Web. En contrepartie, autoriser complètement l'utilisation de ces témoins permet à ceux-ci de s'installer à l'intérieur de l'ordinateur avec les conséquences qui en découlent. Décider de refuser complètement les témoins entraînera bien souvent un refus d'accéder à différents sites Web qui désirent absolument déposer un témoin sur les ordinateurs de leurs visiteurs[190]. Dans un cas comme dans l'autre, l'internaute est perdant. En conséquence, l'effacement du fichier de témoins après chaque séance de navigation sur Internet peut s'avérer une solution intéressante. Il est évident que l'utilisation des témoins dans le commerce électronique porte atteinte à la vie privée des internautes, malgré le fait que certaines entreprises les qualifient d'usage et de pratique de commerce[191].

À l'heure actuelle, la meilleure protection contre ces témoins est proposée par des programmes spéciaux, tels Guard Dog[192] et Cookie Pal[193], qui nettoient régulièrement l'ordinateur d'un internaute tout en lui donnant la possibilité d'avoir accès aux sites conditionnés par l'utilisation des témoins.

À défaut d'interdire l'utilisation des témoins qui ne servent qu'en réalité à mieux cibler les consommateurs potentiels, les navigateurs devraient par défaut être configurés pour les refuser et ainsi, apporter une certaine protection aux internautes non-informés de cette pratique.

---

[190] « Outre de nombreux magasins virtuels, l'internaute ne pourra plus accéder à certains sites Web très utiles, comme les bases de donnés du support technique de Microsoft. » Wolfram GIESEKE, *PC 100 % Pratique, Sécurité et Protection*, traduction de C. STOLL, H. BERTRAND et P. M. WOLF, Paris, Micro Application, 1998, p. 415.

[191] De plus, Jacques Georges BITOUN, avocat à la Cour d'Appel de Paris, se questionne à savoir si « l'usage des cookies, véritable squatter des disques durs, intrus volontaires, alien des réseaux dans sa mécanique même d'implantation ne caractérise-t-il pas une intrusion frauduleuse dans un système de traitement automatisé ? », George BITOUN, *De la protection de la vie privée : des cookies indigestes*, 23 avril 1997, http://www.grolier.fr/cyberlexnet/COM/A970423.htm

[192] http://store.mcafee.com/product.asp?ProductID=25&CategoryID=12

[193] http://www.kburra.com/

2. L'immatriculation du processeur Pentium III d'Intel

Le 26 février 1999, la compagnie Intel[194] lança sa toute nouvelle génération de processeurs Pentium, soit le Pentium III. Après le Pentium, le Pentium Pro et le Pentium II, le Pentium III est la quatrième mouture de ce processeur depuis 1993.

D'un point de vue technique, le Pentium III conserve les grandes spécifications de son prédécesseur ; le Pentium II[195]. Toujours équipé de la technologie MMX, il reçoit désormais 70 nouvelles instructions destinées à accélérer la manipulation d'images en trois dimensions, de vidéo en plein écran et du son en temps réel. L'ajout de la technologie SIMD[196] permet d'exécuter en une seule et unique opération, ce qui en prenait jusqu'à six par le passé. Intel qui propose actuellement des versions fonctionnant à 450 MHz et 500 MHz, prévoit augmenter prochainement la vitesse de son processeur jusqu'à 600 MHz et 800 MHz.

L'ajout le plus marquant du Pentium III, celui qui a créé une polémique quelques semaines avant sa commercialisation est le numéro de série unique (PSN)[197], une espèce d'empreinte digitale de l'âge numérique que l'entreprise a intégrée à tous ses processeurs Pentium III. Aux dires d'Intel, le but premier de ce numéro de série était d'améliorer la sécurité des transactions électroniques en permettant l'authentification des usagers lors des transactions électroniques.[198] En contrepartie, pour Barry Steinhardt de l'ACLU, cette mesure a comme conséquence de faire disparaître l'anonymat et de permettre de suivre les déplacements des internautes[199]. En effet, d'après ce que reconnaît la division française d'Intel, le PSN est l'outil rêvé pour les professionnels du e-marketing : « certains sites pouvant utiliser ce numéro pour générer

---

[194] http://www.intel.com

[195] INTEL, « Intel Pentium III Processor », http://developer.intel.com/design/pentiumiii/details.html

[196] Pour une analyse détaillée à ce sujet : PC EXPERT, « Les promesses du Pentium III », 12 mars 1999, http://www.zdnet.fr/prod/syst/proc/a0007225.html

[197] Le Processeur Serial Number (PSN) est un identifiant destiné à être inscrit en dur dans la mémoire d'un ordinateur sous la forme d'un numéro de série pouvant être utilisé pour identifier le poste de l'utilisateur.

[198] « As part of its new initiative to create a connected world of trusted PCs, Intel has incorporated a number of security initiatives, including a random number generator and marking electronically every processor with a unique serial number. » Robert LEMOS, « Intel: We won't track ID chips », 21 janvier 1999, *ZDNet*, http://www.zdnet.com/zdnn/stories/news/0,4586,2191233,00.html et INTEL, « Numéro de série des processeurs Intel », http://www.intel.fr/français/pentiumiii/utility.html

[199] Robert LEMOS, « Intel to electronically ID chips », 21 janvier 1999, http://www.zdnet.com/zdnn/stories/news/0,4586,2189721,00.html

un numéro unique pour ainsi fidéliser l'internaute à leurs services ou contrôler les accès »[200].

Face à cette polémique et suite aux recommandations de la Commission européenne, Intel a changé sa politique au niveau mondial. Elle a décidé, au début de l'été 1999, de désactiver par défaut le PSN seulement dans les ordinateurs offerts au grand public[201]. En revanche, le PSN inséré dans le matériel professionnel n'a pas été désactivé étant donné que sur les lieux de travail, les moyens de pistages[202] sont déjà en place et que le PSN n'est, jure Intel, qu'un outil efficace de gestion et de maintenance du parc informatique. Toutefois, dans l'une ou l'autre de ces situations, il sera toujours possible d'activer[203] ou de désactiver[204] le numéro de série de leur ordinateur.

Malgré que l'entreprise offre gratuitement l'utilitaire *PSN Utility* qualifié de « tableau de bord » et qui indique à l'utilisateur d'un ordinateur si le PSN est actif ou non, la CNIL regrette que la procédure de désactivation du numéro de série ne soit pas physique plutôt que logique.

Le regret de la CNIL s'est transformé en crainte lorsque peu de temps après cette annonce, l'entreprise montréalaise Zero Knowledge Systems a créé une application ActiveX dissimulable dans un bandeau[205] d'un site Web qui permet de lire le PSN et ce, même s'il a été désactivé[206]. Ainsi, étant donné que les logiciels utilisés pour interroger

---

200 Jerome THOREL, « Le tatouage du Pentium III n'a pas résisté aux critique », 23 novembre 1999, *ZDNet*, http://zdnet.fr/actu/soci/demo/a0011652.html

201 « Néanmoins, il semble qu'on ne puisse pas être certain à 100% qu'un ordinateur neuf acheté à l'automne 1999 incorpore les nouvelles fonctions. À la question : À quelle date est-on sûr – que l'on soit en Europe, aux États-Unis ou ailleurs – que le BIOS de l'ordinateur neuf est à jour ?, le fondateur d'Intel n'a pu se prononcer. » Néanmoins, le magazine ZDNet a diffusé un utilitaire qui détecte l'état du PSN dans le BIOS. Jerome THOREL, « Le tatouage du Pentium III n'a pas résisté aux critique », 23 novembre 1999, *ZDNet*, http://zdnet.fr/actu/soci/demo/a0011652.html

202 Tel l'adresse IP permanente et le nom d'usager de l'employé sur l'intranet.

203 L'utilisateur pourra le configurer de manière à ce qu'il lui demande explicitement son autorisation avant qu'un site Web puisse lire son PSN.

204 Désactivé, le PSN n'est pas une mince affaire puisqu'il faut agir sur le BIOS, c'est-à-dire le programme primaire d'un ordinateur, inscrit sur la carte mère et qui démarre avant le système d'exploitation lors de la mise sous tension de l'ordinateur.

205 Petite annonce comportant une image ou un bref message, qui est affichée généralement dans le haut de la page d'accueil d'un site Web, le plus souvent à caractère commercial, et sur laquelle l'internaute est invité à cliquer. PUBLICATIONS DU QUÉBEC, *Terminologie d'Internet*, http://www.olf.gouv.qc.ca/ressources/internet/fiches/8385012.htm

206 ZERO KNOWLEDGE SYSTEMS, « Zero-Knowledge Systems exposes failure of Intel's Pentium III serial number control utility », 10 mars 1999, http://www.zeroknowledge.com/company/pressrel.asp?rel=03101999, et WIRED NEWS, « News Pentium III Security Flaw? », 11 mars 1999, http://www.wired.com/news/news/business/story/18395.html.

les processeurs ne sont pas sécurisés, il est potentiellement possible pour un connaisseur d'usurper le PSN afin de s'en servir de nouveau[207].

L'intégration des numéros de séries sur les processeurs d'Intel se situe entre l'immatriculation des automobiles et les afficheurs téléphoniques[208]. Dès qu'un utilisateur achète un processeur Pentium III, il est possible de connaître le PSN de cet ordinateur, à moins qu'il n'en existe pas physiquement. Aux dires de l'ACLU, Intel offre d'un côté une prétendue sécurité pour les transactions électroniques et de l'autre, une pure intrusion dans la vie privée de ses utilisateurs en les traquant individuellement sur la toile[209]. Malgré le fait qu'Intel énonce qu'elle n'avait aucunement l'idée de conserver et d'établir des banques de données à l'aide de ces numéros de séries, « the temptation down the road for someone to keep a database will, most likely, be too great. It will happen[210]. »

Plusieurs associations américaines comparent le Pentium III à une désintégration de la vie privée sur la toile et en conséquence, appellent les internautes au boycott du processeur du Pentium III[211]. De plus, un site Web intitulé Big Brother Inside[212], parodiant le slogan « Intel Inside » de l'entreprise, a pris naissance pour contrer ce phénomène. L'instauration du numéro de série dans les processeurs Pentium III a créé un système totalement centralisé autour de l'utilisateur auquel un numéro unique est rattaché. Comparativement aux témoins qui appartiennent à chaque site Web et qui peuvent être effacés, le numéro de série quant à lui, peut traquer et épier tous les faits et

---

[207] À ce sujet, le cryptographe Bruce Schneier énonce : « En tant que cryptographe, je ne peux pas concevoir un système sécurisé pour valider une identification, renforcer la protection contre la copie ou protéger le commerce électronique en utilisant un simple tatouage du processeur. Cela n'apporte rien, c'est simplement facile à pirater », Bruce SCHNEIER, « Du tatouage du Pentium III », 25 mars 1999, *ZDNet*, http://www.zdnet.fr/actu/mate/proc/a0005395.html.

[208] La Cour suprême des États-Unis a confirmé l'existence d'un droit à l'anonymat dans certaines situations où la divulgation de l'identité pourrait embarrasser ou stigmatiser une personne. *Barasch* c. Bell Telephone of Pennsylvania, 605 A. 2d, 1198 (1992). Voir Matthew J. RINALDO, « Caller ID and Fair Credit Reporting : Technology and Traditional Notions of Privacy Clash (includes Draft Amendments to the Fair Credit Reporting Act) (Reflections from the House & Senate) », (juillet 1992) 16 *Seton Hall Legislative Journal* 403-453 et Laurie Lee THOMAS, « U.S. Telecommunications Privacy policy and Caller ID », (Automne 1993) 30 *California Western Law Review* 1-60.

[209] Robert LEMOS, « Intel: We won't track ID chips », 21 janvier 1999, *ZDNet*, http://www.zdnet.com/zdnn/stories/news/0,4586,2191233,00.html

[210] Robert LEMOS, « Intel to electronically ID chips », 21 janvier 1999, *ZDNet*, http://www.zdnet.com/zdnn/stories/news/0,4586,2189721,00.html

[211] CNET, « How serious is Pentium III's privacy risk ? », 11 mars 1999, http://www.news.com/News/Item/0,4,33650,00.html

[212] http://www.bigbrotherinside.com

gestes d'un internaute sur la toile. Le moindre mouvement de souris est ainsi immédiatement attribué à son auteur.

En tenant compte de tous les problèmes soulevés par ce processeur, le but premier visé par Intel tombe à l'eau. Les associations de protection de la vie privée s'inquiètent éperdument des dérives potentielles qui peuvent être attribuées à ce PSN. Ce numéro deviendra une information très importante pour les commerçants qui n'hésiteront pas à le demander[213] ou à le prendre sans le consentement de l'utilisateur.

En conséquence, étant donné qu'Intel a énoncé qu'elle n'a jamais envisagé la création de banques de données découlant des informations recueillies, à quoi donc peut servir ce fameux numéro de série?[214] Une « e-taxe » peut-être ![215]

3. Le moteur de recherche de groupes de discussion Deja.com

Une saga entourant le légendaire moteur de recherche de groupe de discussion Deja.com[216] a pris naissance le 29 avril 1999.

Le site Web Deja.com, fondé par Steve Madere en 1995 et anciennement connu sous le nom de Deja News[217], est le premier site dédié exclusivement aux groupes de discussions. Le site qui contient en outre un service de recherche et d'archivage des forums de discussion usenet[218], offre un service gratuit donnant accès à plus de 45 000

---

[213] Ce phénomène qui existe déjà avec les témoins, peut très bien se transposer aux PSN.

[214] Pour d'autres problématiques faisant appel à des numéros de série pour identifier les utilisateurs du réseau Internet, voir à ce sujet l'article de Chris OAKES qui traite d'un logiciel permettant de modifier le curseur de la souris des visiteurs de certains sites Web et qui assigne un numéro de série distinct à chaque utilisateur. Chris OAKES, « Mouse Pointer Records Clicks », 30 novembre 1999, *Wired,* http://wired.lycos.com/news/print/0,1294,32788,00.html.

Voir aussi FREZZA qui traite de la création du standard Ipv6 qui remplacera le Ipv4 utilisé présentement pour définir le format des adresses IP. La proposition des ingénieurs de l'Internet Engineering Task Force qui vise à inclure dans les adresses IP un identifiant unique à chaque ordinateur branché à Internet, n'a rien pour plaire aux défenseurs de la vie privée. « Where's all the outrage about the Ipv6 privacy threat ? », 4 octobre 1999, *Internet Week*, http:///www.techweb.com/se/directlink.cgi?INW19991004S0052

[215] « The ID chips could only mean one thing: E-tax. This way the man will be able to track individuals to tax them on electronic commerce », Joel DEANE, « What you think about ID chips », *ZDNet*, http://www.zdnet.com/zdnn/stories/news/0,4586,2190801,00.html

[216] http://www.deja.com

[217] Le 10 mars 1999, la compagnie a changé son nom et son adresse Web pour Deja.com. Avec cette refonte, Deja.com veut passer du moteur de recherche de groupes de discussion qu'elle était à une grande communauté Web. Le nouveau site offre plusieurs nouveautés comme les Deja Ratings et amorce une orientation marquée vers le commerce électronique. Voir DEJA.COM, « Deja News Introduces Next Generation Service, Changes Name to Deja.com », 10 mai 1999, http://www.deja.com/corp/press_archives/dnpr_990510.shtml,

[218] Le réseau usenet est un réseau mondial distribué de forums de discussion appelés groupes de nouvelles, constitué d'un ensemble de serveurs où sont centralisés des articles traitant de sujets particuliers et auxquels

forums de discussion. L'entreprise qui se finance à l'aide de la vente de publicité sur son site trône au sommet de sa catégorie avec plus de six millions de pages visionnées par jour[219].

Au courant du mois d'avril 1999, Richard Smith, président de Phar Lap Software et désormais connu pour avoir identifié l'auteur du virus « Melissa »[220] au début de la même année, a trouvé une faille portant préjudice au respect de la vie privée des utilisateurs du site Deja.com[221]. Il a découvert que depuis plus d'un an, l'entreprise accumulait des renseignements contenus dans les courriels acheminés à partir de son site[222].

En principe, pour répondre à un courriel affiché sur le site Deja.com, il suffit de cliquer sur l'adresse de courrier de l'auteur d'un message pour faire parvenir des réponses privées à l'auteur. Toutefois, en analysant l'adresse du destinataire du message réponse, on découvre que celle-ci ne désigne pas seulement l'adresse de courriel de l'auteur. L'adresse de courriel est remplacée par un lien hypertexte qui permet d'envoyer le message à son destinataire et qui fait parvenir une copie du message à l'entreprise Deja.com[223]. Ainsi, pour chaque courriel qui transige par les serveurs de l'entreprise, une copie de chaque courriel est automatiquement copiée et archivée. En conséquence, Deja.com peut sans contredit retrouver tous les messages envoyés par un utilisateur et par le fait même, établir des profils psychologiques[224]. Cette pratique qui a duré un peu plus d'un an, a permis à l'entreprise d'accumuler une quantité importante

---

les internautes ont accès sur demande. PUBLICATIONS DU QUÉBEC, *Terminologie d'Internet*, http://www.olf.gouv.qc.ca/ressources/internet/fiches/2075064.htm

[219] DEJA.COM, « Deja.com Overview », http://www.deja.com/corp/about.shtml

[220] Pour plus d'informations au sujet du virus Melissa, voir le dossier confectionné par le magazine *ZDNet*. http://www.zdnet.com/zdnn/special/melissavirus.html

[221] Will RODGER, « Deja News privacy snafu uncovered », 29 avril 1999, *ZDNet*, http://www.zdnet.com/zdnn/s...ews/0,4586,2249764,00.html?chkpt=hpqs01.html

[222] Selon Tom Philips, président et directeur exécutif de Deja.com, la collecte des informations s'effectuait à leur insu et de façon accidentelle. « The unintentional result has been that when a user has clicked on the e-mail link in a discussion posting, we have recorded information about that link, including the intended recipient's e-mail address. » Will RODGER, « Deja News to stop tracking addresses », 4 mai 1999, *ZDNet*, http://www.zdnet.com/zdnn/stories/news/0,4586,2252593,00.html. Richard Smith ajoute : « We don't know exactly what they're doing with those addresses. I don't think they understand what they've created. », Will RODGER, « Deja News privacy snafu uncovered », 29 avril 1999, *ZDNet*, http://www.zdnet.com/zdnn/s...ews/0,4586,2249764,00.html?chkpt=hpqs01.html

[223] Par exemple: http://www.deja.com/[ST_rn=qs]/jump/mailto:aaaaaaa@bbbbbbb.ccc.

Paul FESTA, « Deja News to terminate email trail », 4 mai 1999, *CNET*, http://www.news.com/News/Item/0,4,36104,00.html

[224] Gaëlle VACHER, « Deja News opte pour la confidentialité », 6 mai 1999, *ZDNet*, http://www.zdnet.fe/cgi-bin/a_actu.zd&ID=9176&Rub=2&Dat.html

de renseignements personnels reliant les individus à leur famille et leurs amis ; ce dont les grandes compagnies de marketing rêvent depuis longtemps déjà.

Membre de l'organisme TRUSTe[225], Deja.com diffuse sur son site un énoncé de ses engagements en matière de protection des données et du respect de la vie privée[226]. Toutefois, il n'est fait aucune allusion à cette pratique dans celui-ci. Alerté de cette pratique douteuse, TRUSTe a pris la question au sérieux et a fait des recommandations à l'entreprise[227]. En contrepartie, suite aux différentes plaintes formulées par les groupes de protection de la vie privée et l'éditeur du Privacy Times, Deja.com a réglé le problème en arrêtant cette pratique douteuse et en certifiant qu'elle avait détruit les informations recueillies auparavant.

Le problème résultant du site Web de Deja.com n'est pas unique en soi. Les problèmes liés à la protection de la vie privée qui subsistent présentement aux États-Unis et particulièrement sur le réseau Internet, résultent du fait qu'il n'existe pas de politique nationale sur la protection de la vie privée sur la toile. Evan Hendricks, avocat et éditeur du Privacy Times, résume bien la situation. « Deja News has a good instincts. When something stinks, they throw it out[228]. » Hendricks requiert donc une meilleure protection de la vie privée et des renseignements personnels sur le réseau Internet.

---

[225] Pour plus d'informations au sujet de cet organisme, nous envoyons le lecteur au deuxième chapitre de la seconde partie de la présente étude.

[226] DEJA.COM, « Deja.com Statement on Privacy - for Members and Visitors », http://www.deja.com/info/privacy.shtml

[227] Will RODGER, « Deja News privacy snafu uncovered », 29 avril 1999, *ZDNet*, http://www.zdnet.com/zdnn/s...ews/0,4586,2249764,00.html?chkpt=hpqs01.html

[228] Will RODGER, « Deja News privacy snafu uncovered », 29 avril 1999, *ZDNet*, http://www.zdnet.com/zdnn/s...ews/0,4586,2249764,00.html?chkpt=hpqs01.html

4. *Les agents intelligents*

L'ascension fulgurante que connaît le commerce électronique depuis le milieu des années quatre-vingt-dix a aussi apporté sa part d'inquiétude auprès des défenseurs de la vie privée. L'utilisation de plus en plus prononcée des agents intelligents a, entre autres, suscité de nombreuses inquiétudes auprès de la communauté internaute lorsque Microsoft a acheté l'entreprise Firefly, propriétaire de l'agent intelligent du même nom[229].

L'immense quantité d'informations disponibles sur le réseau complique, tant pour l'acheteur que pour le vendeur, les transactions commerciales. Il y a quelques années, au moment où les agents intelligents sont apparus sur Internet, ces derniers étaient vus comme une excellente solution visant à faciliter les transactions électroniques. Aujourd'hui, la multitude d'agents intelligents récoltent souvent beaucoup plus d'informations qu'ils nous le laissent croire[230].

Les agents intelligents englobent une large famille d'applications logicielles qui permettent d'automatiser un certain nombre de tâches[231]. « An agent is a software thing that knows how to do things that you could probably do yourself if you had the time[232]. » Pour sa part, Stern les définit ainsi :

> « *The term typically refers to a program (sometimes AI-based though usually just a template or smart form) which tracks someone's behaviour and "learns" from it - for example, a word processor which monitors keystrokes and tries to predict the next letter or word, or an interest profile program that notes the articles selected by a subscriber to a news feed and refines the profile accordingly*[233]. »

---

[229] John MARKOFF, « Microsoft Enters Debate Over Online Privacy by Buying Firefly », 10 avril 1999, *New York Times*, http://search.nytimes.com/search/daily/bin/fastweb?getdoc+site+site+67537+4+wAAA+p3p

[230] Par exemple, le site Bargainbot (http://www.ece.curtin.edu.au/~saounb/bargainbot/) offre un service permettant de trouver un livre au meilleur prix possible sur Internet, alors que Firefly (http://www.firefly.com) offre des recommandations pertinentes en tenant compte des goûts musicaux et cinématographiques de l'utilisateur. Finalement, The Movie Critic (http://www.moviecritic.com) recommande à des utilisateurs indécis, des films à visionner selon leurs goûts et intérêts.

[231] L'agent est un concept qui a environ 25 ans. Il recouvre des réalités aussi disparates que la simple commande macro d'Excel ou de Word jusqu'aux systèmes complexes d'intelligence artificielle, capables d'apprendre, de détecter des crises et de formuler des recommandations. Mark NISSEN, « Intelligent Agents: A Technology and Business Application Analysis », 30 novembre 1995, http://www.ai.univie.ac.at/~paolo/lva/vu-sa/html/heilmann/ et Raphaël RICHARD, « Le Rôle des Agents Intelligents », 18 juin 1998, *Planète Commerce*, http://www.planete-commerce.com/agents98/.

[232] Citation de Ted SELKER du IBM Almaden Research Center cité dans Björn HERMANS, « Intelligent Software Agents on the Internet: An Inventory of Currently Offered Functionality in the Information Society and a Prediction of (Near) Future Developments », *First Monday*, http://www.firstmonday.dk/issues/issue2_3/ch_123/

[233] Michael STERN, « Mobile Agents: Providing Control to the Consumer », présenté dans le cadre du *Fifth Conference on Computer, Freedom and Privacy*, Conférence organisée par le Board of Trustees de l'Université Leland Stanford, juin-juillet 1994, http://www.techlaw.stanford.edu/CFP95.Program.html

Généralement, un agent intelligent regroupe six propriétés :

1. *« **Autonomy** : agents operate without the direct intervention of humans or others, and have some kind of control over their actions and internal state ;*
2. ***Social Ability** : agents interact with other agents and (possibly) humans via some kind of agent communication language ;*
3. ***Reactivity** : agents perceive their environment and respond in a timely fashion to changes that occur in it. This may entail that an agent spends most of its time in a kind of sleep state from which it will awake if certain changes in its environment give rise to it ;*
4. ***Proactivity** : agents do not simply act in response to their environment, they are able to exhibit goal-directed behavior by taking the initiative ;*
5. ***Temporal Continuity** : agents are continuously running processes (either running active in the foreground or sleeping/passive in the background), not once-only computations or scripts that map a single input to a single output and then terminate ;*
6. ***Goal Orientedness** : an agent is capable of handling complex, high-level tasks. The decision how such a task is best split up in smaller sub-tasks, and in which order and in which way these sub-tasks should be best performed, should be made by the agent itself*[234].

Il existe présentement sur Internet deux catégories d'agents intelligents. Premièrement, il y a les agents d'analyse de l'offre dont le but premier est la recherche d'informations. Dans un contexte commercial, ces agents peuvent renseigner un utilisateur [235].

---

[234] Björn HERMANS, « Intelligent Software Agents on the Internet: An Inventory of Currently Offered Functionality in the Information Society and a Prediction of (Near) Future Developments », *First Monday*, http://www.firstmonday.dk/issues/issue2_3/ch_123/

[235] Simon St-Laurent, *Cookies*, Computing McGraw-Hill, New York, 1998.

À ce sujet, Björn Hermans ajoute : « Agents that fit the stronger notion of agent usually have one or more of the following characteristics :

1. Mobility: the ability of an agent to move around an electronic network;
2. Benevolence: is the assumption that agents do not have conflicting goals, and that every agent will therefore always try to do what is asked of it;
3. Rationality: is (crudely) the assumption that an agent will act in order to achieve its goals and will not act in such a way as to prevent its goals being achieved - at least insofar as its beliefs permit;
4. Adaptivity: an agent should be able to adjust itself to the habits, working methods and preferences of its user;
5. Collaboration: an agent should not unthinkingly accept (and execute) instructions, but should take into account that the human user makes mistakes (e.g. give an order that contains conflicting goals), omits important information and/or provides ambiguous information. For instance, an agent should check things by asking questions to the user, or use a built-up user model to solve problems like these. An agent should even be allowed to refuse to execute certain tasks, because (for instance) they would put an unacceptable high load on the network resources or because it would cause

- Sur la disponibilité d'un produit en effectuant une recherche par marque ou par catégorie ;
- Sur l'identification des distributeurs d'un produit en tenant compte ou non de différentes spécificités ;
- En traitant les informations collectées par la création de tableaux comparatifs selon différents critères ;
- En établissant une présélection automatique d'articles en fonction des préférences de l'utilisateur ; et/ou
- En réalisant la transaction de façon automatique ou semi-automatique.

En fonction des critères prédéterminés par l'utilisateur, l'agent d'analyse de l'offre tente de trouver le meilleur produit reflétant les objectifs prédéterminés par l'utilisateur. En conséquence, cette catégorie d'agents existe seulement pour soulager la tâche des internautes désireux de retrouver un produit spécifique sur le réseau.

Si les agents les plus spectaculaires sont ceux qui s'adressent aux consommateurs, il n'en reste pas moins que les plus utiles aux entreprises proviennent de la seconde catégorie. Le second type d'agents se spécialisent dans l'analyse de la demande globale dans le but de permettre aux entreprises d'adapter leurs nouvelles offres aux besoins du marché[236]. De tels agents qui existent présentement sur plusieurs sites, permettent aux entreprises :

- L'enregistrement du profil et des préférences des internautes grâce aux informations générales recueillies par des questionnaires. Celles-ci peuvent refléter les goûts, les types de produits consommés, etc.

  En conséquence, lors d'une prochaine visite sur le site en question, l'utilisateur recevra, entre autres, un accueil personnalisé et des propositions commerciales personnalisées.

- L'enregistrement des demandes successives d'un consommateur.

  Ceci permettra aux entreprises de suivre en temps réel l'évolution des profils des consommateurs pour en principe, mieux les servir. Ces agents établissent des synthèses des demandes successives faites par les internautes et des tests ponctuels d'analyse de la demande dans le temps.

---

damage to other users. » Björn HERMANS, « Intelligent Software Agents on the Internet: An Inventory of Currently Offered Functionality in the Information Society and a Prediction of (Near) Future Developments », *First Monday*, http://www.firstmonday.dk/issues/issue2_3/ch_123/

[236] Une des plus célèbres entreprises dans ce domaine est Broadvision (http://www.broadvision.com), qui, créée en 1993, se consacre au développement de systèmes intégrés de gestion des relations de marketing individualisés, c'est-à-dire le « marketing one-to-one ».

- D'effectuer des recommandations sur l'évolution de l'offre commerciale.

  Ces agents ont accès à des statistiques sur la demande globale des consommateurs et sont à même d'analyser les raisons de leurs succès ou de leurs échecs pour ainsi proposer des recommandations quant aux orientations futures de la politique commerciale de leur société [237].

L'utilisation de ces agents entraîne une méfiance croissante des internautes vis-à-vis les entreprises qui font appel à ces agents. La masse d'information et de renseignements personnels que peuvent récolter et emmagasiner ces agents est au cœur du débat. Ils contiennent un nombre important d'informations susceptibles de créer des profils très réalistes.

Ce qui est intéressant avec ces agents intelligents c'est qu'il est possible pour un internaute de ne pas dévoiler tout à fait la vérité. L'utilisateur a le contrôle total sur l'information qu'il donnera à l'agent. Par exemple, rien n'empêche un internaute de ne pas dire toute la vérité aux questions posées. Toutefois, ces systèmes étant basés sur l'analyse des réponses, il se pourrait fortement qu'en contrepartie, les résultats proposés par l'agent intelligent ne soient pas semblables aux goûts de l'internaute. Ainsi, quelle est l'utilité de se servir de l'un de ces agents si l'utilisateur ne lui dit pas la vérité? Néanmoins, il convient de retenir que, dans tous les cas, les informations dévoilées, vraies ou fausses, seront conservées pour que les entreprises puissent mieux cibler leurs futurs consommateurs.

Selon John Markoff, journaliste spécialisé dans les questions de technologies de l'information au « New York Times », le contrôle des internautes sur leurs renseignements personnels ne peut être que bénéfique dans cette ère où ils sont de plus en plus réticents à naviguer sur Internet et où les entreprises s'arrachent les banques de renseignements personnels. Il ajoute en traitant spécifiquement de l'agent Firefly : « The debate among privacy advocates stems from the fact that Firefly's standards represent a compromise between those who want to unleash the power of the Internet to aim individualized advertising in a way never before possible and those who want to curb potential abuses by corporations and government agencies[238]. »

---

[237] Simon St-Laurent, *Cookies*, New York, Computing McGraw-Hill, 1998 et Raphaël RICHARD, « Le Rôle des Agents Intelligents », 18 juin 1998, *Planète Commerce*, http://www.planete-commerce.com/agents98/

[238] John MARKOFF, « Microsoft Enters Debate Over Online Privacy by Buying Firefly », 10 avril, 1999, *New York Times*, http://search.nytimes.com/search/daily/bin/fastweb?getdoc+site+site+67537+4+wAAA+p3p

Malgré la crainte que suscite l'utilisation de ces agents intelligents en ce qui a trait au respect des renseignements personnels[239], il semble qu'ils peuvent, dans une certaine mesure, être bénéfiques pour les consommateurs et les entreprises[240]. Mieux cibler les consommateurs et par le fait même, obtenir le meilleur rapport qualité-prix dans un court laps de temps, peut être avantageux pour les deux parties.

Les professionnels du marketing ont déjà réalisé l'importance de la maîtrise de l'image d'une société sur Internet : Intel en particulier a fait cette expérience à ces frais avec le PSN du Pentium III. Déjà, des sociétés ont franchi une étape supérieure et étudient les réactions de la communauté des internautes en critiquant elles-mêmes leurs propres produits. Lorsque des systèmes d'agents intelligents mesureront la qualité d'un produit grâce aux critiques de consommateur sur Internet, il y a fort à parier que les fournisseurs tenteront de manipuler ces systèmes. La capacité des fournisseurs à prouver leur éthique et leur refus de ce type de procédé deviendra probablement un élément déterminant. De plus, il est sans contredit que l'augmentation du volume des informations collectées sur le consommateur devra s'accompagner de garanties concernant la confidentialité des informations collectées.

5. Un espion sur les sites : Third Voice

La présentation du nouveau logiciel Third Voice au mois de mai 1999 a amorcé une révolution sur Internet en permettant aux visiteurs d'un site Web, d'y laisser leurs commentaires sans que les webmestres[241] ne puissent s'y opposer.

> « *The launch of Third Voice marks the first time Internet users will be able to post their thoughts and opinions directly on any Web site and interact with other visitors on the same page*[242]. »

---

[239] « There are two main types of privacy threats that are posed by the use of Intelligent Software Agents: threats caused by agents acting on behalf of a user (through the disclosure of the user's personal information) and threats caused by foreign agents that act on behalf of others (via traffic flow monitoring, data mining, and even covert attempts to obtain personal information directly from the user's agent). » INFORMATION AND PRIVACY COMMISSIONER / ONTARIO, *Intelligent Software Agents: Turning a Privacy Threat into a Privacy Protector*, Avril 1999, http://www.ipc.on.ca/WEB_SITE.ENG/MATTERS/SUM_PAP/PAPERS/isat.htm

[240] Suzanne SMED, « Intelligent Software Agents and Agency Law », V14 1998, *Santa Clara Computer & High Tech. L.J.* 503, p.504

[241] « Personne dont la principale responsabilité est la maintenance d'un site Web et la bonne marche d'un serveur Web, qui peut également être chargée de la mise à jour ou même de la création des documents Web diffusés par l'organisme auquel elle est rattachée. », PUBLICATIONS DU QUÉBEC, *Terminologie d'Internet*, http://www.olf.gouv.qc.ca/ressources/internet/fiches/2075046.htm

[242] THIRD VOICE, Press release, *Third Voice Launches Affiliates Program*, http://www.thirdvoice.com/about/news.htm

Fondée par Eng-Siong Tan, Vui-Chiap Lam et Thai-Wey Then en septembre 1998, l'entreprise a conçu un logiciel qui permet aux visiteurs de sites Web de devenir des acteurs actifs du réseau. Motivés par la liberté que les webmestres ont de créer des sites dynamiques et animés, les fondateurs offrent aux visiteurs l'habilité d'ajouter leurs idées et leurs opinions sur des sites Web. Dès sa disponibilité sur le réseau, Third Voice a révolutionné l'industrie des logiciels de communications en ligne.

Third Voice est un plugiciel distribué gratuitement et qui fonctionne seulement sur un ordinateur équipé du navigateur Internet Explorer 4[243]. Il permet à un visiteur d'y laisser ses idées et/ou opinions directement sur un site Web. En contrepartie, les graffitis électroniques ne modifient pas le contenu du site, étant donné qu'ils sont en principe sauvegardés sur les serveurs de l'entreprise située à Sillicon Valley.

En pratique, pour visualiser les messages laissés par les autres utilisateurs de Third Voice, le visiteur devra avoir le plugiciel. Lorsqu'un internaute visite un site Web qui contient des messages laissés par d'autres utilisateurs, le plugiciel apparaît sur une portion de son écran et il peut alors les consulter. Chaque message laissé sur le site Web est indiqué par un signet sur lequel le visiteur doit cliquer pour en prendre connaissance. Ces signets se comparent aux « Post-It », ces petits aide-mémoire autocollants.

Third Voice offre de plus la possibilité à ses utilisateurs de choisir la catégorie de messages qu'ils désirent concevoir. La première version du plugiciel permet de concevoir trois catégories de messages. L'utilisateur peut créer des notes personnelles, c'est-à-dire qui sont seulement enregistrées sur l'ordinateur de l'utilisateur et que lui seul peut lire. Il peut aussi concevoir des notes publiques qui sont enregistrées sur les serveurs de l'entreprise Third Voice et qui peuvent être lues par tous les utilisateurs de Third Voice. Finalement, l'utilisateur peut confectionner des notes de groupes qui sont seulement accessibles aux membres d'une communauté virtuelle réunis autour d'un thème prédéfini.

À première vue, ce plugiciel peut avoir maintes utilisations et ce, dans différents domaines. Par exemple, dans le domaine de l'éducation lorsque des textes sont

---

[243] Les versions pour Internet Explorer 5.0 et Netscape Communicator 4.0 devrait être disponible d'ici peu, Glenn MCDONALD, « Third Voice : Invisible Web Graffiti », 18 mai 1999, *PC World*, http://www.pcworld.com/pcwtoday/article/0,1510,11016,00.html

disponibles en-ligne, il permet d'y faire des annotations ou, dans le monde de la consommation, dans la mesure où il permet aux consommateurs de se communiquer des informations sur des produits[244].

Cette nouvelle ère révolutionnaire introduite par Third Voice suscite malgré tous deux questionnements juridiques. La première interrogation juridique qu'amène ce plugiciel réside dans le fait que les messages apposés sur un site Web le sont, sans l'autorisation du webmestre. À l'heure actuelle, il est impossible pour les webmestres de retirer les commentaires publics affichés sur leur site Web[245]. Une fois le message composé, celui-ci peut être attaché à n'importe quel site du World Wide Web, « from the front page of Yahoo.com to the lowest reaches of personal sites », sans que les webmestres ne puissent y faire quoi que ce soit[246].

Selon l'avis de plusieurs avocats américains, Third Voice contrevient directement, par l'apposition de ces messages sur les sites Web, au droit de propriété intellectuelle des créateurs de ces sites[247]. Néanmoins, un débat subsiste présentement à cet effet pour tenter de déterminer si réellement ce plugiciel viole le droit d'auteur des créateurs de sites Web ou si, tel que l'énonce l'entreprise, ce sont les utilisateurs qui ont le plein pouvoir en utilisant le plugiciel[248].

Le second questionnement juridique suscité par le plugiciel Third Voice est plus pertinent à la présente étude. La problématique que soulève le plugiciel provient du système même sur lequel il est conçu, c'est-à-dire le modèle client-serveur. Ce modèle informatique est basé sur le traitement distribué selon lequel un utilisateur lance un

---

[244] Francis PISANI, « Tremblez, journalistes », 19 mai 1999, *Le Monde interactif*, http://www.lemonde.fr/nvtechno/branche/sticker.html

[245] En effet, la difficulté réside dans le fait que ces messages sont sauvegardés sur les serveurs de l'entreprise Third Voice. « Technically there is no means to block Third Voice since reader comments are stored on Third Voice's own server, a completely distinct channel from the site they refer to. » Penelope PATSURIS, « Talking back on the web », 21 mai 1999, *Forbes e-business*, http://www.forbes.com/tool/html/99/may/0521/featb.htm

[246] Stephen BUEL, « Virtual Post-it notes for the Web », 28 mai 1999, *San Jose Mercury News*, http://www.sjmercury.com/business/top/059363.htm

[247] Voir Stephen BUEL, « Virtual Post-it notes for the Web », 28 mai 1999, *San Jose Mercury News*, http://www.sjmercury.com/business/top/059363.htm, Penelope PATSURIS, « Talking back on the web », 21 mai 1999, *Forbes e-business*, http://www.forbes.com/tool/html/99/may/0521/featb.htm, Tom REGAN, « Cyberspace graffiti may be sticking to your site », 20 mai 1999, *The Christian Science Monitor, electronic edition,* http://www.csmonitor.com/durable/1999/05/20/fp14s1-csm.shtml et Kurt KLEINER, « Digital graffiti », 29 mai 1999, *New Scientiste*, http://www.newscientist.com/cgi-bin/pageserver.cgi?/ns/19990529/newsstory5.html

[248] « We do not change or touch the original content, the users themselves have full control. », Stephen BUEL, « Virtual Post-it notes for the Web », 28 mai 1999, *San Jose Mercury News*, http://www.sjmercury.com/business/top/059363.htm

logiciel client à partir d'un ordinateur relié à un réseau et déclenche simultanément le lancement d'un logiciel serveur situé dans un autre ordinateur possédant les ressources souhaitées par l'utilisateur[249]. Plus spécifiquement, dans le cas de Third Voice, l'utilisateur apercevra une petite interface client dans le coin gauche de son navigateur signalant la présence du plugiciel.

L'utilisation de ce modèle informatique soulève un questionnement en ce qui a trait à la protection de la vie privée. Tel qu'il fut discuté auparavant, les messages créés par l'utilisation de plugiciel sont en principe sauvegardés sur les serveurs de l'entreprise avec, pour chaque message, l'adresse du site Web auquel il est rattachée.

Pour afficher les messages afférents à un site Web, le navigateur de l'internaute doit absolument fournir aux serveurs de l'entreprise l'adresse du site Web que l'internaute visite. En conséquence, Third Voice est en mesure de suivre à la trace et sans trop de difficultés les allées et venues de ses utilisateurs. Évidemment, elle a aussi potentiellement accès à tous les messages enregistrés sur ses serveurs. De plus, la collecte de ces adresses URL[250] permet à l'entreprise de créer des profils psychologiques et/ou de consommation qui, au fil du temps, peuvent devenir de plus en plus analogues à ceux des usagers.

En contrepartie, l'entreprise qui est membre de TRUSTe[251], diffuse sur son site Web un énoncé de ses engagements en matière de protection des données et du respect de la vie privée[252]. Toutefois, le problème relié aux adresses Web n'y est pas spécifiquement mentionné. À dire vrai, les engagements énoncés par Third Voice se rapportent seulement à son site Web et non pas à son logiciel.

Cette problématique auquelle est confrontée l'organisme TRUSTe n'est pas unique à Third Voice. En effet, suite une controverse semblable mettant en cause l'entreprise RealNetworks[253], TRUSTe, pour tenter de prouver sa bonne foi, s'est joint à cette

---

[249] PUBLICATIONS DU QUÉBEC, *Terminologie d'Internet*, http://www.olf.gouv.qc.ca/ressources/internet/fiches/2076577.htm

[250] À l'heure actuelle, en vertu des dispositions législatives en vigueur, il serait difficile de qualifier les adresses URL des sites Web comme étant des informations personnelles servant à identifier les usagers.

[251] Pour plus d'information au sujet de cet organisme, nous envoyons le lecteur au deuxième chapitre de la seconde partie de la présente étude.

[252] THIRD VOICE, *Third Voice Privacy Statement*, 2000, http://www.thirdvoice.com/about/privacy.htm

[253] L'édition du 1er novembre 1999 du New York Time, rapportait que le logiciel RealJukebox de l'entreprise RealNetworks répertoriait à leur dépens, les habitudes musicales et l'identité de ses 13,5 millions d'utilisateurs du logiciel. Aux dires de l'entreprise qui distribue gratuitement le logiciel et qui n'avait pas prévenu ses

dernière pour mettre en place un Pilot Privacy Seal Program for Software Applications. À ce sujet, ils édictent : « The recent incident involving RealNetworks prompted a broad set of solutions for addressing consumer concerns about personally identifiable information[254]. » Annoncé depuis le 8 novembre 1999, l'association de ces deux entreprises devait travailler de concert pour présenter un programme complet et fonctionnel dans les six mois suivant leur annonce. Toutefois, à l'heure actuelle, la création de ce programme est toujours à l'étape préliminaire.

Concrètement, TRUSTe et RealNetworks désire concevoir un programme en cinq points visant à regagner la confiance des utilisateurs des logiciels de RealNetworks.

> *« In cooperation with TRUSTe, RealNetworks will :*
>
> 1. ***Conduct a third party audit** : The audit will verify that RealJukebox GUIDs[255] have been disabled and are no longer associated with email or other registration data. TRUSTe and one of the major auditing firms familiar with the fair information requirements of TRUSTe's program will conduct the audit. A report will be issued upon the conclusion of the audit process.*
> 2. ***Update its privacy statement** : The Web privacy statement that has been certified by TRUSTe will be modified to inform consumers that the audit described above is underway.*
> 3. ***Require consumers to 'opt in' to use of GUIDs** : RealNetworks will anonymize GUIDs and require consumers to opt-in to enable the use of this feature.*
> 4. ***Appoint a company privacy officer** : RealNetworks will identify a key privacy officer who is responsible for handling the company's privacy practices and policies, customer privacy complaints, and who will serve as a liaison to TRUSTe.*
> 5. ***Create online privacy consumer education programs** : These programs include educational forums, Web sites, and other*

---

utilisateurs qu'ils étaient identifiés, mis en mémoire, répertoriés et numérotés par un GUID (Globally Unique Identifier), cette façon de procéder ne représente pas une violation de la vie privée. Selon l'entreprise qui affiche un sceau TRUSTe, les informations ne sont pas stockées par la compagnie ou réutilisées par d'autres. Néanmoins, TRUSTe a recommandé à l'entreprise un programme visant à restaurer la confiance de ses usagers. En contre partie, pour Jason Catlett, fondateur et président de Junkbuster : «TRUSTe has proven to be more of a lapdog than a watchdog.» De plus, il ajoute que le retrait du sceau TRUSTe ne diminuerait aucunement les opérations de l'entreprise. Leander KAHNEY, « RealNetworks Probe Begins », 1 novembre 1999, *Wired*, http://www.wired.com/news/print/0,1294,32250,00.html.

[254] « Just as we did more than two years ago with our Web site privacy seal program, TRUSTe will begin working to establish a seal program with oversight on software privacy practices that utilize personal data. » TRUSTe, *TRUSTe & Realnetworks collaborate to close privacy gap: Pilot Privacy Seal Program for Software Applications Initiated*, 2000, http://www.truste.org/about/about_software.html.

[255] Globally Unique IDentifiers (GUID).

communications activities aimed at educating consumers about privacy issues on the Internet[256]*. »*

En conséquence, les sceaux TRUSTe pour les logiciels seront similaires aux sceaux déjà existants concernant les politiques en matière de vie privée. Tel que l'énonce TRUSTe : « The time is ripe now to evolve the program, Regardless of whether you're collecting information on a Web site or from software, you must disclose these practices to the consumer[257]. »

---

[256] Jennifer MACK, « RealNetworks drafts new privacy plan », 8 novembre 1999, *ZDNet*, http://www.zdnet.com/zdnn/stories/news/0,4586,2390239,00.html et TRUSTe, *TRUSTe & Realnetworks collaborate to close privacy gap: Pilot Privacy Seal Program for Software Applications Initiated*, 2000, http://www.truste.org/about/about_software.html.

[257] TRUSTe, *TRUSTe & Realnetworks collaborate to close privacy gap: Pilot Privacy Seal Program for Software Applications Initiated*, 2000, http://www.truste.org/about/about_software.html.

DEUXIÈME PARTIE

LA PROTECTION DES RENSEIGNEMENTS PERSONNELS SUR INTERNET

Chapitre 1

Les diverses solutions préconisées pour la protection des renseignements personnels sur Internet

Les dernières années ont vu s'opposer des conceptions divergentes sur la question des renseignements personnels. Celles-ci se sont surtout cristallisées autours de deux pôles antagonistes : l'Europe et les États-Unis, chacun proposant son modèle au reste du monde. Le premier chapitre de cette étude traitera des diverses solutions préconisées qui découlent de ces deux pôles antagonistes. En premier lieu, nous nous attarderons sur la position européenne qui rejoint la position canadienne et québécoise (A). En deuxième temps, une démarche semblable sera effectuée, mais en analysant plutôt la position américaine et les solutions qu'elle préconise pour protéger les renseignements personnels sur le réseau Internet (B). Finalement, nous concluerons ce chapitre en étudiant la situation conflictuelle engendrée par ces deux positions antagonistes dans un environnement électronique décentralisé qui fait fi des frontières géographiques et politiques (C).

A. L'Europe, le Canada et le Québec

1. La position européenne, canadienne et québécoise

Contrairement aux États-Unis, de nombreux pays font davantage confiance à l'État pour élaborer des dispositifs de protection des renseignements personnels. La plupart des nations européennes ont ainsi, par le passé, promulgué des lois visant à protéger la vie privée de leurs citoyens, tant à l'égard de l'État que des entreprises. Néanmoins, au sein de la Commission européenne, la grande diversité de mise en œuvre de ces dispositifs a amené les individus à s'inquiéter des flux transfrontaliers croissants de données au sein de la Commission[258].

Dans le but d'harmoniser les règles en son sein et d'y favoriser la libre circulation des données, la Commission européenne s'est dotée en 1995 d'une directive s'appliquant à la fois aux secteurs publics et privés, que les technologies de l'information soient

utilisées ou non[259]. Cette directive, obligatoire pour tous les pays membres de l'Union européenne, possède une particularité propre : elle s'applique au-delà des frontières européennes[260].

Entrée en vigueur le 24 octobre 1998 dans chacun des États membres, les principes de la *Directive* visent :

- La récolte des renseignements personnels ;
- L'obtention du consentement de la personne visée ;
- L'exactitude et la sécurité des informations obtenues ; et
- Le traitement loyal de ces informations, ce qui implique l'obligation d'informer les personnes concernées de l'usage qui est fait de leurs renseignements personnels[261].

La *Directive* reconnaît les droits traditionnels des individus, tels les droits d'accès et de rectification des informations, de même que les droits de connaître l'origine des informations et celui de ne pas être soumis à une décision basée sur un portrait personnel produit par un traitement informatisé[262]. Elle comprend ainsi, les principes juridiques en matière de collecte de renseignements qui ont force de loi au Québec et au Canada[263]. En fait, la *Directive* est « intended to protect individual privacy by prohibiting the improper collection, use, and transfer of data relating to individuals, while at the

---

[258] Pour une étude détaillée des critères qui ont amené à l'élaboration de la *Directive*, voir Peter P. SWIRE, « Of Elephants, Mice, and Privacy: International Choice of Law and the Internet », *Draft submitted to International Lawyer*, 23 août 1998, http://www.acs.-ohio-state.edu/units/law/swire1/elephants.htm

[259] En vertu de l'article 4 de la *Directive*, elle s'applique à tous les états membres de l'Union européenne. Toutefois, l'article 25 énonce une condition aux transferts de données à caractère personnel vers des pays tiers.

[260] Une disposition de la *Directive* obligeait les pays européens à adopter leur législation avant le 24 octobre 1998.

De plus, selon le professeur Bennet, la Directive est déjà une norme *de facto* internationale de protection de la vie privée. Colin BENNETT, *Réflexions sur une norme internationale de protection des renseignements personnels*, Conclusions, Groupe de travail sur le commerce électronique d'Industrie Canada, http://e-com.ic.gc.ca/francais/privee/632d29c.html

[261] Peter P. SWIRE, « Of Elephants, Mice, and Privacy: International Choice of Law and the Internet », *Draft submitted to The International Lawyer*, 23 août 1998, http://www.acs-ohio-state.edu/units/law/swire1/elephants.htm

[262] « The Directive is built around a list of rights of data subjects, and duties of data processors, that track, in broad brush, the same fair information handling practices principles described above. In that regard, while the Directive contemplates a greater government role in privacy regulation, it must still be considered fundamentally a « privacy peacemaker » regulation. » Karl D. BELGUM, « Who Leads at Half-time?: Three Conflicting Visions of Internet Privacy Policy », 6 *Rich. J.L. & Tech.* 1, (Symposium 1999), http://www.richmond.edu/jolt/v6i1/belgum.html. Voir aussi : Graham GREENLEAF, «The European Privacy Directive - completed » (1995) 2 *PLPR* 81, http://www.austlii.edu.au/au/other/plpr/vol2/Vol2No05/v02n05a.htm

[263] À ce sujet, lire la section intitulée « Les principes juridiques en matière de collectes » dans le deuxième chapitre de cette étude.

same time encouraging the free movement of personal data among European Union member countries[264]. »

La *Directive* inclut aussi une règle dite de proportionnalité visant à maintenir l'équilibre entre les besoins d'informations et le respect de la vie privée, ne fait toutefois pas l'unanimité auprès des acteurs du réseau. Aux États-Unis, la *Directive* et plus spécifiquement l'article 25 qui traite du transfert de données à caractère personnel vers les pays tiers, fait l'objet de nombreuses critiques par les acteurs américains[265]. En effet, selon la Commission européenne, les États-Unis ne disposent pas d'un niveau de protection adéquat pour y exporter des renseignements personnels[266].

Soucieuse de préserver ce qu'elle considère comme un véritable droit fondamental, la Commission européenne est opposée au système d'autoréglementation américain[267]. De plus, on constate que depuis peu, nombreux sont les pays partenaires commerciaux de l'Union européenne, dont le Canada, qui ont suivi la voie de l'intervention législative pour composer des régimes de protection des renseignements personnels des usagers.

Au Canada, le gouvernement fédéral et la majorité des provinces ont des législations régissant la collecte, l'utilisation, et la communication des renseignements personnels conservés par le secteur public. Néanmoins, seuls le Québec et le gouvernement fédéral disposent d'une loi détaillée visant la protection des renseignements personnels dans le secteur privé. Dans le reste du pays, la protection est sporadique et inégale, ce

---

[264] Susan E. GINDIN, « As The Cyber-World Turns: The European Union's Data Protection Directive and Transborder Flows of Personal Data », Décembre 1997, *Internet Legal Practice Newsletter*, http://www.collegehill.com/ilp-news/gindin1.html

[265] Voir l'article 25 (1) cité à la page 28 de la présente étude.

[266] « Because the Directive provides that data may not be exported from the EU to any country that does not provide roughly equivalent privacy protection, the threat that data flows from the EU to the U.S. will be cut off has prompted extensive negotiations between Clinton administration officials and EU privacy negotiators. The United States' position in those negotiations has been to urge that self-regulatory measures by industry trade associations can constitute adequate protection to qualify members of those associations to receive data flows from entities in the EU. » Karl D. BELGUM, « Who Leads at Half-time?: Three Conflicting Visions of Internet Privacy Policy », 6 *Rich. J.L. & Tech.* 1, (Symposium 1999), http://www.richmond.edu/jolt/v6i1/belgum.html.

[267] Voir le « International Safe Harbor Privacy Principles » qui est un ensemble de règles négociées entre la Commission européenne et les États-Unis pour que les entreprises américaines obtiennent un degré adéquat de protection des données personnelles conformément à la *Directive*. ELECTONIC COMMERCE TASK FORCE, *International Safe Harbor Privacy Principles - DRAFT*, 19 avril 1999, http://www.ita.doc.gov/ecom/shprin.html et ELECTONIC COMMERCE TASK FORCE, *Joint Report on Data Protection Dialogue to the EU/US Summit*, 21 juin 1999, http://www.ita.doc.gov/ecom/jointreport2617.htm. En ce qui a trait aux difficultés liées aux négociations, voir « EU rejects U.S. data privacy protection plan », 23 novembre 198, *Fox Market Wire*, http://www.foxmarketwire.com/wires/1123/f_rt_1123_18.sml et Declan McCULLAG, « Safe Harbor Swimming in Circles », 29 avril 1999, *Wired*, http://www.wired.com/news/print_version/politics/story/19414.html?wnpg=all.

qui suscite l'incertitude chez les entreprises et n'assure pas, par le fait même, une protection uniforme pour les consommateurs[268].

Au moment où certains pensaient que les autorités canadiennes demeureraient à l'ombre de leur puissant voisin, elles ont, au contraire, opté pour la solution européenne. L'adoption de la *Loi sur la protection des renseignements personnels et les documents électroniques* le 13 avril 2000 et rétroactive au 15 octobre 1999, fut une priorité pour le gouvernement canadien[269].

La loi vise à réglementer les activités commerciales impliquant la collecte de renseignements personnels, et oblige les personnes qui se livrent à ces activités à rendre compte de la façon dont elles recueillent, utilisent et divulguent ces renseignements[270]. Elle offre aussi aux particuliers, le droit de déterminer quand, comment et dans quelle mesure ils doivent accepter le partage de leurs renseignements.

Depuis son entrée en vigueur, la loi ne s'applique qu'aux secteurs réglementés par le gouvernement fédéral, tels les banques, les télécommunications et le transport interprovincial. Néanmoins, trois ans après son entrée en vigueur, soit le 15 octobre 2002, la loi s'appliquera à toutes les activités commerciales dans l'ensemble du pays, sauf dans les provinces et territoires qui auront adopté des lois analogues en matière de protection de la vie privée.

Au Québec, il est fort à parier que la *Loi sur la protection des renseignements personnels et les documents électroniques* ne trouvera pas application. La *Loi dans le secteur privé* adoptée en 1993 et mise en vigueur en 1994, offre une protection semblable à la directive européenne[271].

---

[268] INDUSTRIE CANADA, *Groupe de travail sur le commerce électronique : Évolution de la protection des données dans le monde*, http://com-e.ic.gc.ca/francais/fastfacts/43d10.html

[269] Cette loi est l'une des composantes de la Stratégie sur le commerce électronique dévoilé par le gouvernement canadien en octobre 1998. INDUSTRIE CANADA, *Groupe de travail sur le commerce électronique - Vie privée: protection des renseignements personnels*, http://strategis.ic.gc.ca/virtual_hosts/e-com/francais/privee/632d1.html. Pour plus d'informations concernant les discussions entourant la création de cette loi, voir Denis C. KRATCHANOV, « Protection de la vie privée dans le secteur privé », *Annexe M dans le Compte-rendu de la réunion de 1995 de la Conférence pour l'harmonisation de lois au Canada*, 1995, http://www.law.ualberta.ca/alri/ulc/95pro/f95m.htm

[270] Il est important de souligner que la loi ne s'appliquera pas au renseignements personnels de nature non commerciale, tels ceux portant sur la santé et l'éducation, puisque ces domaines sont de compétence provinciale.

[271] Susan E. GINDIN, « As The Cyber-World Turns: The European Union's Data Protection Directive and Transborder Flows of Personal Data », décembre 1997, *Internet Legal Practice Newsletter*, http://www.collegehill.com/ilp-news/gindin1.html, André GIROUX, « La vie privée est-elle protégée : Québec un

L'élaboration de la *Loi sur la protection des renseignements personnels et les documents électroniques* s'est appuyée sur les différents sondages qui ont démontré que les Canadiens sont préoccupés par leur vie privée sur les réseaux informatiques[272]. Le gouvernement a agit rapidement pour clarifier les règles du marché en consultation avec le secteur privé.

Pour clarifier les règles du marché et concevoir une loi facile d'application et surtout conforme aux pratiques déjà existantes de l'industrie, les législateurs se sont inspirés du *Code type de protection des renseignements personnels* de la CSA qui est devenu une norme nationale en 1996[273]. Élaboré par des entreprises, des consommateurs et des gouvernements, le code énonce dix principes visant la protection des renseignements personnels[274].

En conséquence, la *Loi sur la protection des renseignements personnels et les documents électroniques* est une réponse directe à la directive européenne. Selon le commissaire à la vie privée de l'Ontario : « There was [no similar law] in Canada except in the province of Quebec, so Quebec could do business with Europe, but the rest of Canada couldn't[275]. »

---

chef de file dans le domaine », *J. du B.*, Volume 29, Numéro 20, http://www.www.barreau.qc.ca/journal/vol29/no20/viepriveeprotegee.html et Matt FRIEDMAN, « Canada Aligns with EU on Privacy », 20 avril 1999, *Wired*, http://wired.com/news/print_version/politics/story/19210.html?wnpg=all

[272] INDUSTRIE CANADA - BUREAU DE LA CONSOMMATION, *Bulletin trimestriel sur la consommation*, mars 1998, Volume 4, Numéro 1, http://strategis.ic.gc.ca/SSGF/ca01128f.html

[273] La CSA est un organisme sans but lucratif indépendant qui exerce ses activités à l'échelle nationale et internationale. Elle est un chef de file dans le domaine de l'élaboration des normes et de leur application, par l'entremise de la certification des produits, de l'enregistrement des systèmes de contrôle de la qualité et de gestion de l'environnement, et des produits d'information.

Le Canada a été le premier pays du monde à se donner une norme volontaire nationale pour la protection des renseignements personnels. Les ministres fédéraux, provinciaux et territoriaux chargés de l'autoroute de l'information ont convenu de souscrire au code type de la CSA à titre de norme minimum pour la protection de la vie privée dans les différents gouvernements.

Le gouvernement fédéral reconnaît la valeur de la norme volontaire de protection de la vie privée et les efforts déployés par les entreprises et les organisations qui la respectent; il croit cependant opportun d'adopter des mesures législatives pour protéger la vie privée de tous les Canadiens. Voir CANADIAN STANDARDS ASSOCIATION, http://www.csa.ca/

Au sujet du Code type de protection des renseignements personnels de la CSA, voir : Colin J. BENNETT, « The Canadian Standards Association Model Code for the Protection of Personal Information: Reaching Consensus on Principles and Developing Enforcement Mechanisms » dans *Privacy and Self-regulation* - Chapter 4: Elements of a Self-regulatory Regime , http://www.ntia.doc.gov/reports/privacy/selfreg4.htm#4D et Colin J. BENNETT, « Private sector privacy reform in Canada: lessons for Australia », (1997) 4 *PLPR* 61, http://www.austlii.edu.au/au/other/plpr/vol4/no4/61.html

[274] Voir l'annexe 1 de la présente étude.

[275] Matt FRIEDMAN, « Canada Aligns with EU on Privacy », 20 avril 1999, *Wired*, http://wired.com/news/print_version/politics/story/19210.html?wnpg=all

Par cette intervention législative, le gouvernement canadien a rejoint le camp de ceux pour qui la protection des renseignements personnels passe par un corpus juridique.[276]

2. *L'initiative française « Votre Vie Privée » (VVP)*

Destiné à sensibiliser les usagers et les acteurs de l'Internet à la protection et la gestion des renseignements personnels, le concept VVP est une initiative de l'association à but sans lucratif Panor@net.

Créée en janvier 1998 par M^es^ Laurent Caron et Frédéric Monéger, l'association a annoncé, au courant du mois de février 1998, la création du code de bonne conduite VVP. Au sujet de code, ils énoncent :

> *« Nous ne voulons pas qu'Internet et les réseaux de télécommunications transforment le monde en libre service des informations personnelles. [...]*
>
> *Pour prendre la mesure de ce qui est en train de se passer, il suffit de consulter les annuaires et les moteurs de recherche qui indexent tout ce qui se dit sur le réseau*[277]*. »*

Par la création de cette initiative, les fondateurs s'engagent dans un combat pour les droits des usagers dans l'ère de l'information. Ils désirent de plus, mobiliser la conscience des usagers entourant les enjeux de la protection de la vie privée sur Internet. En conséquence, l'initiative vise précisément à contribuer à la création d'un climat de confiance en matière de protection de la vie privée sur Internet.

VVP regroupe sous son appellation tous les éléments de la vie privée au regard duquel un usager du réseau peut légitimement revendiquer ses droits. L'initiative est à la fois un esprit et une vision de la vie privée sur les réseaux informatiques[278]. Pour les acteurs de l'Internet, l'initiative VVP se concrétise par deux options :

- La simple reprise du logo sur un site Web, ou
- La simple reprise du logo et prochainement, par l'adhésion à la charte VVP.

---

[276] Matt FRIEDMAN, « Canadian Privacy Law Dying », 11 juin 1999, *Wired*, http://wired.com/news/print_version/politics/story/20175.html?wnpg=all

[277] PANOR@NET, *Pourquoi l'initiative francophone « VVP » ?*, 1999, http://www.panoranet.org/vvp/actions/pourquoi.htm

[278] PANOR@NET, *Votre Vie Privée : le FAQ*, 1999, http://www.panoranet.org/vvp/vvpfaq.htm

Par opposition aux différentes solutions américaines préconisées, telles TRUSTe et BBBOnLine, l'initiative VVP ne se veut aucunement une initiative d'autoréglementation du réseau Internet. En outre, la France dispose déjà de législations protégeant la vie privée. Nous y reviendrons.

La première option, soit la simple reprise du logo VVP sur un site Web constitue seulement un acte de solidarité avec la campagne de sensibilisation à la protection de la vie privée sur Internet, sans plus, ni moins. Tout site désirant afficher le logo VVP peut l'obtenir en se rendant sur le site Web de l'association. À cet effet, la seule condition est de donner l'adresse URL du site où l'on désire afficher le logo[279]. La procédure est simple et il n'y a aucun frais pour obtenir le logo. Néanmoins, étant donné que l'association ne se veut pas une association d'autoréglementation et surtout, qu'elle n'effectue aucune vérification lors de l'inscription, et ultérieurement, il se peut très bien qu'un site Web prônant l'effigie du VVP ne respecte pas les lois traitant de la protection des renseignements personnels et de la vie privée. Il est donc important de se rendre compte, à l'heure actuelle, que le simple affichage du logo VVP sur un site correspond à un acte de solidarité avec la campagne de sensibilisation à la protection de la vie privée sur Internet et non pas à un site vérifié et approuvé par l'association et qui respecte intégralement les exigences législatives traitant du respect de la vie privée et des renseignements personnels[280].

Néanmoins, la seconde option de l'initiative, soit la future charte VVP, viendra peut-être changer cette vision. Ne disposant à l'heure actuelle que de très peu d'information à son sujet[281], il appert que cette charte sera un engagement supplémentaire pour tous ceux désireux d'afficher leur attachement à de fortes valeurs en matière de vie privée.

La création d'un tel code de bonne conduite devra obligatoirement être conforme aux dispositions législatives françaises en ce qui a trait à la protection de renseignements personnels. La France étant déjà réglementée par plusieurs dispositions législatives

---

[279] PANOR@NET, *Reprenez le logo VVP !*, 1999, http://www.panoranet.org/vvp/actions/logovvp.htm

[280] Ceci est différent des programmes TRUSTe et BBB, où une analyse de la politique en matière de vie privée est effectuée avant d'octroyer un sceau et où il est impossible de copier un sceau et de le déposer par la suite sur un autre site.

[281] De plus, à la suite d'une récente visite sur le site Web de l'initiative VVP, on constate qu'il subsiste présentement un doute quant à la création imminente de cette charte. Le peu d'information disponible et le retrait de l'annonce de la création prochaine de cette charte, laisse planer le doute que cette charte pourrait fort bien être reléguée aux oubliettes.

traitant du respect de la vie privée et des renseignements personnels, les principes prônés par la charte VVP devront, bien entendu, respecter ces dispositions législatives. L'association devra de plus, obligatoirement s'adjoindre d'un moyen pour vérifier les sites Web adhérant à sa charte.

En tenant compte des obligations énoncées dans sa charte, l'association devra être en mesure de faire des vérifications pour établir si les sites Web adhérant à leur charte la respectent intégralement. De plus, il serait important de concevoir un mécanisme de plaintes et de sanctions pour les sites membres qui ne la respecteront pas. Cette condition s'avère extrêmement importante, car sinon, à quoi bon créer une initiative qui sert à sécuriser les usagers sans vérifier les faits et gestes des acteurs ? Contrairement au simple logo VVP qui démontre seulement un acte de solidarité, la charte VVP sera un engagement qui devra être respecté en tout temps par ses adhérents[282].

Finalement, comme on le constate, le rôle de l'initiative est quelque peu confus. Il importe de se questionner sur l'utilité d'une telle initiative dans un pays où il existe une législation sur la protection de la vie privée et un organisme, la Commission nationale de l'information et des libertés (CNIL), chargée de la faire respecter ?

L'évaluation de cent sites français de commerce électroniques publiée par la CNIL au courant du mois d'avril 2000, nous donne une certaine réponse[283]. L'objet de cette étude était de savoir si les entreprises adeptes de la vente en ligne respectent la loi en matière de données personnelles, dont la *Directive*. Comme nous l'avons constaté précédemment, si ces entreprises collectent de nombreuses informations sur leurs visiteurs, telles leurs noms, prénoms et adresses, elles doivent, au minimum, informer ses visiteurs de leurs droits et de la-dite collecte.

Malgré une large partie du bilan considérée comme positif[284], l'autre partie est beaucoup plus préoccupante. Selon cette étude, près de 40% de sites web n'indiquent pas

---

[282] Il est bien facile de créer une apparence de sécurité pour les usagers qui naviguent sur Internet; toutefois, lorsque nous sommes face aux renseignements personnels et à la vie privée des usagers, l'illusion de sécurité doit laisser sa place à une véritable sécurité.

[283] COMMISSION NATIONALE DE L'INFORMATION ET DES LIBERTÉS, *Protection des données personnelles et e-commerce en France*, Avril 2000, http://www.cnil.fr/thematic/them01.htm#100sites

[284] À ce sujet, 96% des sites marchands étudiés sécurisent la transmission des coordonnées bancaires et 70% donnent des informations complémentaires sur le dispositif. 97% des sites, qui ont la volonté de céder les informations à des tiers, informent les internautes de leur droit de s'y opposer. Dernier bon score : 69% des sites comportent une information spécifique sur la loi française Informatique et libertés. Philippe GUERRIER,

l'adresse physique du responsable du site et 55% des sites étudiés n'ont pas été déclarés à la CNIL[285]. Ces conclusions paraissent comme un fossé compte tenu du développement actuel du commerce électronique[286]. Les résultats de cette étude présentés à la conférence européenne des commissaires à la protection des données réunie le 6 et 7 avril 2000 à Stockholm, seront à la disposition du « Groupe 29 », un comité de la Commission européenne, pour promouvoir un label européen autour des renseignements personnels sur Internet.

Étant donné que les règles de transparence appliquées à l'Internet ne sont pas les mêmes dans tous les pays européens[287] et vu qu'il est présentement impossible pour les internautes d'être certain que les sites Web auxquels ils accèdent respectent les lois, la CNIL avec la coopération avec ses homologues européens, désire créer des labels au niveau européen.

> « *Il est impossible pour la CNIL de contrôler chaque site Web. On nous déclare 400 à 500 sites par mois. Nous sommes vingt-huit personnes à la direction juridique. C'est pourquoi nous proposons des labels. Toute une série d'organisations professionnelles se sont mises à en créer. Mais pour le moment, ces labels viseraient davantage à garantir la qualité d'un service commercial. Il faudrait qu'ils prennent en compte le niveau de protection de la vie privée.*
>
> *Il faut agir vite. C'est au moment où l'Internet se démocratise que ces règles de transparence deviennent nécessaires*[288]*.* »

« Un grand site marchand sur deux n'est pas déclaré à la CNIL », 17 avril 2000, *Le Journal du Net*, http://www.journaldunet.com/0004/000417cnil.shtml

[285] Le chiffre de 55% d'entreprises oublieuses est en soi inquiétant, car, « *une très forte corrélation est observée entre la déclaration à la CNIL et la qualité de l'information délivrée aux internautes* ». COMMISSION NATIONALE DE L'INFORMATION ET DES LIBERTÉS, *Protection des données personnelles et e-commerce en France*, avril 2000, http://www.cnil.fr/thematic/them01.htm#100sites

[286] « Nous voulons privilégier la pédagogie. Nous allons envoyer des courriers aux responsables des sites pour les informer des manquements observés. Mais nous ne voulons pas pointer du doigt les sites de manière nominative. Ce n'est pas le rôle de la CNIL », explique Cécile Alvergnat de la CNIL. Philippe GUERRIER, « Un grand site marchand sur deux n'est pas déclaré à la CNIL », 17 avril 2000, *Le Journal du Net*, http://www.journaldunet.com/0004/000417cnil.shtml

[287] La déclaration obligatoire de site n'existe pas partout. Tous les pays n'imposent pas non plus de préciser le lieu où s'exerce le droit d'accès aux informations recueillies sur les internautes. Toutefois, ce travail d'harmonisation est en train de se faire. La CNIL croit qu'il sera achevé dans deux mois, soit avant l'été. Joël BOYER - secrétaire général de la CNIL chargé des affaires juridiques, « Sur le Net, effacer ses traces requiert un savoir-faire », 14 avril 2000, *Libération*, http://www.liberation.fr/multi/actu/20001004/20000414venzc.html

[288] Joël BOYER - secrétaire général de la CNIL chargé des affaires juridiques, « Sur le Net, effacer ses traces requiert un savoir-faire », 14 avril 2000, *Libération*, http://www.liberation.fr/multi/actu/20001004/20000414venzc.html

À la lumière des commentaires de la CNIL, il appert que les fondateurs de l'initiative VVP ont vu juste. L'initiative VVP est sur la bonne voie. Néanmoins, à l'heure actuelle, un usager ne peut se référer en toute sécurité au logo VVP affiché sur un site Web. Malgré l'impression qu'il laisse croire, il n'offre aucune garantie que le site respecte les dispositions législatives en vigueur en France[289].

B. Les États-Unis

1. La position américaine

En ce qui a trait à la protection de la vie privée, les États-Unis font bande à part parmi les nations développées de l'Occident. Tant au niveau fédéral qu'à celui des États, ils ont un ensemble disparate de mesures législatives[290]. À cet effet, un abrégé de la législation internationale sur la protection des renseignements personnels intitule comme suit son chapitre sur la législation américaine : « Les États-Unis, premiers en technologies et derniers en protection des données[291]. »

À la conférence des commissaires à la protection internationale des renseignements personnels de 1994, Evan Hendricks a déclaré qu'en dépit de certaines améliorations, les États-Unis ne peuvent être perçus comme sérieusement engagés sur la voie d'un système adéquat de protection des renseignements personnels[292].

Néanmoins, il ne faut pas oublier, d'une certaine manière, qu'il fut un temps où les États-Unis étaient en avance sur tous les autres pays de Common Law en ce qui a trait à la protection de la vie privée[293]. Depuis le siècle dernier, ils ont un système de protection

---

289 « A Web site may have a privacy policy, but it doesn't mean the site has good practices ». Kathleen OHLSON, « Better Business Bureau joins online privacy fray », 17 mars 1999, *Computer World*, http://www.omputerworld.com/home/news.nsf/all/9903173bbb.htm

290 L'ensemble disparate de lois fédérales et des États américains, comprend les lois régissant les renseignements sur le crédit, le transfert électronique des fonds, la protection des fichiers des médias contre les perquisitions gouvernementales, la confidentialité des renseignements ayant trait aux abonnés de la télévision par câble, l'usage de l'écoute électronique, la confidentialité des enregistrements vidéo de location, les activités fédérales de couplage informatique, les systèmes de sécurité informatisés du gouvernement, etc. Jonathan ROSENOER, *CyberLaw, The Law of the Internet*, New York, Springer-Verlag, 1996, p. 132 et Susan E. GINDIN, « As The Cyber-World Turns : The European Union's Data Protection Directive and Transborder Flows of Personal Data », Décembre 1997, *Internet Legal Practice Newsletter*, http://www.collegehill.com/ilp-news/gindin1.html

291 INDUSTRIE Canada, *Protection de la vie privée et autoroute de l'information : Les options du Canada en matière de réglementation*, Ottawa, 1997, http://strategis.ic.gc.ca/SSGF/ca00268f.htm

292 INDUSTRIE Canada, *Protection de la vie privée et autoroute de l'information : Les options du Canada en matière de réglementation*, Ottawa, 1997, http://strategis.ic.gc.ca/SSGF/ca00268f.htm

293 Jusqu'à l'adoption en 1982 de la Loi sur la protection des renseignements personnels qui s'applique à tous les ministères fédéraux, à la majorité des organismes fédéraux et à certaines sociétés d'États fédérales, les États-

de la vie privée hautement perfectionné en vertu du droit des « torts »[294]. De plus, la vie privée a également été reconnue comme un droit constitutionnel et ce, malgré qu'elle ait obtenu une attention limitée et connu peu d'élaboration judiciaire dans les causes de droits civils[295].

Ces différentes formes de protection de la vie privée purement individuelles et commandées par des ardeurs, sont, il faut le reconnaître, peu satisfaisantes[296]. Néanmoins, elles ont accordé plusieurs protections dans des situations où, il y a quelques années, elles n'en auraient obtenu aucune dans divers pays occidentaux dont le Canada et l'Australie[297]. En fait, les États-Unis ont, d'une certaine manière, le même cadre de protection générale de la vie privée que celui qui existe en Europe en vertu des droits de l'homme et des droits constitutionnels ; ce qui laisse une fois de plus les autres pays de Common Law loin derrière[298].

Le *Privacy Act of 1974* qui s'applique seulement au secteur public fédéral est un bel exemple de l'approche purement sectorielle[299] de la protection de la vie privée et des

---

Unis offraient une meilleure protection de la vie privée que la Common Law canadienne. S.B. PETERSEN, « Your Life as an Open Book : Has Technology Rendered Personal Privacy Virtually Obsolete ? », Volume 48, Numéro 1, *Federal Communications Law Journal*, http://www.law.indiana.edu/fclj/pubs/v48/no1/petersen.html

294 Peter BURNS, « The law and Privacy : the Canadian Experience », (1976) 54 *Can. Bar Rev.* 1 et Karl D. BELGUM, « Who Leads at Half-time?: Three Conflicting Visions of Internet Privacy Policy », 6 *Rich. J.L. & Tech.* 1, (Symposium 1999), http://www.richmond.edu/jolt/v6i1/belgum.html.

295 « The Supreme Court has found the concept of privacy to be protected by the Fourth Amendment. Thus, privacy is know as a penumbra right. It is the essence of the Bill of rights and thus a guaranteed right. » Timothy J. WALTON, *Internet Privacy Law*, 20 décembre 1998, http://www.netatty.com/privacy/privacy.html#5 et *Schmerber* c. *California*, 384 U.S. 757. 779, 86 Ct. 1826, 16 L.Ed.2d 908 (1966).

296 « For years, the United States has relied on narrow, ad hoc legal rights enacted in response to particular scandals involving abusive information practices. The approach has led to incoherence and significant gaps in the protection of citizens' privacy. For example, substance abusers have stronger privacy rights than web users in the United States. Yet, rather than revise American privacy protection, the Magaziner Report adopted a position enshrining the status quo. » Joel REIDENBERG, « Restoring Americans' Privacy in Electronic Commerce », *Berkeley Technology Law Journal*, Volume 14-2, http://www.law.berkeley.edu/journals/btlj/articles/14_2/Reidenberg/html/reader.html.

297 Karim BENYEKHLEF, *La protection de la vie privée dans les échanges internationaux d'informations*, Montréal, Éditions Thémis, 1992, 475 p.

298 Voir à ce sujet : Pierre KAYSER, *La protection de la vie privée : Protection du secret de la vie privée*, 3e éd., Paris Aix-en-Provence, Économica, Presse Universitaires d'Aix Marseille, 1995, 605 p., Karim BENYEKHLEF, « Réflexions sur le droit de la protection des données personnelles à la lumière des propositions de la Commissions des Communautés européennes », (1992) 2 *M.C.L.R.* 149 et Gregory SHAFFER, « The Power of EU Collective Action: The Impact of EU Data Privacy Regulation on US Business Practice », *European Law Journal*, Volume 5:4, http://www.iue.it/LAW/ELJ/archives/1999/1999_volume_4d3.htm

299 « Legislative protection of privacy in the United States is sometimes charitably referred to as « sectoral », meaning that legislation is directed in piecemeal fashion toward specific industries or issues, rather than constituting a global privacy policy for the nation as a whole. Apologists for the American system stress the flexibility of this form of regulation, its ability to tailor regulation closely to the needs of individual situations, and its tendency to avoid the sins of over regulation which might accompany a more comprehensive, « one-size-fits-all » regulatory scheme. » Karl D. BELGUM, « Who Leads at Half-time?: Three Conflicting Visions of Internet Privacy Policy », *Rich. J.L.. & Tech.*, Volume VI, Issue 1, Symposium 1999,

renseignements personnels prônée par les Américains[300]. Plus précisément, cette loi impose aux organismes gouvernementaux de se conformer aux règles régissant la collecte et la conservation des renseignements personnels.

Dans le style caractéristique des Américains, un individu mécontent du geste d'un organisme gouvernemental peut obtenir une réparation civile en ayant recours aux tribunaux[301]. Les États-Unis est le seul pays membre de l'OCDE où la protection de la vie privée et les principes de réglementation de la protection des renseignements personnels sont entièrement laissés à la personne concernée, sans l'aide d'aucune forme d'organisme indépendant[302].

L'avènement de l'informatisation et du réseau Internet n'a rien changé à l'attitude des Américains ; ils conservent toujours leur approche sectorielle ! Contrairement à la Commission européenne, les Américains prônent une approche exclusivement autoréglementaire pour la protection des renseignements personnels sur Internet[303]. Ils préfèrent laisser les acteurs du réseau tenter de s'autoréglementer pour mieux intervenir par la suite si cette tentative devait échouer[304].

---

http://www.richmond.edu/jolt/v6i1/belgum.html#f41. Voir aussi : Joel REIDENBERG, « Privacy in the Information Economy: A Fortress or Frontier for Individual Rights », 44 *Fed. Comm. L. J.*, 195, 208 (1992) et

300 La Cour suprême des États-Unis a reconnu un droit constitutionnel au respect de la vie privée en 1967 dans la décision *Griswold* c. *Connecticut*, (1967) 381 U.S. 479. De plus, l'article A) 4) de la section 2 du Privacy Act of 1974 énonce que le droit à la vie privée est un droit personnel et fondamental protégé par la Constitution des États-Unis. *Privacy Act of 1974 and Amendments*, 5 USC Sec. 552a (1988), http://www.eff.org/pub/Legislation/privacy_act_74_5usc_s552a.law. Voir S.E. GINDIN, « Lost and found in cyberspace : Information privacy in the age of the Internet », 1997 *San Diego Law Review*, http://www.info-law.com/lost.html.

Le 25 juin 1999, le magazine *Wired* révélait qu'un site Web du gouvernement fédéral américain s'était fait retirer son sceau TRUSTe lorsqu'un représentant de l'organisme a réalisé que la politique en matière de protection des renseignements personnels ne rencontrait pas les exigences minimales du Privacy Act of 1974. James GLAVE, « Federal Site Yanks TRUSTe Seal », 25 juin 1999, *Wired*, http://www.wired.com/news/news/politics/story/20419.html

301 « Les États-Unis sont presque le seul pays du monde industriel moderne à compter sur leur appareil judiciaire et divers organismes d'exécution qui ont bien d'autres responsabilités, pour contrôler leur politique de protection de la vie privée. » Colin BENNETT, *Réflexions sur une norme internationale de protection des renseignements personnels, Chapitre 1 - Définition de la portée de la question,* Groupe de travail sur le commerce électronique d'Industrie Canada, http://e-com.ic.gc.ca/francais/privee/632d291.html

302 INDUSTRIE CANADA, *Protection de la vie privée et autoroute de l'information : Les options du Canada en matière de réglementation*, Ottawa, 1997, http://strategis.ic.gc.ca/SSGF/ca00268f.htm

303 À ce sujet, le professeur Peter Swire oppose le « pure market model », soit l'autoréglementation par l'industrie, au « pure enforcement model », soit la réglementation par le gouvernement. Peter S. SWIRE, « Markets, Self-Regulation, and Government Enforcement in the Protection of Personal Information », 23 décembre 1996, http://www.acs-ohio-state.edu/units/law/swire1/psntia6.htm. Voir aussi : Jay KRASOVEC, « Cyberspace : The Final Frontier, For Regulation? », *Akron Law Review*, Volume 31, Numéro 1 (1997-1998), http://www.uakron.edu/lawrev/krasovec.html.

304 « The Administration considers data protection critically important. We believe that private efforts of industry working in cooperation with consumer groups are preferable to government regulation, but if effective privacy protection cannot be provided in this way, we will re-evaluate this policy. » William J. CLINTON & Albert

Fondée en grande partie sur le programme *The Framework for Global Electronic Commerce*, la position américaine repose sur des principes ultra-libéraux[305].

> « *In july 1997, the Clinton Administration expressed its support for the use of self-regulatory measures and technological innovations for protecting Internet privacy when the Administration issued it's a Framework for Global Electronic Commerce. The Framework generally favors a laissez-faire, market-driven approach to regulating the Internet in an effort to stimulate electronic commerce* [306]. »

Sur le réseau Internet, l'autoréglementation est entendue comme « un recours aux normes volontairement développées et acceptées par ceux qui y prennent part[307] ». Tel que nous le démontre la position américaine, l'autoréglementation est une façon « d'alléger la réglementation publique en prenant avantage des motivations existant au sein de l'industrie[308] ». Néanmoins, avant de continuer l'étude de la position américaine, il convient de définir ce que nous entendons par l'autoréglementation. Larry Irving, assistant secrétaire au Département américain du Commerce défini l'autoréglementation comme suit :

> « *Most basically, we need to define what we mean, as the term « self-regulation » itself has a range of definitions. At one end of the spectrum, term is used quite narrowly, to refer only to those instances where the government has formally delegate the power to regulate, as in the delegation of securities industry oversight to the stock exchanges. At the other end of the spectrum, the term is used when the private sector perceives the need to*

GORE, JR., *A Framework for Global Electronic Commerce*, 1 juillet 1997, http://www.iitf.nist.gov/eleccomm/ecomm.htm. Voir aussi : Jay KRASOVEC, « Cyberspace : The Final Frontier, For Regulation? », *Akron Law Review*, Volume 31, Numéro 1 (1997-1998), http://www.uakron.edu/lawrev/krasovec.html.

[305] « Many scholars have also touted the benefits of self-regulation, but self-regulation is not without its critics. » Nous y reviendrons. Angela J. CAMPBELL, « Self-Regulation and the Media », *Fed. Comm. L.J.*, Volume 51, Numéro 3 (Mai 1999), http://www.law.indiana.edu/fclj/pubs/v51/no3/v51no3.html.

Le professeur Reidenberg critique le rapport de la Maison Blanche en y énoncant : « The fair treatment of personal information and citizen confidence in such treatment are each necessary conditions for electronic commerce over the next decade. Yet, sadly, at the political birth of the electronic commerce movement in 1997, the White House's report, *A Framework for Global Electronic Commerce*, more commonly referred to as the Magaziner Report, missed a key opportunity to assure the protection of citizens' privacy on the Internet. » Joel REIDENBERG, « Restoring Americans' Privacy in Electronic Commerce », *Berkeley Technology Law Journal*, Volume 14-2, http://www.law.berkeley.edu/journals/btlj/articles/14_2/Reidenberg/html/reader.html.

[306] Le *Framework for Global Electronic Commerce* fut rendu public le 1er juillet 1997, William J. CLINTON & Albert GORE, JR., *A Framework for Global Electronic Commerce*, 1er juillet 1997, http://www.iitf.nist.gov/eleccomm/ecomm.htm. Voir aussi S.E. GINDIN, « Lost and found in cyberspace : Information privacy in the age of the Internet », 1997 *San Diego Law Review*, http://www.info-law.com/lost.html.

[307] Pierre TRUDEL, France ABRAN, Karim BENYEKHLEF et Sophie HEIN, *Droit du cyberespace*, Montréal, Éditions Thémis, 1996, p. 3-34.

[308] Pierre TRUDEL, « Les effets juridiques de l'autoréglementation », (1989) 19 *R.D.U.S.* 247, p.251.

regulate itself for whatever reason – to respond to consumer demand, to carry out its ethical beliefs, to enhance industry reputation, or to level the market playing field – and does so[309]*. »*

Le terme « autoréglementation » se compose de deux mots, soit « auto » et « réglementation »[310]. Premièrement, le terme « auto » réfère aux acteurs et plus particulièrement à l'industrie dans le cas de l'autoréglementation américaine[311]. Le second terme quant à lui, réfère à ce que font les acteurs. Plus spécifiquement, le terme « réglementation » comporte les trois composantes traditionnelles de la séparation des pouvoirs, soit[312] :

1. La fonction législative : Celle par laquelle on édicte des règles,
2. La fonction exécutive : Celle qui réfère, tel que le définit le professeur Swire, à la question « who should initiate enforcement actions », et
3. La fonction judiciaire : Celle par laquelle les tribunaux et les juges rendent des jugements, c'est-à-dire qui décide s'il y a eu ou non une violation et par le fait même, qui définit les sanctions appropriées.

En résumé, l'autoréglementation « means that the industry or profession rather than the government is doing the regulation[313] ».

En 1998, le Département américain du Commerce a émis un nouveau document intitulé : *Elements of Effective Self-Regulation for the Protection of Privacy and Questions Related to Online Privacy*[314]. Ce document est une directive à l'usage des entreprises

---

309 Larry IRVING, « Introduction » dans *Privacy and Self-Regulation in the Information Age*, National Telecommunications and Information Administration, Juin 1997, http://www.ntia.doc.gov/reports/privacy/privacy_rpt.htm

310 Angela J. CAMPBELL, « Self-Regulation and the Media », *Fed. Comm. L.J.*, Volume 51, Numéro 3 (Mai 1999), http://www.law.indiana.edu/fclj/pubs/v51/no3/v51no3.html.

311 Selon Everette E. Denis, « it is used to refer to a group of companies acting collectively, for example » through a trade association ». Everette E DENIS, « Internal Examination: Self-Regulation and the American Media » 13 *Cardozo Arts & Ent. L.J.* 697 (1995)

312 Peter S. SWIRE, « Markets, Self-Regulation, and Government Enforcement in the Protection of Personal Information », 23 décembre 1996, http://www.acs-ohio-state.edu/units/law/swire1/psntia6.htm et Henry BRUN et Guy TREMBLAY, *Droit Constitutionnel*, 2ième edition, Éditions Yvon Blais Inc., Cowansville, 1990, 1232 pages, p: 80.

313 Angela J. CAMPBELL, « Self-Regulation and the Media », *Fed. Comm. L.J.*, volume 51, numéro 3 (Mai 1999), http://www.law.indiana.edu/fclj/pubs/v51/no3/v51no3.html.

314 Department of Commerce, *Elements of Effective Self Regulation for the Protection of Privacy and Questions Related to Online Privacy*, No. 980422102-8102-01, http://www.ntia.doc/ntiahome/privacy/6_5_98fedreg.htm.

qui détiennent des renseignements personnels sur les internautes[315]. À cet effet, neuf principes sont dégagés :

1. *« **Awareness** : Disclosure of the identity of the data collecting party and means for avoiding participating in such transactions ;*
2. ***Choice** : A mechanism to exercise options, including « affirmative choice » for certain « sensitive » categories of information relating to, for example, medical conditions, or children ;*
3. ***Data security** : Protections against improper alteration or misappropriation of data ;*
4. ***Data integrity** : Keeping data which is accurate and relevant for the purposes for which it was collected ;*
5. ***Consumer access** : The ability of consumers to review and correct data about themselves, although the document warns that the extent of access may vary by industry, due to the costs involved ; et*
6. ***Accountability** : Companies should be accountable in some manner for compliance with their own policies.*

In addition, the Principles include three « enforcement principles » :

1. ***Consumer recourse** : A way to resolve disputes that is "readily available and affordable" ;*
2. ***Verification** : A third-party check on compliance ; et*
3. ***Consequences** : Sanctions for failure to comply. »*

Selon les Américains, le commerce électronique a tout à gagner d'une non-intervention de l'État dans l'élaboration des règles juridiques visant à régir les comportements dans les environnements électroniques décentralisés[316]. Ces dernières doivent plutôt être établies par les acteurs mêmes de l'économie : les entreprises. À ce sujet, au mois de

---

[315] « These norms include specification of the purpose for data collection, the consent of individuals to processing of personal information, the transparency of data processing, such as notice to individuals and access to their personal information, special treatment of particularly sensitive information, such as medical data, and the existence of enforcement remedies and mechanisms. » Joel REIDENBERG, « Restoring Americans' Privacy in Electronic Commerce », *Berkeley Technology Law Journal*, Volume 14-2, http://www.law.berkeley.edu/journals/btlj/articles/14_2/Reidenberg/html/reader.html. Voir aussi Mary J. CULNAN, *A Methodology to Assess the Implementation of the Elements of Effective Self- Regulation for Protection of Privacy*, Discussion Draft - 6/17/98, http://www.georgetown.edu/culnan/privacy/ntia~1.htm.

[316] « The Administration indicated that it currently supports the use of self-regulatory codes of conduct by industry along with technological privacy protection measures as the preferred means for privacy protection. » Susan E. GINDIN, « As The Cyber-World Turns : The European Union's Data Protection Directive and Transborder Flows of Personal Data », Décembre 1997, *Internet Legal Practice Newsletter*, http://www.collegehill.com/ilp-news/gindin1.html.

De plus, selon TRUSTe, « Because the Internet is still in its early growth stages, we believe it's too early to impose regulation without understanding the full impact it would have on growth ». TRUSTe, *About TRUSTe*, 1999, http://www.truste.org/about/about_faqs.htm et Maureen S. DORNEY, « Privacy in the Internet », *Hastings Communications and Entertainment Law Journal, (comm/ent)* V19, 1996-1997 635.

juin 1997, le Département américain du Commerce écrivait dans un document intitulé *Privacy and Self-Regulation in the Information Age :*

> *« The philosophy of the self-regulation will accomplish the most meaningful protection of privacy without intrusive government interference, and with the greatest flexibility for dynamically developing technologies. The theory holds that the marketplace will protect privacy because the fair treatment of personal information is valuable to consumers ; in other words, industry will seek to protect personal information in order to gain consumer confidence and maximize profits* [317]. »

Pour la communauté américaine, l'État doit avoir un rôle des plus limités. Il ne doit pas intervenir en édictant des lois contraignantes concernant la protection des renseignements personnels des internautes.

La première motivation américaine pour l'autoréglementation est culturelle. Les Américains tiennent à la protection de leur vie privée et la considèrent comme l'un des fondements de la liberté de la personne. En cette matière, la démarche américaine découle de la tradition et s'explique par la méfiance des Américains à l'égard de l'État et de ses interventions. Ils préfèrent manifestement la décentralisation et sont réticents à réglementer le secteur privé en l'absence d'un besoin évident[318]. Évidemment, les Américains se soucient davantage des pratiques douteuses que l'État peut perpétrer en manipulant les renseignements personnels que des activités illicites des entreprises[319].

---

[317] U.S. DEPARTMENT OF COMMERCE, NATIONAL TELECOMMUNICATION AND INFORMATION ADMINISTRATION, *Privacy and Self-Regulation in the Information Age*, Ch. I.A., Juin 1997, http://www.ntia.doc.gov/reports/privacy/privacy_rpt.htm.

[318] Dans une entrevue au quotidien Le Devoir, Alan Westin énonçait qu'en 1970, seulement 24 % des Américains étaient soucieux du respect de leur vie privée. En 1978, immédiatement après le scandale du Watergate, ce pourcentage a grimpé à 78 %, et il atteignait 82 % en 1995. Michel VENNE, « Alan F. Westin : Le pape de la vie privée », 8 juillet 1996, *Le Devoir*, http://www.ledevoir.com/REDaction/SOCiete/SOC_priv210597/SOC_priv080796.htm. Voir aussi André GIROUX, « La protection en Europe: Effets outre-frontière d'une nouvelle directive sur la vie privée », *J. du B.*, Volume 29, Numéro 20, http://www.barreau.qc.ca/journal/vol29,no20/protectioneurope.htm et Alan WESTIN, *The U.S. and the EU Directive*, http://www.privacyexchange.org/iss/confpro/aicgsberlin.html.

[319] Un sondage mené aux États-Unis aux mois de juin et juillet 1994 par Louis Harris et Alan Westin révèle que la population américaine ne croit pas que l'adoption de lois ou de règlement par le gouvernement est souhaitable pour solutionner les problèmes reliés à la vie privée. Selon le sondage, 73 % des répondants opteraient plutôt pour l'adoption de politiques volontaires de la part des entreprises. Louis HARRIS et Alan F. WESTIN, « Privacy of Consumer Transaction Records in Future Home Interactive Services : What the Public Says - What the Public Wants, (Reports from and Commentaries on a National Survey of Consumers, Interactive Services, and Privacy) », présenté dans le cadre du *Fifth Conference on Computer, Freedom and Privacy*, Conférence organisée par le Board of Trustees de l'Université Leland Stanford, Juin-juillet 1994, http://www.techlaw.stanford.edu/CFP95.Program.html.

Le professeur Reidenberg ajoute à ce sujet : « For networks to develop and sustain the confidence of thei participants, citizens and businesses must both be afforded a high degree of involvement in the decisions

La seconde motivation pour l'autoréglementation est plutôt opportuniste. Pour l'administration Clinton, elle vise à éviter à tout prix de brider les activités du commerce électronique dans lesquelles les entreprises américaines ont actuellement un avantage important par rapport au reste du monde[320].

Par rapport aux textes législatifs, l'approche autoréglementaire de l'administration Clinton présente les avantages d'être[321] :

- Plus efficace,

  Les entreprises américaines ont vraisemblablement une connaissance supérieure de l'industrie comparativement au gouvernement. En conséquence, il est plus efficace pour l'administration américaine de se fier à l'expertise de l'industrie que de tenter de reproduire la même expertise à l'intérieure même du gouvernement[322].

- Plus flexible et évolutive,

  L'autoréglementation est sans contredit plus flexible que les textes législatifs[323]. Il est plus facile pour les associations issues de l'industrie de modifier les règles face aux circonstances changeantes et évolutives du marché. De plus, l'industrie est la mieux placée pour déterminer quand une règle doit être modifiée pour mieux répondre aux besoins évolutifs du marché[324].

  Le caractère transfrontaliers du réseau et les difficultés liées à l'application des différentes législations justifient par le fait même l'autoréglementation par

---

about the circulation of identifying data. » Joel REIDENBERG et Françoise GAMET-POL, « The Fundamental Role of Privacy and Confidence in the Network », (1995) 30 *Wake Forest L. R.* 105, 109.

320 « The administration is aware that profit is the goal of businesses operating on the Internet [...], a lawyer for the National Telecommunications and Information Administration in the Commerce Department. » Margret JOHNSTON, « Take Net privacy into your own », *CNN*, http://cnn.com.

321 Angela J. CAMPBELL, « Self-Regulation and the Media », *Fed. Comm. L.J.*, Volume 51, Numéro 3 (Mai 1999), http://www.law.indiana.edu/fclj/pubs/v51/no3/v51no3.html

322 « This factor may be particularly important where technical knowledge is needed to develop appropriate rules and determine whether they have been violated. » Angela J. CAMPBELL, « Self-Regulation and the Media », *Fed. Comm. L.J.*, Volume 51, Numéro 3 (Mai 1999), http://www.law.indiana.edu/fclj/pubs/v51/no3/v51no3.html et Peter S. SWIRE, « Markets, Self-Regulation, and Government Enforcement in the Protection of Personal Information », 23 décembre 1996, http://www.acs-ohio-state.edu/units/law/swire1/psntia6.htm

323 Douglas C. MICHAEL, « Federal Agency Use of Audited Self-Regulation as a Regulatory Technique », *Admin. L. Rev* 171, 181-82 (1995).

324 « Self-regulation can be more tailored to the particular industry than government regulation. » Douglas C. MICHAEL, « Federal Agency Use of Audited Self-Regulation as a Regulatory Technique », *Admin. L. Rev* 171, 181-82 (1995).

l'industrie. « Specifically, the argument is sometimes made with respect to the Internet, where jurisdictional and sovereignty issues make it difficult for nations to enforce their law[325]. »

- Mieux adaptée aux réalités pratiques, techniques et économiques du réseau Internet, car elle émane de ces acteurs[326], et

  Il appert selon l'administration américaine, que les internautes percevront plus raisonnables les règles étant donné qu'elles seront développées par l'industrie. Tel que l'énonce le professeur Swire :

  > « *Self-regulation might promote the reputation of the industry as a whole, and it might facilitate the creation of technical standards that will benefit the industry itself and society more generally. [...] Companies may be more willing to comply with rules developed by their peers rather than those coming from the outside*[327]. »

- Moins coûteuse pour la collectivité nationale.

  L'autoréglementation est moins coûteuse pour le gouvernement, car celui-ci délègue les coûts afférents au développement et au respect des règles à l'industrie[328]. Selon les auteurs Ayres et Braithwaite, l'autoréglementation est une bonne alternative à la réglementation gouvernementale parce que l'état « cannot afford to do an adequate job on its own[329] ». Néanmoins, il ne faut pas oublier que l'autoréglementation américaine a aussi ses limites[330].

---

[325] David R. JOHNSON & David POST, « Law and Borders – the Rise of Law in Cyberspace », 48 *Stan L. Rev.*, 1367, 1370-76 (1996).

[326] Douglas C. MICHAEL, « Federal Agency Use of Audited Self-Regulation as a Regulatory Technique », *Admin. L. Rev* 171, 181-82 (1995) et Ian AYRES & John BRATHWAITE, *Responsive Regulation: Transcending the Deregulation Debate* 103 (1992).

[327] Peter S. SWIRE, « Markets, Self-Regulation, and Government Enforcement in the Protection of Personal Information », 23 décembre 1996, http://www.acs-ohio-state.edu/units/law/swire1/psntia6.htm.

[328] Toutefois, il importe de souligner que : « the self-regulation will only result in a net reduction of cost if the costs to industry are lower than the government's cost savings. » Douglas C. MICHAEL, « Federal Agency Use of Audited Self-Regulation as a Regulatory Technique », *Admin. L. Rev* 171, 181-82 (1995) et Ian AYRES & John BRATHWAITE, *Responsive Regulation: Transcending the Deregulation Debate* 103 (1992).

[329] Ian AYRES & John BRATHWAITE, *Responsive Regulation: Transcending the Deregulation Debate* 103 (1992).

[330] « Because [the market] efforts to protect privacy are subject to significant limitations, the question arises whether a different approach, such as self-regulation, might create the reasonable protection of privacy without excessive cost. » Nous y reviendrons. Peter S. SWIRE, « Markets, Self-Regulation, and Government Enforcement in the Protection of Personal Information », 23 décembre 1996, http://www.acs-ohio-state.edu/units/law/swire1/psntia6.htm.

Finalement, en optant pour l'autoréglementation, l'administration américaine s'est donné le droit de faire indirectement ce qu'elle ne pouvait faire directement. Comme le souligne Duncan A. MacDonald, vice-président de Citicorp Credit Services Inc. : « Self-regulation may be used instead of governmental regulation to avoid constitutional issues[331]. » Par exemple, il serait surprenant que le gouvernement américain puisse interdire la publicité de boissons alcooliques en vertu du premier Amendement[332]. Néanmoins, il n'existerait aucune atteinte au droit constitutionnel, « if a station or group of stations independently decides not to accept alcohol advertising[333] ».

Pour ce faire, comme nous le constaterons dans la prochaine section, différentes entreprises et organisations professionnelles ont conçu des labels, des sceaux de qualité et des codes de conduite dans le but de protéger les renseignements personnels des internautes. Outre toute la bonne volonté de ces entreprises et organisations, il se cache derrière ceci un important intérêt pécuniaire[334].

2. *Les solutions préconisées*

Le gouvernement américain encourage le secteur privé à établir des codes de conduites et des labels de qualité pour contrôler les récoltes et par le fait même, accorder une protection aux renseignements personnels des usagers du réseau Internet. Depuis quelques années, l'industrie et les groupes de consommateurs ont créé, à une vitesse phénoménale[335], une foule d'organismes visant à rendre plus sécuritaire les transactions électroniques sur la toile[336]. Les labels destinés à la protection de la vie privée en ligne

---

[331] Duncan A. MACDONALD pour le U.S. Department of Commerce, « Privacy, Self-Regulation, and the Contractual Model: A Report from Citicorp Credit Services, Inc. » dans *Privacy and Self-Regulation in the Information Age*, National Telecommunications and Information Administration, Juin 1997, http://www.ntia.doc.gov/reports/privacy/privacy_rpt.htm

[332] Voir *44 Liquormart, Inc.* c. *Rhode Island*, 517 U.S. 484 (1996).

[333] Angela J. CAMPBELL, « Self-Regulation and the Media », *Fed. Comm. L.J.*, Volume 51, Numéro 3 (Mai 1999), http://www.law.indiana.edu/fclj/pubs/v51/no3/v51no3.html

[334] Comme le souligne le professeur Reidenberg, la protection de la vie privée et des renseignements personnels des internautes est primordiale pour la croissance du commerce électronique. Joel REIDENBERG, « Restoring Americans' Privacy in Electronic Commerce », *Berkeley Technology Law Journal*, Volume 14-2, http://www.law.berkeley.edu/journals/btlj/articles/14_2/Reidenberg/html/reader.html.

[335] Comme le souligne le professeur Swire, la raison de cette vitesse phénoménale est fort simple : « the incentives for industry to protect privacy are entirely financial ». Peter S. SWIRE, « Markets, Self-Regulation, and Government Enforcement in the Protection of Personal Information », 23 décembre 1996, http://www.acs-ohio-state.edu/units/law/swire1/psntia6.htm.

[336] « The patchwork nature of the laws governing privacy rights, and the lack of clear regulations to guide companies doing business on the Internet, have made it necessary for industry and consumer groups to take action to ensure privacy is protected. » Maureen S. DORNEY, « Privacy in the Internet », *Hastings Communications and Entertainment Law Journal, (comm/ent)* V19 1996-1997 635, 650.

se font maintenant concurrence sur la toile[337]. Néanmoins, parmi les *CPA Webtrust*, *TruSecure*[338], *Watchdog*[339] et *OPS*[340], il y a trois organismes qui se démarquent de façon significative.

a) TRUSTe

Numéro un mondial des « online privacy seal programs », TRUSTe[341] est une organisation indépendante sans but lucratif qui, par la création d'une infrastructure visant la protection des renseignements personnels sur Internet, vise à établir un environnement de confiance pour les transactions électroniques[342]. « Making the Net self-regulated instead of controlled by the government is the goal of TRUSTe[343]. » Aux dires de l'organisme, leur sceau est l'un des meilleurs exemples de la démarche autoréglementaire américaine pour la protection des renseignements personnels sur Internet[344].

Le sceau TRUSTe est la pierre angulaire de cet environnement de confiance que l'organisme tente de concrétiser. Guidé par deux principes directeurs,

---

337 Leslie MILLER et Elizabeth WEISE, « Keeping pry out of the privacy debate », 31 mars 1999, *USA Today*, 1999, http://www.usatoday.com/life/cyber/tech/cte755.htm

338 « For the security of both businesses and consumers, ICSA's TruSecure Web Site Certification program performs on-site and electronic assessment of 11 categories of security vulnerability risks, like data transmissions, viruses, hackers, passwords and credit cards. The site was launched in April 1997, and so for about 100 companies display the Web Certification badge. The licensing fee, based on the number of Web servers, begins at $12,500. In addition to protecting the Web site from the bad guys, ICSA Certification assures that browsing users are also protected from unethical exploits and invasions of privacy. The CPA Webtrust seal, an authenticated digital certificate distributed by VerySign, must be re-certified at least every 90 days. » Karen L. MILLER, « Good Webkeeping Seals of Approval », *New York Times*, http://search.nytimes.com/search/daily/bi.tewb?getdoc+sitesite+67773+9+wAAA+truste

339 Watchdog, une initiative du CDT, offre aux usagers de l'Internet, la possibilité de vérifier, à l'aide de simples questions, si la politique en matière de renseignements personnels d'un site Web spécifique correspond aux normes de l'organisme. WATCHDOG, *Our Mission*, 1999, http://www.watchdog.cdt.org/register.cfm

340 NETSCAPE TECHSEARCH, *Open Profiling Standard Frequently Asked Questions*, 27 mai 1997, http://devedge.netscape.com/ops/opsfaq.html et NETSCAPE TECHSEARCH, *The Open Profiling Standard*, 1999, http://devedge.netscape.com/ops/ops.html.

341 Formellement appelé eTRUST.

342 « The TRUSTe model provides a mechanism for industry self-regulation that can provide public assurance of privacy. It utilizes an approach that combines long-term sustainability through industry financial support with consumer credibility through a process of independent assessment and monitoring of business practices. » Andy BLACKBURN, Lori FENA et Gigi WANG, « A Description of the eTRUST Model », dans *Privacy and Self-Regulation in the Information Age*, *Chapter 5: Technology and Privacy Policy*, National Telecommunications and Information Administration, Juin 1997, http://www.ntia.doc.gov/reports/privacy/selfreg5.htm#5D

343 Esther DYSON, « Labeling Practices for Privacy Protection », dans *Privacy and Self-Regulation in the Information Age*, *Chapter 5: Technology and Privacy Policy*, National Telecommunications and Information Administration, Juin 1997, http://www.ntia.doc.gov/reports/privacy/selfreg5.htm#5C

344 L'un des buts de TRUSTe est de démontrer avec évidence aux régulateurs gouvernementaux, que l'industrie peut très bien réussir à s'autoréglementer sur Internet. TRUSTe, *How the TRUSTe Program Works*, 1999, http://www.truste.org/webpublishers/pub_how.html

1. « Users have a right to informed consent » ; et
2. « No single privacy principle is adequate for all situations »,

l'apposition d'un sceau TRUSTe sur un site Web se veut une marque de confiance à l'intention des internautes[345]. Ainsi, en apercevant un sceau TRUSTe sur un site Web, un visiteur peut, par un simple cliquement de souris sur le sceau, avoir accès à la politique en matière de protection des renseignements personnels du site en question[346]. Il pourra de plus, obtenir des informations spécifiques sur les procédures de collectes et de gestion des renseignements personnels. En conséquence, TRUSTe offre aux webmestres « a standardized and cost-effective solution for both satisfying the business model of their site and addressing consumers' anxiety over sharing personal information online[347]. »

Fondé en mars 1996 par Lori Fena, directrice exécutive de l'EFF, et Charles Jennings, fondateur de l'entreprise Portland Software, l'idée de créer TRUSTe leur est venue lorsqu'ils se sont rencontrés pour la première fois au Esther Dyson's PC Forum. Durant les mois qui suivirent cette rencontre, quelques pionniers du commerce électronique se sont joints à eux pour jeter les bases de ce qui devait se concrétiser près d'un an après, soit TRUSTe.

Dès la création du projet pilote en octobre 1996 avec l'aide de l'EFF et de Commerce.Net, TRUSTe a obtenu une popularité toujours grandissante à ce jour. L'organisme obtient ses revenus de ses commanditaires et des sites Web qui déboursent un certain montant d'argent pour obtenir leur sceau. En l'espace de trois ans, TRUSTe a su recruter les grands noms de l'informatique et de l'Internet, tels

---

345 « In order to be successful in its mission, eTRUST must build consensus within the online business community that the self-regulation represented by the eTRUST licensing program is worthwhile from a business and societal perspective. It will also establish awareness and confidence with online consumers that the eTRUST logo provides adequate assurance that their personal information is being protected. » Andy BLACKBURN, Lori FENA et Gigi WANG, « A Description of the eTRUST Model », dans *Privacy and Self-Regulation in the Information Age, Chapter 5: Technology and Privacy Policy*, National Telecommunications and Information Administration, Juin 1997, http://www.ntia.doc.gov/reports/privacy/selfreg5.htm#5D

346 « Seeing the TRUSTe mark assures consumers that a Web site discloses and stands behind its policies on what personal information it collects and how that information is used » Bob METCALFE, « TRUSTe uses consents and disclosures to protect privacy on the Internet », 10 novembre 1997, *Info World*, http://www.infoworld.com/cgi-bin/displayNews.pl?/metcalfe/971110bm.html et TRUSTe, *The TRUSTe Program : How It Protects Your Privacy*, 1999, http://www.truste.org/users/users_how.html.

347 TRUSTe, *How the TRUSTe Program Works*, 1999, http://www.truste.org/webpublishers/pub_how.html

GeoCities, CNET, Infoseek, Yahoo, America Online, CyberCash, Excite, Microsoft, IBM et Compaq[348].

L'unique but de l'organisme est de créer un environnement de confiance mutuelle permettant aux internautes de transiger en toute sécurité. Toutefois, dans la recherche de leur objectif, le professeur Reidenberg résume bien l'une des premières faiblesses du programme.

> *« Although about 450 companies are licensed to use the logo to date, this number is trivial compared to the number of website operators in the United States. In fact, one of the companies, GeoCities, holds the distinction of being the first company prosecuted by the Federal Trade Commission for information trafficking, and fifty percent of the TRUSTe sponsors do not bother to subscribe to the program and license the logo. TRUSTe even features a link on its web page to a look-up service site that fails to disclose its privacy policy and is owned by a company that is not even listed as a TRUSTe licensee*[349]*. »*

Les usagers sont en droit d'obtenir une protection efficace de leurs renseignements personnels dans les environnements électroniques et par le fait même, de choisir les renseignements personnels et les moyens utilisés pour effectuer ces collectes[350]. En conséquence, selon TRUSTe, leur sceau est le moyen idéal pour sécuriser le réseau

---

[348] « One hundred sites participated in the pilot program, offering feedback and guidance. By June 10, 1997, TRUSTe had a staff of its own, a fully developed program and two official auditors, Price Waterhouse Coopers and KPMG Peat Marwick. TRUSTe was launched worldwide on June 10, 1997 at the FTC online privacy hearings. » TRUSTe, *The TRUSTe Story*, 1999, http://www.truste.org/about/about_truste.html et TRUSTe, *TRUSTe Approves 1000th Web Site*, 12 janvier 2000, http://www.truste.org/about/about_1000th.html

[349] Joel REIDENBERG, « Restoring Americans' Privacy in Electronic Commerce », *Berkeley Technology Law Journal*, Volume 14-2, http://www.law.berkeley.edu/journals/btlj/articles/14_2/Reidenberg/html/reader.html.

[350] « The eTRUST concept is modeled on approaches that have proven effective in the self-regulation of other industries, and includes:

- A branded, integrated system of « trustmarks », which represents assurance of privacy and transactional security. These « trustmarks » are backed by an accreditation procedure with guidelines and standards for businesses or organizations who license them.
- An extensive education and awareness campaign for both businesses and consumers.
- An assurance/enforcement/compliance process involving self-assessment, community monitoring, spot checks and professional third- party auditing.
- A scalable system for the components of the program, including the compliance process, based on the different types and sizes of businesses and organizations and the changing marketplace.
- An open process and infrastructure for establishing and modifying guidelines as market needs change. »

Andy BLACKBURN, Lori FENA et Gigi WANG, « A Description of the eTRUST Model », dans *Privacy and Self-Regulation in the Information Age, Chapter 5: Technology and Privacy Policy*, National Telecommunications and Information Administration, Juin 1997, http://www.ntia.doc.gov/reports/privacy/selfreg5.htm#5D

Internet et par le fait même, enrayer les collectes injustifiées de renseignements personnels[351].

Tout site qui désire être certifié par TRUSTe doit en faire la demande à l'organisme[352]. La procédure d'attribution est fort simple ; peut-être trop même! D'où la première faiblesse ou limite de l'organisme et, par le fait même, de l'autoréglementation américaine. Pour ce faire, le propriétaire ou l'administrateur d'un site Web doit remplir une demande d'adhésion, payer les frais d'admission et faire parvenir sa politique en matière de vie privée à TRUSTe.

Une fois le tout complété, TRUSTe analysera la réquisition et communiquera avec le requérant pour :

- Discuter des modifications à apporter à sa politique en matière de vie privée pour la rendre conforme aux principes prônés par TRUSTe[353] ou,
- Confirmer l'adhésion du site Web au programme TRUSTe.

Les principes prônés par TRUSTe en matière de protection des renseignements personnels sont ceux approuvés par la Federal Trade Commission (FTC). Plus spécifiquement, ils réfèrent à :

- L'adoption et l'implantation d'une politique en matière de protection des renseignements personnels qui vise à réduire l'anxiété des usagers en ce qui a trait à la protection des renseignements personnels [Choice],
- Des avis et mise en garde en ce qui a trait à la collecte et à l'échange de renseignements personnels [Notice],
- Un droit de l'usager à exercer un contrôle sur ses renseignements personnels [Access], et
- Une qualité, une protection et une accessibilité aux renseignements personnels récoltés [Security][354].

---

[351] Esther DYSON, « Labeling Practices for Privacy Protection », dans *Privacy and Self-Regulation in the Information Age, Chapter 5: Technology and Privacy Policy*, National Telecommunications and Information Administration, Juin 1997, http://www.ntia.doc.gov/reports/privacy/selfreg5.htm#5C

[352] TRUSTe, *How to Join the TRUSTe Program*, 1999, http://www.truste.org/webpublishers/pub_join.html

[353] TRUSTe, *The TRUSTe Program: How It Protects Your Privacy*, 1999, http://www.truste.org/users/users_how.html

[354] FEDERAL TRADE COMMISSION, *Privacy Online: Fair Information Practices in the Electronic Marketplace: A Federal Trade Commission Report to Congress*, 22 mai 2000, http://www.ftc.gov/os/2000/05/index.htm#22

En conséquence, les principes retenus par TRUSTe et comme nous le constaterons ultérieurement, par le BBBOnLine, sont vagues. Ils sont en réalité des objectifs à rencontrer sans toutefois accorder et préciser les moyens pour y parvenir.

La première faiblesse de TRUSTe et des autres programmes semblables résulte du manque d'« Oversight » et d'« Enforcement »[355]. Sans de bonnes méthodes permettant d'assurer aux internautes l'adhérence des sites Web à de bonnes politiques en matière de vie privée et de renseignements personnels, l'autoréglementation est condamner à être inadéquate et, par le fait même, à être perçue par la population comme ayant besoin d'une législation pour la supporter[356]. Tel que le soulignait la FTC en 1998, « Enforcement – the use of a reliable mechanism to provide sanctions for non-compliance – as a critical component of any governmental of self-regulatory program to protect privacy online[357]. » De plus, en analysant l'utilisation des labels pour la protection de la vie privée, le professeur Dyson énonce :

> « *For example, while many trade associations put forth model policies, few have the ability to enforce member companies adherence. Often it is precisely this lack of oversight and enforcement power that eventually drives good-industry actors to seek legislation codifying self-regulatory principles in an effort to bind bad-industry actors who are tarnishing the reputation of the industry as a whole. Without a strong commitment to oversight and enforcement of industry supported policy, self-regulation will ultimately fail*[358]. »

À cet effet, le rapport de la FTC intitulé *Privacy Online : Fair Information Practices in the Electronic Marketplace : A Federal Trade Commission Report to Congress* et datant du 22 mai 2000 énonce que seulement 20% des sites Web très fréquentés et revus par l'étude ont appliqué les quatre standards de respect de la vie privé recommandés par la

---

[355] « Oversight and enforcement often have been missing components of industry self-regulation. » Deidre K. MULLIGAN et Janlori GOLDMAN, « The Limits and the Necessity of Self-Regulation: The Case for Both » dans *Privacy and Self-Regulation in the Information Age, Chapter 1: Theory of Markets and Privacy*, National Telecommunications and Information Administration, Juin 1997, http://www.ntia.doc.gov/reports/privacy/selfreg1.htm#1G.

Voir aussi l'article de Michelle V. Rafter qui répertorie les déboires de TRUSTe. Michelle V. RAFTER, « Trust or Bust? », 6 mars 2000, *The Standard*, http://www.thestandard.com/article/display/0,1151,12445,00.html

[356] Michelle V. Rafter, « Consumer privacy seals abound, but shopper beware », 2 6 avril 2000, *Individual.com*, http://finance.individual.com/display_news.asp?doc_id=RTD26a2547reuff&page=news

[357] FEDERAL TRADE COMMISSION, *Privacy Online: A Report to Congress*, 1998, http://www.ftc.gov

[358] Esther DYSON, « Labeling Practices for Privacy Protection », dans *Privacy and Self-Regulation in the Information Age, Chapter 5: Technology and Privacy Policy*, National Telecommunications and Information Administration, Juin 1997, http://www.ntia.doc.gov/reports/privacy/selfreg5.htm#5C

FTC[359]. De plus, alors que la FTC a soutenu l'apparition des « Online Privacy Seal Programs » il y a quelques années, il est intéressant de constater qu'actuellement, le rapport établit que moins d'un dixième des sites Web analysés affichent un tel sceau[360].

L'adhésion au programme TRUSTe implique la délivrance d'un sceau au site Web requérant. En fonction de l'analyse de la politique en matière de vie privée du site Web, TRUSTe a discrétion pour fournir l'un de ses trois sceaux[361].

Le premier sceau offert par TRUSTe est le sceau *Anonymous*. Apposé sur un site Web, il indique aux visiteurs qu'aucun renseignement personnel n'est récolté lors de son passage. Le second sceau, le sceau *One-to-one Exchange*, indique pour sa part que des renseignements personnels sont récoltés, mais que ces informations ne sont pas communiquées à d'autres entités. En conséquence, seul le site qui récolte ces informations les conserve et en prend connaissance. Finalement, le dernier sceau offert par TRUSTe est le sceau *Third Party Exchange*. Apposé sur un site, il indique aux visiteurs que des renseignements personnels sont récoltés et que certains de ceux-ci sont communiqués à d'autres entités[362].

TRUSTe vérifie de façon périodique, les sites Web qu'il a certifiés pour s'assurer qu'ils respectent toujours leur politique[363]. De plus, l'organisme dispose d'un mécanisme de

---

[359] FEDERAL TRADE COMMISSION, *Privacy Online: Fair Information Practices in the Electronic Marketplace: A Federal Trade Commission Report to Congress*, 22 mai 2000, http://www.ftc.gov/os/2000/05/index.htm#22

[360] « Notwithstanding, several years of industry and government effort, only 8% of heavily-trafficked Web sites display a seal from one of the self-regulatory programs ». FEDERAL TRADE COMMISSION, *Privacy Online: Fair Information Practices in the Electronic Marketplace: A Federal Trade Commission Report to Congress*, 22 mai 2000, http://www.ftc.gov/os/2000/05/index.htm#22

[361] TRUSTe, *How to Join the TRUSTe Program*, 1999, http://www.truste.org/webpublishers/pub_join.html, Maureen S. DORNEY, « Privacy in the Internet », *Hastings Communications and Entertainment Law Journal*, (comm/ent) V19 1996-1997 635 et Laurie J. FLYNN, « Group to Monitor Web Sites For Respect of Consumer Privacy », 16 juillet 1996, *New York Times*, http://search.nytimes.com/web/docsroot/library/cyber/week/0716privacy.html.

De plus, suite aux différents logiciels permettant des atteintes à la vie privée des utilisateurs, TRUSTe travaille présentement à la création de sceaux pour ces logiciels. « The recent incident involving RealNetworks prompted a broad set of solutions for addressing consumer concerns about personally identifiable information », TRUSTe, *TRUSTe & Realnetworks collaborate to close privacy gap*, 1999, http://www.truste.org/about/about_software.html

[362] Dans ce cas, il sera spécifiquement indiqué aux usagers quels seront les renseignements personnels partagés

[363] « Officials for TRUSTe say that they constantly monitor, review and investigate their certified sites. If they find an infraction, they say they will withdraw their seals from the Web site. » Esther DYSON, « Labeling Practices for Privacy Protection », dans *Privacy and Self-Regulation in the Information Age, Chapter 5: Technology and Privacy Policy*, National Telecommunications and Information Administration, Juin 1997, http://www.ntia.doc.gov/reports/privacy/selfreg5.htm#5C et Lisa GUERNSEY, « Web Surfers' Fears Prompt Privacy Seals », 29 avril 1999, *New York Times*, http://search.nytimes.com/search/daily/bi...tweb?getdoc+site+site+71840+0+wAAA+truste

plaintes qui permet aux usagers de dénoncer les sites certifiés qui ne respectent pas leur politique en matière de vie privée[364]. Advenant une plainte, TRUSTe agit à titre de médiateur entre les parties et peut faire des suggestions pour améliorer la politique du site Web poursuivi. De plus, advenant le cas où un site Web n'appliquerait pas les améliorations suggérées par TRUSTe, dépendant de la gravité de la faute invoquée, le sceau pourrait être révoqué et dans des situations critiques, des dénonciations pourraient être portées devant les autorités compétentes[365].

L'absence de sanctions efficaces et adéquates s'avère la seconde faiblesse des « Online Privacy Seal Programs » et, par le fait même, de l'autoréglementation[366]. Présentement, ces programmes offrent peu ou pas de moyens concrets et surtout, impartiaux[367], aux internautes ayant subi une atteinte à leur vie privée. « Without meaningful opportunity to have grievances addressed, and to be compensated for breaches of policy, consumers will find policies – whether they be self-regulatory or legislative, sorely lacking[368]. »

Comme le souligne Angela J. Campbell, « Industry may be unwilling to commit the resources needed for vigorous self-enforcement. It is also unclear whether industry has the power to enforce adequate sanctions[369]. » Dans la plupart des situations, l'expulsion du programme ou la révocation du sceau sont des sanctions insuffisantes[370]. Étant

---

[364] TRUSTe, *The TRUSTe Watchdog*, 2000, http://www.truste.org/users/users_watchdog.html.

[365] À cet effet, TRUSTe est excessivement vague. Il énonce : « We monitor our licensees for compliance through a variety of measures, including initial and periodic reviews, technology tools, and online community and user input. In fact, we encourage you to contact us directly with inquiries or complaints regarding how your personal information is collected and used by a TRUSTe-licensed Web site. If we cannot reach a satisfactory resolution to an inquiry or complaint, an escalating investigation is conducted. The process may result in an on-site compliance review of the site by an outside CPA firm, revocation of the trustmark, termination from the TRUSTe program, breach of contract proceedings, or referral to the appropriate law enforcement authority. » TRUSTe, *How does TRUSTe ensure that Web sites stick to their privacy policies ?*, 2000, http://www.truste.org/users/users_faqs.html#ensure

[366] Deidre K. MULLIGAN et Janlori GOLDMAN, « The Limits and the Necessity of Self-Regulation: The Case for Both » dans *Privacy and Self-Regulation in the Information Age, Chapter 1: Theory of Markets and Privacy*, National Telecommunications and Information Administration, Juin 1997, http://www.ntia.doc.gov/reports/privacy/selfreg1.htm#1G.

[367] Nous y reviendrons.

[368] Deidre K. MULLIGAN et Janlori GOLDMAN, « The Limits and the Necessity of Self-Regulation: The Case for Both » dans *Privacy and Self-Regulation in the Information Age, Chapter 1: Theory of Markets and Privacy*, National Telecommunications and Information Administration, Juin 1997, http://www.ntia.doc.gov/reports/privacy/selfreg1.htm#1G.

[369] Angela J. CAMPBELL, « Self-Regulation and the Media », *Fed. Comm. L.J.*, volume 51, numéro 3 (Mai 1999), http://www.law.indiana.edu/fclj/pubs/v51/no3/v51no3.html.

[370] « Such sanctions may be ineffective where consumers lack the knowledge of how a company is viewed by its peers. Moreover, trade associations generally are reluctant to expel their members, especially when the members pay dues to support the association's activities. » Angela J. CAMPBELL, « Self-Regulation and the

donné que la sanction la plus grave que TRUSTe peut ordonner envers l'un de ces membres est l'expulsion du programme, il serait surprenant de voir cette sanction imposée vu l'importance des bénéfices qui résultent de l'adhésion de leurs membres[371].

Sans moyens et incitatifs adéquats pour que les « mauvais membres » se conforment complètement au programme, les « bons membres » sont ainsi placés dans un désavantage compétitif[372]. « Where company can make a greater profit by ignoring self-regulation than complying it is likely to do so, especially where non-compliance is not easily detected by the consumer or likely the harm the particular company's reputation[373]. » En conséquence, les lignes directrices de l'autoréglementation, et plus particulièrement les « online privacy seal programs », s'effilochent en grande partie à cause des tricheurs[374].

b) Better Business Bureau (BBB)

Conçu en tout point semblable comme TRUSTe, le programme de standardisation développé par le Better Business Bureau, le BBBOnLine, représente selon l'organisme, le nouveau concept de protection et de gestion des renseignements personnels sur la toile[375].

Fondé en 1912, l'organisme sans but lucratif BBB regroupe près de 250 000 entreprises en Amérique du Nord. Cet organisme est dédié à encourager les relations justes et honnêtes entre les commerçants et les consommateurs, à l'instauration d'un environnement de confiance pour les transactions et à l'implantation d'une éthique

---

Media », *Fed. Comm. L.J.*, volume 51, numéro 3 (Mai 1999), http://www.law.indiana.edu/fclj/pubs/v51/no3/v51no3.html.

[371] Henry H. PERRIT, JR. « Regulatory Models for Protection Privacy in the Internet », dans *Privacy and Self-Regulation in the Information Age, Chapter 3: Models For Self-regulation*, National Telecommunications and Information Administration, Juin 1997,

[372] « The problem with self-regulation is that it rewards bad actors. Once a Web site begins generating revenue by selling user profiles and personal information, other Web sites will have to follow suit in order to remain competitive. » PC WORLD, « Legal Remedies », Juin 2000, *PC World*, http://www.pcworld.com/current_issue/article/0,1212,16444+1+6,00.html

[373] Peter S. SWIRE, « Markets, Self-Regulation, and Government Enforcement in the Protection of Personal Information », 23 décembre 1996, http://www.acs-ohio-state.edu/units/law/swire1/psntia6.htm.

[374] Nous y reviendrons.

Voir Henry H. PERRIT, JR. « Regulatory Models for Protection Privacy in the Internet », dans *Privacy and Self-Regulation in the Information Age, Chapter 3: Models For Self-regulation*, National Telecommunications and Information Administration, Juin 1997,

[375] Selon le BBBOnLine, « The seal program are being touted by leading companies in electronic commerce as the best way to protect consumers without resorting to Federal legislation. » Lisa GUERNSEY, « Web Surfers' Fears Prompt Privacy Seals », 29 avril 1999, *New York Times*, http://search.nytimes.com/search/daily/bi...tweb?getdoc+site+site+71840+0+wAAA+truste

d'affaire ; la mission du BBB se concrétise dans sa volonté à laisser les acteurs du réseau s'autoréglementer[376]. Plus spécifiquement, le BBB offre à ses entreprises membres :

- « Reports on business firms that will be helpful to you before making a purchase. The BBB system responds to millions of such inquiries each year[377],
- Information about charity groups and organisations,
- Help resolve consumers' disputes with businesses through telephone conciliation, mediation and arbitration and,
- Promote ethical business standards and voluntary self-regulation of business practices[378]. »

L'avènement des environnements électroniques décentralisés a créé plusieurs défis concernant la protection et la gestion des renseignements personnels. Focalisant sur la promotion de l'honnêteté et de la confiance lors des transactions électroniques, le BBBOnLine tente de transposer sur Internet près de 85 années d'expérience en dehors des environnements électroniques pour encourager un « ethical online marketplace[379]. »

Lancé au mois d'avril 1997, le BBBOnLine compte déjà plus de 1 200 participants dont Netscape, J.C. Penney, AT&T[380] Corp., Hewlett-Packard Company, Sony Electronics, Equifax[381], Kodak[382] et Visa U.S.A.

La mission du BBBOnLine est de promouvoir l'honnêteté et la confiance lors des transactions électroniques. Comme TRUSTe, il offre trois différents sceaux pour les commerçants désireux de rencontrer les exigences du programme en ce qui a trait à la protection des renseignements personnels. Les principes prônés par le BBBOnLine en matière de protection des renseignements personnels sont les mêmes que ceux retenus

---

[376] BBB, *Council of Better Business Bureau*, 1999, http://www.bbb.org/about/aboutCouncil.html

[377] À cet effet, le BBB maintien des rapports de fiabilité sur plus de 3 millions d'entreprises en Amérique du Nord. BBB, *Using BBB services*, 1999, http://www.bbbonline.org/consumers/usingbbb.html

[378] BBB, *What is a BBB ?*, 1999, http://www.bbb.org/about/index.html

[379] Karen L. MILLER, « Good Webkeeping Seals of Approval », 1999, *New York Times*, http://www.search.nytimes.com/search/daily/bi/...tweb?getdoc+site+site+67773+9+wAAA+truste

[380] AT&T, *AT&T study shows posting a privacy policy and the BBBOnLine Privacy Seal gives consumers the most confidence*, 1999, http://www.research.att.com/projects/pricacystudy/

[381] EQUIFAX, *Equifax Chairman urges consumers to look for sites with the BBBOnLine Privacy Seal*, 1999, http://www.equifax.com/about.news release/april99/41599.html

[382] KODAK, *Kodak.com Earns BBBOnLine Privacy Seal; BBBOnLine Recognizes Kodak's Firm Commitment to Protecting Consumer Privacy*, http://www.businesswire.com/webbox/bw.051399/191331446.html

par TRUSTe, soit les quatre principes élaborés par la FTC en 1998[383]. Toutefois, sur son site Web, BBBOnLine réduit ces quatre principes à une simple expression qui, sans contredit, est plutôt vague ; « They must disclose what « individually identifiable information » they collect and how they use it[384]. » En conséquence, BBBOnLine utilise un terme nébuleux et aucunement circonscrit, soit « individually identifiable information », pour définir l'étendu des obligations de ses membres. Aux yeux des internautes, cette délimitation se conçoit comme un avantage indu pour le commerçant.

L'idée première derrière ces sceaux est d'augmenter la confiance des usagers envers les commerçants lors des transactions électroniques. Ainsi, par un simple cliquement sur un sceau affiché sur le site d'un commerçant, le consommateur a accès instantanément à sa politique en matière de vie privée approuvée par le BBBOnLine[385].

Le premier sceau dispensé par le BBBOnLine est le sceau *Reliability*. Disponible depuis le mois d'avril 1997, le sceau *Reliability* compte déjà plus de 2 700 entreprises participantes. Il offre aux consommateurs la possibilité d'identifier les commerçants qui font affaires sur Internet. Plus particulièrement, il offre aux consommateurs des historiques détaillés sur les pratiques et usages des commerçants, ce qui leur permet de connaître la place d'affaires du commerçant et d'évaluer sa capacité et sa fiabilité à livrer ses produits[386]. De plus, s'il s'avère nécessaire, le BBBOnLine dispose aussi d'un mécanisme de plainte et d'arbitrage pour les consommateurs. Plus spécifiquement, ce

---

[383] À titre de rappel, les quatre principes sont :

- Avertissement: Une notice expose sur le site le type d'information collectée et l'usage qui en est fait.
- Choix: Le consommateur peut décider si ses informations personnelles seront utilisées à d'autres fins que celle de la transaction initiale.
- Accès: Le consommateur peut vérifier la véracité des informations récoltées sur son compte.
- Sécurité: Les sites sont tenus de prendre «des mesures raisonnables» pour assurer l'intégrité et la sécurité de ces données.

[384] Lisa GUERNSEY, « Web Surfers' Fears Prompt Privacy Seals », 29 avril 1999, *New York Times*, http://search.nytimes.com/search/daily/bi...tweb?getdoc+site+site+71840+0+wAAA+truste

[385] « The logo means that the site post -- and agrees to adhere to -- a statement disclosing what personal data the company collects from a consumers and what it does with that information. » Chris OAKES et James GLAVE, « The Web Privacy Seal, Take 2 », 17 mars 1999, *Wired*, http://www.wired.com/news/print_version/politics/story/18517.html?wnpg=all.

À ce sujet, le président de Brighstreet.com, une entreprise spécialisée dans le développement des promotions sur Internet, énonçe au sujet du BBBOnLine : « If a seal program's agreement with a site contains basic elements that establish trust between a consumer and a Web business, I except that consumers will see the seal and say., O.K., this site is O.K. to do business with. » Lisa GUERNSEY, « Web Surfers' Fears Prompt Privacy Seals », 29 avril 1999, *New York Times*, http://search.nytimes.com/search/daily/bi...tweb?getdoc+site+site+71840+0+wAAA+truste

[386] « Companies in BBBOnLine liability make a commitment to high levels of ethical business practices and customer satisfaction that are not required by many other seal programs. » BBB, *BBBOnLine Privacy*, 1999, http://www.bbbonline.org/about/FAQs.html#privacy1

sceau offre aux internautes « an easy way to distinguish reliable websites and online services while promoting consumer trust and confidence online[387]. »

Le second et le plus important sceau offert par le BBBOnLine est le sceau *Privacy*. Lancé le 17 mars 1999, le sceau compte déjà plus de 3 000 participants. Apposé sur un site Web, le sceau *Privacy* indique que le commerçant a rencontré, selon le BBBOnLine, les plus hauts standards concernant la gestion et la protection des renseignements personnels[388]. L'organisme effectue de plus une surveillance accrue des sites participants pour vérifier s'ils répondent toujours, une fois le sceau accordé, aux critères du BBBOnLine. Finalement, sensiblement comme les autres organismes, le BBBOnLine offre un processus de résolution des conflits[389]. Néanmoins, à l'heure actuelle, il serait mieux d'énoncer que BBBOnLine désire offrir un processus de résolution des conflits. Pour le moment, malgré le fait que l'organisme fonctionne depuis plus d'une année et qu'il compte plus de 3 000 membres, ce processus de résolution est toujours hypothétique[390].

La visibilité du sceau *Privacy* apporte un renforcement au niveau de la confiance des consommateurs envers les transactions électroniques. Plus spécifiquement[391]:

- « Awards an easily recognizable and affordable « seal » to businesses that post online privacy policies that meet the required "core" principles, such as disclosure, choice, and security,

---

[387] BBB, *BBBOnLine Reliability*, 1999, http://www.bbbonline.org/consumers/index.html

[388] À ce sujet, sans établir aucune référence à des dispositions législatives, le BBB énonce : « Companies that qualify must post privacy notices telling consumers what personal information is being collected and how it will be used. These practices including clearly posted privacy policies meeting rigorous privacy principals (including notice to consumer, disclosure, choice and consent, access and security) ». BBB, *BBBOnLine Privacy*, 1999, http://www.bbbonline.org/about/FAQs.html#privacy1 et Kathleen OHLSON, « Better Business Bureau joins online privacy fray », 17 mars 1999, *Computer World*, http://www.omputerworld.com/home/news.nsf/all/9903173bbb.htm

[389] The BBB*OnLine's* privacy seal is backed by an association noted for its expertise and experience in conducting successful national self-regulation and dispute resolution programs - the Council of Better Business Bureaus (CBBB). The BBB*OnLine's* privacy seal enjoys such high name recognition and trust as an extension of the BBB brand. And, only BBB*OnLine's* privacy seal offers consumers a mechanism for resolving disputes while giving businesses a way to meet the standards for effective self-regulation being sought by regulators in the United States and abroad. BBB, *BBBOnLine Privacy*, 1999, http://www.bbbonline.org/about/FAQs.html#privacy1

[390] Joel REIDENBERG, « Restoring Americans' Privacy in Electronic Commerce », *Berkeley Technology Law Journal*, Volume 14-2, http://www.law.berkeley.edu/journals/btlj/articles/14_2/Reidenberg/html/reader.html

« While the program officially launched on March 17, 1999, BBBOnLine ignores the issue that consent might not be an appropriate basis for the processing of some personal information, such as health data, only requires that websites disclose particular practices, fails to require that remedies be afforded to victims of information abuse, and fails to require that individuals be granted complete access to their personal information. » Robert O'HARROW, « Better Business Bureaus Offer Online Privacy Seal », 17 mars 1999, *Washington Post*, p. E1.

- Provides consumer-friendly dispute settlement,
- Monitors compliance through rigorous requirements for participating companies to undertake, at least annually, an assessment of their online privacy practices, et
- Offers specific consequences for non-compliance, such as seal withdrawal, publicity and referral to government enforcement agencies. »

Finalement, le dernier sceau dispensé par le BBBOnLine est le sceau *Kid's Privacy*. Conçu spécialement pour la protection des enfants, les sites qui désirent afficher ce sceau doivent *a priori*, obtenir le sceau *Privacy* et se conformer par la suite à ces autres conditions[392] :

- « Obtain parental consent before any personal information can be collected, used or disclosed,
- Obtain parental consent before children are allowed to post or communicate directly with others,
- Provide warnings and explanations in easy-to-understand language,
- Avoid collecting more information than necessary to provide children's games and activities,
- Be careful in the way they provide hyperlinks, et
- Follow strict rules when sending email. »

Tout site désirant être approuvé et certifié par le BBBOnLine doit en faire la demande à l'organisme et bien entendu, défrayer les coûts d'adhésion au programme[393]. Un commerçant désireux d'afficher un des sceaux du BBBOnLine sur son site Web doit nécessairement avoir une politique en matière de vie privée. De plus, le BBBOnLine ajoute comme condition que chaque site doit obligatoirement permettre aux consommateurs de prendre connaissance de leur renseignements personnels récoltés et, ce qui est surprenant, à condition que le commerçant « has a way to provide the data

---

391 BBB, *BBBOnLine Online Privacy Program*, 1999, http://www.bbbonline.org/businesses/privacy/self-regulation.html

392 BBB, *BBBOnLine Children's Privacy*, 1999, http://www.bbbonline.org/about/FAQs.html

393 À l'instar de TRUSTe, le BBBOnLine obtient ses revenus des commanditaires qui contribuent jusqu'à 100 000$ par année, et des sites Web qui déboursent une certaine somme d'argent pour obtenir leur sceau du BBBOnLine. Les coûts d'adhésion au programme vont de 150 $ à 3000 $ par année, en fonction du montant total des ventes de l'entreprise. Chris OAKES et James GLAVE, « The Web Privacy Seal, Take 2 », 17 mars 1999, *Wired*, http://www.wired.com/news/print_version/politics/story/18517.html?wnpg=all et BBB, *How Much Will It Cost ?*, 1999, http://www.bbbonline.org/businesses/privacy/cost.html

easily[394]. » Ainsi, un commerçant membre du BBBOnLine peut récolter des renseignements personnels sur ses consommateurs et leurs refuser l'accès à leurs informations recueillies sur le motif que le commerçant est présentement dans l'impossibilité de fournir aisément ces-dits renseignements. Cette situation qui peut paraître *a priori* totalement illogique et improbable pour certain, est néanmoins courante[395]. Elle démontre, par le fait même, une autre énorme lacune du programme.

Toutefois, à quel moment exactement un commerçant pourra refuser de fournir les informations ? L'imprécision du terme « easily » laisse présager un avantage en faveur du commerçant. C'est celui-ci et non le consommateur qui pourra dire s'il peut ou non « provide the data easily » ! En conséquence, dans une industrie où les profils de consommation sont des atouts majeurs dans la recherche du profit[396], le consommateur devra se fier à la parole du commerçant. Tel que l'écrivait le professeur Reidenberg :

> « *A marketplace can only function efficiently if there is transparency ; citizens must be able to identify the collectors and users of their personal information. [...]*
>
> *Without transparency, an information trafficking industry has emerged in the United States with no accountability and minimal risk of harm to corporate financial interests from abuses of personal information. Not surprisingly, an analysis of industry codes of privacy practice reveals policies that fail to address the most basic principles of citizens' rights to personal information*[397]. »

---

[394] Lisa GUERNSEY, « Web Surfers' Fears Prompt Privacy Seals », 29 avril 1999, *New York Times*, http://search.nytimes.com/search/daily/bi...tweb?getdoc+site+site+71840+0+wAAA+truste

[395] La récente découverte par les médias du « Fichier longitudinal sur la main-d'œuvre » détenue par le Ministère du Développement des Ressources Humaines du Canada (DRHC) est sans contredit un bon exemple. Depuis 1979, le gouvernement fédéral tenait à jour un fichier central contenant des renseignements personnels sur tous les citoyens, et ce, à leur insu. Pas moins de 34 millions de personnes, certaines maintenant décédées, y sont fichées avec quelque 2000 données sur chacune d'elles.

« Selon M. Ghislain Charron, un porte-parole de DRHC, le Fichier est en fait une banque de données virtuelle où les entrées sont dépersonnalisées. «Il faut retracer et re-identifier les données rattachées au citoyen dans des champs de la banque de données, très disparates et peu uniformes, a-t-il dit. Il faut retourner au fichier original, d'avant les analyses et les études statistiques faites sur ces données, afin de les décrypter et les remettre aux citoyens. Nous n'avons pas d'outils qui permettent de faire cela à grande échelle et nous sommes présentement à l'étude des différentes solutions, entre autres des logiciels faits sur mesure, qui nous permettront de remplir cette tâche. » Dominic FUGÈRE, « Big Brother n'est pas pressé de parler », 19 mai 2000, *Multimédium*, http://www.mmedium.com/cgi-bin/nouvelles.cgi?Id=3685 et Hélène BUZZETTI, « Big Brother existe », 17 mai 2000, *Le Devoir*, http://www.ledevoir.com/ott/2000b/brot170500.html.

[396] « Companies make significant profits from the secret collection and sale of personal information; the $1.5 billion market in personal information is largely hidden from public view. » Joel REIDENBERG, « Restoring Americans' Privacy in Electronic Commerce », *Berkeley Technology Law Journal*, Volume 14-2, http://www.law.berkeley.edu/journals/btlj/articles/14_2/Reidenberg/html/reader.html.

[397] Joel REIDENBERG, « Restoring Americans' Privacy in Electronic Commerce », *Berkeley Technology Law Journal*, Volume 14-2, http://www.law.berkeley.edu/journals/btlj/articles/14_2/Reidenberg/html/reader.html

Pour le BBBOnLine, l'autorégulation de l'Internet fait partie de la culture même du réseau. Par le fait même, c'est aussi une composante intégrale de la mission du BBB. À ce sujet, pour appuyer les politiques en matière de protection et de gestion des renseignements personnels sur Internet, le BBB a tout récemment développé un *Code of Online Business Practices*.[398] Ce code renferme les principes de protection des renseignements personnels prônés par l'organisme. Pour le BBB, l'autorégulation du commerce électronique et de la protection des renseignements personnels est la voie de l'avenir pour sécuriser le réseau aux yeux des consommateurs. Steve Salter, directeur du BBBOnLine, ajoute à ce sujet : « Self-regulation is needed to tone down of the Wild West reputation the Web has to star to kick out some of the bad actors[399]. »

En contrepartie, pendant que TRUSTe et le BBB croient que l'autoréglementation est la solution pour éloigner les mauvais acteurs, certains auteurs pensent au contraire qu'ils sont la raison pour laquelle l'autoréglementation ne peut fonctionner[400]. On ne peut le cacher, il existe des mauvais acteurs membres de TRUSTe, de BBBOnLine ou de tout autre programme semblable. Les différentes faiblesses de ces programmes offrent des avantages indus à ces mauvais acteurs.

Les incitatives de l'industrie pour la protection des renseignements personnels sur le réseau Internet sont entièrement financières[401]. Comme le souligne le professeur Swire :

> *« The assumption, for now, is that there is no legal enforcement against a company that discloses personal information about its customers. Customers can be directly attracted by a strong privacy protection policy or repelled by breaches of privacy. In at least some instances, privacy may be a salient enough marketing point to induce consumers to switch from one company to another*[402]. »

---

398 BBB, *BBBOnLine to Develop Code of Online Business Practices*, 1999, http://www.bbbonline.org

399 Karen L. MILLER, « Good Webkeeping Seals of Approval », 17 mai 1998, *New York Times*, http://search.nytimes.com/search/daily/bin/fastweb?getdoc+site+site+72966+0+wAAA+karen%7Emiller%7Ewebkeeping

400 Henry H. PERRIT, JR. « Regulatory Models for Protection Privacy in the Internet », dans *Privacy and Self-Regulation in the Information Age, Chapter 3: Models For Self-regulation*, National Telecommunications and Information Administration, Juin 1997,

401 « For example, while acknowledging that industry may possess greater technical expertise than government [...] companies will use that expertise to the benefit of the public, suggesting instead that they are more likely to employ their expertise to maximize the industry's profits. » Angela J. CAMPBELL, « Self-Regulation and the Media », *Fed. Comm. L.J.*, Volume 51, Numéro 3 (Mai 1999), http://www.law.indiana.edu/fclj/pubs/v51/no3/v51no3.html.

402 Peter S. SWIRE, « Markets, Self-Regulation, and Government Enforcement in the Protection of Personal Information », 23 décembre 1996, http://www.acs-ohio-state.edu/units/law/swire1/psntia6.htm.

Laissez l'industrie autoréglementer la protection des renseignements personnels sur le réseau Internet crée la possibilité que l'industrie puisse renverser les buts visés par l'autoréglementation, soit la protection des internautes, pour les remplacer par les siens, soit la recherche du profit. En conséquence, la nature même de l'autoréglementation peut faire échouer la poursuite de son but ultime. Comme le souligne les auteurs Baker et Miller : « Self-regulators often combine – and sometimes confuse – self-regulation with self-service[403] ».

c) Platform for Privacy Preferences (P3P)

Depuis 1997, le W3C[404] travaille à la création d'un nouveau standard pour la gestion des renseignements personnels sur Internet. Le 24 avril 2000, le W3C a présenté la troisième révision du « last call draft »[405]. N'ayant toujours par fixé une date pour mettre opérationnel le P3P[406], le W3C a toutefois tenu un « Test Drive Implementations of

---

[403] Donald I. BAKER & W. Todd MILLER, « Privacy, Antitrust and the National Information Infrastructure: Is Self-Regulation of Telecommunications-Related Personal Information a Workable Tool? », dans *Privacy and Self-Regulation in the Information Age, Chapter* , National Telecommunications and Information Administration, Juin 1997.

[404] Le W3C est l'organisme responsable de l'harmonisation à l'échelle mondiale des normes techniques du Web. Il se compose du laboratoire des sciences informatiques du MIT, de l'INRIA et du CERN. Il vise à réaliser le plein potentiel de l'Internet en développant des normes et des logiciels de références. Il fournit en outre les services publics suivants :

- A repository of information about the World Wide Web for developers and users, especially specifications about the Web;
- A reference code implementation to embody and promote standards;
- Various prototype and sample applications to demonstrate use of new technology.

W3C, *About the World Wide Web Consortium*, http://www.w3.org/pub/WWW/Consortium.

[405] W3C, Platform for Privacy Preferences (P3P) Project, http://www.w3.org/P3P/ et W3C, *World Wide Web Consortium Announces First Demonstration of Web Privacy Framework*, 6 avril 2000, http://www.w3.org/2000/04/p3pinterop-pressrelease .

[406] Au sujet de la lenteur du W3C à mettre le P3P opérationnel, Andy ORAM, journaliste au *Webreview* et modérateur du « Cyber Rights mailing list for Computer Professionals for Social Responsibility », énonce :

> *« More than two and a half years have passed since the kick-off meeting of the P3P working group in June 1997. If the World Wide Web Consortium is going to help us preserve privacy, it would be nice to get the protocol finalized and see some browser implementations before e-commerce sites have a complete record of all the books we read, the music we listen to, and the medicines we take.*
>
> *But P3P may also be fading in relevance. The kick-off meeting was announced just in time for a 1997 workshop by the FTC on privacy, and the promise of P3P may have helped persuade the commission to endorse industry « self-regulation ».*
>
> *The public has become frustrated with the failures of self-regulation, particularly the inability of TRUSTe to discover or stop several alarming practices. In December 1999, the EPIC released one of their annual reviews of popular Web sites and found their privacy statements to be superficial and inadequate.*
>
> *In the current atmosphere, calls for legislation in the U.S. are growing despite the frantic efforts of direct marketers. Meanwhile, after two years of negotiations, the United States government concluded a deal last month with the European Union requiring U.S. companies to limit the use and sharing of data strictly whenever they operate in Europe.* [Nous y reviendrons]
>
> *One readily sympathizes with the difficulties faced by those who try to formalize policies enough to turn them into a networking protocol. The P3P working group experienced tremendous pressure, caught*

P3P » le 21 juin 2000 à New York[407]. En conséquence, étant donné que le système ne sera pas, sous toutes réserves, fonctionnel d'ici plusieurs mois encore, nous nous en tiendrons seulement à la description du P3P[408].

Totalement différent des sceaux de confiance précédemment analysés, le P3P s'avère l'une des solutions exemplaires pour gérer et protéger les renseignements personnels des usagers des environnements électroniques. En s'appuyant sur les propositions faites par différentes sociétés, le standard communément appelé P3P, permet aux utilisateurs de filtrer confortablement et en toute sécurité leurs renseignements personnels lorsqu'ils naviguent sur la toile[409].

Appuyée par l'entreprise Microsoft et le Center for Democracy and Technology (CDT), l'idée du P3P est de permettre à chaque usager de créer lui-même son propre profil d'utilisateur. Ce nouveau standard utilise le système Platform for Internet Content Selection (PICS)[410] et crée un langage de communication client-serveur entre les sites Web et les usagers du réseau.

Ainsi, au lieu de lire chacune des politiques en matière de vie privée émise par les sites Web, le système P3P permet à un usager de configurer son fureteur à son goût pour ainsi naviguer sans se soucier des collectes de renseignements personnels exécutées à son insu. En conséquence, un site Web désireux d'obtenir des renseignements

---

between those who want a policy friendly to businesses and those like the European Union who want unambiguous pronouncements of protection for data. The problems faced by P3P can teach us a lot of basic lessons about the relationship between computers and society. »

Andy ORAM, « Promises, Promises, Promises », 7 avril 2000, *Webreview*, http://webreview.com/pub/2000/04/07/platform/index.html

[407] W3C, Platform for Privacy Preferences (P3P) Project, http://www.w3.org/P3P/ et W3C, *World Wide Web Consortium Announces First Demonstration of Web Privacy Framework*, 6 avril 2000, http://www.w3.org/2000/04/p3pinterop-pressrelease .

[408] Néanmoins, pour obtenir une critique du P3P en ce qui a trait au standard pour la protection de la vie privée qu'il désire instaurer, lire : EPIC, *Pretty Poor Privacy : An Assessment of P3P and Internet Privacy*, Juin 2000, http://www.epic.org/reports/prettypoorprivacy.html

[409] Jon Weinberg, « Hardware-Based ID, Rights Management, and Trusted Systems », *Wayne State University, W3C - Privacy Activity Statement*, 1999, http://www.w3.org/Privacy/Activity.html et W3C, *Privacy Overview*, 1999, http://www.w3.org/Privacy/Overview.html

[410] À ce sujet, il est important de savoir que PICS n'est pas encore un système de filtrage concret. Le W3C s'est contenté de créer avec ces spécifications une plate-forme sur la base de laquelle peuvent être construits des systèmes de filtres. Les indications générales concernant la technique et les procédés employés permettent à PICS de s'assurer que tous les systèmes développés sur cette base sont compatibles entre eux. Voir W3C, *PICS Statement of Principles*, http://www.w3.org/pub/WWW/PICS/Principles.html, Joel R. REIDENBERG, « The Use of Technology to Assure Internet Privacy : Adaption Labels and Filters to Data Protection », *Lex Electronica*, Volume 3, Numéro 2, http://www.lex-electronica.org/reidenbe.html, Jonathan WEINBERG, « Rating the Net », 19 *Hastings Comm/ent L.J.* 453 (1997) http://www.msen.com/~weinberg/rating.htm et Ari STAIMAN, « Shielding Internet Users from Undesirable Content : The advantage of a PICS Based Rating System », *20 Fordham Int'l L.J.* 866 (1997).

personnels sur son visiteur devra négocier *a priori* avec le fureteur pour vérifier s'il a le droit de récolter des renseignements personnels.

Chaque profil d'utilisateur contient les renseignements personnels et les informations concernant les préférences et les centres d'intérêts de l'usager. En principe, P3P permet d'enregistrer divers types d'informations. Il existe cependant certaines informations obligatoires, dont celles d'un identifiant unique qui désigne le profil et les sites Web visités que les usagers doivent obligatoirement remplir. Néanmoins, dix autres catégories de données transmissibles sont présentement définies parmi lesquels il existe, par exemple, la possibilité de fournir exclusivement des identificateurs uniques à caractère non commercial[411].

En pratique, lorsqu'un usager visite un site Web qui accepte la technologie P3P, le serveur du site Web interroge le profil de l'usager contenu dans son fureteur et transfère les renseignements personnels en fonction des préférences pré-définies par l'usager. Un usager peut, par exemple, choisir de transmettre des informations concernant ses centres d'intérêts et interdire la transmission de renseignements personnels, tels son nom et son adresse de courrier électronique. De plus, si lors de la visite le serveur du site Web visité tente d'obtenir plus d'informations que l'usager ne l'autorise, il sera automatiquement avisé de cette tentative et pourra soit décider de quitter le site ou d'accepter de transférer les informations demandées[412]. Il est important de souligner que la transmission des renseignements personnels, ceux inscrits dans les catégories obligatoires, n'est autorisée qu'en cas de nécessité absolue, tel lors d'un achat dans un magasin virtuel.

---

[411] Les catégories sont destinées à classer l'usager dans l'une des dix catégories de données transmissibles lors de la consultation d'un site Web :

1. Renseignements pour une prise de contact physique (adresse, numéro de téléphone),
2. Renseignements pour une prise de contact en ligne (adresse de courrier électronique),
3. Identificateur unique à caractère non commercial (numéro d'assurance ou de sécurité sociale),
4. Renseignements financiers (numéro de carte de crédit ou de compte bancaire),
5. Données informatiques (numéro IP, version de fureteur),
6. Données transactionnelles (mots clés utilisés lors de l'interrogation de moteurs de recherche, achats en ligne effectués),
7. Données de navigation (les sites que l'usager a visités, achats en ligne effectués),
8. Données démographiques ou socio-économiques (âge, sexe, revenu disponible),
9. Données sur les préférences personnelles de l'usager (couleurs, musique),
10. Données sur le contenu (mots et expressions utilisés dans une communication avec un site).

[412] W3C, *Platform for Privacy Preferences (P3P1.0) Specification*, 1999, http://www.w3.org/P3P/Overview/WD-P3P.html, Joseph REAGLE et Lorrie Faith CRANOR, « The Platform for Privacy Preferences », *P3P Note Draft 31 july 1998*, W3C, Cambridge, Massachusetts, http://www.w3.org/TR/1998/NOTE-P3P-CACM-19980731 et Elizabeth WEISE, « Net Privacy Standards Rolled Out for Federal Hearings », *New York Times*, http://search.nytimes.com/search/daily/bi...tweb?getdoc+site+site+16344+1+wAAA+etrust.html

Le standard P3P vise ainsi à permettre la vérification automatique des préférences d'un usager lorsque celui-ci visite un site Web et par le fait même, de permettre aux usagers de mieux contrôler et gérer les collectes de leurs renseignements personnels[413].

C. La situation conflictuelle

À l'intérieur des environnements électroniques décentralisés, les récoltes et l'utilisation des renseignements personnels sont encadrés par différentes juridictions. Tel que le soulignent Raysman et Brown :

> *« Legal protection of personal information varies from country to country and may be based on laws, ordinances, directives and industry self-regulation.*
>
> *Although there is a wide range in the rigorousness of the legal standards for balancing indidivuals' needs for privacy with commercial requirements for data collection in various countries, the principles that guide the developing laws and voluntary codes of commercial practice have some similarities*[414]*. »*

Bien qu'il soit rassurant de constater que la grande majorité des pays industrialisés disposent de législations visant à protéger les renseignements personnels des usagers des réseaux informatiques, cela ne règle toutefois pas les difficultés pratiques d'applications suscitées par la délocalisation et l'intangibilité de cette information numérique[415].

L'application des règles consacrées par les différentes législations et instruments internationaux s'avère relativement aisée lorsqu'il s'agit de policer l'État et les groupes industriels qui ont pignon sur rue dans les divers ressorts nationaux[416]. Toutefois, vu la nature même d'Internet, c'est-à-dire un réseau transfrontière soumis aux différentes législations nationales, la véritable difficulté se trouve au plan international.

---

[413] Bob METCALFE, « TRUSTe uses consents and disclosures to protect privacy on the Internet », 10 novembre 1997, *Info World*, http://www.infoworld.com/cgi-bin/displayNews.pl?/metcalfe/971110bm.html, W3C, *Platform for Privacy Preferences (P3P1.0) Specification*, 1999, http://www.w3.org/P3P/Overview/WD-P3P.html, Joseph REAGLE et Lorrie Faith CRANOR, « The Platform for Privacy Preferences », *P3P Note Draft 31 july 1998*, W3C, Cambridge, Massachusetts, http://www.w3.org/TR/1998/NOTE-P3P-CACM-19980731

[414] Richard RAYSMAN et Peter BROWN, « Privacy in the Internet », 12 mai 1998, *New York Law Journal*, http://www.ljx.com/securitynet/articles/0512privacy.html

[415] Karim BENYEKHLEF et Pierre TRUDEL, *Approches et stratégies pour améliorer la protection de la vie privée dans le contexte des inforoutes*, Mémoire présenté à la Commission de la culture de l'Assemblée nationale dans le cadre de son mandat sur l'étude du Rapport quinquennal de la Commission d'accès à l'information, septembre 1997, p. 18.

[416] Karim BENYEKHLEF et Pierre TRUDEL, *Approches et stratégies pour améliorer la protection de la vie privée dans le contexte des inforoutes*, Mémoire présenté à la Commission de la culture de l'Assemblée nationale

La protection des renseignements personnels dans les environnements électroniques pose plusieurs difficultés. En particulier, elle met en exergue l'intérêt des pays usagers de ces réseaux, d'harmoniser leurs mécanismes relatifs à la protection des renseignements personnels[417].

La popularité du réseau Internet a créé un effet de loupe sur la protection des renseignements personnels. Au moment où il est possible, en quelques secondes seulement, d'avoir accès à une multitude d'information sur un individu, de concevoir des profils de consommation et de transiger rapidement ces informations d'un pays à l'autre, le réseau Internet a accentué l'intérêt des usagers à protéger leur vie privée[418]. Ironiquement, il se dégage de l'intérêt des pays à protéger les renseignements personnels, deux méthodes de protection tout à fait à l'opposé l'une de l'autre.

Tout d'abord, on retrouve les États-Unis où l'essentiel des sites Web qui effectuent du commerce électronique sont localisés. Les Américains prônent l'adoption de mécanismes d'autorégulation à l'aide de codes de bonne conduite issus de l'industrie. Ils privilégient l'autorégulation du réseau en laissant les acteurs du secteur privé établir leur politique en matière de récolte et d'exploitation des renseignements personnels. En second lieu, il y a les États européens qui, à l'aide de la *Directive*, encouragent aussi l'adoption de codes de bonne conduite, mais en imposant l'adoption de législations de protection des renseignements personnels octroyant aux consommateurs un droit à l'accès et de rectification des informations les concernant[419].

---

dans le cadre de son mandat sur l'étude du Rapport quinquennal de la Commission d'accès à l'information, septembre 1997, p. 18.

417 Pierre TRUDEL, France ABRAN, Karim BENYEKHLEF et Sophie HEIN, *Droit du cyberespace*, Montréal, Éditions Thémis, 1996, p. 11-37.

418 « Les environnements électroniques supposent l'interconnexion des réseaux et l'interaction informatisée. Ils multiplient la masse d'informations à caractère personnel disponible. Ce phénomène, que l'on qualifie de dépossession informationnelle, suscite une série de questions quant aux mécanismes de protection de la vie privée existants. » Pierre TRUDEL, France ABRAN, Karim BENYEKHLEF et Sophie HEIN, *Droit du cyberespace,* Montréal, Éditions Thémis, 1996, p. 11-37.

419 « The Directive is perceived to be substantially more protective of privacy than the current American regulatory scheme for various reasons. First, the Directive contemplates the establishment of national privacy regulators in each EU member state, something unknown in the United States. Moreover, the Directive establishes and requires adoption of a nationwide privacy law in each member state, governing all processing of personal data, whether by computer or manually, and applying across the board to all industry segments and transactions. The Directive is not limited to the regulation of handling information obtained at the data gathering stage, nor to that obtained through a particular medium. The Directive applies to all processing of data, regardless of how that data came into the hands of the processor, and it contains an expanded list of subjects deemed to be sensitive, as to which special restrictions on use and transfer apply. » Karl D. BELGUM, « Who Leads at Half-time?: Three Conflicting Visions of Internet Privacy Policy », 6 *Rich. J.L. & Tech.* 1, (Symposium 1999), http://www.richmond.edu/jolt/v6i1/belgum.html

Le caractère résolument international du réseau Internet soulève, notamment au niveau de l'équivalence des protections offertes, de difficiles questions liées à la protection transnationale des renseignements personnels[420]. L'opposition des Américains face à la *Directive* pose un bémol à la coopération internationale pour la protection des renseignements personnels sur le réseau Internet.

Plus particulièrement, l'article 10 de la *Directive* qui édicte :

> *« Le responsable du traitement ou son représentant doit fournir à la personne auprès de laquelle il collecte des données la concernant, au moins les informations énumérées ci-dessous, sauf si la personne en est déjà informée :*
>
> *a) L'identité du responsable du traitement et, le cas échéant, de son représentant,*
>
> *b) Les finalités du traitement auquel les données sont destinées,*
>
> *c) Toute information supplémentaire telle que :* [...] »

va, comme le souligne le professeur Swire, à l'encontre de la pratique établie par l'industrie américaine en ce domaine[421]. « Contrary to the common U.S. practice of permitting a company to use personal data for unlimited purposes, data can only be processed for the announced purposes[422]. »

Outre les obligations concernant les collectes de renseignements, la *Directive* envisage notamment la lutte contre la délocalisation des traitements des bases de données dans les pays en interdisant le transfert des renseignements personnels vers un pays n'offrant pas une protection adéquate. Plus spécifiquement, l'article 25 édicte que le transfert de données à caractère personnel ne peut avoir lieu que si, sous réserve du respect des

---

[420] Constatant les multiples fonctionnalités potentielles des autoroutes de l'information et leur caractère résolument international, il semble nécessaire, parallèlement à ces instruments, de développer des règles complémentaires ou spécifiques pour encadrer l'exercice des principes qu'ils reconnaissent. Le fait que la protection des renseignements personnels ne soit pas uniforme internationalement, soulève de sérieuses questions autour de l'application du principe d'équivalence. Pierre TRUDEL, France ABRAN, Karim BENYEKHLEF et Sophie HEIN, *Droit du cyberespace*, Montréal, Éditions Thémis, 1996, p. 11-38. Voir Joel REIDENBERG et Françoise GAMET-POL, « The Fundamental Role of Privacy and Confidence in the Network », (1995) 30 *Wake Forest Law Review* 105, 110-111 et Karim BENYEKHLEF, « Les normes internationales de protection des données personnelles et l'autoroute de l'information », dans *Le respect de la vie privée dans l'entreprise*, Actes des Journées Maximilien Caron, Montréal, Éditions Thémis, 1996, p. 66.

[421] De plus, au mois de juillet 1998, Reidenberg soulignait que les États-Unis ne rencontreraient pas les exigences de la *Directive*. John MARKOFF, « U.S. and Europe Clash Over Internet Consumer Privacy », 1 juillet 1998, *New York Times*, http://search.nytimes.com/search/daily/bin/fastweb?getdoc+site+sie+68392+0+wAAA+p3p

[422] Peter P. SWIRE, « Of Elephants, Mice, and Privacy: International Choice of Law and the Internet », *Draft submitted to International Lawyer*, 23 août 1998, http://www.acs.-ohio-state.edu/units/law/swire1/elephants.htm.

dispositions nationales prises en application des autres dispositions de la présente directive, le pays tiers en question assure un niveau de protection adéquat.

Sur le plan international, la *Directive* risque d'avoir un effet défavorable sur l'industrie de l'information, tels les bureaux de crédit, les services financiers et toutes les autres entreprises qui dépendent directement ou indirectement des collectes et transferts des renseignements personnels. Tel que l'écrit Gindin : « Because the EU takes such an all-encompassing approach to data protection, the Directive would also seem to affect entities with Internet Web sites which collect personal data from Web site visitors, even if the entity does not actually transact business with anyone in the EU[423]. »

Depuis plus de deux ans, le gouvernement américain met néanmoins la protection des renseignements personnels au premier plan de ses priorités. L'entrée en vigueur de la *Directive* en octobre 1998 a soumis les pouvoirs publics américains à une double pression, soit :

- L'imposition de barrières à la transmission de fichiers, et
- L'opinion publique américaine qui dénonce de façon générale l'absence de législation.

Attardons-nous tout particulièrement à la première pression qui pèse sur les autorités publiques américaines, soit l'article 25 de la *Directive*. Cet article oblige les pays non-européens à garantir une protection adéquate lors d'un transfert de renseignements personnels.

En vertu de l'article 25(2), le caractère adéquat du niveau de protection offert par un pays tiers s'apprécie :

> « [...] *Au regard de toutes les circonstances relatives à un transfert ou à une catégorie de transferts de données ; en particulier, sont prises en considération la nature des données, la finalité et la durée du ou des traitements envisagés, les pays d'origine et de destination finale, les règles de droit, générales ou sectorielles, en vigueur dans le pays tiers en cause, ainsi que les règles professionnelles et les mesures de sécurité qui y sont respectées.* »

---

[423] Susan E. GINDIN, « Lost and found in cyberspace: Information privacy in the age of the Internet », 1997 *San Diego Law Review*, http://www.info-law.com/lost.html.

La notion de protection adéquate doit ainsi être évaluée au cas par cas, selon une approche simple, ouverte et fonctionnelle[424]. Les premiers jugements relatifs au caractère adéquat de la protection offerte en vertu de la *Directive* seront rendus par les autorités nationales responsables de la protection des données. Les articles 25 (3), (4) et (5) énoncent à ce sujet :

> « *Les États membres et la Commission s'informent mutuellement des cas dans lesquels ils estiment qu'un pays tiers n'assure pas un niveau de protection adéquat au sens du paragraphe 2.*
>
> *Lorsque la Commission constate [...] qu'un pays tiers n'assure pas un niveau de protection adéquat au sens du paragraphe 2 du présent article, les États membres prennent les mesures nécessaires en vue d'empêcher tout transfert de même nature vers le pays tiers en cause.*
>
> *La Commission engage, au moment opportun, des négociations en vue de remédier à la situation résultant de la constatation faire en application du paragraphe 4*[425]. »

À la lecture de cet article, il appert, sans équivoque, que l'Union européenne désire que leur *Directive* reçoive une application mondiale[426]. En conséquence, le Canada est entré dans la valse européenne[427]. Néanmoins, depuis quelque temps, on voit aux États-Unis, se dessiner certaines initiatives en vue d'éviter des problèmes sérieux résultant des récoltes de renseignements personnels. Malgré leur différence, l'objectif est toujours le même ; minimiser les inconvénients éventuels. Elles visent à assurer et maintenir une circulation normale des renseignements personnels qui est nécessaire et

---

[424] André GIROUX, « La vie privée est-elle protégée : Québec un chef de file dans le domaine », *J. du B.*, Volume 29, Numéro 20, http://www.www.barreau.qc.ca/journal/vol29/no20/viepriveeprotegee.html.

[425] Il convient de souligner que, si la Commission estime que le niveau de protection fourni n'est pas adéquat, les États membres se trouvent tenus d'interdire le transfert – et ne sont pas seulement autorisés à l'interdire –, au moyen de ce que Paul Schwartz a appelé « l'imposition d'un embargo sur les données ». Colin BENNETT, *Réflexions sur une norme internationale de protection des renseignements personnels, Chapitre 3 - Instruments de réglementation des flux de données transfrontières*, Groupe de travail sur le commerce électronique d'Industrie Canada, http://e-com.ic.gc.ca/francais/privee/632d29.html

[426] Selon le professeur Reidenberg, la *Directive* sera reprise au niveau mondial même en l'absence de législations des États. Le marché européen est tel que les entreprises n'auront pas le choix. Joel REIDENBERG et P. SCHWARTZ, *Online Services and Data Protection Law: Regulatory Responses*, EUR-OP: 1998, http://europa.eu.int/comm/internal_market/en/media/dataprot/studies/regul.pdf

Néanmoins, le professeur BENNETT quant à lui est plus sceptique et soulève quelques interrogations face à la Directive. Colin BENNETT, *Réflexions sur une norme internationale de protection des renseignements personnels, Chapitre 3 - Instruments de réglementation des flux de données transfrontières*, Groupe de travail sur le commerce électronique d'Industrie Canada, http://e-com.ic.gc.ca/francais/privee/632d29.html.

[427] À cet effet, le commissaire de la vie privée pour la province de l'Ontario stipule que le Canada n'avait pas d'autres choix que d'adopter une législation pour la protection des renseignements personnels. « There was [no similar law] in Canada except in the province of Quebec, so Quebec could do business with Europe, but the rest of Canada couldn't. » Matt FRIEDMAN, « Canada Aligns with EU on Privacy », 20 avril 1999, *Wired*, http://wired.com/news/print_version/politics/story/19210.html?wnpg=all

indispensable dans les secteurs névralgiques de l'activité économique et même politique.

À la face même de la protection offerte aux États-Unis et en consultant la liste blanche de l'Union européenne qui recense tous les pays répondants à leur critère de protection adéquate, on constate que les protections offertes en sol américain ne sont pas adéquates[428]. « Assurément, tous les gains réels en terme de protection des renseignements personnels aux États-Unis s'avèrent très modestes. Ces gains semblent particulièrement limités quand on les compare aux progrès réalisés dans certains pays d'Europe[429]. »

Pour contrer l'effet que la *Directive* produit aux États-Unis, les Américains ont décidé de passer à l'action. Le dialogue entre les États-Unis et la Commission européenne a commencé avant même que la directive relative à la protection des données n'entre en vigueur en octobre 1998. Ainsi, dans le double but d'assurer un niveau élevé de protection des données et de préserver le libre transfert de données par delà l'Atlantique, les Américains ont présenté à l'Union européenne, au courant du printemps 1998, les « Safe Harbor Principles[430] ». Avec ces principes, les Américains désirent que les entreprises américaines continuent de collecter des renseignements personnels sur les usagers européens dans certaines circonstances.

Au cours des deux dernières années, les Américains et les Européens se sont chamaillés sur le niveau de protection à garantir aux individus quant aux

---

[428] « The Commission also indicated that those countries which have ratified the Council of Europe Convention 108 on data protection would be included on the white list as long as the country has an appropriate regulatory mechanism, and the country is the final destination of the data transfer.

In the policy paper, the Commission also mentioned that countries with data privacy protection legislation covering certain sectors might merit a partial white listing or that regulated industries would be included in a white list of sectors within countries. Such partial listings would seem appropriate for transfers of data to certain industry or government entities within the U.S., Canada, Australia, and Japan, which all have data privacy protection policies covering information handling by the federal governments and certain industry sectors. » Susan E. GINDIN, « Lost and found in cyberspace: Information privacy in the age of the Internet », 1997 San Diego Law Review, http://www.info-law.com/lost.html. Voir EUROPEAN COMMISSION, *First Orientations on Transfers of Personal Data to Third Countries: Possible Ways Forward in Assessing Adequacy*, 26 juin 1997, http://zeus.bna.com/e-law/docs/eudata1.html

[429] Joel REIDENBERG et P. SCHWARTZ, *Online Services and Data Protection Law: Regulatory Responses*, EUR-OP: 1998, http://europa.eu.int/comm/internal_market/en/media/dataprot/studies/regul.pdf

[430] « The principles were developed in consultation with industry and the general public to facilitate trade and commerce between the United States and European Union. They are intended for use solely by U.S. organizations receiving personal data from the European Union for the purpose of qualifying for the Safe Harbor and the presumption of adequacy it creates. Because these principles were solely designed to serve this specific purpose, their adoption for other purposes may be inappropriate. » *International Safe Harbor Privacy Principles*, 19 avril 1999, http://www.ita.doc.gov/ecom/menu.html

renseignements personnels récoltés sur Internet et échangés entre les sites Web, avec ou sans le consentement des internautes[431]. À maintes reprises, les experts européens ont déploré le fait que le cadre de « havre de paix[432] » prôné par les Américains ne répondait pas aux principes minimaux établis par la *Directive*[433]. Outre l'Union européenne, plusieurs grandes entreprises américaines telles AOL et Disney, se sont aussi opposées à ces principes à ce moment là[434].

Les débats internationaux ont été virulents[435] et peu de gens s'attendaient au début de l'année 2000 à un accord prochain entre les parties. À ce moment là, l'Union européenne énonçait au sujet de la version des principes du Safe Harbor présentée au mois de février 2000, qu'ils « doesn't go far enough to protect Internet users' data privacy[436]. » De plus, Jim Murray, directeur de l'OCDE ajoutait : « We do not feel that the Safe Harbor proposal provides adequate enforcement to safeguard the interest of European citizens.[437] »

Toutefois, au courant des mois d'avril et de mai 2000, la vapeur fut renversée. Le 30 mai 2000, à la grande surprise de plusieurs, la Communauté européenne accepta une nouvelle version des principes du Safe Harbor concernant la protection des renseignements personnels. Au sujet de cet accord, M. William M. Daley, Secrétaire d'État au Commerce, énonce :

---

[431] Plus particulièrement, cette querelle résulte de l'article 25 de la *Directive*.

[432] Communément nommé « Safe Harbor » en anglais.

[433] J. THOREL, « L'Europe et les États-Unis en désaccord sur les données nominatives », 10 décembre 1999, *ZDNet*, http://www.zdnet.fr/actu/inte/a0011939.html.

[434] Maria SEMINERIO, « AOL, Disney oppose privacy plan, companies balks to U.S.-European Union privacy compromise », 16 mars 1999, *ZDNet*, http://www.zdnet.com/xdnn/stories/news/0,4586,2226769,00.html

[435] Comme le souligne la Commission européenne, « The topic of consumer data privacy has been particularly contentious during these negotiations, which have spanned two years. Each side of the Atlantic has its own privacy philosophy: The EU favors stricter government regulation, while the United States generally advises a more laissez-faire approach. » Declan MCCULLAGH, « U.S., E.U. Approach Safe Harbor », 9 mai 2000, *Wired*, http://www.wired.com/news/politics/0,1283,36235,00.html

[436] « The latest draft of Safe Harbor [...] indicates the points that have stalled negotiation. Specifically, the EU isn't satisfied with the US proposal to allow consumers access to data kept about them, or with the plan's enforcement provisions. » James GLAVE, « Safe Harbor: No Port in a Storm? », 28 avril 1999, *Wired*, http://www.wired.com/news/print_version/politics/story/19389.html?wnpg=all

[437] Maria SEMINERIO, « Groups take EU privacy fight public », 28 avril 1999, *ZDNet*, http://www.zdnet.com/zdnn/storie/news/0,4586,2248878,00.html.

> *« The accord will enable U.S. organizations to comply with European privacy regulations and continue to receive personal data from Europe.*
>
> *This is a landmark accord for e-commerce because it bridges the differences between EU and U.S. approaches to privacy protection. [...] Once the accord is implemented, it will enhance consumer confidence by protecting European citizens' privacy, reduce business costs, and keep data flowing across the Atlantic.*
>
> *The safe harbor is a mechanism which, through an exchange of documents, enables the EU to certify that participating U.S. companies meet the EU requirements for adequate privacy protection. Participation in the safe harbor is voluntarily. Organizations will need to adhere to the privacy requirements laid out in the safe harbor documents for all received from the EU*[438]*. »*

Cet accord qui reste à être approuvé par la Commission européenne au mois de juillet 2000, devrait être en vigueur au courant de l'automne prochain. Grâce à cette entente, la Commission européenne certifie que les entreprises américaines rencontreront les exigences de la *Directive* pour la protection des renseignements personnels[439]. L'accord qui repose sur l'adoption volontaire de codes de bonne conduite par les entreprises américaines est ainsi censé protéger de manière «adéquate» le citoyen européen des récoltes de renseignements personnels outre-Atlantique.

Selon cet accord[440], le ministère du commerce américain dressera une liste des entreprises qui adhèrent à un ensemble de règles de protection des données et de critères de respect dont la Commission a jugé qu'il assurait une protection « appropriée ». Les adhérents seront donc prémunis contre le blocage des données, les entreprises de l'Union européenne sauront à quelles entreprises américaines elles peuvent transférer des données sans rechercher d'autres sauvegardes, et les citoyens de l'Union européenne auront l'assurance que leurs données sont convenablement protégées. Pour ainsi bénéficier des avantages procurés par cet accord, les entreprises américaines devront s'engager publiquement à en respecter les principes. Le respect des conditions sera vérifié en premier lieu par des organismes du secteur privé, et leur

---

[438] UNITED STATES – DEPARTMENT OF COMMERCE, *Commerce Secretary William M. Daley – Hails EU approval of Safe Harbor Privacy Arrangement*, 31 mai 2000, http://www.ita.doc.gov/media/safeharbor531.htm

[439] Jason SPINGARN-KOFF, « European Union OKs 'Safe Harbor' », 31 mai 2000, *Wired*, http://www.wired.com/news/politics/0,1283,36671,00.html

[440] Pour plus de détails au sujet de l'accord, voir l'Annexe 2.

non-respect fera l'objet de sanctions légales[441], notamment au titre de l'article 5 du *US Federal Trade Commission Act*, qui interdit les fausses déclarations et les pratiques commerciales trompeuses consistant par exemple à annoncer le respect d'une disposition relative à la préservation de la vie privée et à l'ignorer par la suite[442].

Selon la Commission européenne, une fois approuvée, l'accord du Safe Harbor[443] :

- Aboutira à une meilleure protection des données transférées aux États-Unis
- Créera un cadre plus prévisible et moins administratif pour les contrôleurs de données de l'Union européenne qui doivent opérer un transfert à destination des Etats-Unis ;
- Fournira des indications aux entreprises et autres organisations implantées aux États-Unis qui veulent satisfaire à la norme de « protection adéquate » et
- Instaurera la sécurité juridique nécessaire à ceux qui y adhèrent et qui sauront que leurs transferts de données ne seront pas interrompus.

Pour les défenseurs de l'autoréglementation américaine, cet accord négocié est un gain important. Selon Andrew Pincus, conseiller général pour le Ministère du Commerce Américain : « This is important because of the recognition that self-regulation can enforce privacy ... at a lower cost and (with) simpler means[444]. » De plus, cet accord permet de mettre fin aux négociations qui auraient pu sérieusement affecter les échanges commerciaux entre les deux parties qui étaient évalués à 350 milliards en 1999[445].

Néanmoins, cet accord n'emballe pas tout le monde. En annonçant la signature du Safe Harbor avec le ministère américain du Commerce, la Commission européenne est allée

---

[441] Selon la Commission européenne, « One of the issues that is of course still outstanding -- and that we are putting enormous emphasis on -- is enforcement. That's the key difference between legislation and self-regulation, and that's why we're spending a lot of time on it. The difference here is that enforcement will be entirely on the shoulders of the industry, while in Europe the enforcement is done, of course, by data privacy commissioners. » Declan MCCULLAGH, « U.S., E.U. Approach Safe Harbor », 9 mai 2000, *Wired*, http://www.wired.com/news/politics/0,1283,36235,00.html

[442] COMMISSION EUROPÉENNE, « Protection des données: la Commission approuve l'arrangement relatif au « port sûr » avec les Etats-Unis », 5 juin 2000, http://europa.eu.int/comm/internal_market/fr/media/dataprot/news/harbor4.htm

[443] COMMISSION EUROPÉENNE, « Protection des données: la Commission approuve l'arrangement relatif au « port sûr » avec les Etats-Unis », 5 juin 2000, http://europa.eu.int/comm/internal_market/fr/media/dataprot/news/harbor4.htm

[444] Declan MCCULLAGH, « U.S. , E.U. Approach Safe Harbor », 9 mai 2000, *Wired*, http://www.wired.com/news/politics/0,1283,36235,00.html

[445] UNITED STATES – DEPARTMENT OF COMMERCE, *Commerce Secretary William M. Daley – Hails EU approval of Safe Harbor Privacy Arrangement*, 31 mai 2000, http://www.ita.doc.gov/media/safeharbor531.htm

trop vite selon une résolution émise par une commission du Parlement de Strasbourg. Elle énonce à ce sujet :

> « *Le citoyen européen n'est en rien protégé par le Safe Harbor. Une protection adéquate n'implique pas ipso facto que le pays tiers dispose de règles analogues à celles de l'Union, mais que le propriétaire des données [le citoyen] doit être protégé de manière effective. Cette protection existera lorsque son efficacité [pourra] être mesurée sur la base de données objectives, comme la possibilité d'identifier les personnes auxquelles incombent des obligations, le type de données traitées, l'utilisation susceptible d'en être faite et les mécanismes mis en œuvre pour les protéger*[446]. »

Le *Safe Harbor* repose sur des « normes volontaires qui ne constituent pas un engagement contractuel opposable aux entreprises qui ne les respectent pas »[447]. Aux États-Unis, la collecte de renseignements personnels repose sur la seule bonne volonté des entreprises. Celles-ci ne sont pas soumises aux lois européennes très strictes en la matière. En Europe, contrairement à ce qui se produit aux États-Unis, tout citoyen a le droit d'accéder aux données numériques qui le concernent et de les faire rectifier ou détruire. De plus, des sanctions sont aussi prévues pour les contrevenants. En vertu du Safe Harbor, le seul recours qui sera possible pour un internaute lésé sera de porter plainte auprès de la FTC. Ce recours est très limité étant donné que la FTC n'est pas obligée de le prendre en considération et d'y donner suite ; il s'ensuit que l'examen des milliers de plaintes introduites par des citoyens américains est laissé à la discrétion de la commission fédérale du commerce qui n'intervient, en fait, que sporadiquement[448]. À la lumière de ces précisions, il appert que les internautes européens seront les grands perdants de ce nouvel accord.

Comme nous le constatons, l'application pratique et opérationnelle des législations et/ou de codes de conduite nationaux n'est pas aisée sur le réseau Internet. Une coopération

---

[446] Jerome THOREL, « Vie privée : le Parlement européen prêt à torpiller le *Safe Harbor* », 10 juin 2000, *ZdNet*, http://www.zdnet.fr/actu/soci/a0014633.html

[447] Jerome THOREL, « Vie privée : le Parlement européen prêt à torpiller le *Safe Harbor* », 10 juin 2000, *ZdNet*, http://www.zdnet.fr/actu/soci/a0014633.html

[448] Jerome THOREL, « Vie privée : le Parlement européen prêt à torpiller le *Safe Harbor* », 10 juin 2000, *ZdNet*, http://www.zdnet.fr/actu/soci/a0014633.html

internationale est essentielle si l'on désire garantir la protection des renseignements personnels sur Internet[449]. Néanmoins, celle-ci se doit aussi d'être véritable.

Au Canada, l'adoption de la *Loi sur la protection des renseignements personnels et les documents électroniques* a laissé les Américains seuls dans leur camp en Amérique du Nord. Comme le souligne le professeur Friedman : « The imminent passage of the Canadian privacy bill may leave the United States -- Canada's largest single trading partner -- alone in its opposition to the European plan »[450]. En optant pour la solution européenne, le Canada a mit énormément de pression sur l'administration publique américaine. Il a rappelé à l'oncle Sam que le réseau Internet est un médium international où l'on ne peut ignorer la protection des renseignements personnels.

Outre la pression qui découle de l'entrée en vigueur de la *Directive*, les autorités publiques américaines font aussi face à une seconde pression découlant directement de la première. Cette seconde pression remet en question le mode de protection choisi par les Américains pour protéger leurs renseignements personnels. Depuis plusieurs mois, l'opinion publique américaine dénonce, de façon générale, l'absence de législation visant à protéger les renseignements personnels des citoyens américains. Toutefois, nombreux sont les observateurs qui prédisent l'élaboration d'une telle législation prochainement.

En effet, depuis le mois d'avril 1999, l'administration Clinton brandit le spectre d'une législation de protection des renseignements personnels[451]. « New privacy protections were needed because technological advances made it easier than ever to collect and disseminate detailed information about consumers' finances and spending habits[452]. »

> « *Consumers have the right to know who is collecting information about them and how that information is being used* [...]

---

[449] Karim BENYEKHLEF, « Les normes internationales de protection des données personnelles et l'autoroute de l'information », dans *Le respect de la vie privée dans l'entreprise*, Actes des Journées Maximilien Caron, Montréal, Éditions Thémis, 1996, 66, p.101.

[450] Matt FRIEDMAN, « Canada Aligns with EU on Privacy », 20 avril 1999, *Wired*, http://wired.com/news/print_version/politics/story/19210.html?wnpg=all

[451] « We have reached the point that if you have a medical record, credit card or computer, you have a privacy problem » énonce le Sénateur Patrick Leahy. Michele MASTERSON, « Privacy fuels gov't efforts », 9 Mars 2000, *CNN – The financial network*, http://cnnfn.com/2000/03/09/technology/q_legislation/

[452] Donna SMITH, « Clinton Argues for New Privacy Protections », 1 mai 2000, *ZdNet*, http://www.zdnet.com/zdtv/zdtvnews/politicsandlaw/story/0,3685,2559123,00.html

The Internet holds great promise as an international marketplace, but consumers won't use it to its full potential unless they feel safe[453]. »

L'importance de créer une telle législation selon l'EPIC, repose sur la reconnaissance du fait que la méthode d'autoréglementation américaine pour la protection des renseignements personnels n'a jamais et ne fonctionnera jamais. Comme le souligne le professeur Lessig : « The mystery isn't that self-regulation failed ; the mystery is why anyone thought it would succeed[454]. »

Face à la situation éminente laissant présager l'adoption d'une loi de protection des renseignements personnels, les acteurs de l'industrie américaine se mobilisent pour contrer l'instauration d'une telle législation. À ce sujet, Harris Miller, président de l'Information Technology Association of America, énonce :

« We think industry self-regulation is moving forward very constructively.

Any talk of legislative solutions is simply not helpful at this point in time. Obviously, the market demand is out there to put pressure on industry. If consumers are not comfortable, the market will speak and companies will respond. »

La FTC, qui a changé d'opinion depuis et qui reconnaît l'échec de l'autoréglementation, avait recommandé, au mois de juillet 1999, de ne pas adopter une telle législation et de laisser les entreprises réglementer elles-mêmes la collecte et l'utilisation des renseignements personnels[455].

Au soutien de leurs allégations, la FTC croit que l'industrie est sur la bonne voie en raison du progrès énorme qu'elle a fait depuis les dix-huit derniers mois. En effet, le sondage publié au mois de juin 1999 par l'Université Georgetown, démontre que 66 % de sites Web possèdent une politique en matière de vie privée[456]. En conséquence,

---

[453] Jeri CLAUSING, « New Bill Keeps Online Privacy at Center Stage », 17 avril 1999, *New York Times*, http://search.nytimes.com/search/daily/bi...web?getdoc+site+site+71864+13+wAAA+truste. De plus, plusieurs États américains envisagent de légiférer sur la protection des renseignements personnels. Voir Chris OAKES, « Tackling E-Privacy in New York », 3 juin 1999, *Wired*, http://www.wired.com/news/print_version/politics/story/19991.html?wnpg-=all.

[454] Lawrence LESSIG, « Coding privacy », 21 mai 1999, *The Industry Standard*, http://www.thestandard.com/articles/display/0,1449,4620,00.html?01. De plus, selon l'EPIC : « We think there is plenty of evidence that self-regulation has not worked. Self-regulation is leading to a lowering of the expectation of privacy. » Jeri CLAUSING, « Gain for Online Industry on Privacy Issue », 13 juillet 1999, *New York Times*, http://forums.nytimes.com/library/tech/99/07/cyber/articles/13ptivacy.html

[455] Laure NOUALHAT, « L'Amérique veut renforcer la protection des données privées », 24 mai 2000, *ZdNet*, http://www.zdnet.fr/actu/soci/a0014404.html

[456] Georgetown Internet Privacy Policy Study, 21 juillet 1999, http://www.msb.edu/faculty/culnanm/gippshome.html.

comparativement au même sondage effectué en 1998, il y a eu une augmentation de 14 %. Néanmoins, il importe de souligner qu'il existe toujours près de 10 % de sites Web qui ne suivent pas les critères énoncés par la FTC concernant le droit de contrôle et de rectification des usagers[457].

La situation est conflictuelle. D'un côté se retrouvent l'Union européenne et ses alliés dont le Canada, et de l'autre, les États-Unis qui prônent un système sectoriel d'autoréglementation. Toutefois, à l'intérieur même du pays de l'oncle Sam, les idées sont divisées[458]. L'industrie désire à tout prix conserver son droit d'autoréglementation, alors que les consommateurs et l'autorité publique américaine prônent, de façon générale, pour l'approche législative.

Toutefois, il importe de souligner que dans la grande majorité des cas, ces politiques sont souvent de simples pétitions de principes ou de vœux pieux. «Very few Web sites have strong privacy policies-and a surprising number don't even have any policy. Only 3.5% of the 30,000 Web sites reviewed by Enonymous.com were judged to have a "four-star" privacy rating, the top mark given by the survey-and 77.2% had no privacy policy. » En consequence, selon l'EPIC, une politique adéquate en matière de vie privée devrait comporter : « There are many different privacy policies, but all good policies share certain characteristics: they explain the responsibilities of the organization that is collecting personal information and the rights of the individual who provided the personal information. Typically, this means that an organization will explain why information is being collected, how it will be used, and what steps will be taken to limit improper disclosure. It also means that individuals will be able to obtain their own data and make corrections if necessary. » EPIC, *Surfer Beware: Personal Privacy and the Internet*, Juin 1997, http://www.epic.org/reports/surfer-beware.html, Matthew G. NELSON, « Majority Of Web Sites Lack Privacy Policies » 17 avril 2000, *TechWeb*, http://www.techweb.com/se/directlink.cgi?IWK20000417S0076 et Kristen GERENCHER, « Web site privacy policies unclear, survey finds less than 4% of 30,000 sites reviewed get top grade » , 11 avril 2000, *CBS – Marketwatch*, http://cbs.marketwatch.com/archive/20000411/news/current/pf.htx?source=htx/http2_mw

[457] Jeri CLAUSING, « Gain for Online Industry on Privacy Issue », 13 juillet 1999, *New York Times*, http://forums.nytimes.com/library/tech/99/07/cyber/articles/13ptivacy.html.

[458] À ce sujet, Joel Reidenberg énonce : « In the United States today, substance abusers have greater privacy than web users and privacy has become the critical issue for the development of electronic commerce. Yet, the U.S. government's privacy policy relies on industry self-regulation rather than legal rights. » Joel REIDENBERG, « Restoring Americans' Privacy in Electronic Commerce », *Berkeley Technology Law Journal*, Volume 14-2, http://www.law.berkeley.edu/journals/btlj/articles/14_2/Reidenberg/html/reader.html

Chapitre 2

La standardisation comme méthode de protection des renseignements personnels sur Internet

Le phénomène de l'émergence des autoroutes de l'information demeure marqué par la technologie. Cette technologie a rendu possible le concept d'environnement électronique et par la force des choses, a introduit les problèmes liés à la protection de la vie privée. L'avènement des environnements électroniques n'a pas fait disparaître les motifs pour lesquels les législateurs ont trouvé nécessaire de réglementer la protection des renseignements personnels. Au contraire, les caractéristiques spécifiques à ces environnements ont renforcé ce choix.

Aujourd'hui, le défi posé par ces nouveaux médias de communication est celui du « comment » ; comment s'y prendre afin d'obtenir une réglementation applicable, uniforme et plus particulièrement, une protection adéquate des renseignements personnels[459]? Comme nous l'avons préalablement constaté, la technologie peut en grande partie contribuer à réduire ou éliminer les problèmes qu'elle a engendrés. En offrant des techniques performantes pour classifier et canaliser l'information, elle peut aider les usagers à exercer un contrôle approprié sur la circulation de leurs informations[460].

À l'intérieur d'un environnement qui ignore les frontières territoriales et où la capacité de contourner les règles ou tout simplement de s'exclure de leur application est possible et apparaît même plus facile que dans la plupart des autres environnements, il importe de se questionner sur le rôle que joue l'industrie dans la protection des renseignements personnels[461]. Concrètement, la question à poser est celle-ci : est-ce que l'industrie est,

---

[459] Pierre TRUDEL et France ABRAN, Karim BENYEKHLEF et Sophie HEIN, *Droit du cyberespace*, Montréal, Éditions Thémis, 1996, p. 15-1.

[460] David Post énonce à ce sujet : « One can hardly imagine, to be sure, a rule regarding, say, fraudulent transactions that would be capable of digital embodiment in these engineering specifications. One can imagine, however, a digital embodiment of rules regarding other activities – for example, the transmission of anonymous message, or encrypted files – that can be more easily expressed in digital form and thereby enforced at the level of the technical network specifications » dans « Anarchy, State and the Internet : An Essay on Law-Making in Cyberspace » (1995) *J. Online L. art. 3*, http://warthog.cc.wm.edu/law/publications/jol/post.html, par.24. Voir aussi Karim BENYEKHLEF et Pierre TRUDEL, *Approches et stratégies pour améliorer la protection de la vie privée dans le contexte des inforoutes*, Mémoire présenté à la Commission de la culture de l'Assemblée nationale dans le cadre de son mandat sur l'étude du Rapport quinquennal de la Commission d'accès à l'information, septembre 1997, p. 20.

[461] La possibilité de contournement découle du fait que la communication informatique suppose un geste volontaire de l'usager et de la possibilité de se raccorder ailleurs. « The unique nature of the Internet highlights the likelihood that a single actor might be subject to haphazard, uncoordinated, and even outright inconsistent regulation by states that the actor never intended to reach and possibly was unaware were being accessed.

à l'aide de la standardisation, en mesure de réglementer efficacement la protection et l'utilisation des renseignements personnels dans les environnements électroniques décentralisés ? Ou, au contraire, au lieu de voir se concrétiser une « E-industry » des renseignements personnels[462], n'est-il pas préférable d'élaborer une législation au soutien de la standardisation ? Comme le souligne certains auteurs, il appert à première vue que : « Trust can only be earned, not purchased[463] ».

A. La notion de « standardisation »

Il existe actuellement plusieurs outils et méthodes visant à protéger la vie privée et les renseignements personnels des internautes. Comme le souligne Susan E. Gindin : « Certain tools can be used by individuals to help protect their online privacy, and specific procedures can be used by the information industry to safeguard the privacy of individuals[464]. » Vu que la plupart des pays occidentaux disposent de législations visant la protection des renseignements personnels, c'est particulièrement aux États-Unis que l'on retrouve ces « specific procedures », communément appelé « méthodes de standardisation[465] ». Pourquoi ? La réponse est simple.

Aux États-Unis, le mode de protection choisi pour protéger les renseignements personnels, soit l'autoréglementation, laisse une grande marge de manœuvre à l'industrie pour instaurer une standardisation[466]. Pour ses défenseurs, l'autoréglementation est : « the most meaningful protection of privacy without intrusive government interference, and with the greatest flexibility for dynamically developing technologies[467] ». En conséquence, l'industrie se doit inévitablement de protéger ou de

---

Typically, states' jurisdictional limits are related to geography; geography, however, is a virtually meaningless construct on the Internet. » *American Library Association* c. *Pataki*, 969 F. Supp 160 (SDNY 1997).

[462] « Consumer date is big business for Web publishers, who gather it to help advertisers. But now a new industry is springing up that hopes to make money helping consumers evade Web trackers. » REUTERS, « The New E-Industry : Privacy », 11 octobre 1999, *Wired*, http://wired.com/news/print_version/business/story/22178.html?wnpg=all

[463] REUTERS, « The New E-Industry : Privacy », 11 octobre 1999, *Wired*, http://wired.com/news/print_version/business/story/22178.html?wnpg=all

[464] Susan E. GINDIN, « Lost and found in cyberspace: Information privacy in the age of the Internet », 1997 *San Diego Law Review*, http://www.info-law.com/lost.html

[465] Aussi nommé « normalisation technique ».

[466] Pour une étude détaillée du contexte, lire Andy BLACKBURN, Lori FEAN et Gigi WANG, « Description of the eTRUST Model » dans *Privacy and Self-Regulation in the Information Age*, *Chapter 5: Technology and Privacy Policy*, National Telecommunications and Information Administration, Juin 1997, http://www.ntia.doc.gov/reports/privacy/selfreg5.htm#5D

[467] Joel REIDENBERG, « Restoring Americans' Privacy in Electronic Commerce », *Berkeley Technology Law Journal*, Volume 14-2, http://www.law.berkeley.edu/journals/btlj/articles/14_2/Reidenberg/html/reader.html.

laisser croire qu'elle protège de façon juste et équitable les renseignements personnels des internautes. En élaborant des normes et leur mise en œuvre, l'industrie cherche ainsi à protéger les renseignements personnels dans le but d'obtenir la confiance des consommateurs et par le fait même, de maximiser leurs profits. Malgré les incitatifs purement financiers à la base de l'autoréglementation américaine et des méthodes de standardisation qui en découle, celles-ci ont tout de même des avantages comme nous l'avons constaté précédemment ; elles procurent en principe, en l'absence de législation, « a public assurance of privacy[468] ».

Dans le reste des pays occidentaux, la standardisation est quasiment absente en matière de protection des renseignements personnels. La présence de législations sur la protection des renseignements personnels procure une assurance aux internautes en ce qui a trait à leur vie privée lorsqu'ils naviguent sur le réseau. Néanmoins, le développement exponentiel des environnements électroniques multiplie la masse d'informations à caractère personnel disponible[469] et laisse, par le fait même, présager des difficultés de plus en plus importantes en ce qui a trait à l'application de ces lois dans un environnement qui fait fi des frontières physiques. Malgré les différentes législations applicables seulement à certains types précis de renseignements ou à secteurs et qui prévoient divers degrés de protection de la vie privée, l'instauration de méthodes de standardisation reprenant les principes juridiques soutenus par ces législations pourrait s'avérer bénéfique[470].

---

[468] Andy BLACKBURN, Lori FEAN et Gigi WANG, « Description of the eTRUST Model » dans *Privacy and Self-Regulation in the Information Age, Chapter 5: Technology and Privacy Policy*, National Telecommunications and Information Administration, Juin 1997, http://www.ntia.doc.gov/reports/privacy/selfreg5.htm#5D

[469] Les professeurs Trudel et Benyekhlef qualifient ce phénomène de « dépossession informationnelle ». Karim BENYEKHLEF et Pierre TRUDEL, *Approches et stratégies pour améliorer la protection de la vie privée dans le contexte des inforoutes*, Mémoire présenté à la Commission de la culture de l'Assemblée nationale dans le cadre de son mandat sur l'étude du Rapport quinquennal de la Commission d'accès à l'information, septembre 1997, p. 14.

[470] Lire l'article de Joël Boyer où celui-ci rapporte que la CNIL songe un instaurer un label de standardisation. Joël BOYER - secrétaire général de la CNIL chargé des affaires juridiques, « Sur le Net, effacer ses traces requiert un savoir-faire », 14 avril 2000, *Libération*, http://www.liberation.fr/multi/actu/20001004/20000414venzc.html

Selon Conseil canadien des Normes, « les normes ne s'appliquent [...] pas uniquement au commerce ou aux questions techniques. Elles s'appliquent aussi aux questions environnementales et sociales telles que la protection de la vie privée. » CONSEIL CANADIEN DES NORMES, « Un chemin tout tracé », *Revue canadienne d'actualités de normalisation*, Volume 24, Numéro 5 (Septembre 1997), http://www.scc.ca/consensu/1997/sept/ponder2405f.html

Aux États-Unis, la notion de « standardisation » se conçoit au regard des normes volontairement développées et acceptées par l'industrie[471]. Le terme « norme »quant à lui, revêt des sens multiples : « l'expression est parfois utilisée pour désigner un principe servant à prescrire un comportement ou encore pour décrire l'état habituel, conforme à la majorité des cas[472] ». Comme le souligne les professeurs Benyekhlef et Trudel, :

> *« Une norme est un discours (plus ou moins explicite) ou un comportement, descriptif ou prescriptif dans la mesure où cette prescription permet d'évaluer ou de mesurer (et à la limite de sanctionner) la conformité de son sujet à son objet. Partant de cette définition, une analyse des normes suppose l'étude et l'observation de quatre éléments constitutifs, l'objet de la norme (qui régit la norme étudiée ?), l'auteur de la norme (qui produit la norme ?), le sujet de la norme (qui régit la norme ?), la sanction de la norme (quelle punition ? quelle récompense ?)[473].*

Ces normes à caractère purement volontaire peuvent être spontanément plus ou moins suivies et ce, sûrement en raison de la commodité à les observer[474]. D'autres, au contraire, ne sont respectées que moyennant un fort contingent de ressources[475].

Le professeur français Grafmeyer quant à lui, définit la standardisation comme étant :

> *« [...] la recherche a tout prix d'une unicité : un modèle unique, une voie unique, un ensemble répéter indéfiniment à l'identique. Cette recherche se fait a priori selon des critères ou des contraintes spécifiques, mais ces critères sont parfois oubliés derrière la recherche d'un standard, bon ou mauvais, pourvu qu'il y en ait un.*
>
> *En un sens, la standardisation est le corollaire de la spécialisation[476]. »*

---

[471] Il importe de souligner que la standardisation se conçoit tout aussi en dualité avec les règles de droit. Dans le cas par exemple, où la diminution des ressources de l'État engendre des remises en questions, la standardisation peut s'avérer « un moyen de faire en sorte que les acteurs sociaux qui se livrent à une activité déterminée, adoptent un comportement compatible avec les objectifs et les principes sous-tendant les politiques publiques ». Pierre TRUDEL, « Les effets juridiques de l'autoréglementation », (1989) 19 *R.D.U.S.* 247, p.251

[472] Pierre TRUDEL, France ABRAN, Karim BENYEKHLEF et Sophie HEIN, *Droit du cyberespace*, Montréal, Éditions Thémis, 1996, p. 3-4.

[473] Pierre TRUDEL, France ABRAN, Karim BENYEKHLEF et Sophie HEIN, *Droit du cyberespace*, Montréal, Éditions Thémis, 1996, p. 3-5.

[474] Pierre TRUDEL, « Les effets juridiques de l'autoréglementation », (1989) 19 *R.D.U.S.* 247, p.254.

[475] « Certes l'on peut obéir volontairement aux règles de droit, mais leur nature première ne tient pas à cela ; elle tient plutôt, au contraire, au fait que la règle de droit s'impose comme règle obligatoire. » Pierre TRUDEL, « Les effets juridiques de l'autoréglementation », (1989) 19 *R.D.U.S.* 247, p.255.

[476] Michel GRAFMEYER, *La standardisation*, 9 octobre 1995, http://www.fdbd.fr/~mitch/idees/standardiser.html.

Ainsi, la standardisation ou la normalisation que nous considérons comme synonyme dans le cours de la présente étude, se définit comme l'établissement et la mise en application, par voie consensuelle, d'un ensemble de standards[477] et de spécifications par un organisme et ayant pour objet de simplifier, d'unifier et de rationaliser la protection des renseignements personnels sur le réseau Internet[478]. Les initiatives TRUSTe et BBBOnLine que nous avons décrit précédemment, sont de tels organismes.

Aux États-Unis, ces « online privacy seal programs » représente l'un des développements les plus importants des dernières années en ce qui a trait à la protection des renseignements personnels sur Internet. Le législateur a ainsi reconnu le potentiel normalisateur de la technologie et a accordé une très grande marge de manœuvre à ceux qui l'exploitent[479]. En offrant des techniques pour classifier et canaliser l'information, la technologie peut ainsi aider les usagers à exercer un contrôle approprié de la circulation de leurs renseignements personnels[480].

Pour aider les internautes à exercer un contrôle sur leurs données, ces méthodes de standardisation se fondent sur l'expérience et les connaissances techniques acquises dans le milieu industriel où elles se développent[481]. Alors qu'auparavant la qualité et la conformité d'une entreprise reposaient largement sur sa réputation, il est aujourd'hui nécessaire pour bon nombre d'internautes d'obtenir la preuve de cette qualité[482].

Pour établir cette preuve de qualité, les organismes de standardisation utilisent ce que l'on appelle : la certification. La certification est une procédure par laquelle une tierce

---

[477] K.A. Goidich définit ainsi les standards : « A standard is a technical document which describes design, material, processing, safety, or performance characteristics of products. It usually represents the distillation of a great deal of technical knowledge about a product's characteristics. It tells what is important about a product, how it must be produced, how to test it, and how to evaluate the tests results in light of the product's intented use. K.A. GOIDICH, « The Role of Voluntary safety standards in product liability litigation : Evidence or cause in Fact? », [1982] 49 *Insurance Counsel Journal* 320, p. 321.

[478] Dictionnaire Larousse, 2000.

[479] Lire à ce sujet le *Communications Decency Act*. http://www.cdt.org/speech/cda/

[480] David POST, « Anarchy, State and the Internet : An Essay on Law-Making in Cyberspace » (1995) *J, Online L.* art. 3, http://warthog.cc.wm.edu/law/publications/jol/post.html

[481] « Les normes se fondent sur les résultats conjugués de la technologie et de la science telle qu'elle est connue et pratiquée et tiennent compte de l'expérience acquise dans la communauté. » Pierre TRUDEL, « Les effets juridiques de l'autoréglementation », (1989) 19 *R.D.U.S.* 247, p.258.

« Self-regulation might promote the reputation of the industry as a whole, and it might facilitate the creation of technical standards that will benefit the industry itself and society more generally. » Peter S. SWIRE, « Markets, Self-Regulation, and Government Enforcement in the Protection of Personal Information », 23 décembre 1996, http://www.acs-ohio-state.edu/units/law/swire1/psntia6.htm.

[482] Pierre TRUDEL, France ABRAN, Karim BENYEKHLEF et Sophie HEIN, *Droit du cyberespace*, Montréal, Éditions Thémis, 1996, p. 3-46.

partie, soit TRUSTE ou BBBOnLine par exemple, donne une assurance écrite que le site est conforme aux exigences spécifiées et prédéfinies par la tierce partie[483]. Sur Internet, cette assurance écrite se concrétise par la délivrance d'un sceau sur le site Web du requérant. Ce mécanisme d'uniformisation se classe sous la catégorie des normes de comportements pour ce qui est de la protection des renseignements personnels sur Internet[484].

Pour obtenir le sceau d'un organisme de standardisation, l'entreprise requérante se doit de répondre à un ensemble de critères préétablis. L'entreprise qui omet de se soumettre à ces critères se voit, le cas échéant, retirer son accréditation. Il est donc possible, via la standardisation, d'imposer des règles. Toutefois, comme le souligne les professeurs Benyekhlef et Trudel, « reste à savoir si de telles normes sont contraignantes[485] » ? Le processus d'octroi des sceaux des différents organismes américains de standardisation présente deux visages. A priori, celui-ci peut paraître contraignant, à cause de l'obligation pour les participants de se plier aux normes de l'organisme sous peine d'expulsion du programme. Néanmoins, sous sa seconde facette, le processus peut sembler volontaire pour certains étant donné que l'adhésion à l'organisme est purement facultative.

B. La standardisation : source de normativité

Comme nous l'avons constaté tout au long de cette étude, le réseau Internet confère à ses utilisateurs une plus grande maîtrise de leurs choix.

> *« Par conséquent, [l'utilisateur] se voit imputer une plus grande part de responsabilité dans le déroulement des interactions auxquelles il accepte de prendre part. Dans un environnement ouvert comme l'Internet, il est impossible de raisonner comme si les mêmes règles du jeu devaient prévaloir d'un bout à l'autre du réseau. Dans l'Internet, l'individu a la possibilité de fréquenter des sites sécurisés ou de prendre le risque de fréquenter des sites offrant peu ou pas de sécurité. Il peut faire affaire avec*

---

[483] Alain COURET, Jacques IGALENS et Hervé PENAN, *La certification*, coll. « Que sais-je ? », Paris, P.U.F., 1995, p.91.

[484] Pour une étude des catégories de normes, voir CONSEIL CANADIEN DES NORMES, « Réflexion sur la protection de la vie privée : Le Canada s'interroge sur le besoin d'élaboration d'une norme ISO internationale sur la protection des renseignements personnels », *Revue canadienne d'actualités de normalisation*, Volume 24, numéro 5 (Septembre 1997), http://www.scc.ca/consensu/1997/sept/ponder2405f.html et Pierre TRUDEL et France ABRAN, Karim BENYEKHLEF et Sophie HEIN, *Droit du cyberespace*, Montréal, Éditions Thémis, 1996, p. 3-5.

[485] Pierre TRUDEL et France ABRAN, Karim BENYEKHLEF et Sophie HEIN, *Droit du cyberespace*, Montréal, Éditions Thémis, 1996, p. 3-48.

> *une entreprise qui adhère à des normes élevées de rigueur ou de prendre la chance de contracter avec un escroc*[486]*. »*

Actuellement, les États-Unis est le seul pays qui prône une approche exclusivement autoréglementaire. Selon les Américains, le commerce électronique a tout à gagner d'une non-intervention de l'État dans l'élaboration des règles juridiques qui régiront les comportements sur le réseau Internet[487]. Ces dernières doivent plutôt être établies par les acteurs mêmes de l'économie. En conséquence, il appert que les acteurs du réseau, ceux qui sont au cœur de l'action, soit les commerçants et les associations d'entreprises, sont les mieux placés pour répondre efficacement aux problèmes soulevés[488]. Néanmoins, la réalité est quelque peu différente.

> *« Ce phénomène contribue à faire en sorte que la régulation dans l'Internet est une activité soumise à des pressions concurrentielles : aucune autorité ne peut prétendre exercer un monopole sur la fonction d'énonciation des règles, de même que sur celles reliées à leur application. Si les règles ne conviennent pas aux acteurs, il leur est souvent loisible de se localiser ailleurs afin d'échapper aux règles non souhaitées*[489]*. »*

L'absence de contrôle centralisé et le fait que l'Internet fonctionne suivant un principe de concurrence des normes ramène sur les épaules de l'usager le fardeau d'assurer sa propre protection[490]. La mise en place d'outils de standardisation n'est pas seulement qu'une opération technique ; elle nécessite aussi l'exercice d'un jugement éditorial qui doit être entouré de garanties démocratiques ; ce que l'on ne retrouve pas présentement.

---

[486] Pierre TRUDEL et France ABRAN, Karim BENYEKHLEF et Sophie HEIN, *Droit du cyberespace*, Montréal, Éditions Thémis, 1996, p. 3-6.

[487] Joel REIDENBERG, « Restoring Americans' Privacy in Electronic Commerce », *Berkeley Technology Law Journal*, Volume 14-2, http://www.law.berkeley.edu/journals/btlj/articles/14_2/Reidenberg/html/reader.html.

[488] Une récente étude de la FTC énonce à cet effet : « The number of sites enrolled in these programs has increased in absolute terms since last year, the seal programs have yet to establish a significant presence on the Web. » FEDERAL TRADE COMMISSION, *Privacy Online: Fair Information Practices in the Electronic Marketplace: A Federal Trade Commission Report to Congress*, 22 mai 2000, http://www.ftc.gov/os/2000/05/index.htm#22

Voir Peter P. SWIRE, « Of Elephants, Mice, and Privacy: International Choice of Law and the Internet », *Draft submitted to International Lawyer*, 23 août 1998, http://www.acs.-ohio-state.edu/units/law/swire1/elephants.htm et Pierre TRUDEL, France ABRAN, Karim BENYEKHLEF et Sophie HEIN, *Droit du cyberespace*, Montréal, Éditions Thémis, 1996, p. 11-40.

[489] Pierre TRUDEL, France ABRAN, Karim BENYEKHLEF et Sophie HEIN, *Droit du cyberespace*, Montréal, Éditions Thémis, 1996, p. 15-2.

De plus, il importe de souligner que ce n'est pas parce qu'il est possible de déjouer les règles dans une certaine situation que les stratégies de régulation n'ont plus leur raison d'être.

[490] « The lowest level of self-help is unilateral action by an individual. We might capture the sense of this measure with the phrase : if you don't like it, don't do it. Certainly at times this is the appropriate response of the legal

> *« L'adaptation du cadre juridique de l'information au contexte des nouvelles technologies doit permettre la mise en place d'un environnement accueillant et respectueux à la fois des dynamiques qui se manifestent dans les environnements électroniques et des valeurs fondamentales des sociétés. Pour qu'une telle adaptation soit efficace, il faut :*
>
> - *Revoir les réflexes développés dans les anciens contextes informationnels ;*
> - *Évaluer de manière réaliste les possibilités de régir les contenus au niveau de la diffusion ;*
> - *Favoriser la mise en place de mécanismes collectifs afin de faciliter les contrôles à la circulation des informations ;*
> - *Mettre en place un régime de responsabilité approprié pour les dommages résultant de la circulation des informations ;*
> - *Maintenir une activité de « veille juridique »*[491].

L'évidence même de la situation rappelle que les problèmes de juridiction sont une des caractéristiques premières de la protection des renseignements personnels dans les environnements électroniques décentralisés[492]. L'application pratique et opérationnelle des normes nationales et internationales sur la toile n'est pas aisée. Comme le souligne le professeur Benyekhlef, il est essentiel de favoriser la mise en place de mécanismes collectifs afin d'assurer la protection de la vie privée des internautes[493].

Si cela est vrai pour ce qui est des questions sociales, cela l'est également pour celles liées au commerce. Au moment-même où celui-ci se fait mondial de par sa portée, les questions relatives à la protection de la vie privée et au développement durable deviennent-elles aussi mondiales ? Pour savoir s'attaquer à ces questions, il faut faire appel à une nouvelle information, de nouvelles technologies, de nouvelles coalitions, une nouvelle façon de concevoir les normes[494].

US system. » Trotter HARDY, « The Proper Legal Regime for « Cyberspace » », (1994) 55 *U. of Pitt. L.R.* 993, 1016.

[491] Pierre TRUDEL, France ABRAN, Karim BENYEKHLEF et Sophie HEIN, *Droit du cyberespace*, Montréal, Éditions Thémis, 1996, p. 15-10.

[492] Joel REIDENBERG et Françoise GAMET-POL, « The Fundamental Role of Privacy and Confidence in the Network », (1995) 30 *Wake Forest Law Review* 105, 110-111.

[493] Karim BENYEKHLEF, « Les normes internationales de protection des données personnelles et l'autoroute de l'information », dans Le respect de la vie privée dans l'entreprise, Actes des Journées Maximilien Caron, Montréal, Éditions Thémis, 1996. 65, 96.

[494] CONSEIL CANADIEN DES NORMES, *Perspective mondiale 2000 - Le Conseil canadien des normes lance la Stratégie canadienne de normalisation en présence du ministre de l'Industrie et de chefs d'entreprise*, 29 mars 2000, http://www.scc.ca/pressrel/2000/mar29_f.html

S'il est vrai que des normes de toutes sortes émergent du champ de la protection des renseignements personnels, c'est sous l'influence ou la pression de forces sociales qui continuent d'agir après cette apparition, soit pour promouvoir la norme et l'invoquer, soit au contraire pour la neutraliser ou la faire carrément disparaître[495].

> « *Cette typologie des sources du droit est caractérisée par sa fixité et son abstraction de l'ensemble des phénomènes sociaux qui expliquent l'apparition de la norme, ses états intermédiaires et sa disparition*[496]. »

En outre, l'inflation normative donne l'illusion que rien ne se perd en droit, et la proclamation d'une norme, au sens large, laisse l'impression que le problème social qu'elle vise à résoudre est définitivement réglé. Pourtant, autant dans leur énoncé que dans leur mise en œuvre, les normes progressent ou régressent sous la pression des forces sociales intéressées à leur promotion ou à leur négociation[497].

Dans le domaine de la protection des renseignements personnels, comment expliquer que des normes aient émergées des pratiques, et que par rapport aux enjeux, ces normes soient parfois inadéquates, modestes et dans certain cas, en régression ? Dans les environnements électroniques décentralisés, ces variations doivent être attribuées essentiellement aux influences internationales qui ont déterminé dans une large mesure les manifestations locales de l'émergence normative.

Actuellement, les différents « online privacy seal programs » américains tentent de standardiser la protection des renseignements personnels sur le réseau Internet à l'aide de normes volontaires. Ces programmes reposent essentiellement sur trois principes : dire ce que l'on fait, faire ce que l'on dit et montrer à une tierce partie qu'on respecte ce qui a été convenu[498].

---

[495] René LAPERRIÈRE, « L'émergence de normes dans le domaine des communications de renseignements personnels » dans *Entre droit et technique : enjeux normatifs et sociaux* sous la direction de René Côté et Guy Rocher, Éditions Thémis, Montréal, 1994, p.167.

[496] René LAPERRIÈRE, « L'émergence de normes dans le domaine des communications de renseignements personnels » dans *Entre droit et technique : enjeux normatifs et sociaux* sous la direction de René Côté et Guy Rocher, Éditions Thémis, Montréal, 1994, p.167.

[497] René LAPERRIÈRE, « L'émergence de normes dans le domaine des communications de renseignements personnels » dans *Entre droit et technique : enjeux normatifs et sociaux* sous la direction de René Côté et Guy Rocher, Éditions Thémis, Montréal, 1994, p.168.

[498] Colin BENNETT, *Réflexions sur une norme internationale de protection des renseignements personnels*, Groupe de travail sur le commerce électronique d'Industrie Canada, http://e-com.ic.gc.ca/francais/privee/632d294.html

Comme nous l'avons constaté précédemment, les normes volontaires sont celles que s'imposent les organismes d'elles-mêmes, sans y être obligé en droit, mais en vue de rassurer le public ou la communauté internationale sur la légitimité de leurs pratiques en ce qui a trait aux renseignements personnels[499]. Cette démarche d'adoption de « privacy policies » ou communément appelé « codes de conduite », s'inspire généralement des prescriptions des *Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel* de l'OCDE. Leur caractéristique principale qui est en fait leur principal défaut, est de n'être assorties d'aucune mesure de vérification ou de contrôle externe de leur mise en œuvre, et de ne donner aux internautes aucun recours autre que l'appel à la bonne volonté de l'organisme. Ces normes, comme le souligne le professeur Laperrière, sont généralement considérées comme peu efficaces et comme des opérations de relations publiques[500]. L'idéologie de la protection des renseignements personnels est assez limitée : elle est essentiellement réactive, et tend à ériger la liberté individuelle en un absolu. Elle est de plus dénaturée par les entreprises qui la plaident pour échapper à tout contrôle. Ainsi, le principal intérêt qui entraîne l'industrie à faire émerger des normes ou au contraire à les empêcher d'émerger, est la recherche du profit.

> « *If you want to find out how a company feels about your personal privacy, don't look at their privacy statement, look at their business model. It's a question of profit versus privacy, and profits come first every time*[501] ».

On ne peut qu'entretenir un certain scepticisme à l'égard de la viabilité de l'approche américaine qui s'en remet aux règles de conduite adoptées par l'industrie sous la seule pression sociale se manifestant dans un environnement électronique donné. Selon le Conseil canadien des normes, la meilleure forme de normalisation consiste en une collaboration entre l'Industrie, les consommateurs et l'État qui permet d'élaborer un consensus rendant les résultats plus crédibles[502].

---

[499] René LAPERRIÈRE, « L'émergence de normes dans le domaine des communications de renseignements personnels » dans *Entre droit et technique : enjeux normatifs et sociaux* sous la direction de René Côté et Guy Rocher, Éditions Thémis, Montréal, 1994, p.170. Voir aussi Peter S. SWIRE, « Markets, Self-Regulation, and Government Enforcement in the Protection of Personal Information », 23 décembre 1996, http://www.acs-ohio-state.edu/units/law/swire1/psntia6.htm

[500] René LAPERRIÈRE, « L'émergence de normes dans le domaine des communications de renseignements personnels » dans *Entre droit et technique : enjeux normatifs et sociaux* sous la direction de René Côté et Guy Rocher, Éditions Thémis, Montréal, 1994, p.170.

[501] PC WORLD, « Policies Are No Insurance », Juin 2000, *PC World*, http://www.pcworld.com/current_issue/article/0,1212,16444+1+5,00.html

[502] CONSEIL CANADIEN DES NORMES, « L'Industrie, contre ou avec les consommateurs? », *Consensus*, Janvier-février 1999, http://www.scc.ca/consensu/1999/jan_feb/consumers2601f.html

Jusqu'à présent, seule l'industrie américaine a prôné la standardisation comme méthode efficace de protection des renseignements personnels. Comme nous l'avons constaté, ces méthodes de standardisation reçoivent néanmoins de très nombreuses critiques.

> *« Les citoyens américains, tout d'abord, semblent de plus en plus préoccupés par les activités des sites qu'ils visitent. Ils prennent conscience du formidable pouvoir et des pratiques abusives de certaines entreprises et ne craignent plus seulement les interventions de l'État. Ensuite, un courant de plus en plus important d'experts, américains ou étrangers, pointent les insuffisances des mécanismes. Ils soulignent le manque de contrôle et de sanctions effectives pour contraindre les entreprises à respecter leurs engagements et l'orientation essentiellement favorable aux entreprises au détriment des internautes. L'aspect déficient le plus notable du système américain est peut-être son incapacité à se mettre en œuvre : [...] les acteurs privés n'agissent pas. Ils sont réticents à élaborer leurs propres règles... à moins que l'État ne menace d'intervenir !* [503]. »

Les méthodes de standardisation que l'on retrouve actuellement sur le réseau Internet se concrétisent par l'utilisation des sceaux de confiance[504]. Cette certification est à prime abord, importante pour les internautes[505]. Réalisée par un tiers, elle prouve une certaine transparence et inspire confiance aux consommateurs. Le fait que le législateur américain ait reconnu le potentiel normalisateur de la technologie, la mise en place d'outils de contrôle n'est cependant pas qu'une simple opération technique. Elle nécessite souvent l'exercice d'un jugement éditorial qui doit être entouré de garanties démocratiques. Présentement, ce jugement éditorial est quasiment absent du réseau tel que le démontrent entre autres, les diverses problématiques mettant en cause TRUSTe et les logiciels Windows 98 de Microsoft et RealPlayer 7 de RealNetwork[506]. De plus, pour l'EPIC, ces sceaux ne sont en réalité que des liens hypertextes de couleurs qui pointent vers des politiques qui ne veulent rien dire.

---

[503] François-Xavier FARASSE, « Votre vie privée dans le cyberespace: quelle protection avez-vous ? », Hiver 1999, *Dire*, p. 27.

[504] On peut apparenter ce mécanisme d'étiquetage des sites Web aux systèmes de classement des films et vidéos.

[505] De façon général, « the logo means that the site posts - and agrees to adhere to - a statement disclosing what personal data the company collect from consumers and what it does with that information". » Chris OAKES et James GLAVE, « The Web Privacy Seal, Take 2 », 17 mars 1999, *Wired*, http://www.wired.com/news/print_version/politics/story/18517.html?wnpg=all

[506] Après que Microsoft ait admis avoir codé, par « mégarde », l'assistant d'enregistrement de Windows 98 afin qu'il envoie automatiquement et surtout subrepticement des numéros d'identification uniques à chaque poste de travail, l'entreprise Macromedia, éditeur de la plate-forme multimédia Shockwave, a admis que sa procédure de mise à jour automatique lui faisait parvenir certains URLs visités par les utilisateurs de son module de lecture Shockwave. Michelle V. RAFTER, « Trust or Bust? », 6 mars 2000, *The Standard*, http://www.thestandard.com/article/display/0,1151,12445,00.html

> *« The presence of the seals, however, indicates privacy, not secrecy. No seal guarantees that a Web site will not sell or trade your e-mail address, name or phone number, or records of your purchases and online surfing habits. And Web sites with the same privacy seal may have widely different privacy policies. Officials for the seal programs say they are not trying to dictate specific practices ; they do not want to start micromanaging how companies use information that they have gathered legally, with a customer's informed consent*[507]*. »*

En ce qui a trait à la standardisation, ces garanties démocratiques devraient en outre garantir aux internautes que l'organisme : effectue une évaluation approfondie des politiques de ses membres en matière de vie privée, dispose d'un processus de veille juridique et d'un mécanisme de plainte[508]. Un site Web qui affiche un sceau de confiance s'engage ainsi à respecter intégralement et minutieusement sa politique en matière de renseignements personnels. Néanmoins, c'est plus ou moins ce qui se produit actuellement.

Selon le professeur Lessig, l'affichage d'un sceau sur un site Web ne change en rien le niveau de confiance des usagers[509]. Les usagers n'ont pas, à son avis, le temps de s'arrêter pour lire ces politiques et ainsi, savoir exactement quels renseignements personnels seront collectés[510]. À défaut de lire la politique du site Web, les usagers perdent ainsi la protection de leur vie privée. De plus, contrairement à ce que TRUSTe énonce[511], au moment où les usagers commencent à comprendre l'intérêt des commerçants pour la valeur de leurs renseignements personnels, le fait de créer de plus en plus d'organismes de standardisation et d'apposer de plus en plus de sceaux ne peut

---

[507] Lisa GUERNEY, « Web Surfers' Fears Prompt Privacy Seals », *New York Times*, http://search.nytimes.com/search/daily/bi...tweb?getdoc+site+site+71840+0+wAAA+truste

[508] Jonathan WEINBERG, « Rating the Net », 19 *Hastings Comm/ent L.J.* 453 (1997), http:///www.msen.com/~weinberg/rating.html et Pierre TRUDEL, France ABRAN, Karim BENYEKHLEF et Sophie HEIN, *Droit du cyberespace*, Montréal, Éditions Thémis, 1996, p. 15-7.

[509] Outre le fait que quelques entreprises, telle BBB et TRUSTe disposent de mécanisme pour empêcher de copier le sceau et de l'apposer sur un autre site, « some consumer-advocacy groups have major doubts about whether the seals truly signify the level of protection that people want. » Lisa GUERNEY, « Web Surfers' Fears Prompt Privacy Seals », *New York Times*, http://search.nytimes.com/search/daily/bi...tweb?getdoc+site+site+71840+0+wAAA+truste

[510] « But more words are the last thing that privacy on the Net needs. For reading, even if fundamental, is fundamentally inefficient. It costs too much. No on has the time, or the patience, for the multithousand-word privacy policies posted on sites. And thus, if the choice is to read or waive, the rational thing for most to do is simply to waive. » Lisa GUERNEY, « Web Surfers' Fears Prompt Privacy Seals », *New York Times*, http://search.nytimes.com/search/daily/bi...tweb?getdoc+site+site+71840+0+wAAA+truste

[511] « The pervasiveness of the TRUSTe seal is critical if we are to succeed in getting consumers to look for and read privacy statements - a tool that the brick and mortar world never offered. » Lawrence LESSIG, « Coding privacy », 21 mai 1999, *The Industry Standard*, http://www.thestandard.com/articles/display/0,1449,4620,00.html?01.

que décourager l'usager et créer une concurrence malsaine, où les grands perdants seront les internautes.

Toutefois, les résultats du Georgetown Internet Privacy Policy Study du mois de juin 1999 viennent quelque peu contrer l'opinion de professeur Lessig. À ce sujet :

> « *TRUSTe said that the dramatic rise in Web sites offering privacy policies in a short period of time, as evidenced in the Georgetown Internet Privacy Policy Study, is an indication that demonstrable progress has been made. The seal program is a significant factor in mobilizing quick action and promoting trusted relationships between companies and their customers. Bob Lewin (TRUSTe's executive director), just as we predicted from the beginning, the leading Web sites have fully embraced privacy policies and seal programs as mediums to empower consumers, and the masses are following their lead. But while the Georgetown Privacy Study shows great progress, there is still more that must be done to address this issue. Industry, government and watchdog groups must work together to ensure that consumers' expectations of privacy assurances on the Web are met*[512]. »

L'étude démontre « a significant progress in the number of Internet sites that tell visitors how their personal information collected will be used[513]. » De plus, les conclusions d'une étude effectuée pour l'entreprise AT&T indiquent qu'une combinaison de politiques en matières de renseignements personnels et de sceaux ne peuvent qu'augmenter la confiance des internautes. En contrepartie, « the survey responses also suggested that even the consumers who are most familiar with the Web do not completely understand how the seal programs works[514]. »

Toutes proportions gardées, on constate que très peu de sites ont adhéré aux différents sceaux[515]. Toutefois, les plus grands de l'industrie ont presque tous adhéré au

---

[512] TRUSTe, « TRUSTe Comments on Georgetown Internet Privacy Policy Study », 14 mai 1999, http://www.truste.org/about/about_gtowncomments.html

[513] Tom DIEDERICH, « Study: 94% of top 100 Web sites post privacy policies », Mai 1999, *Computer World*, http://computerwolrd.com/home/news.nsf/all/9905123netpriv

[514] « AT&T Labs recently conducted a survey of 381 Net users to determine what they thought about online privacy. The study found that 58 % of the respondents would be morel likely to give a Web site their e-mail addresses if the site had a privacy policy and a privacy seal. But the survey responses also suggested that even the consumers who are most familiar with the Web do not completely understand how the seal programs works. » Lisa GUERNEY, « Web Surfers' Fears Prompt Privacy Seals », *New York Times*, http://search.nytimes.com/search/daily/bi...tweb?getdoc+site+site+71840+0+wAAA+truste et Chris OAKES, « Take My Email, but Not My Date », 14 avril 1999, *Wired*, http://www.wired.com/news/print_version/politics/story/19123.html?wnpg=all.

[515] James GLAVE, « In Ernst & Young we Trust », *Wired*, http://www.wired.com/news/news/business/story/15386.html

minimum, à un organisme de standardisation[516]. La concurrence étant extrêmement forte dans ce nouveau domaine lucratif, il se crée de jour en jour, de nouveaux organismes de standardisation. D'où la difficulté et surtout l'impossibilité pour les entreprises d'adhérer à tous[517].

L'émergence et la popularité d'un sceau par rapport aux autres peu aussi engendrer une baisse de qualité du service. « As the services get bigger, hiring more and more employees to analyse the policies, their consistency will degrade[518]. »

Pour la protection des renseignements personnels sur le réseau Internet, l'élaboration d'une standardisation à l'aide de normes volontaires décrétées par l'industrie, ne peut valablement fonctionner. Cette standardisation pourrait en principe fonctionner parfaitement pourvu que tous les sites affichent des sceaux et que les organismes s'assurent que les sites Web respectent leur politique. Jonathan Weinberg écrit à cet effet : « What are the prospects that a rating service will be able to label even a large percentage of the millions of pages on the Web ? What are the consequences if it cannot ? How do we hire enough policemen to police the Net[519] ? »

De plus, le fait d'avoir présentement une politique en matière de vie privée n'implique pas nécessairement le fait d'avoir une bonne politique et surtout, de la respecter[520]. Dans bien des cas, les autorités américaines soulignent que la plupart des organismes de standardisation sont dans l'incapacité d'effectuer un audit des sites auxquels ils ont accordé un sceau[521]. « Moreover, no service could be big enough to do it. Too many

---

[516] « The depth and breadth of TRUSTe's licensee base makes it a meaningful tool for consumer in deciding whether to trust a Web site. Today, TRUSTe's licensee base is comprised of almost every major vertical industry segment on the Web including auction, insurance, news, real estate, retail, sports and recreation, technology, and travel. Additionally, the seal program has international reach with licensees headquartered in 19 countries. »

[517] Courtney MACAVINTA, « Firms develop privacy seal of approval », 11 mars 1999, *CNET*, http://www.news.com/News/Item/0,4,33662.00html

[518] Jonathan WEINBERG, « Rating the Net », 19 *Hastings Comm/ent L.J.* 453 (1997) http://www.msen.com/~weinberg/rating.htm

[519] Jonathan WEINBERG, « Rating the Net », 19 *Hastings Comm/ent L.J.* 453 (1997) http://www.msen.com/~weinberg/rating.htm

[520] Craddock ASHLEY, « Pretty Poor Privacy », 25 juin 1999, *Wired*, http://www.wired.com/news/news/politics/story/13256.html

[521] Deborah SCOBLIONKOV, « Back Off, Big Brother », 22 juillet 1999, *Wired*, http://www.wired.com/news/news/politics/story/13910.html

new pages come on-line every day. The content associated with any given page is constantly changing[522]. »

> « *Privacy statements can be changed at will, often without notification to users or affiliated sites. EPIC's complaint to the FTC notes that DoubleClick changed its policy three times in the past three years*[523]. »

Comme le constate le professeur Laperrière, cela porte à croire que les normes sont faiblement observées dans le domaine des renseignements personnels[524]. Pour être efficace, il appert que les « online privacy seal programs » devraient s'appuyer sur de bonnes méthodes de surveillance et les appliquer convenablement. Outre la surveillance, le caractère lucratif provenant de l'émission des sceaux de confiance laisse aussi place à une certaine ambiguïté face aux usagers[525]. Le coût élevé que les entreprises déboursent pour adhérer à ces programmes peut inciter les organismes à faire preuve d'un certain laisser-aller lors de la vérification de la politique pour être en mesure de conserver leurs clients[526]. À première vue, il en découle pour plusieurs une apparence de conflit d'intérêt. « They're being paid by sites to post their symbol. There's an inherent conflict of interest in giving a site a poor rating[527]. »

On constate que l'industrie de la standardisation, telle qu'elle existe présentement sur le réseau, est plus ou moins efficace. La réalité le démontre bien ! L'absence d'une

---

[522] Jonathan WEINBERG, « Rating the Net", 19 *Hastings Comm/ent L.J.* 453 (1997) http://www.msen.com/~weinberg/rating.htm

[523] PC WORLD, « Policies Are No Insurance », Juin 2000, *PC World*, http://www.pcworld.com/current_issue/article/0,1212,16444+1+5,00.html

[524] Tout de même près de notre situation, le professeur Laperrière à constaté un phénomène troublant : « à peu près tout les entreprises déclarent recevoir plus de renseignements qu'il n'en diffuse. Peut-être est-ce motivé par une authentique valeur de préservation de la confidentialité. Peut-être est-ce la nature même des communications qui fait que mathématiquement si dix personnes s'échangent entres elles une quantité égale d'information de données, elles en recevront chacune dix fois plus qu'elles n'en ont livrées. Mais il y a là, nous semble-t-il, un problème majeur parce que le système d'échanges ne peut se réaliser à sens unique : il faut des fournisseurs d'informations, et pas seulement des consommateurs. » René LAPERRIÈRE, « L'émergence de normes dans le domaine des communications de renseignements personnels » dans *Entre droit et technique : enjeux normatifs et sociaux* sous la direction de René Côté et Guy Rocher, Éditions Thémis, Montréal, 1994, p.183.

[525] Aux dires du BBB Online, « if it comes down to it, [there] will be a competitive market for seals, and companies will evaluate where they get the best benefit ». Chris OAKES et James GLAVE, « The Web Privacy Seal, Take 2 », 17 mars 1999, *Wired*, http://www.wired.com/news/print_version/politics/story/18517.html?wnpg=all. Voir aussi REUTERS, « The New E-Industry : Privacy », 11 octobre 1999, *Wired*, http://wired.com/news/print_version/business/story/22178.html?wnpg=all

[526] Selon l'éditeur du Privacy Journal, Robert Ellis Smith, les sceaux de confiance peuvent aider les consommateurs, mais il y a toutefois un problème. « They're sponsored by corporate entities! » Les propres entreprises qu'elles certifient, pour lesquelles elle évalue leur politique, sont celles qui la commandite. On peut donc croire à l'apparence d'une situation conflictuelle. Andrea B TERRY, « Following the rules can increase your personal security », Juin 1999, *Online Banking*, http://www.onlinebanking.com

[527] REUTERS, « The New E-Industry : Privacy », 11 octobre 1999, *Wired*, http://wired.com/news/print_version/business/story/22178.html?wnpg=all

législation pour la protection de la vie privée et l'absence de réglementation concernant les organismes de standardisation sont les deux principaux problèmes de son mauvais fonctionnement.

Malgré l'augmentation du nombre de sites affichant des sceaux de confiance selon le Georgetown Internet Privacy Policy Study de 1999, cela ne démontre aucunement de progrès significatifs en ce qui a trait à la protection réelle de la vie privée des internautes. En réalité, il est extrêmement difficile de contrôler et de vérifier réellement ce que font les sites Web avec les renseignements personnels qu'ils détiennent.

Les régimes de sanctions de ces organismes laissent quelque peu perplexes étant donné l'absence de sanction véritable[528]. Les transgresseurs jouissent pratiquement de l'impunité, et les cas d'abus sont la plupart du temps banalisés. À ce sujet, le cyber-magazine *CNet* rapportait récemment qu'au moins trois cyber-commerces ayant fermés boutique dans les dernières semaines ont choisi de vendre les renseignements personnels de leurs clients afin de rembourser les énormes pertes qu'ils ont subies[529]. Les trois cyber-commerces membres de TrustE, ont tout liquidé ou tenté de liquider leurs banques de renseignements sur leur clientèle[530]. La crédibilité de TRUSTe s'effondre quelque peu dans cette affaire car, comme on le constate, son autorité effraie peu de gens. Comme le souligne le professeur Ferrera : « Promises made in the privacy policy are as much a part of the transaction as what is delivered to the consumer[531] ».

En effet, dépendamment du sceau qu'il affiche, un site Web qui contrevient à sa politique en matière de vie privée peut se voir enlever son sceau, et dans les cas graves, se voir dénoncer à la FTC.

---

[528] Lire à ce sujet : Karim BENYEKHLEF, *La protection de la vie privée dans les échanges internationaux d'informations*, Montréal, Éditions Thémis, 1992, p. 75.

[529] Greg SANDOVAL, « Failed dot-coms may be selling your private information », 29 juin 2000, *CNET*, http://news.cnet.com/news/0-1007-202-2176430.html

[530] Dave Steer, un porte-parole de TRUSTe n'a pas manqué de mentionner qu'il est inacceptable et potentiellement illégal de vendre de l'information sur la clientèle alors qu'elle a été ramassée sous le prétexte qu'elle ne serait pas partagée. C'est une invasion de la vie privée et si des actions ne sont pas prises promptement, le mouvement pourrait se répéter.

De plus, Andrew Shen de l'EPIC, juge qu'une loi devrait être adoptée aux États-unis pour empêcher les entreprises en faillite de liquider leurs banques de renseignements. Contrairement aux États-Unis, le Québec et le Canada sont dotés de lois protégeant les renseignements personnels. Il faudrait cependant voir dans quelle mesure elles pourraient empêcher une entreprise en faillite de repayer ses créanciers en vendant les renseignements qu'elle avait promis à ses clients de protéger.

[531] PC WORLD, « Policies Are No Insurance », *PC World*, Juin 2000, http://www.pcworld.com/current_issue/article/0,1212,16444+1+5,00.html

> « *Voluntary programs such as TRUSTe have been lauded by the White House and the Net industry as a key solution for protecting consumers' online privacy, but consumer groups argue that they lack enforcement. If a site fails to comply with its TRUSTe-certified privacy policy, I could have its privacy seal revoked, or in the worst case a complaint could be filed with the Federal Trade Commission*[532]. »

Outre les conflits d'intérêts apparents, les difficultés de vérifier les pratiques des sites Web affichant des sceaux, l'absence d'une législation de protection de la vie privée comme norme de base pour concevoir les politiques en matière de vie privée et les régimes de réparations et de sanctions quelque peu dérisoires[533], ces organismes ne prévoient pas de mécanismes impartiaux et neutres.

Ainsi, il est évident que la protection des renseignements personnels passe par le respect de certains principes juridiques sur lesquels les principaux acteurs de l'Internet se retrouvent peu ou prou[534]. La mise en place d'outils de contrôle nécessite l'exercice d'un jugement éditorial qui doit être entouré de garanties démocratiques[535].

C. Un complément à la législation ?

Le débat sur les moyens d'assurer une protection effective de la vie privée sur le réseau Internet illustre la nécessité d'y aborder la question de la protection des droits en se tenant loin du dogmatisme. Jusqu'à l'adoption et la mise en vigueur de la *Directive*, les

---

[532] Courtney MACAVINTA, « RealNetworks changes privacy policy under scrutiny », 1 novembre 1999, *CNET*, http://news.cnet.com/news/0-1005-202-1426044.html

[533] Il existe en droit international un terme pour désigner les normes non susceptibles de sanction, à signification variable et à application malléable, celui de normes molles – *soft law* en anglais. Ce problème comme le note le professeur Laperrière, « se distingue de celui de concepts flous, car un concept peut être aussi bien défini qu'il se peut en droit dans sa formulation, sans pour autant recevoir d'application concrète en termes de mesures de mise en œuvre par des programmes, des vérifications, des sanctions de type judiciaire. Dans le domaine de la protection des renseignements personnels, le problème de la faible sanction des normes est très répandu et il ne se confond pas non plus avec celui de la valeur symbolique des normes. » René LAPERRIÈRE, « L'émergence de normes dans le domaine des communications de renseignements personnels » dans *Entre droit et technique : enjeux normatifs et sociaux* sous la direction de René Côté et Guy Rocher, Éditions Thémis, Montréal, 1994, p.184.

[534] Soucieuse de préserver ce qu'elle considère comme un véritable droit fondamental, l'Europe semble prête à rester fermement établie sur ses principes et demeure en opposition affirmée avec la position américaine, et il faut constater que depuis peu de très nombreux pays ont suivi la voie de l'intervention législative pour composer des régimes de sauvegarde des droits des individus en ce qui a trait à leur vie privée et leurs renseignements personnels. Voir Joel R. REIDENBERG, « Setting Standards for Fair Information Practice in the U.S. Private Sector », 80, *Iowa Law Review* 497 (1995).

[535] Karim BENYEKHLEF et Pierre TRUDEL, *Approches et stratégies pour améliorer la protection de la vie privée dans le contexte des inforoutes*, Mémoire présenté à la Commission de la culture de l'Assemblée nationale dans le cadre de son mandat sur l'étude du Rapport quinquennal de la Commission d'accès à l'information, septembre 1997, p. 20 et Joel REIDENBERG et Françoise GAMET-POL, « The Fundamental Role of Privacy and Confidence in the Network », (1995) 30 *Wake Forest Law Review* 105, 110-111.

démarches de standardisation américaine s'imposaient de plus en plus comme l'un des principaux vecteurs de la régulation sur le réseau Internet. Néanmoins, comme le soulignent les professeurs Benyekhlef et Trudel, les possibilités offertes dans cet espace virtuel comportent à la fois du bon et du mauvais ; il est imprudent de décréter prématurément des approches trop catégoriques reposant sur un parti pris trop rudimentaire en faveur d'une approche en particulier[536].

La standardisation par l'industrie constitue certes une voie très intéressante, mais incomplète en elle-même. En matière de protection des renseignements personnels, l'utilisation de code de conduite paraît illusoire dans un contexte où les développements techniques nous mènent à la constitution de super-autoroutes électroniques et où la crise économique amène les organisations à privatiser et à réduire les coûts. De plus, en raison de son caractère technique, la standardisation se décide bien souvent dans des forums qui ne sont pas nécessairement ceux au sein desquels les gouvernements sont présents.

La régulation par le marché repose sur des incitatifs purement financiers[537]. Ainsi, en raison de l'internationalisation du réseau, le marchandage de l'information et l'appât du gain qui subsistera sûrement encore autour des « gisements d'informations », donne lieu à craindre le pire.

Le professeur Laperrière dresse une liste de critères nécessaires à retrouver dans un mode de protection des renseignements personnels sur le réseau Internet :

> *« Quelle norme publique peut émerger et résister à une telle poussée ? Il faudra vraisemblablement plus que des sondages où chacun s'inquiète des violations de sa vie privée. Il faudra une prise de conscience générale et une mobilisation populaire pour faire reculer la tendance anarchique actuelle et exiger de véritables mécanismes de contrôle, soit par la technique, soit par la vérification indépendante, soit par l'instauration d'un droit de propriété de la personne sur l'information la concernant. Plus la norme se rapprochera de l'appropriation et du contrôle par les citoyens, plus elle aura*

---

[536] Karim BENYEKHLEF et Pierre TRUDEL, *Approches et stratégies pour améliorer la protection de la vie privée dans le contexte des inforoutes*, Mémoire présenté à la Commission de la culture de l'Assemblée nationale dans le cadre de son mandat sur l'étude du Rapport quinquennal de la Commission d'accès à l'information, septembre 1997, p. 20.

[537] En conséquence, une entreprise décidera de protéger la vie privée de ses clients, seulement si cela peut lui conférer un avantage concurrentiel. Pour plus de détails à ce sujet, lire le second chapitre.

> *de chance de trouver une meilleure efficacité dans sa mise en œuvre, et donc une véritable signification sociale*[538]. »

La standardisation telle qu'elle est utilisée présentement aux États-Unis, soit en dualité avec l'autoréglementation, connaît un succès très mitigé[539]. Le fait que les organismes de standardisation sont des entreprises lucratives soulèvent bien des remous[540]. Comme le souligne le professeur Swire :

> « *Under the pure market model, the incentives for industry to protect privacy are entirely financial. The assumption, for now, is that there in no legal enforcement against a company that disclose personal information about its customers. Customers can be directly attracted by a strong privacy protection policy or repelled by breaches of privacy. In at least some instances, privacy may be a salient enough marketing point to induce consumers to switch from one company to another*[541]. »

Ainsi, comment un usager peut-il s'assurer que ladite entreprise respecte bel et bien les principes qu'elle s'est donnés ? Là est la question !

La régulation législative présente elle aussi des inconvénients lorsque vient le moment de l'appliquer concrètement dans les environnements électroniques décentralisés[542].

---

[538] René LAPERRIÈRE, « L'émergence de normes dans le domaine des communications de renseignements personnels » dans *Entre droit et technique : enjeux normatifs et sociaux* sous la direction de René Côté et Guy Rocher, Éditions Thémis, Montréal, 1994, p.186.

[539] « Market failure can be defined with respect to either the human rights or contractual approaches to the protection of personal information. Under the human rights approach, the goal is to protect individuals' right to privacy according to the moral theory that defines the right. A pure marker model will fail to the extent that it protects privacy less well than is desirable under the moral theory. » Peter SWIRE, « Markets, Self-Regulation, and Government Enforcement in the Protection of Personal Information », http://www.acs.ohio-state.edu/units/law/swire1/psntia6.html.

[540] « First, self-regulation may provide benefits to society compared with an otherwise-unregulated market. The European Community clearly questions the adequacy of informational privacy protection in the United States. Although there is much support in the U.S. for self-regulatory measures and technological privacy innovations, there remains substantial doubt as to whether these measures can be completely effective without some type of enforcement mechanism. Unless there are sanctions available for violations of industry guidelines, some information companies may be inclined to ignore industry guidelines or to minimize their significance in their quests for profits.» Susan E. GINDIN, « Lost and found in cyberspace: Information privacy in the age of the Internet », 1997 *San Diego Law Review*, http://www.info-law.com/lost.html.

À ce sujet, Swire propose : « The topic of self-regulation, by contrast, arises with respect to data collection and use by non-governmental enterprises. A thesis of my own ongoing research is that data collection by private enterprises should be examined in terms of the contractual relationship between the company and the customers. » Peter SWIRE, « Markets, Self-Regulation, and Government Enforcement in the Protection of Personal Information », http://www.acs.ohio-state.edu/units/law/swire1/psntia6.html.

[541] Peter Swire, « Markets, Self-Regulation, and Government Enforcement in the Protection of Personal Information », http://www.acs.ohio-state.edu/units/law/swire1/psntia6.html. Voir Joel R. REIDENBERG, « Setting Standards for Fair Information Practice in the U.S. Private Sector », 80, *Iowa Law Review* 497 (1995).

[542] À ce sujet, Benyekhlef et Trudel rappellent que le problème de la délocalisation et de l'intangibilité de l'information n'est pas vraiment nouveau. « Une lecture attentive des lois de protection des données personnelles, élaborées dans les années soixante-dix, permet de constater que les législateurs européens étaient conscients du fait que le mariage de l'informatique et des télécommunications pouvait faciliter le contournement de leurs législations. » Karim BENYEKHLEF et Pierre TRUDEL, *Approches et stratégies pour*

Pour être utile dans un domaine technique, le droit doit être précis[543] ; mais si on le précise, il est rapidement rendu caduc par le progrès technique[544]. La nouveauté du problème tient au fait qu'une masse toujours croissante d'usagers ont accès au réseau Internet. Il ne s'agit plus dès lors de contrôler simplement les flux informationnels entre de grandes entreprises ou des composantes de l'État. « La décentralisation des réseaux entraîne une augmentation des acteurs et des usagers et de ce fait, rend illusoire les prohibitions édictées dans les différentes législations[545]. »

L'architecture de l'Internet, le nombre croissant d'usagers et le recours aux réseaux pour transiger et conclure tout type de transactions constituent autant de facteurs expliquant les difficultés d'appliquer efficacement les législations[546]. La mise en œuvre de règles consacrées par les législations pose aussi, comme nous l'avons constaté précédemment, de nombreuses difficultés pratiques d'application résultant de l'architecture même du réseau, dont entre autres, la compétence juridique, les difficultés d'application et les recours juridiques[547].

Le fait de déplorer l'inapplicabilité pratique des législations de protection des renseignements personnels et les incitatifs purement financiers qui régissent la

---

améliorer la protection de la vie privée dans le contexte des inforoutes, Mémoire présenté à la Commission de la culture de l'Assemblée nationale dans le cadre de son mandat sur l'étude du Rapport quinquennal de la Commission d'accès à l'information, septembre 1997, p. 20

543 Néanmoins, il importe de souligner un point. Le réseau Internet met en présence des acteurs d'horizons culturels diversifiés. Les niveaux de consensus et les cadres de références sur lesquels ils sont fondés dans les espaces culturels nationaux ne sont plus nécessairement opératoires sur Internet. C'est sans doute pour cela que l'on n'échappe pas, à un certain point, à l'obligation de formuler les normes au moyen de standards et de notions à contenu variable. Pierre TRUDEL, France ABRAN, Karim BENYEKHLEF et Sophie HEIN, *Droit du cyberespace*, Montréal, Éditions Thémis, 1996, p. 3-8.

544 René LAPERRIÈRE, « L'émergence de normes dans le domaine des communications de renseignements personnels » dans *Entre droit et technique : enjeux normatifs et sociaux* sous la direction de René Côté et Guy Rocher, Éditions Thémis, Montréal, 1994, p.184.

545 Pierre TRUDEL, France ABRAN, Karim BENYEKHLEF et Sophie HEIN, *Droit du cyberespace*, Montréal, Éditions Thémis, 1996, p. 15-2. Voir Karim BENYEKHLEF, « Les normes internationales de protection des données personnelles et l'autoroute de l'information », dans *Le respect de la vie privée dans l'entreprise, Actes des Journées Maximilien Caron*, Montréal, Éditions Thémis, 1996, 661, Susan E. GINDIN, « Lost and found in cyberspace : Information privacy in the age of the Internet », 1997 *San Diego Law Review*, http://www.info-law.com/lost.html et Peter P. SWIRE, « Of Elephants, Mice, and Privacy: International Choice of Law and the Internet », *Draft submitted to International Lawyer*, 23 août 1998, http://www.acs.-ohio-state.edu/units/law/swire1/elephants.htm.

546 « Cette architecture électronique a des conséquences sur les principes de territorialité et de juridiction autour desquels s'articule l'action législative classique. » Karim BENYEKHLEF, « Les normes internationales de protection des données personnelles et l'autoroute de l'information », dans *Le respect de la vie privée dans l'entreprise, Actes des Journées Maximilien Caron*, Montréal, Éditions Thémis, 1996, 661 p.97. Voir Karim BENYEKHLEF, « L'Internet : un reflet de la concurrence des souverainetés », dans *Réglementer les inforoutes (Actes du colloque d'octobre 1996)* et Karim BENYEKHLEF, *La protection de la vie privée dans les échanges internationaux d'informations*, Montréal, Éditions Thémis, 1992, 475 p.

régulation par le marché, nous amène à opposer la régulation législative à la régulation par le marché[548]. Le réseau étant ce qu'il est, « une approche unilatérale, qu'elle émane du marché ou du législateur, ne peut répondre adéquatement aux difficultés afférentes à la protection des renseignements personnels[549]. » Il appert donc qu'une solution efficace à la protection des renseignements personnels sur le réseau Internet pourrait naître de la mise en commun de ces deux modes de régulation. La standardisation ne constitue non pas une voie exclusive[550] mais une voie complémentaire intéressante en ce qu'elle traduit les principes fondamentaux dans l'industrie[551].

---

[547] Pour plus d'informations au sujet de problèmes, lire l'étude explicite du professeur Bennett. Colin BENNETT, *Réflexions sur une norme internationale de protection des renseignements personnels*, Groupe de travail sur le commerce électronique d'Industrie Canada, http://e-com.ic.gc.ca/francais/privee/632d293.html

[548] À ce sujet, le professeur Swire écrit : « In the pure market model so far described, there are two important constraints on companies' privacy policies. The first restraint comes from consumer preferences. The more that some or all consumers are willing to change their purchasing decisions based on privacies policies, the greater the market discipline on companies. The second restraint comes from publicity about companies' privacy practises. The prospect of such publicity encourages companies to conform to customers' preferences. Publicity over time may also shape consumers' preferences, such as by making them more concerned as a group about possible privacy problems. The pure market model thus as a dynamic component, in which both customer preferences an company practices can evolve over time as awareness and concern about privacy themselves evolve.

At the opposite extreme from the pure market model is the pure enforcement model. The assumption here is that market discipline is largely or entirely ineffective at protecting individuals' privacy. Instead, vindication of individuals' privacy rights occurs through legal enforcement. [...] Designated parties, such as a government agency or citizen who has been wronged, are allowed to sue to enforce those rules. The suits seek to achieve the twin goals of compensation and deterrence. Compensation takes place when the individual whose privacy is violated is paid to extent of the violation. Deterrence is focused on the incentives of the corporation – the corporation that violates privacy should face and expected cost for violating privacy that exceeds its expected benefit from its bad privacy practices. » Peter SWIRE, « Markets, Self-Regulation, and Government Enforcement in the Protection of Personal Information », http://www.acs.ohio-state.edu/units/law/swire1/psntia6.html

[549] Karim BENYEKHLEF et Pierre TRUDEL, *Approches et stratégies pour améliorer la protection de la vie privée dans le contexte des inforoutes*, Mémoire présenté à la Commission de la culture de l'Assemblée nationale dans le cadre de son mandat sur l'étude du Rapport quinquennal de la Commission d'accès à l'information, septembre 1997, p. 20.

[550] « These recommendations [code de conduite] will, in these circumstances, make a positive contribution. Indeed, the development of voluntary codes is a recognition that data privacy laws are an essential concomitant of automated processing of personal data. Such codes may also have the effect of promoting customer confidence in the services offered so that there may be favourable trade implications [...]. In countries where there is existing data protection legislation, the existence of voluntary codes of practice is seen as a fine-tuning mechanism which translates the general terms of the legislation into practical terms to be adopted by the particular sector or organisation. Doubtless these organisations must comply with the provisions of the legislation, however it is not always easy to determine the precise application of general legislation to specific circumstances in an organisation or sector. From the foregoing, it can be seen that there is voluntary convergence in personal date regulation towards the principles outlined in the OECD Guidelines. It must be added however that voluntary adherence to a code of conduct unsupported by legislation does not provide data subjects with inviolable adherence to a code of conduct unsupported by legislation does not provide data subjects with inviolable rights against data users or collectors so that this must always be a reservation where the voluntary regulatory approach is used. » OCDE, *Present Situation and Trends in Privacy Protection in the OECD Area,* Paris, DSTI/ICCP/88.5, 1er juin 1988, p.19 cité dans Karim BENYEKHLEF, « Les normes internationales de protection des données personnelles et l'autoroute de l'information », dans *Le respect de la vie privée dans l'entreprise, Actes des Journées Maximilien Caron*, Montréal, Éditions Thémis, 1996, 661, note 43.

[551] Karim BENYEKHLEF, « Les normes internationales de protection des données personnelles et l'autoroute de l'information », dans *Le respect de la vie privée dans l'entreprise, Actes des Journées Maximilien Caron*,

« Il est sûr que des normes se développent, sous forme de lois, de directives, de critères, de codes d'éthique ; mais elles ne semblent pas pouvoir être appliquées efficacement, et c'est leur manque de précision qui les rends impuissantes à agir sur la réalité. Étant donné la diversité des activités, une loi générale ne suffit donc pas, en raison de son imprécision, mais elle s'avère nécessaire pour énoncer les principes essentiels, les normes qui se rapprochent le plus de l'éthique[552]*. »*

L'article 27 (1) de la *Directive* reconnaît la complémentarité que peut apporter la standardisation au plan normatif. Toutefois, cette voie ne saurait à elle seule satisfaire aux exigences de la *Directive* ; il s'agit donc d'une simple complémentarité.

CHAPITRE V -
CODES DE CONDUITE

Article 27

1. *Les États membres et la Commission encouragent l'élaboration de codes de conduite destinés à contribuer, en fonction de la spécificité des secteurs, à la bonne application des dispositions nationales prises par les États membres en application de la présente directive.*

2. *Les États membres prévoient que les associations professionnelles et les autres organisations représentant d'autres catégories de responsables du traitement qui ont élaboré des projets de code nationaux ou qui ont l'intention de modifier ou de proroger des codes nationaux existants peuvent les soumettre à l'examen de l'autorité nationale.*

   Les États membres prévoient que cette autorité s'assure, entre autres, de la conformité des projets qui lui sont soumis avec les dispositions nationales prises en application de la présente directive. Si elle l'estime opportun, l'autorité recueille les observations des personnes concernées ou de leurs représentants.

3. *Les projets de codes communautaires, ainsi que les modifications ou prorogations de codes communautaires existants, peuvent être soumis au groupe visé à l'article 29. Celui-ci se prononce, entre autres, sur la conformité des projets qui lui sont soumis avec les dispositions nationales prises en application de la présente directive. S'il l'estime opportun, il recueille les observations des personnes concernées ou de*

Montréal, Éditions Thémis, 1996, 661 p.97, Mathieu O'NEIL, « Internet, ou la fin de la vie privée », septembre 1998, *Le Monde diplomatique*, http://www.monde-diplomatique.fr/1998/09/O_NEIL/10914.html et Suzanne M. THOMPSON, « The Digital Explosion Comes With a Cost: The Loss of Privacy », 4 *Tech. L. & Pol'y* 3 (1999), http://journal.law.ufl.edu/%7Etechlaw/4/Thompson.html.

[552] René LAPERRIÈRE, « L'émergence de normes dans le domaine des communications de renseignements personnels » dans *Entre droit et technique : enjeux normatifs et sociaux* sous la direction de René Côté et Guy Rocher, Éditions Thémis, Montréal, 1994, p.184.

> *leurs représentants. La Commission peut assurer une publicité appropriée aux codes qui ont été approuvés par le groupe.*

Cet article reconnaît la possibilité pour les États membres de développer des codes nationaux de bonne conduite. De tels instruments conçus sous la supervision et la collaboration d'autorités publiques, peuvent certes contribuer à une protection plus efficace de la vie privée informationnelle[553].

La protection des renseignements personnels désigne la capacité d'une personne de déterminer par elle-même quels renseignements à son sujet peuvent être communiqués à autrui, quand et comment. Ainsi, l'instauration d'une norme internationale de protection des renseignements personnels pourrait s'avérer une bonne solution et irait ainsi dans l'intérêt de tous les pays et des usagers. Une norme de l'ISO par exemple, aurait beaucoup de poids et de crédibilité en Europe et aux États-Unis. Les entreprises y accorderaient plus d'attention et feraient plus d'efforts d'accréditation. Elles disposeraient aussi d'un moyen plus fiable et plus uniforme pour montrer qu'elles se conforment aux normes internationales de protection des données. Entre autres, les Postes britanniques ont obtenu la certification ISO 9001 pour leurs services et leurs mesures de protection des données. Sur le réseau Internet, une norme internationale de protection des renseignements personnels pourrait[554] :

- Dissiper les craintes des usagers ;

  Si, comme beaucoup le prétendent, protéger les renseignements personnels constitue une bonne pratique commerciale, les entreprises devraient chercher à dissiper les craintes des consommateurs en adoptant la norme, en faisant savoir qu'elles l'ont adoptée et en se soumettant ainsi à des vérifications. Tel que le souligne le professeur Bennett : « Si l'on peut arriver à définir des procédures fiables d'évaluation de la conformité, l'adoption de la norme signifiera beaucoup plus que l'adoption des Lignes directrices de l'OCDE. La différence réside en ce que la norme entraînerait une vérification objective des pratiques de l'entreprise.

---

[553] Selon la Commission européenne : « One of the issues that is of course still outstanding -- and that we are putting enormous emphasis on -- is enforcement. That's the key difference between legislation and self-regulation, and that's why we're spending a lot of time on it. The difference here is that enforcement will be entirely on the shoulders of the industry, while in Europe the enforcement is done, of course, by data privacy commissioners. » Chris OAKES, « A European's Net View of US », 30 août 1999, *Wired*, http://www.wired.com/news/politics/0,1283,21476,00.html

[554] Colin BENNETT, *Réflexions sur une norme internationale de protection des renseignements personnels*, Groupe de travail sur le commerce électronique d'Industrie Canada, http://e-com.ic.gc.ca/francais/privee/632d294.html

Une telle norme serait un prolongement naturel des codes de pratique volontaire qui sont établis dans le cadre de l'OCDE[555]. »

Malgré tout, les internautes vont vraisemblablement continuer de manifester de vives inquiétudes à l'égard de tous les scandales mettant en cause les « online privacy seal programs ». L'adoption d'une norme de protection de la vie privée aiderait ainsi à apaiser ces inquiétudes.

- Montrer que les données sont adéquatement protégées ;

  L'adoption d'une norme internationale de protection des renseignements personnels permettrait aux entreprises non européennes de montrer aux autorités européennes qu'elles appliquent des mesures adéquates de protection des données.

- Favoriser une plus grande conformité transnationale et intersectorielle ;

  Une norme internationale aiderait à uniformiser les règles du marché à l'échelle internationale. Les entreprises plus respectueuses de la vie privée vont trouver de plus en plus irritant de voir que leur réputation est ternie par des entreprises moins responsables de leur secteur et vont avoir besoin d'un moyen plus sûr et plus fiable pour montrer qu'elles respectent des principes équitables de traitement de l'information.

- Compléter la réglementation ; et

  En étant citée dans les différentes législations nationales et internationales. « Au Canada, les vérifications de la CSA sont vues comme un moyen rentable d'application de la législation par des gouvernements qui n'ont ni la volonté ni les moyens d'instituer de coûteux régimes de contrôle[556]. »

- Promouvoir l'adoption de pratiques respectueuses de la vie privée sur l'Internet.

  Compte tenu de le jugement de la Cour suprême des États-Unis qui a annulé le *Communications Decency Act*, on peut s'attendre à ce qu'il soit fait un recours croissant à l'emploi de normes pour contrôler le contenu et les communications de l'Internet. Ainsi, il serait particulièrement important de standardiser les mesures de protection de la vie privée pour offrir une meilleure protection aux

---

[555] Colin BENNETT, *Réflexions sur une norme internationale de protection des renseignements personnels*, Groupe de travail sur le commerce électronique d'Industrie Canada, http://e-com.ic.gc.ca/francais/privee/632d294.html

[556] Colin BENNETT, *Réflexions sur une norme internationale de protection des renseignements personnels*, Groupe de travail sur le commerce électronique d'Industrie Canada, http://e-com.ic.gc.ca/francais/privee/632d294.html

usagers et par le fait même, promouvoir la mondialisation du commerce électronique.

Pour les gouvernements, les normes se sont révélées de précieux outils dans la libéralisation des échanges commerciaux et la réforme des régimes réglementaires. Quant aux entreprises, elles ont constaté que ces normes contribuent au changement en tenant compte de leurs préoccupations[557].

Concrètement, une des plus récentes propositions avancées pour régler les problèmes découlant de l'utilisation des organismes de standardisation serait de créer une autorité impartiale et indépendante qui délivrait les nouveaux sceaux de confiance. Un organisme, tel un Personal Date Privacy Bureau, pourrait résoudre cette problématique. « It's clear that we need better legal standard for privacy protection. Without such standards, as an independent privacy agency within the government to help interpret them and advocate for privacy protection[558]. »

En effet, le développement de normes par un organisme semblable en conjonction avec les autorités publiques, pourrait assurer une protection de la vie privée informationnelle. De plus, une telle autorité impartiale et indépendante pourrait contrôler la manière dont les entreprises respectent les principes fondamentaux et les législations en matière de protection des renseignements personnels.

On pourrait confier à cet organisme la tâche d'élaborer des normes propres à assurer la mise en œuvre des législations internationales et nationales. Il pourrait ainsi policer le comportement des entreprises par voie de recommandations ou de mise en garde formelle[559]. La création d'une telle autorité suppose l'existence d'une législation nationale ou internationale qui tracerait les normes minimales à suivre. Évidemment, un tel organisme pourrait être à l'échelle nationale et/ou internationale mais devrait nécessairement appliquer soit un accord international ou les usages en ce domaine. En effet, une coopération internationale apparaît nécessaire si l'on désire assurer

---

[557] CONSEIL CANADIEN DES NORMES, *Normalisation – Une stratégie du Canada pour favoriser la compétitivité et promouvoir les intérêts sociétaux*, 31 août 1998, http://www.scc.ca/pressrel/1998/aug31-f.html

[558] Declan MCCULLAGH, « A Personal Data Privacy Bureau ? » 6 mai 1999, *Wired*, http://www.wired.com/news/print_version/politics/story/19537.html?wnpg=all

[559] Peter P. SWIRE, « Of Elephants, Mice, and Privacy: International Choice of Law and the Internet », *Draft submitted to International Lawyer*, 23 août 1998, http://www.acs.-ohio-state.edu/units/law/swire1/elephants.htm et Karim BENYEKHLEF, *La protection de la vie privée dans les échanges internationaux d'informations*, Montréal, Éditions Thémis, 1992, 475 p, p.75.

pleinement la protection de la vie privée sur Internet comme le souligne le professeur Benyekhlef.

Le développement de normes autoréglementaires par des associations ne saurait être négligé. Bien que la voie autoréglementaire puisse apparaître déficiente au regard du contrôle et de la sanction des normes qu'elle institue, elle peut constituer une voie complémentaire - et non pas exclusive - intéressante en ce qu'elle traduit les principes fondamentaux dans l'industrie ou le secteur concerné[560].

Ainsi, les principes fondamentaux en matière de gestion des renseignements personnels consacrés dans les documents internationaux paraissent être en mesure de garantir la protection de la vie privée sur les inforoutes. En raison de l'intangibilité du cyberespace et la délocalisation des acteurs, leurs applicabilités semblent difficiles. Dans l'intérêt de tous les pays et de tous les internautes, une coopération internationale, soit par l'instauration d'une norme distincte de protection de la vie privée au soutient d'une législation, s'avère primordiale.[561].

---

[560] Karim BENYEKHLEF, « Les normes internationales de protection des données personnelles et l'autoroute de l'information », dans *Le respect de la vie privée dans l'entreprise, Actes des Journées Maximilien Caron*, Montréal, Éditions Thémis, 1996, 661 p.97.

[561] Karim BENYEKHLEF et Pierre TRUDEL, *Approches et stratégies pour améliorer la protection de la vie privée dans le contexte des inforoutes*, Mémoire présenté à la Commission de la culture de l'Assemblée nationale dans le cadre de son mandat sur l'étude du Rapport quinquennal de la Commission d'accès à l'information, septembre 1997, p. 20 et Joel REIDENBERG et Françoise GAMET-POL, « The Fundamental Role of Privacy and Confidence in the Network », (1995) 30 *Wake Forest Law Review* 105, 110-111.

CONCLUSION

En permettant à tous les ordinateurs du monde de communiquer entre eux, Internet constitue le plus abouti et pour l'instant, le plus fabuleux instrument que la société de l'information ait bâtit à l'échelle mondiale. L'ouverture des réseaux informatiques à une population qui de jour en jour devient plus nombreuse, a toutefois permis d'avoir une vision plus précise et plus réaliste des nombreuses pratiques néfastes qui subsistent sur le réseau Internet.

En effet, on assiste actuellement à une expansion continue des possibilités d'intrusion dans la vie privée due aux progrès considérables des moyens de communication et de diffusion de l'information et au développement foudroyant des technologies informatiques, qui permettent la cueillette, le traitement et la conservation de renseignements personnels, soit la constitution de fichiers informations et de banques de données.

Les diverses possibilités d'intrusions dans la vie privée donnent lieu à des préoccupations sans précédent quant aux moyens de protéger la zone d'intimité personnelle nécessaire à la vie humaine et à son développement dans la société[562]. Le respect de la vie privée prend une toute autre signification en raison de la collecte généralisée de renseignements personnels et de l'utilisation qui en est faite. Les individus, qui sont la source originelle des renseignements personnels, n'exigent pas habituellement que ce déversement industriel de l'information leur soit retourné. Ce qui les préoccupe, c'est que les qualités et l'identité des personnes soient prises et utilisées avec une désinvolture injustifiée, à leur insu ou sans leur consentement, qu'elles soient vendues plusieurs fois aux intervenants du marché sans aucune assurance que la source originelle y conserve son exactitude et sa pureté. Toutefois, face aux divers abus produits depuis quelques années, les internautes désirent maintenant contrôler l'utilisation des données les concernant[563]. Ainsi, il semble nécessaire pour répondre aux craintes qui subsistent, de tenter de protéger, conserver et réglementer l'utilisation

---

[562] Pierre KAYSER, *La protection de la vie privée par le droit, protection du secret de la vie privée*, 3e éd., Économica-Presses Universitaires d'Aix-Marseille, Paris 1995, p.15.

[563] Colin BENNETT, *Réflexions sur une norme internationale de protection des renseignements personnels*, Groupe de travail sur le commerce électronique d'Industrie Canada, http://e-com.ic.gc.ca/francais/privee/632d29.html

des courants d'information dans ce nouvel environnement électronique issu de la « société de l'information[564] ».

Comme nous l'avons constaté précédemment, la protection des renseignements personnels sur l'autoroute de l'information soulève d'importantes difficultés. Ni la dimension mondiale des réseaux, ni leur ouverture totale, ni l'immédiateté de la communication qu'ils offrent, n'empêchent que soient respectés sur Internet comme sur les autres réseaux ouverts ou fermés, les principes fondamentaux en matière de protection de la vie privée et des renseignements personnels[565]. Toutefois, en pratique cette appréciation reste théorique. L'intangibilité du réseau et la délocalisation des acteurs rendent ces principes difficilement applicables. Le développement de l'informatique a permis l'intégration et la centralisation d'informations confidentielles privées.

Que l'on soit ou non d'accord, un point semble acquis : les questions concernant l'exactitude des données et l'identité de ceux pouvant y accéder prennent un tour nouveau avec le développement des réseaux. Avec Internet, l'accès se généralise brutalement. Plus de cloisonnement : tout est instantanément disponible depuis n'importe quel endroit. La question de la protection de la vie privée passe de l'échelle locale et nationale à l'échelle internationale. Nous estimons avec le professeur Benyekhlef, que :

> *« les principes fondamentaux en matière de gestion de l'information personnelle, consacrés dans les documents internationaux sont, de prime abord en mesure d'assurer la protection de la vie privée sur les nouvelles voies de communications. Mais, cette appréciation est théorique. L'intangibilité du cyberespace et la délocalisation des acteurs télématiques rendent ces principes difficilement applicables au plan pratique. La coopération internationale semble donc primordiale.[566] »*

---

[564] Anne WELLS-BRANSCONB, *Who Owns Information?*, New York, Harper-Collins Publishers inc., 1994, p.5.

[565] Plus spécifiquement, nous faisons référence aux principes fondamentaux qui sont appliqués dans la plupart des états occidentaux et consignés entre autres dans la *Directive* et les législations québécoises et canadiennes.

[566] Karim BENYEKHLEF, « Les normes internationales de protection des données personnelles et l'autoroute de l'information », dans *Le respect de la vie privée dans l'entreprise*, Actes des Journées Maximilien Caron, Montréal, Éditions Thémis, 1996, 65, p.101

En tout état de cause, la défense de la protection des renseignements personnels sur Internet relève de l'urgence dès lors qu'elle est confrontée à de considérables enjeux technologiques, commerciaux, économiques et industriels. Ainsi, il se développe sur Internet un marché de la vie privée et la célèbre phrase « Sur la Toile, personne ne sait que vous êtes un chien », devient obsolète.

Même si pour l'instant, le commerce électronique en est encore à son tout début, l'exploitation des renseignements personnels représente incontestablement la matière première de l'Internet commercial. Dans ce cadre, le développement du commerce électronique par le réseau repose sur la confiance des consommateurs. Les usagers souhaitent naturellement avoir l'assurance que leurs renseignements personnels ne seront pas exploités par n'importe qui, n'importe comment et à leur insu.

Rien d'étonnant à ce que le débat ouvert Outre-Atlantique sur la protection des renseignements personnels puise effectivement son origine dans le problème posé par la collecte systématique de nombreux renseignements concernant les internautes, le plus souvent à leur insu. Les acteurs du commerce électronique doivent pouvoir concilier au plan mondial le développement de ce nouveau marché tout en permettant le respect de la vie privée des usagers.

C'est l'architecture des réseaux qui complique la mise en œuvre pratique des principes fondamentaux en matière de protection et de gestion de l'information personnelle. Appliquées seules, les législations et les méthodes de standardisation présentent des inconvénients. En cette matière, tel que le soulignent Benyekhlef et Trudel, il faut se tenir loin de tout dogmatisme. Une approche unilatérale, qu'elle émane du marché ou du législateur, ne peut répondre adéquatement aux difficultés afférentes à la protection des renseignements personnels sur les inforoutes[567].

En conséquence, en offrant des techniques performantes pour classifier et canaliser l'information, il appert que la technologie en dualité avec une législation s'avère une solution performante pour aider les utilisateurs à exercer un contrôle approprié sur leurs renseignements personnels. Le tout récent accord intervenu entre l'Europe et les États-

---

[567] Karim BENYEKHLEF et Pierre TRUDEL, *Approches et stratégies pour améliorer la protection de la vie privée dans le contexte des inforoutes*, Mémoire présenté à la Commission de la culture de l'Assemblée nationale dans le cadre de son mandat sur l'étude du Rapport quinquennal de la Commission d'accès à l'information, septembre 1997, p. 20.

Unis démontre bien l'importance de cette avenue[568]. La Directive sur la protection des données de l'Union européenne est déjà une norme *de facto* internationale de protection de la vie privée.

> *« Europeans are protected from the commercial gathering and selling of personal data -- including the kind of information gathered my many Web sites -- without their informed consent, while in the United States, industry is allowed to police itself*[569]*. »*

Les instruments d'interventions actuels présentent des lacunes diverses : confusion des champs de compétence; inadaptation à la complexité et à l'interactivité des flux de données transfrontières; approche corrective fondée sur des recours individuels par opposition à une approche proactive de recherche de solutions à long terme; divergences d'interprétation et d'application; accent mis sur l'évaluation du contenu et de la procédure plutôt que de la pratique. Ainsi, la standardisation n'est pas dénudée d'intérêt. Tel que nous l'avons constaté, elle peut constituer une technique souple et adaptable au réseau Internet pour répondre convenablement aux nouveaux défis posés par la révolution des communications électroniques[570].

La protection de la vie privée est l'élément clé d'un environnement national et international bien organisé pour les internautes. Les individus ne sont pas les seuls à réclamer que l'usage des renseignements personnels obtenus et transmis sur le réseau Internet soit soumis à certaines restrictions et réglementations ; cette protection fait partie intégrante des saines pratiques en affaires qui assurent le libre accès aux marchés internationaux.

---

[568] Le département américain du Commerce a proposé à l'Union européenne un compromis qui instituerait un label aux entreprises respectant un ensemble de principes sur la protection des renseignements personnels. Les deux parties ont décidé en décembre 1999 d'une date limite pour trouver un accord, fixée à la fin du mois de mars 2000. L'union européenne se préoccupait de la possibilité de poursuivre les entreprises labellisées qui dérogeraient à leurs engagements. Toutefois, une visite aux États-Unis effectuée en janvier 2000 par les autorités de protection des renseignements personnels a permis de rassurer l'Europe. EUROPEAN COMMISSION, *Data protection: significant progress made at February 21/22 talks on facilitating EU/US data transfers*, 24 février 2000, http://europa.eu.int/comm/dg15/en/media/dataprot/news/talks.htm et Jeri CLAUSING, « U.S. and Europe Reach Tentative Pact on Personal Data », 23 février 2000, *New York Times*, http://www.nytimes.com/library/tech/yr/mo/cyber/articles/24privacy.html.

[569] Jeri CLAUSING, « U.S. and Europe Reach Tentative Pact on Personal Data », 23 février 2000, *New York Times*, http://www.nytimes.com/library/tech/yr/mo/cyber/articles/24privacy.html.

[570] Karim BENYEKHLEF, « Les normes internationales de protection des données personnelles et l'autoroute de l'information », dans *Le respect de la vie privée dans l'entreprise, Actes des Journées Maximilien Caron*, Montréal, Éditions Thémis, 1996, 661 p.100.

BIBLIOGRAPHIE

Monographies et recueils

BAUDOUIN, J-L., *La responsabilité civile*, 4e éd., Cowansville, Éditions Yvon Blais, 1241p.

BENYEKHLEF, K., *La protection de la vie privée dans les échanges internationaux d'informations*, Montréal, Éditions Thémis, 1992, 475 p.

BERGERON, M. et C. KEMPA, *Vocabulaire d'Internet : terminologie des technologies de l'information*, Office de la langue français, Montréal, 1995, http://www.olf.gouv.qc.ca/service/pages/internet2.html

BRUN, H. et G.TREMBLAY, *Droit Constitutionnel*, 2ième édition, Éditions Yvon Blais Inc., Cowansville, 1990, 1232 pages, p: 80.

CHEVRETTE, F. et H. MARX, *Droit constitutionnel : notes et jurisprudences*, Montréal, P.U.M. 1982.

CLINTON, W. J. et A. GORE, JR., *A Framework for Global Electronic Commerce*, 1 juillet 1997, http://www.iitf.nist.gov/eleccomm/ecomm.htm.

COMITÉ CONSULTATIF SUR L'AUTOROUTE DE L'INFORMATION, *Contact, communauté, contenu : Le défi de l'autoroute de l'information* (rapport final), Ottawa, Ministère des Approvisionnements et Services Canada, 1995.

CONSEIL DES SCIENCES DU CANADA, *Atelier sur les technologies de l'information et la protection de la vie privée au Canada*, 1985, 70 p.

COOLEY, T.M., *A Treatise on the Law of Torts or the Wrongs which Arise Independents of Contract*, 2d. ed., Chicago, Callaghan & Co., 1888.

DE WOLF, H., *The Jargon File : The World Wide Web version*, http://yardim.bilkent.edu.tr/Online/Jargon30/JARGON_A/ARMM.HTML

GARFINKEL, S., et G. SPAFFORD, « Chapter IV - Cryptography »,*Web Security & Commerce*, O'Reilly & Associates Inc., 1997, Sebastopol CA.

GIESEKE, W., *PC 100 % Pratique, Sécurité et Protection*, traduction de C. STOLL, H. BERTRAND et P. M. WOLF, Paris, Micro Application, 1998, 560 p.

INDUSTRIE CANADA, *Groupe de travail sur le commerce électronique : Évolution de la protection des données dans le monde*, http://com-e.ic.gc.ca/francais/fastfacts/43d10.html

INDUSTRIE CANADA, *Groupe de travail sur le commerce électronique - Vie privée: protection des renseignements personnels*, http://strategis.ic.gc.ca/virtual_hosts/e-com/francais/privee/632d1.html.

INDUSTRIE CANADA, *L'autoroute canadienne de l'information : Une nouvelle infrastructure de l'information et des télécommunications au Canada*, Ottawa, Strategis, 1996, http://www.strategis.ic.gc.ca/SSGF/ca00257f.html.

INDUSTRIE CANADA, *La protection de la vie privée et l'autoroute canadienne de l'information*, Ottawa, Ministères des Approvisionnements et Services Canada, 1994, 23 p.

INDUSTRIE CANADA, *Protection de la vie privée et autoroute de l'information : Les options du Canada en matière de réglementation*, Ottawa, Ministères des Approvisionnements et Services Canada, 1994, 23 p.

INDUSTRIE CANADA, *Résumé de la politique du Canada en matière de cryptographie*, http://strategis.ic.gc.ca/virtual_hosts/e-com/francais/fastfacts/43d7.html.

INDUSTRIE CANADA - BUREAU DE LA CONSOMMATION, *Bulletin trimestriel sur la consommation*, mars 1998, Volume 4, Numéro 1, http://strategis.ic.gc.ca/SSGF/ca01128f.html

KAYSER, P. *La protection de la vie privée : Protection du secret de la vie privée*, 3e éd., Paris Aix-en-Provence, Économica, Presse Universitaires d'Aix Marseille, 1995, 605 p.

MICHAUD, M., *Le droit au respect de la vie privée dans le contexte médiatique : de Warren et Brandis à l'inforoute*, Montréal, Éditions Wilson & Lafleur, 1996, 118 p.

MINISTÈRE DES AFFAIRES ÉTRANGÈRES ET DU COMMERCE INTERNATIONAL, *Contrôle à l'exportation sur les produits de la cryptographie*, 23 décembre 1998, http://www.dfait-maeci.gc.ca/~eicb/notices/ser113-f.htm

ORWELL, G., *1984*, Mass Market Paperback, Reissue edition (May 1990), 268 p

PARISIEN, S. et P. TRUDEL, *L'identification et la certification dans le commerce électronique*, Québec, Publications du Québec, 1996.

PATENAUDE, P., *La preuve, les techniques modernes et le respect des valeurs fondamentales : enquête, surveillance et conservation des données*, Sherbrooke, Éditions R.D.U.S., 1990, p. 23-24.

RAYMOND, E.S., *The New Hacker's Dictionary*, 1 novembre 1996, http://www.elsewhere.org/jargon_search/TAG38.html

ROSENOER, J., *CyberLaw, The law of the Internet*, New York, Springer-Verlag, 1997.

ST-LAURENT, S., *Cookies*, Computing McGraw-Hill, New York, 1998.

STINSON, D.R., *Cryptography : Theory and Practice*, Londres, CRC Press, 1995,

TRUDEL, P., F. ABRAN, K. BENYEKHLEF et S. HEIN, *Droit du cyberespace*, Montréal, Éditions Thémis, 1991, 1180 p.

TRUDEL, P., G. LEFEBVRE et S. PARISIEN, *La preuve et la signature dans l'échange de documents informatisés au Québec*, Québec, Publications du Québec, 1993.

WELLS-BRANSCONB, A., *Who Owns Information?*, New York, Harper-Collins Publishers inc., 1994, p.5.

WESTIN, A.F., *Privacy and Freedom*, New York, Atheneum, 1970, p.350.

Articles de revue et recueils d'études

BAKER, D.I. et W. Todd MILLER, « Privacy, Antitrust and the National Information Infrastructure: Is Self-Regulation of Telecommunications-Related Personal Information a Workable Tool? », dans *Privacy and Self-Regulation in the Information Age, Chapter* , National Telecommunications and Information Administration, Juin 1997.

BELGUM, K. D., « Who Leads at Half-time?: Three Conflicting Visions of Internet Privacy Policy », 6 *Rich. J.L. & Tech.* 1, (Symposium 1999), http://www.richmond.edu/jolt/v6i1/belgum.html

BENNETT, C. J., *Réflexions sur une norme internationale de protection des renseignements personnels*, Groupe de travail sur le commerce électronique d'Industrie Canada, http://e-com.ic.gc.ca/francais/privee/632d29.html

BENNETT, C.J., « The Canadian Standards Association Model Code for the Protection of Personal Information : Reaching Consensus on Principles and Developing Enforcement Mechanisms », *Privacy and Self-regulation - chapter 4*, http://www.ntia.doc.gov/reports/privacy/selfreg4.htm.

BENYEKHLEF, K., « Les dimensions constitutionnelles du droit à la vie privée », dans Pierre TRUDEL et France ABRAN, *Droit du public à l'information et vie privée : deux droits irréconciliables ?*, Montréal, Éditions Thémis, 1992.

BENYEKHLEF, K., « Les libertés : voie médiatrice de la protection des données personnelles », dans *Le droit de la communicatique, Acte du colloque conjoint des Facultés de droit de l'Université de Poitiers et de l'Université de Montréal*, Montréal, Éditions Thémis, 1992, p.61.

BENYEKHLEF, K., « Les normes internationales de protection de données personnelles et l'autoroute de l'information », dans André POUPART (dir.), *Le respect de la vie privée dans l'entreprise : de l'Affirmation à l'Exercice d'un droit,* Les journées Maximilien-Caron, Montréal, Éditions Thémis, 1996, p.65.

BENYEKHLEF, K., « Les transactions dématérialisées sur les voies électroniques ; panorama des questions juridiques », dans Daniel POULIN, Pierre TRUDEL et Ejan MACKAAY (dir.), *Les autoroutes électroniques : usages, droit et promesses*, Cowansville, Éditions Yvon Blais Inc., 1995, http://www.droit.umontreal.ca/crdp/fr/equipes/technologie/conferences/ae/benyekhlef.html

BENYEKHLEF, K., « L'Internet : un reflet de la concurrence des souverainetés », dans *Réglementer les inforoutes (Actes du colloque d'octobre 1996)*.

BENYEKHLEF, K., « Réflexions sur le droit de la protection des données personnelles à la lumière des propositions de la Commissions des Communautés européennes », (1992) 2 *M.C.L.R.* 149

BENYEKHLEF, K. et P. TRUDEL, « Approches et stratégies pour améliorer la protection de la vie privée dans le contexte des inforoutes », *Mémoire présenté à la Commission de la culture de l'Assemblée nationale dans le cadre de son mandat sur l'étude du Rapport quinquennal de la Commission d'accès à l'information*, Centre de recherche en droit public, Faculté de droit - Université de Montréal, septembre 1997.

BICKNELL, C., « Database Marketing on the Web », *Wired*, 7 octobre 1999, http://www.wired.com/news/news/business/story/15456.html

BITOUN, G., « De la protection de la vie privée : Des cookies indigestes », 23 avril 1997, http://www.grolier.fr/cyberlexnet/COM/A970423.html

BLACKBURN, A., L. FEAN et G. WANG, « Description of the eTRUST Model » dans *Privacy and Self-Regulation in the Information Age, Chapter 5: Technology and Privacy Policy*, National Telecommunications and Information Administration, Juin 1997, http://www.ntia.doc.gov/reports/privacy/selfreg5.htm#5D

BLOOMBERG NEWS, « Survey : Personal data flows for freebies », 14 juillet 1999, http://www.news.com/News/Item/0,4,39156,00.html?pfv.

BRANSCOMB, A.W., « Anonymity, Autonomy and Accountability : Challenge to the First Amendment in Cyberspaces », (1995) 104 *Yale L.J.* 1639, p. 1655.

BUEL, S., « Virtual Post-it notes for the Web », 28 mai 1999, *San Jose Mercury News*, http://www.sjmercury.com/business/top/059363.htm

BURNS, P., « The law and Privacy : the Canadian Experience », (1976) 54 *Can. Bar Rev.* 1

CAMPBELL, A. J., « Self-Regulation and the Media », *Fed. Comm. L.J.*, Volume 51, Numéro 3 (Mai 1999), http://www.law.indiana.edu/fclj/pubs/v51/no3/v51no3.html

CAPRIOLI, E.A., « Sécurité technique et cryptologie dans le commerce électronique en droit français », *Lex Electronica*, Volume 3, Numéro 1 (hiver 1997), http://www.lex-electronica.org/articles/v3-1/caprio.html.

CAVOUKIAN, A., « Preserving privacy on the information highway : Fact or fiction? », *Free spech and privacy in the information age presented at a special symposium at the University of Waterloo*, 26 novembre 1994, gopher://insight.mcmaster.ca/00/org/efc/doc/sfsp/cavoukian.html

CLAUSING, J., « Gain for Online Industry on Privacy Issue », 13 juillet 1999, *New York Times*, http://forums.nytimes.com/library/tech/99/07/cyber/articles/13ptivacy.html

CLAUSING, J., « FTC Asked To Examine Data Profiling Practices », *New York Times*, 9 novembre 1999, http:///www.nytimes.com/library/tech/99/11/cyber/capital/09capital.html.

CLAUSING, J., « New Bill keeps online privacy at center stage », 17 avril 1999, *New York Times*, http://search.nytimes.com/search/daily/bin/fastweb?getdoc+site+site+73193+13+wAAA+TRUSTe

CLAUSING, J., « U.S. and Europe Reach Tentative Pact on Personal Data », 23 février 2000, *New York Times*, http://www.nytimes.com/library/tech/yr/mo/cyber/articles/24privacy.html.

COLLETT, S. et J. DASH, « Internet advertiser to develop standard for exchanging customer profiles », *Online News*, 15 novembre 1999, http://www.computerw...m/home/news.nsf/all/9911151privacy

COMEAU, P-A., « La vie privée : droit et culture » dans *Le respect de la vie privée dans l'entreprise : de l'affirmation à l'exercice d'un droit*, Les journées Maximilien-Caron 1995, Montréal, Éditions Thémis, 1995, p.3

COMMISSAIRE À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Le dépistage génétique et la vie privée,* ministre des Approvisionnements et Services Canada, Ottawa, Ontario, 1992, p2.

COMMISSION EUROPÉENNE, « Protection des données: la Commission approuve l'arrangement relatif au « port sûr » avec les Etats-Unis », 5 juin 2000, http://europa.eu.int/comm/internal_market/fr/media/dataprot/news/harbor4.htm

COMMISSION NATIONALE DE L'INFORMATION ET DES LIBERTÉS, *Protection des données personnelles et e-commerce en France*, Avril 2000, http://www.cnil.fr/thematic/them01.htm#100sites

COMMISSION NATIONALE DE L'INFORMATION ET DES LIBERTÉS, *Informatique et libertés dans le monde*, 1999, http://www.cnil.fr/thematic/tdoss3.htm

CONSEIL CANADIEN DES NORMES, « L'Industrie, contre ou avec les consommateurs? », *Consensus*, Janvier-février 1999, http://www.scc.ca/consensu/1999/jan_feb/consumers2601f.html

CONSEIL CANADIEN DES NORMES, *Normalisation – Une stratégie du Canada pour favoriser la compétitivité et promouvoir les intérêts sociétaux*, 31 août 1998, http://www.scc.ca/pressrel/1998/aug31-f.html

CONSEIL CANADIEN DES NORMES, *Perspective mondiale 2000 – Le Conseil canadien des normes lance la Stratégie canadienne de normalisation en présence du ministre de l'Industrie et de chefs d'entreprise*, 29 mars 2000, http://www.scc.ca/pressrel/2000/mar29_f.html

CONSEIL CANADIEN DES NORMES, « Réflexion sur la protection de la vie privée : Le Canada s'interroge sur le besoin d'élaboration d'une norme ISO internationale sur la protection des renseignements personnels », *Revue canadienne d'actualités de normalisation*, Volume 24, numéro 5 (Septembre 1997), http://www.scc.ca/consensu/1997/sept/ponder2405f.html

CONSEIL CANADIEN DES NORMES, « Un chemin tout tracé », *Revue canadienne d'actualités de normalisation*, Volume 24, Numéro 5 (Septembre 1997), http://www.scc.ca/consensu/1997/sept/ponder2405f.html

CRÉPEAU, C., « La Cryptographie : pour que les secrets le restent », *Québec - Science*, 8 juin 1997, http://www.cybersciences.com/cyber/4.0/dec_jan98/net.htm.

CULNAN, M. J. *A Methodology to Assess the Implementation of the Elements of Effective Self- Regulation for Protection of Privacy*, Discussion Draft - 6/17/98, http://www.georgetown.edu/culnan/privacy/ntia~1.htm.

DEANE, J., « What you think about ID chips », *ZDNet*, http://www.zdnet.com/zdnn/stories/news/0,4586,2190801,00.html

DENIS, E. E., « Internal Examination: Self-Regulation and the American Media » 13 *Cardozo Arts & Ent. L.J.* 697 (1995)

DENNING, D.E. et H.S. LIN (dir.), *Rights and Responsibilities of participants in Networked Communities*, Washington, National Academy Press, 1994.

DETWEILER, L., « Identity, Privacy, And Anonymity on the Internet », http://www.csis.ohio-state.edu/hypertext/faq/usenet/net-privacy/part1/faq.html

DIERKS, M.L., « Computer Network Abuse », (1993) 6 *Harvard Journal of Law and Technology* 307.

DOBEUS, V. J., « Rating Internet Content and the Spectre of Government Regulation », 16 *J. Marshall J. Computer & Info L.* 625 (1998)

DORAY, R., « La protection de la vie privée et des renseignements personnels », dans *Service de la formation permanente, Barreau du Québec, Développements récents en droit administratif (1995)*, Cowansville, Éditions Yvon Blais Inc. 1995, 111.

DORAY, R., « Mise à jour, mise au point et mise en garde au sujet de la protection des renseignements personnels dans le secteur privé », dans *Développements récents en droit administratif (1998), Service de la formation permanente, Barreau du Québec*, Montréal, Éditions Yvon Blais Inc., 1998, 135.

DORNEY, M., « Privacy in the Internet », (1996-97) 46 *Hastings Communications and Entertainment Law Journal (comm/ent)* 635.

DYSON, E., « Labeling Practices for Privacy Protection », dans *Privacy and Self-Regulation in the Information Age, Chapter 5: Technology and Privacy Policy*, National Telecommunications and Information Administration, Juin 1997, http://www.ntia.doc.gov/reports/privacy/selfreg5.htm#5C

ELECTONIC COMMERCE TASK FORCE, *International Safe Harbor Privacy Principles - DRAFT*, 19 avril 1999, http://www.ita.doc.gov/ecom/shprin.html

ELECTONIC COMMERCE TASK FORCE, *Joint Report on Data Protection Dialogue to the EU/US Summit*, 21 juin 1999, http://www.ita.doc.gov/ecom/jointreport2617.htm

EUROPEAN COMMISSION, *Data protection: significant progress made at February 21/22 talks on facilitating EU/US data transfers*, 24 février 2000, http://europa.eu.int/comm/dg15/en/media/dataprot/news/talks.htm

EUROPEAN COMMISSION, *First Orientations on Transfers of Personal Data to Third Countries : Possible Ways Forward in Assessing Adequacy*, 26 juin 1997, http://zeus.bna.com/e-law/docs/eudata1.html

FARASSE, F-A., « Votre vie privée dans le cyberespace, quelle protection avez-vous ? », Hiver 1999 *Dire*, p.26.

FAIRLEY RANEY, R., « Judge Rejects Online Critic's Efforts to Remain Anonymous », *New York Times*, 15 juin 1999. http://www.nytimes.com/library/tech/99/06/cyber/articles/15identity.html.

FEDERAL TRADE COMMISSION, *Privacy Online: Fair Information Practices in the Electronic Marketplace: A Federal Trade Commission Report to Congress*, 22 mai 2000, http://www.ftc.gov/os/2000/05/index.htm#22

FESTA, P., « Deja News to terminate email trail », 4 mai 1999, *CNET*, http://www.news.com/News/Item/0,4,36104,00.html

FESTA, P., « Macromedia patching Shockwave privacy hole », March 11, 1999, *CNET*, http://www.news.com/News/Item/0,4,33648,00.html.

FLYNN, L.J., « Group to monitor web sites for respect of consumer privacy », 16 juillet 1996, *New York Times*, http://search.nytimes.com/search/daily/bin/fastweb?getdoc+site+site+15027+0+wAAA+laurie%7Eflynn%7Erespect%7Econsumer%7Eprivacy

FRIEDMAN, M., « Canada Aligns with EU on Privacy », 20 avril 1999, *Wired*, http://wired.com/news/print_version/politics/story/19210.html?wnpg=all

FRIEDMAN, M., « Canadian Privacy Law Dying », 11 juin 1999, *Wired*, http://wired.com/news/print_version/politics/story/20175.html?wnpg=all

FROOMKIN, M., « Anonymity and Its Enmities », (1995) *J. Online L.*, art2, http://warthog.cc.wm.edu/law/publications/jol/froomkin.html

FROOMKIN, M., « Flood control on the information ocean : Living with anonymity, digital cash, and distributed databases », (1996) 15 *U. of Pitt. J. of L. & C.* 395, http://www.law.miami.edu/~froomkin/articles/ocean.html

FROOMKIN, M., « The Internet As A Source Of Regulatory Arbitrage », 1996, http://www.law.miami.edu/~froomkin/articles/arbitr.htm#xtocid158346.

FEDERAL TRADE COMMISSION, *Privacy Online: Fair Information Practices in the Electronic Marketplace: A Federal Trade Commission Report to Congress*, 22 mai 2000, http://www.ftc.gov/os/2000/05/index.htm#22

GAGNON, C., *Les «cookies» démystifiés*, 23 mars 1999, http://www.tactika.com/cookie/.

GELSI, S., « DoubleClick buying Abacus Direct », *CBC Market Watch*, 14 juin 1999, http://cbs.marketwatch.com/archive/19990614/news/current/dclk.htx?source=blq/yhoo&dist=yhoo

GEORGETOWN INTERNET PRIVACY POLICY STUDY, *Georgetown Internet Privacy Policy Survey*, 21 juin 1999, http://www.msb.edu/faculty/culnanm/gippshome.html

GINDIN, S.E., « As The Cyber-World Turns : The European Union's Data Protection Directive and Transborder Flows of Personal Data », Décembre 1997, *Internet Legal Practice Newsletter*, http://www.collegehill.com/ilp-news/gindin1.html

GINDIN, S.E., « Lost and found in cyberspace : Information privacy in the age of the Internet », 1997 *San Diego L.R.*, http://www.info-law.com/lost.html

GIROUX, A., « La protection en Europe : Effets outre-frontière d'une nouvelle directive sur la vie privée », *J. du B.*, Volume 29, Numéro 20, http://www.barreau.qc.ca/journal/vol29,no20/protectioneurope.htm

GIROUX, A., « La vie privée est-elle protégée : Québec un chef de file dans le domaine », *J. du B.*, Volume 29, Numéro 20, http://www.www.barreau.qc.ca/journal/vol29/no20/viepriveeprotegee.html

GLAVE, J., « Federal Site Yanks TRUSTe Seal », 25 juin 1999, *Wired*, http://www.wired.com/news/news/politics/story/20419.html

GLAVE, J., « Safe Harbor : No Port in a Storm? », 28 avril 1999, *Wired*, http://www.wired.com/news/print_version/politics/story/19389.html?wnpg=all

GLENN, H.P., « Le droit au respect de la vie privée », (1979) 39 *R. du B.* 879.

GLENN, H.P., « Le droit en l'an 2000 : L'envahissement des contrôles gouvernementaux et des technologies nouvelles dans la vie privée des citoyens », (1987) 18 *R.G.D.* 705.

GOIDICH, K. A.,« The Role of Voluntary safety standards in product liability litigation : Evidence or cause in Fact? », [1982] 49 *Insurance Counsel Journal* 320, p. 321.

GRAFMEYER, M., « La standardisation », 9 octobre 1995, http://www.fdbd.fr/~mitch/idees/standardiser.html

GREENLEAF, G., «The European Privacy Directive - completed » (1995) 2 *PLPR* 81, http://www.austlii.edu.au/au/other/plpr/vol2/Vol2No05/v02n05a.htm

GUERNSEY, L., « Web surfers' fears prompt privacy seals », 29 avril 1999, *New York Times*, http://search.nytimes.com/search/daily/bin/fastweb?getdoc+site+site+73169+0+wAAA+guernsey%7Eweb%7Esurfers%7Eprivacy

GUERRIER, P.,« Un grand site marchand sur deux n'est pas déclaré à la CNIL », 17 avril 2000, *Le Journal du Net*, http://www.journaldunet.com/0004/000417cnil.shtml

HARDY, T.,« The Proper Legal Regime for « Cyberspace » », (1994) 55 *U. of Pitt. L.R.* 993, 1016.

HARRIS, L. et A.F. WESTIN, « Privacy of Consumer Transaction Records in Future Home Interactive Services : What the Public Says - What the Public Wants (Reports from and Commentaires on a National Survey of Consumers, Interactive Services, and Privacy) », *présenté dans le cadre du Fifth Conference on Computer, Freedom and Privacy*, Conférence organisée par le Board of Trustees de l'Université Leland Stanford, juin-juillet 1994, http://www.techlaw.stanford.edu/CFP95.Program.html

HARNOIS, I., « La protection constitutionnelle et quasi constitutionnelle du droit au respect de la vie privée et les banques de données informatisées », dans *Service de la formation permanente, Barreau du Québec, Congrès annuel du Barreau du Québec (1997)*, 1997, p.667.

HERMANS, B., « Intelligent Software Agents on the Internet: An Inventory of Currently Offered Functionality in the Information Society and a Prediction of (Near) Future Developments », *First Monday*, http://www.firstmonday.dk/issues/issue2_3/ch_123/

HOFFMAN, L. J. et K. A. METIVIER CARREIRO, « Computer Technology to Balance Accountability and Anonymity in Self-regulatory Privacy Regimes » dans *Privacy and Self-Regulation in the Information Age, Chapter 5: Technology and Privacy Policy*, National Telecommunications and Information Administration, Juin 1997, http://www.ntia.doc.gov/reports/privacy/selfreg5.htm#5A

INFORMATION AND PRIVACY COMMISSIONER / ONTARIO, *Intelligent Software Agents: Turning a Privacy Threat into a Privacy Protector*, Avril 1999, http://www.ipc.on.ca/WEB_SITE.ENG/MATTERS/SUM_PAP/PAPERS/isat.htm

INTEL, « Intel Pentium III Processor », http://developer.intel.com/design/pentiumiii/details.html

INTEL, « Numéro de série des processeurs Intel », http://www.intel.fr/français/pentiumiii/utillity.html

INTERNATIONAL SAFE HARBOR PRIVACY PRINCIPLES, http://www.ita.doc.gov/ecom/shprin.html

IRVING, L., « Introduction » dans *Privacy and Self-Regulation in the Information Age*, National Telecommunications and Information Administration, Juin 1997,

JOHNSON, D. R. et D. POST, « Law and Borders – the Rise of Law in Cyberspace », 48 *Stan L. Rev.*, 1367, 1370-76 (1996).

JOHNSTON, M., « Take Net privacy into your own », *CNN*, http://cnn.com.

KAHNEY, L., « RealNetworks Probe Begins », 1 novembre 1999, *Wired*, http://www.wired.com/news/print/0,1294,32250,00.html.

KAPLAN, C.S, « Lawsuit Says Web Cookies Allow Illegal Stalking », 18 février 2000, *New York Times – Cyber Law Journal*, http://www.nytimes.com/library/tech/00/02/cyber/cyberlaw/18law.html.

KLEINER, K., « Digital graffiti », 29 mai 1999, *New Scientist*, http://www.newscientist.com/cgi-bin/pageserver.cgi?/ns/19990529/newsstory5.html

KRASOVEC, J., « Cyberspace : The final frontier, for regulation ? », Volume 31, Numéro 1 (1997-1998), *Akron Law Review*, http://www.uakron.edu/lawrev/krasovec.html

KRATCHANOV, D.C., « Protection de la vie privée dans le secteur privé », *Annexe M dans le Compte-rendu de la réunion de 1995 de la Conférence pour l'harmonisation de lois au Canada*, 1995, http://www.law.ualberta.ca/alri/ulc/95pro/f95m.htm

KRISTOL,. D. et L. MONTULLI, *HTTP State Management Mechanism*, Février 1997, http://www.cis.ohio-state.edu/htbin/rfc/rfc2109.html

LAPERRIÈRE, R., « La protection des renseignements personnels dans le secteur privé et la loi québécoise de 1993 », dans R. CÔTÉ et R. LAPERRIÈRE (dir.), *Vie privée sur surveillance : la protection des renseignements personnels en droit québécois et comparé*, Cowansville, Éditions Yvon Blais Inc., 1994, p.55.

LAPERRIÈRE, R., « L'émergence de normes dans le domaine des communications de renseignements personnels » dans *Entre droit et technique : enjeux normatifs et sociaux* sous la direction de René Côté et Guy Rocher, Éditions Thémis, Montréal, 1994, p.167.

LAPLANTE, L., « L'Internet et l'emploi », dans *Congrès annuel du Barreau du Québec (1997), Service de la formation permanente, Barreau du Québec*, Cowansville, Éditions Yvon Blais, 1997, p.711.

LEMOS, R., « Intel to electronically ID chips », 21 janvier 1999, *ZDNet*, http://www.zdnet.com/zdnn/stories/news/0,4586,2189721,00.html

LEMOS, R., « Intel : We won't track ID chips », 21 janvier 1999, *ZDNet*, http://www.zdnet.com/zdnn/stories/news/0,4586,2191233,00.html

LESSIG, L., « Coding privacy », 21 mai 1999, *The Industry Standard*, http://www.thestandard.com/articles/display/0,1449,4620,00.html?01.

LINDON, R., « La protection de la vie privée : champ d'application », (1971) *J.T.* 713,

LONG, G.P., « Who Are You ? : Identity and Anonymity in Cyberspace », (1994) 55 *U. of Pitt. L.R.* 1210.

MACAVINTA, C., « Data Privacy Activists Decry FTC recommendation », 13 juillet 1999, *CNET*, http://www.news.com/News/Item/Textonly/0,25,39021,00.html

MACAVINTA, C., « DoubleClik, Abacus merge in $1.7 billion deal », *CNET*, 24 novembre 1999, http://news.cnet.com/news/0-1005-202-1463444.html

MACAVINTA, C., « Is no privacy the price of personalization? », 10 mars 1999, *CNET*, http://www.news.com/News/Item/0,4,33560,00.html

MACAVINTA,C., « RealNetworks changes privacy policy under scrutiny », 1 novembre 1999, *CNET*, http://news.cnet.com/news/0-1005-202-1426044.html

MARKOFF, J., « Microsoft enters debate over online privacy by buying firefly », 10 avril 1998, *New York Times*, http://search.nytimes.com/search/daily/bin/fastweb?getdoc+site+site+68672+4+wAAA+p3p

MARKOFF, J., « U.S. and Europe clash over Internet consumer privacy », 1 juillet 1998, *New York Times*, http://search.nytimes.com/search/daily/bin/fastweb?getdoc+site+site+69277+2+wAAA+p3p

MARSHALL, G., « The Right to Privacy : A Sceptical View », (1975) 21 *McGill L. J.* 242.

MASTERSON, M., « Privacy fuels gov't efforts », 9 Mars 2000, *CNN – The financial network*, http://cnnfn.com/2000/03/09/technology/q_legislation/

MAYER-SCOENBERGER, V., « The Internet and privacy legislation : Cookies for a treat ? », Volume 1, Numéro. 1, *W. Va. J. L. & Tech.*, http://www.wvjolt.wvu.edu/wvjolt/current/issue1/articles/mayer/mayer.htm

MCCULLAGH, D., « U.S. , E.U. Approach Safe Harbor », 9 mai 2000, *Wired*, http://www.wired.com/news/politics/0,1283,36235,00.html

MCCULLAGH, D., « Miffed Judge Subpoenas AOL », *Wired*, 9 avril 1999, http://www.wired.com/news/news/politics/story/19044.html

MCCULLAGH, D., « Safe Harbor Swimming in Circles », 29 avril 1999, *Wired*, http://www.wired.com/news/print_version/politics/story/19414.html?wnpg=all.

MCDONALD, G., « Third Voice : Invisible Web Graffiti », *PC World*, 18 mai 1999, http://www.pcworld.com/pcwtoday/article/0,1510,11016,00.html

MELL, P., « Seeking shade in a land of perpetual sunlight : privacy as property in the electronic wilderness », Volume 11, Numéro 1, (spring 1996), *Berkeley Technology Law Journal*, http://www.law.berkeley.edu/journals/btlj/articles/11-1/mell.html

METCALFE, B., « TRUSTe uses consents and disclosures to protect privacy on the Internet », 10 novembre 1997, *Info World*, http://www.infoworld.com/cgi-bin/displayNews.pl?/metcalfe/971110bm.html

MICHAEL, D. C., « Federal Agency Use of Audited Self-Regulation as a Regulatory Technique », *Admin. L. Rev* 171, 181-82 (1995).

MIASTKOWSKI, S., « Hushmail Offers E-Mail Encryption », *PC World*, 28 mai 1999,

MILLER, L. et E. WEISE, « FTC studies Web site profiling », *USA Today*, 23 novembre 1999, http://www.usatoday.com/life/cyber/tech/review/crg570.htm

MILLER, K.L., « Good webkeeping seals of Approval », 17 mai 1998, *New York Times*, http://search.nytimes.com/search/daily/bin/fastweb?getdoc+site+site+68908+9+wAAA+TRUSTe

MILLER, L. et Elizabeth WEISE, « Keeping 'pry' out of the privacy debate », *USA Today*, 31 mars 1999, http://www.usatoday.com/life/cyber/tech/cte755.htm.

MOLINARI, P.A. et P. TRUDEL, « Le droit au respect de l'honneur, de la réputation et de la vie privée : aspects généraux et applications », dans *Service de la formation permanente, Barreau du Québec, Application des Chartes des droits et libertés en matière civile*, Cowansville, Éditions Yvon Blais Inc. 1988, p. 197.

MULLIGAN, D. K. et J. GOLDMAN, « The Limits and the Necessity of Self-Regulation: The Case for Both » dans *Privacy and Self-Regulation in the Information Age, Chapter 1: Theory of Markets and Privacy*, National Telecommunications and Information Administration, Juin 1997, http://www.ntia.doc.gov/reports/privacy/selfreg1.htm#1G.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY, *FIPS Publication 46-1 : Data Encryption Standard*, 22 janvier 1988.

NESSON, C., et D. MARGLIN, « The day the Internet met the first amendment : Time and the communications decency act », 10 *Harvard Journal of Law and Technology* 113 (fall 1996).

NISSEN, M., « Intelligent Agents: A Technology and Business Application Analysis », 30 novembre 1995, http://www.ai.univie.ac.at/~paolo/lva/vu-sa/html/heilmann/

OAKES, C., « A European's Net View of US », 30 août 1999, *Wired*, http://www.wired.com/news/politics/0,1283,21476,00.html

OAKES, C., « Marketers Adopt Privacy Rules », 7 juillet 1999, *Wired*, http://www.wired.com/news/news/politics/story/20604.html

OAKES, C., « Mouse Pointer Records Clicks », *Wired*, 30 novembre 1999, http://wired.lycos.com/news/print/0,1294,32788,00.html.

OAKES, C., « Tackling E-Privacy in New York », 3 juin 1999, *Wired*, http://www.wired.com/news/print_version/politics/story/19991.html?wnpg-=all.

OAKES, C. et James GLAVE, « The Web Privacy Seal, Take 2 », 17 mars 1999, *Wired*, http://www.wired.com/news/print_version/politics/story/18517.html?wnpg=all.

OHLSON, K., « Better Business Bureau joins online privacy fray », 17 mars 1999, *Computer World*, http://www.omputerworld.com/home/news.nsf/all/9903173bbb.htm

OLSON, K., « Better Business Bureau joins online privacy fray », 17 mars 1999, *Computer World*, http://www.omputerworld.com/home/news.nsf/all/9903173bbb.htm

OUIMET, A., « Vers un régime universel de protection des renseignements personnels dans le secteur privé » dans *Service de la formation permanente, Barreau du Québec, Développements récents en droit de l'accès à l'information (1991)*, Cowansville, Éditions Yvon Blais Inc. 1991, p.183.

PARENT, D., « La reconnaissance et les limites du droit à la vie privée en droit québécois », dans *Développements récents en droit administratif (1994), Service de la formation permanente, Barreau du Québec*, Cowansville, Éditions Yvon Blais Inc., 1994, p. 219.

PATSURIS, P., « Talking back on the web », 21 mai 1999, *Forbes e-business*, http://www.forbes.com/tool/html/99/may/0521/featb.htm

PC EXPERT, « Les promesses du Pentium III », 12 mars 1999, http://www.zdnet.fr/prod/syst/proc/a0007225.html

PERRIT, JR., H.R., « Regulatory Models for Protection Privacy in the Internet », dans *Privacy and Self-Regulation in the Information Age, Chapter 3: Models For Self-regulation*, National Telecommunications and Information Administration, Juin 1997,

PETERSEN, S.B., « Your Life as an Open Book : Has Technology Rendered Personal Privacy Virtually Obsolete ? », Volume 48, Numéro 1, *Federal Communications Law Journal*, http://www.law.indiana.edu/fclj/pubs/v48/no1/petersen.html

PISANI, F., « Tremblez, journalistes », *Le Monde interactif*, 19 mai 1999, http://www.lemonde.fr/nvtechno/branche/sticker.html

POST, D.,« Anarchy, State and the Internet : An Essay on Law-Making in Cyberspace » (1995) *J, Online L.* art. 3, http://warthog.cc.wm.edu/law/publications/jol/post.html

POST, D., « Thoughts on Anonymity, Pseudonymity and Limited Liability in Cyberspace », présenté à la conférence des 3 et 4 novembre 1996 à la faculté de droit de l'Université de Chicago. http://www-law.lib.uchicago.edu/forum/96vol.html

PRADEL, J., « L'information personnelle : entre le commerce et les libertés », dans *Le droit de la communicatique, Acte du colloque conjoint des Facultés de droit de l'Université de Poitiers et de l'Université de Montréal*, Montréal, Éditions Thémis, 1992, p.61.

RAFTER, M., « Trust or Bust? », 6 mars 2000, *The Standard*, http://www.thestandard.com/article/display/0,1151,12445,00.html

RANKIN, M., « Privacy & Technology : A Canadian Perspective », [1984] 22 *Alberta L.R.* 323, p. 325.

RAYSMAN, R. et P. BROWN, « Privacy on the Internet », 12 mai 1998, *New York Law Journal*, http://www.ljx.com/securitynet/articles/0512privacy.html

REAGLE, J. et L.F. CRANOR, « The Platform for Privacy Preferences », *P3P Note Draft 31 july 1998*, W3C, Cambridge, Massachusetts, http://www.w3.org/TR/1998/NOTE-P3P-CACM-19980731

REGAN, T., « Cyberspace graffiti may be sticking to your site », 20 mai 1999, *The Christian Science Monitor - Electronic edition*, http://www.csmonitor.com/durable/1999/05/20/fp14s1-csm.shtml

REIDENBERG, J., « Privacy in the Information Economy : A Fortress or Frontier for Individual Rights » (1992) 44 *Fed. Comm. L.J.* 195.

REIDENBERG, J., « Restoring Americans' Privacy in Electronic Commerce », *Berkeley Technology Law Journal*, Volume 14-2, http://www.law.berkeley.edu/journals/btlj/articles/14_2/Reidenberg/html/reader.html.

REIDENBERG, J., « Setting Standards for Fair Information Pratice in the U.S. Private Sector », 80, *Iowa Law Review* 497 (1995).

REIDENBERG, J., « The use of technology to assure Internet privacy : Adapting labels and filters for Data protection », Volume 3, Numéro. 2, *Lex Electronica*, http://www.lex-electronica.org/reidenbe.html

REIDENBERG, J. et F. GAMET-POL, « The Fundamental Role of Privacy and Confidence in the Network », (1995) 30 *Wake Forest L. R.* 105, 109.

REIDENBERG, J., et P. SCHWARTZ, *Online Services and Data Protection Law: Regulatory Responses*, EUR-OP: 1998, http://europa.eu.int/comm/internal_market/en/media/dataprot/studies/regul.pdf

RICHARD, R. « Le Rôle des Agents Intelligents », 18 juin 1998, *Planète Commerce*, http://www.planete-commerce.com/agents98/.

RINALDO, M.J., « Caller ID and Fair Credit Reporting : Technology and Traditional Notions of Privacy Clash (includes Draft Amendments to the Fair Credit Reporting Act) (Reflections from the House & Senate) », (juillet 1992) 16 *Seton Hall Legislative Journal* 403-453

ROBERTS, D., « On the Plurality of Ratings », 15 *Cardozo Arts & Ent. L.J.* 105 (1997).

RODGER, W., « Deja News privacy snafu uncovered », 29 avril 1999, ZDNet, http://www.zdnet.com/zdnn/s...ews/0,4586,2249764,00.html?chkpt=hpqs01.html

RODGER, W., « Deja News to stop tracking addresses », 4 mai 1999, *ZDNet*, http://www.zdnet.com/zdnn/stories/news/0,4586,2252593,00.html.

ROY, P. « La loi sur la protection des renseignements personnels dans le secteur privé, un acte de foi dans les vertus de l'autoréglementation », dans R. CÔTÉ et R. LAPERRIÈRE (dir.), *Vie privée sur surveillance : la protection des renseignements personnels en droit québécois et comparé*, Cowansville, Éditions Yvon Blais Inc., 1994, p.55.

RUCCIUTI, M., « Microsoft admits privacy problem, plans fix », 7 mars 1999, *CNET*, http://www.news.com/News/Item/0,4,334413,00.html

SCHNEIER, B., « Du tatouage du Pentium III », 25 mars 1999, *ZDNet*, http://www.zdnet.fr/actu/mate/proc/a0005395.html.

SCOBLIONKOV, D., « Back Off, Big Brother », 22 juillet 1999, *Wired*, http://www.wired.com/news/news/politics/story/13910.html

SÉDALLIAN, V., « Les problèmes posés par la législation française en matière de chiffrement », octobre 1998, http://62.161.196.163/lij/cryptoTC.html, à paraître dans la revue *Droit de l'Informatique et des télécommunications*.

SEGAL, G.R., « The Threat From Within : Cable Television and the Invasion of Privacy », (1986) 7 *Computer L.J.* 89, 91

SEMINERIO, M., « Groups take EU privacy fight public », 28 avril 1999, *ZDNet*, http://www.zdnet.com/zdnn/storie/news/0,4586,2248878,00.html.

SEMINERIO, M., « AOL, Disney oppose privacy plan, companies balks to U.S.-European Union privacy compromise »,16 mars 1999, *ZDNet*, http://www.zdnet.com/xdnn/stories/news/0,4586,2226769,00.html

SHAFFER, G., « The Power of EU Collective Action: The Impact of EU Data Privacy Regulation on US Business Practice », *European Law Journal*, Volume 5:4, http://www.iue.it/LAW/ELJ/archives/1999/1999_volume_4d3.htm

SHAPIRO, A. L., « Privacy for Sale : Peddling Data on the Internet », juin 1997, *The Nation*.

SMED, S., « Intelligent Software Agents and Agency Law », V14 1998 *Santa Clara Computer & High.* 503.

SPRINGER, K.A., « In god we trust ; All others who enter in this store are subject to surveillance », Volume 48, Numéro 1, *Fed. Comm. L.J.*, http://www.law.indiana.edu/fclj/pubs/v48/no1/springer.html

STAIMAN, A., « Shielding Internet Users from Undesirable Content : The advantage of a PICS Based Rating System », 20 *Fordham Int'l L.J.* 866 (1997).

STEPANEK, M., « Getting Doctors and Lawyers to Pay HushMail », Business Week Online, 10 août 1999, http://www.businessweek.com/cgi-bin/ebiz/ebiz_frame.pl?url=/ebiz/9908/ec0810.htm,

STERN, M., « Mobile Agents : Providing Control to the Consumer », *présenté dans le cadre du Fifth Conference on Computer, Freedom and Privacy*, Conférence organisée par le Board of Trustees de l'Université Leland Stanford, juin-juillet 1994, http//www.techlaw.stanford.edu/CFP95.Program.html

SULLIVAN, J., « Your Data on the Black Market », 12 janvier 1999, *Wired*, http://www.wirednews.com/print_version/email/explode-infobeat/story/17297.html?wnpg=all

SWIRE, P.P., « Markets, Self-Regulation, and government enforcement in the protection of personal information », http://www.acs.ohio-state.edu/units/law/swire1/psntia6.html

SWIRE, P.P., « Of Elephants, Mice, and Privacy : International Choice of Law and the Internet », *Draft submitted to International Lawyer*, 23 août 1998, http://www.acs.-ohio-state.edu/units/law/swire1/elephants.htm

TEDESCHI, B., « Targeted Marketing Confronts Privacy Concerns », 10 mai 1999, *New York Times - E Commerce Report*, http://search.nytimes.com/search/daily/bin/fastweb?getdoc+site+site+78182+0+wAAA+tedeschi%7Etargeted%7Emarketing%7Econfronts

TERRY, A. B., « Following the rules can increase your personal security », Juin 1999, *Online Banking*, http://www.onlinebanking.com

THOMAS, L.L.,« U.S. Telecommunications Privacy policy and Caller ID », (Automne 1993) 30 *California Western Law Review* 1-60.

THOMPSON, S.M., « The digital explosion comes with a cost : The loss of privacy », 4 *Journal of Technology Law and Policy* (spring 1999), http://www.journal.law.ufl.edu/~techlaw/4/Thompson.html

THOREL, J., « L'Europe et les États-Unis en désaccord sur les données nominatives », 10 décembre 1999, *ZDNet*, http://www.zdnet.fr/actu/inte/a0011939.html.

THOREL, J., « Le tatouage du Pentium III n'a pas résisté aux critique », *ZDNet*, 23 novembre 1999, http://zdnet.fr/actu/soci/demo/a0011652.html

TRUDEL, P. (avec la collaboration de R. GÉRIN-LAJOIE), « La protection des droits et valeurs dans la gestions des réseaux ouverts », dans Daniel POULIN, Pierre TRUDEL et Ejan MACKAAY (dir.), *Les autoroutes électroniques : usages, droit et promesses*, Cowansville, Éditions Yvon Blais Inc. 1995, http://www.droit.umontreal.ca/crdp/fr/equipes/technologie/conferences/ae/trudelgerinlajoie.html

TRUDEL, P., « Les effets juridiques de l'autoréglementation », (1989) 19 *R.D.U.S.* 247, 251.

TRUDEL, P., « Le rôle de la loi, de la déontologie et des décisions judiciaires dans l'articulation du droit à la vie privée et de la liberté de presse », dans *Droits irréconciliables*, *Droit du public à l'information et vie privée : deux droits irréconciliables ?*, Montréal, Éditions Thémis, 1992, p. 195.

UNITED STATES – DEPARTMENT OF COMMERCE, *Commerce Secretary William M. Daley – Hails EU approval of Safe Harbor Privacy Arrangement*, 31 mai 2000, http://www.ita.doc.gov/media/safeharbor531.htm

VACHER, G., « Deja News opte pour la confidentialité », 6 mai 1999, *ZDNet*, http://www.zdnet.fe/cgi-bin/a_actu.zd&ID=9176&Rub=2&Dat.html

VARNEY, C., « You Call This Self-Regulation? », 21 juillet 1999, *Wired*, http://www.wired.com/news/print_version/politics/story/12823.html?wnpg=all

VENNE, M., « Alan F. Westin : Le pape de la vie privée », 8 juillet 1996, *Le Devoir*, http://www.ledevoir.com/REDaction/SOCiete/SOC_priv210597/SOC_priv080796.htm.

WALLACE, C., « De la protection des renseignements personnels à l'évaluation publique des systèmes d'information : *sine qua non* de la démocratie à l'ère informatique », dans CÔTÉ, R. et R. LAPERRIÈRE (dir.), *Vie privée sur surveillance : la protection des renseignements personnels en droit québécois et comparé*, Cowansville, Éditions Yvon Blais Inc., 1994.

WALTON, T.J., *Internet Privacy Law*, 20 décembre 1998, http://www.netatty.com/privacy/privacy.html#5

WARREN et BRANDEIS, « The Right to Privacy », (1890) 4 *Harvard L.R.* 193.

WASHBURN, P., « Electronic Journalism, Computers and Privacy » (1982) 3 *Computer L.J.* 189

WEINBERG, J., « Hardware-Based ID, Rights Management, and Trusted Systems », *Wayne State University, W3C - Privacy Activity Statement*, 1999, http://www.w3.org/Privacy/Activity.html

WEINBERG, J., « Rating the Net », (1997) 19 *Hastings Comm/ent Law Journal* 453, http://www.msen.com/~weinberg/rating.html

WEISE, E., « Net privacy standards rolled out for federal hearings », 4 juin 1997, *New Yorks Times*, http://search.nytimes.com/search/daily/bin/fastweb?getdoc+site+site+16499+1+wAAA+weise%7Enet%7Eprivacy

WESTIN, A., « The U.S. and the EU Directive », http://www.privacyexchange.org/iss/confpro/aicgsberlin.html.

TABLE DE JURISPRUDENCE

ANNEXE 1

Les 10 principes de protection des renseignements personnels selon l'Association canadienne de normalisation[571].

1. **Responsabilité** : Un organisme est responsable des renseignements personnels dont il a la gestion et doit désigner une ou des personnes qui devront s'assurer du respect des principes énoncés ci-dessous.

2. **Détermination des fins de la collecte des renseignements** : Les fins pour lesquelles des renseignements personnels sont recueillis doivent être déterminées par l'organisme avant ou au moment de la collecte.

3. **Consentement** : Toute personne doit être informée et consentir à toute collecte, utilisation ou communication de renseignements personnels qui la concernent, à moins qu'il ne soit pas approprié de le faire.

4. **Limitation de la collecte** : L'organisme ne peut recueillir que les renseignements personnels nécessaires aux fins déterminées, et doit procéder de façon honnête et licite.

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 finalités déterminées.

6. **Exactitude** : Les renseignements personnels doivent être aussi exacts, complets et à jour que l'exigent les fins pour lesquelles ils sont utilisés.

7. **Mesures de sécurité** : Les renseignements personnels doivent être protégés au moyen de mesures de sécurité correspondant à leur degré de sensibilité.

---

[571] CANADIAN STANDARDS ASSOCIATION, Guide d'utilisation du Code CSA sur la protection des renseignements personnels, Service aux consommateurs de la CSA, Mars 1997 et INDUSTRIE CANADA - BUREAU DE LA CONSOMMATION, Bulletin trimestriel sur la consommation, Mars 1998, Volume 4, Numéro 1, http://strategis.ic.gc.ca/SSGF/ca01128f.html.

8. **Transparence** : Un organisme doit mettre à la disposition de toute personne des renseignements précis sur ses politiques et ses pratiques concernant la gestion des renseignements personnels.

9. **Accès aux renseignements personnels** : Un organisme 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 du fait qu'ils ont été communiqués à des tiers, et lui permettre de les consulter. Il sera aussi possible de contester l'exactitude et l'état complet des renseignements et y faire apporter les corrections appropriées.

10. **Possibilité de porter plainte contre le 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 individus responsables de les faire respecter au sein de l'organisme concerné.

ANNEXE 2

DRAFT[572]

SAFE HARBOR PRIVACY PRINCIPLES ISSUED BY THE
U.S. DEPARTMENT OF COMMERCE

The European Union's comprehensive privacy legislation, the Directive on Data Protection (the Directive), became effective on October 25, 1998. It requires that transfers of personal data take place only to non-EU countries that provide an "adequate" level of privacy protection. While the United States and the European Union share the goal of enhancing privacy protection for their citizens, the United States takes a different approach to privacy from that taken by the European Community. The United States uses a sectoral approach that relies on a mix of legislation, regulation, and self regulation. Given those differences, many U.S. organizations have expressed uncertainty about the impact of the EU-required "adequacy standard" on personal data transfers from the European Community to the United States.

To diminish this uncertainty and provide a more predictable framework for such data transfers, the Department of Commerce is issuing this document and Frequently Asked Questions (the Principles) under its statutory authority to foster, promote, and develop international commerce. The Principles were developed in consultation with industry and the general public to facilitate trade and commerce between the United States and European Union. They are intended for use solely by U.S. organizations receiving personal data from the European Union for the purpose of qualifying for the safe harbor and the presumption of "adequacy" it creates. Because the Principles were solely designed to serve this specific purpose, their adoption for other purposes may be inappropriate. The Principles ~~are not~~ cannot be used as a substitute for ~~the~~ national provisions implementing the Directive ~~in situations where those national provisions~~that apply to the processing of personal data in the Member States.

Decisions by organizations to qualify for the safe harbor are entirely voluntary, and organizations may qualify for the safe harbor in different ways. Organizations that decide to adhere to the Principles must comply with the Principles in order to obtain and retain the benefits of the safe harbor and publicly declare that they do so. For example, if an

---

[572] U.S. DEPARTMENT OF COMMERCE, *Draft – Safe Harbor Privacy Principles issued by the U.S. Department of Commerce*, 9 juin 2000, http://www.ita.doc.gov/td/ecom/USPrinciplesJune2000.htm

organization joins a self regulatory privacy program that adheres to the Principles, it qualifies for the safe harbor.

Organizations may also qualify by developing their own self regulatory privacy policies provided that they conform with the Principles. Where in complying with the Principles, an organization relies in whole or in part on self regulation, its failure to comply with such self regulation must also be actionable under Section 5 of the Federal Trade Commission Act prohibiting unfair and deceptive acts or another law or regulation prohibiting such acts. ~~Organizations~~ *(See annex 1 for the list of U.S. statutory bodies recognized by the EU.)* In addition, organizations subject to a statutory, regulatory, administrative or other body of law (or of rules) that effectively protects personal privacy may ~~assure~~also qualify for safe harbor benefits ~~by self-certifying to the Department of Commerce (or its designee)~~. In all instances, safe harbor benefits are assured from the date on which each organization wishing to qualify for the safe harbor ~~self-certifies~~self-certifies to the Department of Commerce (or its designee) its adherence to the Principles in accordance with the guidance set forth in the Frequently Asked Question on Self Certification.

Adherence to these Principles may be limited: (a) to the extent necessary to meet national security, public interest, or law enforcement requirements ; (b) by statute, government regulation, or case law that create conflicting obligations or explicit authorizations, provided that, in exercising any such authorization, an organization can demonstrate that its non-compliance with the Principles is limited to the extent necessary to meet the overriding legitimate interests furthered by such authorization ; or (c) if the effect of the Directive or Member State law is to allow exceptions or derogations, provided such exceptions or derogations are applied in comparable contexts. Consistent with the goal of enhancing privacy protection, organizations should strive to implement these Principles fully and transparently~~.~~, including indicating in their privacy policies where exceptions to the Principles permitted by (b) above will apply on a regular basis. For the same reason, where the option is allowable under the Principles and/or U.S. law, organizations are expected to opt for the higher protection under U.S. law where possible.

Organizations may wish for practical or other reasons to apply the Principles to all their data processing operations, but they are only obligated to apply them to data transferred

after they enter the safe harbor. To qualify for the safe harbor, organizations are not obligated to apply these Principles to personal information in manually processed filing systems. Organizations wishing to benefit from the safe harbor for receiving ~~such~~ information in manually processed filing systems from the EU must apply the Principles to any such information transferred after they enter the safe harbor.

An organization that wishes to extend safe harbor benefits to human resources personal information transferred from the EU for use in the context of an employment relationship must indicate this when it self-certifies to the Department of Commerce (or its designee) and conform to the requirements set forth in the Frequently Asked Question on Self Certification.Organizations will also be able to provide the safeguards necessary under Article 26 of the Directive if they include the Principles in written agreements with parties transferring data from the EU for the substantive privacy provisions, once the other provisions for such model contracts are authorized by the Commission and the Member States.

U.S. law will apply to questions of interpretation and compliance with the Safe Harbor Principles (including the Frequently Asked Questions) and relevant privacy policies by safe harbor organizations, except where organizations have committed to cooperate with European Data Protection Authorities. Unless otherwise stated, all provisions of the Safe Harbor Principles and Frequently Asked Questions apply where they are relevant.

"Personal data" and "personal information" are data about an identified or identifiable individual that are within the scope of the Directive, received by a U.S. organization from the European Union, and recorded in any form.

Notice : An organization must inform individuals about the purposes for which it collects and uses information about them, how to contact the organization with any inquiries or complaints, the types of third parties to which it discloses the information, and the choices and means the organization offers individuals for limiting its use and disclosure. This notice must be provided in clear and conspicuous language when individuals are first asked to provide personal information to the organization or as soon thereafter as is practicable, but in any event before the organization uses such information for a purpose other than that for which it was originally collected or processed by the transferring organization or discloses it for the first time to a third party(1).

Choice : An organization must offer individuals the opportunity to choose (opt out) whether ~~and how~~ their personal information is (a) to be disclosed to ~~third parties where disclosure is for a purpose other than the purpose for which it was originally collected or subsequently authorized by the individual,~~ a third party[573] or (b) to be used ~~where such use is~~ for a purpose that is incompatible with the purpose(s) for which it was originally collected or subsequently authorized by the individual. Individuals must be provided with clear and conspicuous, readily available, and affordable mechanisms to exercise choice.

For sensitive information (i.e. personal information specifying medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or information specifying the sex life of the individual), they must be given affirmative or explicit (opt in) choice if the information is to be disclosed to a third party or used for a purpose other than those for which it was originally collected or subsequently authorized by the individual through the exercise of opt in choice. In any case, an organization should treat as sensitive any information received from a third party where the third party treats and identifies it as sensitive.

Onward Transfer : ~~An organization may only~~To disclose ~~personal~~ information to a third ~~parties consistent with~~ party, organizations must apply the ~~principles of~~ notice and choice Principles. Where an ~~organization has not provided choice and the~~ organization wishes to transfer ~~the data~~information to a third party that is acting as an agent, as described in the endnote, it may do so if it first either ascertains that the third party subscribes to the Principles or is subject to the Directive or another adequacy finding or enters into a written agreement with such third party requiring that the third party provide at least the same level of privacy protection as is required by the relevant Principles. If the organization complies with these requirements, it shall not be held responsible (unless the organization agrees otherwise) when a third party to which it transfers such information processes it in a way contrary to any restrictions or representations, unless the organization knew or should have known the third party would process it in such a contrary way and the organization has not taken reasonable steps to prevent or stop such processing.

---

[573] It is not necessary to provide notice or choice when disclosure is made to a third party that is acting as an agent to perform task(s) on behalf of and under the instructions of the organization. The onward transfer principle, on the other hand, does apply to such disclosures.

Security : Organizations creating, maintaining, using or disseminating personal information must take reasonable precautions to protect it from loss, misuse and unauthorized access, disclosure, alteration and destruction.

Data integrity : Consistent with the Principles, personal information must be relevant for the purposes for which it is to be used. An organization may not process personal information in a way that is incompatible with the purposes for which it has been collected or subsequently authorized by the individual. To the extent necessary for those purposes, an organization should take reasonable steps to ensure that data is reliable for its intended use, accurate, complete, and current.

Access : Individuals must have access to personal information about them that an organization holds and be able to correct, amend, or delete that information where it is inaccurate, except where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy in the case in question, or where the rights of persons other than the individual would be violated.

Enforcement : Effective privacy protection must include mechanisms for assuring compliance with the Principles, recourse for individuals to whom the data relate affected by non-compliance with the Principles, and consequences for the organization when the Principles are not followed. At a minimum, such mechanisms must include (a) readily available and affordable independent recourse mechanisms by which each individual's complaints and disputes are investigated and resolved by reference to the Principles and damages awarded where the applicable law or private sector initiatives so provide ; (b) follow up procedures for verifying that the attestations and assertions businesses make about their privacy practices are true and that privacy practices have been implemented as presented ; and (c) obligations to remedy problems arising out of failure to comply with the Principles by organizations announcing their adherence to them and consequences for such organizations. Sanctions must be sufficiently rigorous to ensure compliance by organizations.