UNIVERSITÉ DE MONTRÉAL

La protection de la vie privée sur le Web avec P3P : l'arrimage incertain du technique et du juridique.

Présenté par :
Bertrand Salvas

Faculté de droit

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

Décembre 2001

Liste des abréviations utilisées

a) Juridiques

CcQ	Code civil du Québec
D.L.R.	Dominion Law Reports
L.C.J.	Lower Canada Jurist
LPRP	Loi sur la protection des renseignements personnels
R.C.S.	Recueil des arrêts de la Cour suprême du Canada

b) Autres

AOL	America Online
CDT	Center for Democracy and Technology
CERN	Organisation Européenne pour la Recherche Nucléaire
CSA	Canadian Standards Association
DARPA	U.S. Defense Advanced Research Project Agency
EPIC	Electronic privacy information center
FTC	Federal Trade Commission
HTML	Hypertext markup language
HTTP	Hypertext transfer protocol
OPS	Open Profiling Standard
P3P	Platform for Privacy Preferences
PICS	Platform for Internet Content Selection
URI	Uniform Ressource Identifier
W3C	World Wide Web Consortium
XML	Extended markup language

***

À Louis-Nicolas, né avec ce projet de recherche,
pour qui Internet est déjà aussi banal que
la télévision l'aura été pour son père.

Un monde gagné pour la technique est perdu pour la liberté.
Georges Bernanos
« La France contre les robots », 1944

TABLE DES MATIÈRES

***

Introduction

Depuis la nuit des temps, l'humain a toujours vécu en société. Tout d'abord simplement pour survivre dans un environnement hostile, et ensuite pour se développer et se dépasser. C'est en groupe qu'il a chassé des bêtes plus puissantes que lui, en groupe qu'il a bâti pyramides, temples et cathédrales, en groupe qu'il a construit des fusées pour toucher les étoiles. Malgré tout, l'humain préfère encore mener certaines parties de sa vie loin du regard de la société qui l'abrite et le fait vivre. L'industrialisation des grandes villes avait permis de rêver d'un meilleur anonymat et d'oublier la promiscuité des sociétés rurales traditionnelles. Les nouveaux médias du 20^{e} siècle devaient briser ce rêve en accordant à la masse le pouvoir de focaliser à tout moment toute son attention sur un de ses membres, donnant naissance à des mouvements voués à la protection de la vie privée. Les premiers balbutiements de la société informatique, en décuplant les possibilités de cueillette et de partage de l'information, aura tôt fait d'attirer l'attention des États sur la protection des renseignements recueillis sur les individus.

Issu des laboratoires de la guerre froide en tant qu'outil de travail pour militaires et scientifiques, Internet est entré grâce au Web dans le quotidien de centaines de millions de gens. L'engouement qu'il suscite aujourd'hui ne fait qu'exacerber les craintes sur le sort réservé aux renseignements personnels sur les grands réseaux. Les nouvelles technologies de l'information fournissent des moyens puissants et efficaces pour glaner et partager des informations sans que le sujet n'en ait nécessairement connaissance et, pis encore, pour les accumuler et les réutiliser. Le Web est efficace, le Web est ouvert, le Web est discret et le Web n'oublie jamais.

La multiplication des occasions d'interactions et de transactions entre commerçants et individus sur le réseau provoque une augmentation phénoménale de la quantité et de la qualité des informations recueillies. L'éclosion de compagnies vouées à la création de profils très précis et bien ciblés sur les cyber-consommateurs, rendus possibles par les prodigieuses capacités technologiques quand vient le temps de procéder à des croisement d'informations, a rapidement sonné l'alarme. Les craintes des usagers qui

ont résulté de ces pratiques ont diminué leur confiance dans le réseau, freiné l'essor du commerce électronique et invité les gouvernants à prendre position.

Différentes initiatives ont suivi, l'Europe adoptant sa *Directive Européenne en matière de protection des données à caractère personnel*[1], les États-Unis favorisant plutôt l'auto-réglementation du réseau par ses principaux acteurs techniques et économiques. Parallèlement à ces débats, plusieurs chercheurs en droit ont commencé à rechercher la meilleure façon de réglementer le réseau. La possibilité d'utiliser ses composantes techniques pour encadrer les activités qui y ont cours est souvent revenue à l'avant-scène. La table était mise pour l'arrivée d'un protocole technique comme P3P.

Nous tenterons dans cette étude d'évaluer les chances de ce projet de régler de façon satisfaisante la question de la protection de la vie privée et des renseignements personnels sur le Web. Pour ce faire, nous examinerons en premier lieu les conditions qui ont entouré sa naissance puis à une revue des principales normes juridiques régissant la question. Nous poserons par la suite un regard de juriste sur la rédaction des détails du protocole tel qu'il a été mis en vigueur pour finalement synthétiser les notions étudiées et tirer nos conclusions.

Quelques remarques s'imposent avant de commencer l'exposé des résultats de notre étude. Tout d'abord, pour simplifier la rédaction et la lecture de ce texte, nous prendrons pour acquis que les termes « *Internet* » et « *Web* » sont équivalents. En effet, bien que l'infrastructure technique qu'est le réseau Internet soit en place depuis la fin des années soixante, c'est l'apparition du Web et de son immense toile de sites dans les années quatre-vingt-dix qui en a fait un objet du quotidien. C'est à travers le Web que des millions d'individus ont connu Internet. Pour eux, qui sont à chaque jour appelés à y dévoiler un peu plus d'eux-mêmes, Web et Internet sont synonymes. La

[1] *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 caractère personnel et à la libre circulation de ces données.*
http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=fr&numdoc=31995L0046&model=guichett

distinction technique entre ces deux réalités n'emportant pas vraiment de conséquences pour nos fins, nous ferons comme eux en faisant comme si…

Ensuite, bien que le projet P3P ait subi de nombreuses transformations pendant la période où nous l'avons étudié, nous présumerons souvent qu'il sera un jour mis en vigueur intégralement. Cette approche nous permettra d'aborder avec plus de recul ses fonctions principales, leur impact sur le réseau et leurs chances de bien s'harmoniser à nos systèmes juridiques. Nous n'aborderons que vers la fin de notre analyse les étapes et le calendrier de mise en application prévus du protocole afin de nous aider à dégager certaines conclusions.

Abordons sans plus tarder la première partie de notre étude.

***

CHAPITRE 1 Contexte, origine, et but du projet de plate-forme P3P

1.1 Contextes

1.1.1 Contexte juridique du cyberespace

Internet suscite bien des débats depuis quelques années. L'accroissement spectaculaire du nombre de ses adeptes, la découverte qu'ils ont pu y faire d'un contexte de communication informel, et d'usages qui lui sont propres, ont projeté l'image d'un univers à part, en marge des États et de leurs lois. Plusieurs expressions vinrent consacrer cette perception : « *cyberculture », « cyberpunk », « netizens », « village virtuel »* et même, à la limite, « *cyberespace*». Ces mots ont pu donner l'impression qu'Internet était le début d'un temps nouveau, la découverte d'une nouvelle dimension transcendant et englobant une planète connue dans ses moindres recoins.

Mais le rêve a vite fait place à la réalité : le cyberespace n'est pas exempt de droit et s'il est parfois plus ardu de l'y faire appliquer, les lois existantes y produisent tout de même leurs effets, que cela plaise ou non. Ainsi, comme le concluait déjà une étude menée en 1996-97 :

> *«La nouveauté de la révolution Internet ainsi que le fait que des millions de participants utilisent Internet de nouvelles façons et ont recours à de nouvelles méthodes de communication sur une base quotidienne, voire horaire, rendent l'application des lois existantes difficile. Toutefois, les résultats de notre étude indiquent qu'à ce jour, et dans la plupart des cas, aucun problème manifeste n'a été relevé qui justifie une intervention à grande échelle du législateur.»*[2]

Une fois admis qu'il était possible d'imposer un cadre juridique sur le Web, s'est posé le défi de trouver la meilleure façon d'y parvenir. Comment en effet arriver, de façon pratique et efficace, à atteindre sur le Web les objectifs souhaités par un législateur donné, ou encore à s'assurer que les lois en vigueur y soient respectées?

[2] Michel RACICOT, Mark S. HAYES, Alec R. SZIBBO, Pierre TRUDEL, *L'espace cybernétique n'est pas une terre sans loi : étude des questions relatives à la responsabilité à l'égard du contenu sur Internet*, http://strategis.ic.gc.ca/pics/itf/1603118f.pdf

Répondre à ces interrogations impose une connaissance importante du Web, de son contexte et des habitudes de ses adeptes. Plusieurs auteurs se sont penchés sur cette question de la régulation d'Internet et ont suggéré différents types d'approches pour la solutionner. Tous concluent cependant à une réticence innée du réseau à une approche de gouvernance centralisée traditionnelle. Tout type de gouvernance devra ainsi tenir compte des éléments structurants du réseau. Selon David Post :

> *«Any discussion of rule-making in cyberspace therefore should begin by looking at the role of the entities and institutions defining the network protocols, because this level of organizational controller has what might be termed "competitive advantages" over other controllers in electronic network communities. »*[3]

De plus, la régulation d'une activité humaine ne peut provenir d'une seule source. Elle résulte presque invariablement des interactions et des luttes d'influence de plusieurs éléments de la société, qui sont autant de sources de droit. C'est l'idée principale avancée par le professeur Lawrence Lessig. Sur le Web, ce constat ne fait que s'amplifier. Ainsi, selon le professeur Trudel:

> « *La régulation, dans les environnements électroniques, est une activité soumise à la concurrence: aucune autorité ne peut prétendre exercer un monopole sur la fonction d'énonciation des règles de même que sur celle reliée à leur application*. »[4]

David Post va plus loin en déclarant que plusieurs jeux de normes pourraient voir le jour sur le Web, comme autant de résultantes distinctes des interactions particulières qui ont cours sur les réseaux qui le composent. Pour lui, chaque compétition entre les diverses sources de droit ne respecte pas nécessairement les mêmes règles et rapports de forces selon le milieu où elle a lieu. La compétition entre ces différents régimes réglementaires étant en dernière ligne arbitrée par les choix que font les usagers d'accepter les règles de l'un et de refuser celles de l'autre, créant à la longue un droit uniformisé pour le Web :

---

[3] David G. POST, *Anarchy, State, and the Internet: An Essay on Law-Making in Cyberspace (Article 3),* 1995, http://www.cli.org/DPost/X0023_ANARCHY.html {par. 21}

[4] Pierre TRUDEL et al, *Droit du cyberespace*, Montréal, Éditions Themis, 1997 p.3-11

> *« A kind of competition between individual networks to design and implement rule-sets compatible with the preferences of individual internetwork (sic) users will thus materialize in a new and largely unregulated, because largely unregulatable, market for rules. The outcome of the individual decisions within this market -the aggregated choices of individual users seeking particular network rule-sets most to their liking- will therefore, to a significant extent, determine the contours of the law of cyberspace. »*[5]

Pourquoi cette compétition entre règles de droit devrait-elle survenir sur le Web plus qu'ailleurs? Tout simplement en raison de ses caractéristiques fondamentales qui créent un contexte tout à fait original et différent de tout ce que nous connaissions auparavant. Passons en revue certaines de ces caractéristiques en utilisant la nomenclature adoptée dans l'ouvrage «*Droit du cyberespace*» au chapitre des rationalités.[6]

Première carte dans cette nouvelle donne, la ***numérisation*** qui rend possible la transmission de tout type de document et la réalisation de toutes sortes d'activités sur le Web, et ouvrant la porte à la convergence des médias et des techniques sur le réseau. Ethan Katsh a soutenu que tout format choisi pour les échanges d'information impose des règles et des contraintes qui lui sont propres. Le changement de format qu'impose le passage au numérique d'une civilisation habituée depuis des siècles à l'usage de l'imprimé, offre une relation différente à l'écrit et impose une révolution des façons de faire, notamment en matière de droit :

> *«In a variety of ways, our sense of place is different. This should not be surprising since the electronic media treats space and distance so differently from any previous medium of communication. [...] new technologies remove the constraints of time and speed. They blur boundaries of various kinds and, as a consequence, move various elements of the legal process into a different and, compared to print, less differentiated space.*[7]

Comme cristallisation manifeste de ce nouveau paradigme en droit québécois, nous pouvons citer la " *Loi concernant le cadre juridique des technologies de*

[5] David G. POST, *Anarchy, State, and the Internet: An Essay on Law-Making in Cyberspace (Article 3),* 1995, http://www.cli.org/DPost/X0023_ANARCHY.html, paragraphe 42, (extraits)
[6] Pierre TRUDEL et al, *Droit du cyberespace*, Montréal, Éditions Themis, 1997 chapitre 1
[7] Ethan KATSH, *Law in a digital world*, New York, Oxford university Press, 1995, p 238

l'information "[8], que nous désignerons Loi 161 d'après le numéro sous lequel elle fut déposée, qui constate la dissociation entre un document et le support sur lequel il est inscrit. La numérisation offre donc comme caractéristique fondamentale de pouvoir libérer juridiquement le document de son support, concept qui aurait été plutôt ardu à soutenir dans le contexte traditionnel. Elle permet également de faire converger plusieurs types de pièces, écrits ou fichiers sous ce vocable de " document ", même des banques de données :

> *3. Un document est constitué d'information portée par un support. L'information y est délimitée et structurée, de façon tangible ou logique selon le support qui la porte, et elle est intelligible sous forme de mots, de sons ou d'images. L'information peut être rendue au moyen de tout mode d'écriture, y compris d'un système de symboles transcriptibles sous l'une de ces formes ou en un autre système de symboles.*
>
> *Pour l'application de la présente loi, est assimilée au document toute banque de données dont les éléments structurants permettent la création de documents par la délimitation et la structuration de l'information qui y est inscrite.*[9]

En droit québécois donc, le fait qu'un document soit conservé sur papier ou sur support électronique seulement est donc désormais tout à fait inutile dans l'appréciation de sa valeur juridique.[10]

Deuxième élément, le caractère ***interactif*** du réseau qui sort les récepteurs de communications de leur passivité traditionnelle, avec toutes les conséquences juridiques que cela implique. Les constants renvois d'ascenseurs et «*feedbacks*» des internautes, la facilité avec laquelle ils peuvent naviguer d'un bout à l'autre du réseau par le simple jeu des liens hypertexte et d'y interagir à divers titres, changeant de rôle au passage pour devenir à loisir diffuseur ou récepteur selon les situations, contribuent à la nouveauté de la situation sur le Web. Ce nouveau contexte rend

[8] *Loi concernant le cadre juridique des technologies de l'information*, L.Q. 2001, c. 32
[9] Id., art.3
[10] *Loi concernant le cadre juridique des technologies de l'information*, L.Q. 2001, c. 32, articles 3 et suivants. Voir plus particulièrement l'article 5.

originales tant les relations qui s'y tissent, que les conséquences légales qui en découlent. Ainsi qu'on peut le lire dans l'affaire *ACLU c. Reno* :

> *55. Users of online systems are also content providers (that is, they are publishers), because they can transmit and distribute their own communications and can create a permanent archive of information accessible by other users. There is no limit to the number of people on either side of the sending or receiving end of computer communications.*
>
> *56. Online communications are interactive. This means, part, that users of online systems must seek out with the information they wish to retrieve and the kinds of communications they wish to engage in. It also means that users can easily respond to the material they receive or view online.*[11]

L'impact de l'interactivité du Web se fait largement sentir dans le domaine de l'échange d'information. La multiplication extrêmement rapide des fichiers et l'aisance avec laquelle ils peuvent circuler entraînent des bouleversements dans l'équilibre juridique réglé depuis des décennies par le droit de la propriété intellectuelle. L'exemple récent des systèmes de partage de fichiers, comme *Napster* et ses semblables dans le domaine musical, a démontré combien l'interactivité du Web peut venir bouleverser les façons de faire traditionnelles et les règles de droit qui les régissent.

Troisième élément, la ***décentralisation*** du Web, qui rend obsolètes frontières et juridictions traditionnelles. De tous temps, les relations entre les individus, et les contrats qui les consacrent, ne se sont pas arrêtées aux limites territoriales des états nationaux. La naissance de règles propres au commerce international, la *Lex Mercatoria* au Moyen-Âge, l'établissement de traités bilatéraux et plus récemment de commissions internationales, ont consacré la recherche d'une normalisation juridique globale. La conclusion de contrats entre des parties sujettes à des juridictions différentes et la recherche de la juridiction compétente n'est pas un phénomène inédit puisqu'il constitue, depuis des années, le sujet d'étude du droit international privé. Le Web ne fait que provoquer l'accroissement du nombre d'occasions dont dispose une personne (physique ou morale) de transiger en dehors de sa juridiction d'origine. Une autre nouveauté que nous apporte l'ouverture du Web est la plus grande complexité

de ces transactions. Elles comportent en effet dans le cyberespace de multiples parties ou intervenants qui ne se connaissent pas entre eux, et qui ignorent souvent leur localisation respective réelle. Les parties impliquées ignorent même parfois carrément l'existence ou le rôle de certains intervenants aux transactions, comme les autorités de certification ou les services d'hébergement, qui peuvent changer de juridiction en quelques mouvements de souris. Le caractère foncièrement ouvert du Web dévoile ainsi encore quelques-unes de ses nouveautés. Sur ce point, Post observe :

> *«Moving through the World Wide Web, for example, by following hypertext links from one Internet site to another, the user is almost completely indifferent (and, indeed, may have no way of knowing) whether the file he is viewing resides on a computer down the street or across the globe; similarly, whether control of the Cyberia listserver is exercised by a computer in Williamsburg, Virginia or Williams Corner, New South Wales, has almost no effect on the functional capabilities of that particular network or the ease with which any individual with Internet access can participate in the activities taking place on that network. [...]*
>
> *This independence from geographical constraints results from both the electronic nature of the message transmission, which largely decouples the physical distance between communicating machines from message travel times and, more significantly, from the decentralized design of the Internet. [...]»* [12]

Autre élément à ne pas négliger, la relative cohésion de certains quartiers de la communauté virtuelle. Car s'il est faux de prétendre à l'existence d'un véritable village virtuel qui serait indépendant et autonome par rapport aux territoires et États nationaux connus, il n'en demeure pas moins que certains mouvements d'opinions sur Internet ont eu, et continuent d'avoir une influence importante. Cette influence se manifeste principalement en réaction à certaines situations décriées par plusieurs groupes de pression. Nous citerons en exemple les levées de bouclier qui suivent régulièrement la découverte d'atteintes à la vie privée ou à la sécurité des communications sur le Web, par exemple à l'égard du circuit témoin de la puce

---

[11] *ACLU c. Reno*, http://www.aclu.org/court/renovacludec.html, § 55 et 56

[12] David G. POST, *Anarchy, State, and the Internet: An Essay on Law-Making in Cyberspace (Article 3),* 1995, http://www.cli.org/DPost/X0023_ANARCHY.html, par. 37 & 38, (extraits)

Pentium III[13], des pratiques douteuses de Microsoft lors de l'enregistrement des acheteurs de Windows 98[14] et du silence troublant de *TRUSTe*[15], des pratiques douteuses de sites comme *DejaNews* (maintenant repris par Google)[16], de la tentative de vente de listes d'informations nominatives par les liquidateurs de *Toysmart.com*[17], etc... S'il est assez fréquent dans le monde dit traditionnel, d'être témoin de pareilles réactions de masse, il demeure assez rare de voir des solutions concrètes être trouvées aussi rapidement de cette façon ailleurs que sur le Web.

Tous ces phénomènes contribuent à faire de l'auto-régulation le véhicule de choix retenu par plusieurs dans la recherche d'un certain contrôle sur les activités qui ont cours sur Internet. En effet, la régulation de toute activité humaine, sur Internet ou non, peut s'accomplir de différentes façons. L'adoption de normes étatiques appliquées de façon impérative et sanctionnées par le système judiciaire est probablement la plus connue. La mise en place de ces normes peut se faire de façon plus ou moins démocratique, leur justification sociale peut être variable et la sanction imposée en cas de défaut à leurs prescriptions peut également être rigoureuse ou pas. L'autorégulation quant à elle suggère plutôt de laisser aux intervenants concernés le soin d'élaborer les normes qui les gouverneront, soutenant que cette façon de faire encouragera leur acceptation, leur pertinence et donc, leur application effective.

Nous devons cependant constater que la décision de respecter ou non les normes, peu importe leur mode d'adoption, dépend en grande partie des individus et que leur choix repose principalement sur le risque encouru (sanction vs. bénéfice), les probabilités d'être pris en défaut, la justesse sociale ou la désuétude des normes en jeu.

Un récent courant doctrinal aborde la question sous un angle différent. Plutôt que de rechercher, comme les modes classiques de régulation le font, à imposer des règles

[13] Polly SPRENGER *Intel on Privacy: 'Whoops*!, WiredNews, http://www.wired.com/news/news/politics/story/17513.html
[14] EPICALERT, *Microsoft Tracks Users, But Watchdog is Mute*, Volume 6.05, March 25, 1999, http://www.epic.org/alert/EPIC_Alert_6.05.html , 4e article
[15] *Microsoft Statement of Finding*, Truste, Watchdog #1723, http://www.truste.org/news/padvisories/users_w1723.html
[16] http://groups.google.com/googlegroups/deja_announcement.html
[17] *FTC v. Toysmart.com*, (District of Massachusetts) (Civil Action No. 00-11341-RGS). Voir sur le Web: http://www.privacysecuritynetwork.com/library/display.cfm?catID=28&Level=3

qui entraîneront des sanctions pour ceux qui les violent, les tenants de ce mouvement doctrinal suggèrent plutôt d'encadrer le réseau en réglementant les éléments techniques qui le sous-tendent et en permettent l'existence. La *régulation par l'architecture*, comme il est convenu de l'appeler, joue ainsi sur un autre registre en utilisant l'imposition de contraintes techniques, difficilement évitables ou carrément incontournables, pour modeler le comportement des individus à la volonté de l'autorité qui les édicte.

Ce type de régulation, si on y pense bien, n'est pas nouveau. La suspension de structures métalliques sous les viaducs afin d'empêcher l'entrée de camions dans un tunnel, ou l'ajout de dos d'ânes dans les rues des quartiers résidentiels pour réduire la vitesse des véhicules en sont de bons exemples. Mais sur le Web il prend un sens nouveau car il peut s'y exprimer dans un environnement créé de toutes pièces par la technique, où les règles informatiques règnent en maître absolu. Leur utilisation à des fins régulatoires peut donc avoir sur le Web des effets tout à fait péremptoires. La capacité de l'individu de contourner une telle norme ou d'essayer de l'enfreindre délibérément se trouve alors réduite de façon importante ou même, dans certain cas, totalement éliminée.

Dans le contexte particulier du réseau, ce courant doctrinal s'avère très prometteur et semble particulièrement bien adapté à notre sujet d'étude, le *Platform for Privacy Preferences* (*P3P*). Il nous paraît donc tout à fait approprié d'examiner ici les travaux des premiers auteurs à avoir suggéré cette piste, à savoir Joel Reidenberg, Graham Greenleaf et, surtout, Lawrence Lessig.

Joel R. Reidenberg est l'un des principaux auteurs à s'être intéressé aux questions de régulation du cyberespace et l'un des premiers, bien qu'il n'utilise pas directement cette terminologie, à ouvrir la porte à l'utilisation de l'architecture technique à des fins normatives.

Déjà dans un article publié en 1996[18] , il offrait un panorama de la question de la régulation du cyberespace en s'attaquant au paradigme traditionnel de la souveraineté nationale. Il concluait à l'émergence d'un nouveau paradigme de gouvernance du réseau, en exposant son évolution et son incongruité avec les modes traditionnels de régulation. Pour Reidenberg, l'autorité régulatrice traditionnelle des États se fonde sur la proximité de communautés politiques, sociales et économiques. Le droit international, comme le droit constitutionnel, accordent en effet la légitimité aux gouvernements qui exercent la souveraineté sur un territoire physique et la population qui l'habite. L'absence de frontières dans le cyberespace constitue donc une atteinte à ce fondement de légitimité, limitant la souveraineté traditionnelle des États sur l'établissement des règles et des politiques qui y ont cours. Il expose ainsi la difficulté d'adaptation des modes traditionnels de régulation à la situation prévalant sur le Web, notamment à cause des caractéristiques fondamentales du réseau comme l'absence de frontières ou de territoires identifiés, ou encore de citoyens reconnus. Les institutions américaines, objet d'étude principal de Reidenberg, ne lui semblent pas être bien adaptées à la mouvance «physique» et technologique d'un réseau comme le Web.

Cette situation, sans entraîner la disparition des droits nationaux, mettra cependant de plus en plus en conflit des lois incompatibles ou discordantes en créant des situations nouvelles où elles pourront s'affronter. Reidenberg souligne du même souffle que la tentation pour les États de chercher à appliquer leurs lois à l'extérieur de leurs frontières s'en trouvera accrue.

Face à cette érosion du pouvoir des États sur le Web, Reidenberg constate l'émergence de nouvelles souverainetés exercées par les entités qui l'animent comme *AOL, Compuserve, Prodigy*, etc... Ces organismes exercent leur influence sur le réseau et le marché qui s'y déploie par un jeu d'ententes et de contrats. Mais encore, élément intéressant pour nos fins, l'auteur assimile les limites techniques qu'elles imposent à autant de frontières balisant le Web. Reidenberg cite en exemple les capacités qu'ont les protocoles de gérer l'usage et la diffusion d'informations

[18] Joel R. REIDENBERG, *Governing networks and rule-making in cyberspace*, 45 Emory Law Journal 911 (1996); sur le Web: http://www.law.emory.edu/ELJ/volumes/sum96/reiden.html

personnelles, comme l'acceptation systématique de l'enregistrement de témoins (« *cookies »)* sur l'ordinateur d'un internaute et la possibilité offerte aux opérateurs des sites d'y accéder. Reidenberg pointe également comme source de normativité les technologies de protection d'œuvres artistiques qui peuvent empêcher ou limiter leur reproduction.

Pour lui, la création de ces «frontières» techniques découle d'un processus complexe de gouvernance. Cette normalisation technique peut découler de contraintes purement commerciales, concept qui trouve son écho dans les travaux de Lessig que nous survolerons un peu plus loin, ou être adoptées par un organisme particulier, gouvernemental ou non. De telles contraintes peuvent aussi naître de façon tout à fait anodine, sans avoir fait l'objet de réflexion ou d'analyse préalable de leurs conséquences, ce qui n'enlève pourtant rien à leur efficacité. L'exemple de l'adoption des réglages systématiques des premiers navigateurs, justement en ce qui a trait aux témoins, est un exemple flagrant de cette possibilité. L'usage du témoin est ainsi accepté d'avance, souvent sans même que l'usager n'en ait connaissance ou ne soit au courant des conséquences potentielles, parce que l'entreprise qui crée le logiciel impose de facto ses propres choix.

En définitive pour Reidenberg, la solution ne se trouve pas dans un système de règles imposées par l'État car ce dernier ne doit se concevoir que comme l'un des multiples participants à l'évolution interactive du Web et des règles qui le régissent. La façon d'influencer et de gouverner le réseau doit plutôt tenir compte de sa structure. L'auteur propose donc sa vision d'une *Lex Informatica* qui, sans se substituer aux lois nationales, saura intégrer les rôles et attributions de chaque intervenant. Pour Reidenberg, cette *Lex Informatica* est constituée de l'ensemble des règles imposées par la technologie pour encadrer les flux d'informations. L'État, dans ce contexte, doit se contenter d'intervenir dans les seuls cas d'absolue nécessité et laisser les acteurs régler les détails des relations juridiques tissées sur le Web. Reidenberg considère d'ailleurs que l'État, pour augmenter ses chances de succès, devrait intervenir indirectement sur le réseau notamment en imposant son influence dans l'adoption de normes techniques :

> *The recognition of new network borders opens new instruments for the achievement of regulatory objectives. Executive and legislative fora lose a degree of relevance to technical standards organizations. Standards decisions affect fundamental public concerns and are no longer technical rules of purely commercial interest. Standards now contain significant policy rules. [...] Governments can and should seek standards that facilitate or incorporate broader policy objectives. Without a widening of the policy concerns inherent in technical standards, the results may be distorted. For instance, standards of electronic rights management for intellectual property may transgress policy goals for fair information practices if the technical decisions do not consider the privacy implications. The Canadian experience and growing government interest in technologies of privacy, including encryption, are beginning to force this broader consideration at standards bodies.*[19]

Lessig peut être considéré comme le principal défenseur des théories de régulation par l'architecture bien que, nous le verrons, il n'emploie pas lui-même ce terme. Il a présenté les résultats de ses travaux dans quelques articles comme « *The Law of the Horse: What Cyberlaw Might Teach* », « *Reading the Constitution in Cyberspace* » et plus récemment dans un ouvrage complet consacré au sujet : « *Code and other laws of cyberspace* »[20].

Spécialiste du droit constitutionnel américain et professeur à Stanford, il fonde ses théories sur son constat que l'encadrement de tout comportement humain est le fruit d'une compétition entre quatre types de contraintes : légales, sociales, économiques et naturelles. Pour lui, cette théorie s'applique également dans le cyberespace, la contrainte naturelle y étant cependant remplacée par ce qu'il appelle le " code ".

Lessig retrouve les contraintes *juridiques* aux activités ayant cours sur le Web dans les lois sur la propriété intellectuelle, la diffamation, ou l'obscénité. Leurs interventions se font a posteriori, pour sanctionner des comportements illégaux tout comme dans le monde dit «réel». Leur efficacité dans le cyberespace est de ce fait très variable à ses yeux quand on tient compte de la difficulté d'y imposer une

[19] Id.
[20] Lawrence LESSIG, *The Law of the Horse: What Cyberlaw Might Teach*, http://stlr.stanford.edu/STLR/Working_Papers/97_Lessig_1/article.htm ; Lawrence LESSIG, Reading *the Constitution in Cyberspace* (1997) 45 Emory L. J. 869-910 ; Lawrence LESSIG, Code *and other laws of cyberspace* ", NewYork, Basic Books, 1999.

sanction à un comportement illégal ou d'y faire exécuter un jugement, mais elles n'en demeurent pas moins possibles.

Les contraintes *sociales*, désignées par Lessig sous le vocable de «*norms*», ont pour rôle d'inviter à l'observance des lois en culpabilisant les individus qui négligent de les observer ou en leur faisant craindre le ridicule ou le déshonneur en les violant. Cette approche est particulièrement efficace lorsque les chances d'être sanctionné par les modes traditionnels sont minimes. Ce type de contrainte pourrait donc, par exemple, être plus efficace que tout corps policier pour empêcher un citoyen de brûler un feu rouge au beau milieu de la nuit. Les contraintes sociales s'incarnent sous différentes formes sur le Web, comme dans certains éléments de *netiquette* réglant le comportement à suivre dans l'utilisation du courrier électronique ou des groupes de discussion. Les sanctions y sont bien connues : «*flaming*», «*bozo list*», «*mail bomb*» viendront punir les intervenants qui sont trop bavards sur les groupes Usenet, ou qui les utilisent à des fins publicitaires.

Les contraintes de *marché* ont de plus en plus leur place sur Internet. Lessig le voit bien. L'imposition de tarifs ou d'abonnements pour contrôler l'accès à certains sites ou l'intégration de publicité par le biais des bandeaux publicitaires viennent d'abord à l'esprit du lecteur. L'accès à certaines informations sera donc contrôlé par des mécanismes de paiement ou par l'acceptation préalable d'une présence publicitaire dans l'espace virtuel visité. Cependant, et peut-être mieux encore, la façon dont un outil technique aux origines obscures comme le fichier témoin a pu être rapidement et efficacement récupéré pour fonder une industrie du renseignement personnel si florissante qu'elle force les États à réagir, témoigne de manière éloquente de l'importance des enjeux économiques dans l'évolution et la construction d'un Web de plus en plus commercial. Nous trouvons ici un écho à l'étude faite par Reidenberg sur les nouvelles souverainetés du Web que constituent des géants comme *Compuserve* ou *America Online* (*AOL)*. Il est intéressant de constater que les nouvelles souverainetés du Web prennent souvent la forme d'entreprises commerciales, mues exclusivement par des mobiles économiques.

Quant au *code*, nous avons vu que Lessig le voit comme l'équivalent cybernétique de la nature puisqu'il intervient dans la structure même du réseau et impose ses diktats de façon aussi péremptoire qu'incontournable. Il introduit ici la contrainte technique à son équation : "*nature*" et "*code*" étant pour lui des concepts équivalents, chacun dans son domaine, à la seule différence de leur plasticité, ou malléabilité. Le " code " serait ainsi plus susceptible d'être modifié ou influencé que la nature puisqu'il est une invention de l'homme. Sa dictature demeure toutefois aussi dominante sur le Web que celle de la nature l'est dans le monde réel. Son pouvoir apparaît même être encore plus grand lorsqu'on considère qu'il peut être modelé selon les désirs de l'homme. Contrairement à la nature, Lessig lui attribue donc un très grand facteur de plasticité. Mots de passe, enregistrement des agissements des individus, cryptographie, signatures électroniques, sont autant de moyens incontournables pour l'usager mais infiniment adaptables par les acteurs du réseau.

La présence et l'usage de ces techniques posent des conditions incontournables qui, si on les intègre à une structure juridique, peuvent être d'une efficacité redoutable. Lessig avance même que les contrats conclus dans un tel environnement technico-légal, pour encadrer l'accès à un site par exemple, peuvent carrément remplacer la Loi. Une fois les ententes conclues, leur exécution pourra se faire dans un cadre technique imposé qui découlera directement et automatiquement de leurs termes, sans possibilité d'y déroger. Les stipulations peuvent donc devenir quasi incontournables et emporter l'imposition de conséquences, sans que les parties impliquées ne puissent reculer ou invoquer les exceptions usuelles du droit pour les éviter. Dans ce contexte, selon Lessig, le code remplace la loi.

Un dernier auteur, Graham Greenleaf, résume et refond cette approche en en reprenant l'essence et en la re-baptisant «*regulation by architecture*».[21] Greenleaf présente ce concept dans un survol des différentes positions déjà formulées par d'autres auteurs qui abordent tous, à des degrés et dans des contextes divers, cet aspect particulier de gouvernance issu du Web.

[21] Graham GREENLEAF, *An endnote on regulating cyberspace: architecture vs Law*, http://www.austlii.edu.au/au/other/unswlj/thematic/1998/vol21no2/greenleaf.html

Greenleaf manifeste son désaccord avec les penseurs libertaires qui clament l'impossibilité de gouverner Internet par des législations nationales. Pour lui, l'impuissance des États à réglementer le Web est exagérée. En constatant un certain alignement des lois sur des standards internationaux émergeants, il conclut que les interventions concertées se multiplient. Il confirme ainsi l'affirmation de Reidenberg quant à la compétition entre les législations nationales provoquées par l'arrivée d'un médium global comme le Web.

La prémisse de Greenleaf est que l'architecture du réseau n'est pas un élément neutre, mais qu'elle intègre différents choix et valeurs qui reflètent les intérêts et les prises de positions de concepteurs qui la réinventent quotidiennement. Les processus très variés, parfois tout à fait arbitraires ou inconscients, entourant l'adoption et la mise en vigueur de tels choix techniques remettent cependant parfois leur légitimité en question. Greenleaf isole d'ailleurs les conséquences insoupçonnées de certaines technologies émergentes. Il observe par exemple que l'implantation d'un système de cryptographie à clé publique et l'utilisation grandissante de modes de certification par signatures électroniques, qui vise à permettre plus de confidentialité et de sécurité dans les échanges virtuels, pourraient paradoxalement fournir des procédés très efficaces d'identification des internautes. Toute médaille ayant un revers, nous pourrons constater plus tard que le projet P3P, objet principal de notre étude, comporte lui aussi un tel aspect imprévu et même contradictoire.

Greenleaf insiste plus particulièrement sur la vision de Lawrence Lessig qu'il adopte et cherche à compléter. Nous présenterons donc ses arguments sur la base des réponses aux principales propositions de Lessig.

Tout d'abord, Greenleaf ajoute à la pensée de Lessig quant à l'effet mitigé de la Loi comme source de régulation du Web. Pour Lessig, la sanction a posteriori des comportements, inhérent aux modes traditionnels d'intervention, limite leur portée sur le Web. Bien qu'il ne développe pas ce point de manière importante, Greenleaf entrevoit néanmoins que la Loi sera plus efficace sur le Web si elle cherche à influencer indirectement les trois autres types de contraintes (sociales, économiques,

techniques) que dans des tentatives d'interventions directes. Il abonde donc au fond dans le même sens que Lessig et Reidenberg : la Loi a peu d'effet direct sur le Web, mais elle conserve son effet de levier sur les autres sources d'influence.

Greenleaf souligne aussi que le cyberespace connaît des normes sociales qui, sans recevoir de sanction directe, sont néanmoins respectées à grande échelle. Il cite aussi en exemple les règles de la *netiquette*, et invoque Foucault[22] qui soutient que le respect d'une norme sociale par un individu varie habituellement selon les probabilités que d'autres soient témoins du comportement «déviant». Ainsi plus un individu croit qu'il a des chances d'être vu, plus il aura tendance à respecter une contrainte sociale, ce qui rejoint aussi la vision de Lessig.

Dans le même ordre d'idées, et en lien avec l'objet principal de notre étude, Greenleaf estime qu'aucune règle de droit positif ne sanctionnera le non-respect des politiques P3P que s'imposeront les sites. Seule la présence de certaines obligations *de facto* découlant du respect d'une telle contrainte sociale en milieu virtuel pourrait forcer au respect des politiques. Le succès de P3P ne reposerait-il que sur une telle obligation morale?

Le thème principal abordé par Greenleaf porte sur la notion de code proposée par Lessig, qu'il désigne quant à lui sous le vocable «*architecture*» et qu'il considère aussi comme étant en proportion beaucoup plus important dans le cyberespace que la «*nature*» peut l'être dans le monde réel. Il justifie son choix du mot «*architecture*» parce que le terme représente mieux la situation prévalant sur le Web, mais aussi parce qu'il désigne une notion plus large que le «code» proposé par Lessig. Pour lui, le terme «*architecture*» désigne plus que les logiciels, et il comprend toute composante technique requise au fonctionnement du Web :

- les composantes physiques des réseaux (ordinateurs, câbles, «*routers*», satellites...) ;

[22] Michel FOUCAULT, *Discipline and Punish: the Birth of the Prison*, Peregrine books 1977, cité par Greenleaf (voir note 21)

- les protocoles, actuels ou proposés (incluant PICS et P3P);

- la biologie humaine (comme composantes d'identification);

- les composantes physiques additionnelles (cartes à puces, puces «*clipper*», etc..).

Nous croyons personnellement aussi que le concept « d'architecture » élaboré par Greenleaf est mieux adapté au Web que le seul " code ", car il comporte l'avantage de mieux englober un réseau en perpétuelle re-définition.

Greenleaf s'attache par la suite à analyser les qualités de l'architecture comme type de contrainte à la régulation du cyberespace. Il la considère comme étant hautement malléable («*high plasticity*»), puisqu'au contraire de la nature elle résulte entièrement du génie humain. Il lui ajoute aussi la propriété de pouvoir être immédiate dans ses effets, car elle peut affecter ou encadrer un comportement *a priori*, à l'inverse de la Loi qui n'intervient généralement qu'*a posteriori* pour sanctionner une infraction.

Notons que sur ce point, Lessig conclut à une très grande, peut-être même trop grande, efficacité de la régulation technique. Le fait que les normes appliquées peuvent être adoptées par des organismes échappant à tout contrôle démocratique l'inquiète particulièrement :

> *As the Net grows, as its regulatory power increases, as its power as a source of values becomes established, the values of real-space sovereigns will at first lose out. In many cases, no doubt, that is a very good thing. But there is no reason to believe that it will be a good thing generally or indefinitely. There is nothing to guarantee that the regime of values constituted by code will be a liberal regime; and little reason to expect that an invisible hand of code writers will push it in that direction.*.[23]

Il n'en demeure pas moins que cette approche proposée par Lessig, avec les adaptations fournies par Greenleaf, nous fournit un cadre d'étude bien adapté à l'analyse de tout mode d'intervention utilisant la technologie comme vecteur. Les enjeux de l'implantation possible de P3P sur le Web tombent dans cette catégorie, et

ils fournissent un terrain d'étude idéal pour cette théorie. Décrivons tout d'abord ce qu'est ce projet P3P. Il nous sera par la suite plus facile d'expliquer en quoi il tombe dans cette catégorie des modes de régulation par l'architecture.

3.1.1 Contexte de la vie privée dans le cyberespace

Tout d'abord, pourquoi intervenir pour protéger la vie privée dans le cyberespace? De quelle façon y est-elle menacée? Le Web n'est au fond qu'un reflet du monde dans lequel nous vivons. Une session de navigation peut ressembler à une balade au centre-ville : on peut magasiner, trouver de l'information, faire du lèche-vitrines, y rencontrer des gens intéressants... On peut aussi y faire de mauvaises rencontres, se faire voler son porte-feuille, se faire suivre jusqu'à la maison... Sans trop s'alarmer et sans se priver du plaisir de sortir, il faut rester conscient des risques. Survolons brièvement ces principaux risques afin de comprendre ce à quoi les tenants du projet P3P ont voulu s'attaquer. Notre survol sera volontairement bref, puisque nous aurons l'occasion de revenir sur les particularités de ces situations tout au cours de notre exposé, à la faveur de l'étude des caractéristiques de P3P ou des lois en vigueur dans le domaine de la protection de la vie privée.

Un premier risque peux sembler tout à fait apparent, puisqu'il découle des activités de collecte active d'informations personnelles par les sites sur leurs visiteurs. Cette activité pourra se faire ouvertement, lors de la conclusion d'une transaction électronique par exemple. Le client est invité à fournir son nom, son adresse et ses coordonnées de paiement. Diverses « informations statiques », selon la nomenclature de P3P, peuvent être accumulées. On lui demande pour ce faire des informations additionnelles, ou optionnelles, comme son occupation, le domaine d'activité où il oeuvre, son niveau de revenus.

L'ordinateur du site visité peut aussi inscrire un témoin sur l'ordinateur du visiteur. Ce type de fichier texte s'y loge afin de l'identifier et de le reconnaître lors d'une prochaine visite. Le but de l'exercice peut être technique, statistique ou commercial. Il est technique lorsqu'il a simplement pour but de maintenir la communication avec

[23] Lawrence LESSIG, *The Law of the Horse: What Cyberlaw Might Teach*.

un usager donné à travers ses déplacements à l'intérieur du site. Il est statistique lorsqu'il a pour but de reconnaître un visiteur donné pour le calcul des données relatives au site, comme les parties les plus consultées, le parcours type d'un usager. Il est commercial lorsqu'il a pour but d'orienter les prochaines visites de l'usager vers une partie du site qu'il n'a pas encore visité, pour lui présenter des offres conformes aux intérêts déduits de ses visites précédentes ou pour diriger l'apparition des bannières insérées sur les pages qu'il consultera. Il importe de noter que le but initial ayant motivé la création des témoins était technique, puisqu'il aurait autrement été impossible d'identifier un usager au cours d'une session donnée sur un site en particulier. Le caractère « *stateless* » du Web fait en effet en sorte qu'il est impossible de reconnaître un usager donné entre les téléchargements successifs de pages qu'il demande sur un site en particulier. Sans un témoin il serait impossible, par exemple, de penser à un système de services bancaires en ligne ou encore à des services comme Amazon.com où un visiteur peut consulter les informations sur plusieurs ouvrages avant de passer à l'étape du paiement pour en acquérir seulement quelques-uns. Les autres usages qui en sont faits lui ont été trouvés par la suite.

Un second risque tient à la journalisation d'informations accumulées sur les internautes au cours de leur visite. Il a trait à l'accumulation « d'information dynamiques » dans les termes du projet P3P. La plupart des internautes ignorent toujours que de nombreuses informations sont instantanément recueillies sur eux, à leur insu, par tout site qu'ils visitent : l'adresse IP du fournisseur d'accès ou le sien le cas échéant, le système d'exploitation et le type de navigateur utilisé, les documents qu'il consulte, les fichiers qu'il télécharge, sont autant d'informations facilement obtenues. Certains sites conservent également les historiques de leurs navigations, la liste des questions qu'ils ont formulé sur des engins de recherche ou des achats qu'ils ont fait.[24]

Un troisième risque, le plus sérieux peut-être, découle du croisement des informations recueillies par différents sites sur un même internaute et de la création de profils

---

http://cyber.law.harvard.edu/works/lessig/finalhls.pdf , page 546.

extrêmement précis de son identité, de ses habitudes et parfois même de ses opinions. De tels croisements sont facilités par la présence de témoins qui permettent de reconnaître un internaute lors de ses déplacements sur la toile, d'accumuler les informations sur ses agissements, de constituer son profil et de vendre les informations à une banque de données spécialisée qui les consolidera les données accumulées par plusieurs sites en utilisant un identificateur commun comme l'adresse courriel.

La création de telles banques d'informations a consacré la valeur des informations recueillies et stimulé leur commerce ce qui induit un quatrième risque : le partage ou le commerce des informations recueillies sur les individus. L'affaire *Toysmart.com*[25] précitée illustre bien ce risque. Rappelons que les liquidateurs à la faillite de la compagnie opérant ce site de commerce électronique spécialisé dans la distribution de jouets, ont considéré la banque de données sur les clients comme un actif de la compagnie et ont tenté de la vendre. Ils contrevenaient ainsi à la politique de vie privée affichée sur le site de l'entreprise, et s'attiraient les foudres de la *Federal Trade Commission*. Un règlement ultérieur a finalement permis la destruction des données[26].

Ces risques d'intrusions dans la vie privée des internautes a donc été à l'origine de craintes chez les usagers du réseau et d'inquiétude chez leurs gouvernants. Le projet P3P allait suivre peu après, à titre de réponse technique à cette problématique. Voyons maintenant d'où il tire ses origines.

1.1.2 Contexte d'élaboration du projet P3P

P3P est l'acronyme de *Platform for Privacy Preferences*. Ce projet a été initié et est mené par le W3C, le *World Wide Web Consortium*, avec l'objectif de régir globalement les interactions sur le Web au niveau de la protection de la vie privée,

[24] Nous n'élaborerons pas trop ici sur les risques potentiels courus sur le réseau quant à la lecture de données enregistrées sur l'ordinateur de l'usager, puisqu'il s'agit plutôt de questions de sécurité.
[25] *FTC c. Toysmart.com*, (District of Massachusetts) (Civil Action No. 00-11341-RGS).
[26] Des liens vers le texte de la plainte et de l'entente sont disponibles à cette adresse : http://www.privacysecuritynetwork.com/library/display.cfm?catID=28&Level=3

plus particulièrement quant à la dissémination et à l'usage des renseignements personnels recueillis et accumulés sur les internautes. P3P vise donc à fournir au Web un cadre technique qui permettrait le respect de certains principes juridiques minimaux communs en matière de protection de la vie privée. Il constitue un exemple de tentative d'intégration de la règle de droit à l'architecture technique du réseau.

Le W3C a été fondé en octobre 1994 par un consortium international de centres de recherche et d'entreprises impliquées en technologies informatiques, sous le parrainage initial du CERN (*Laboratoire Européen pour la Physique des Particules*), lieu de naissance du Web[27]. Actuellement, le W3C compte plus de cinq cent (500) membres. [28] Le W3C, qui a débuté ses activités avec l'aide financière de la *Commission Européenne* et de la *DARPA (U.S. Defense Advanced Research Project Agency*), est désormais financé par ses membres. Sa crédibilité et ses moyens financiers ne semblent donc pas être mis en question. Il ne dispose d'aucun pouvoir réel pour imposer ses décisions, autre que son influence «morale», le poids économique de ses membres, et son rôle de centre de conservation et de discussion des standards techniques. Il ne faut pas non plus perdre de vue que tout regroupement de compagnies privées aux intérêts compétitifs divergents peut engendrer des luttes «politiques» au sein de l'organisme, dont la virulence peut nuire à la mise en œuvre des décisions et des projets adoptés.

L'objectif de départ du W3C était de permettre le développement du Web par le développement de protocoles communs qui alimenteraient sa croissance et assureraient la compatibilité des réseaux. Le premier moyen utilisé fût la création de dépôts d'informations techniques, notamment les protocoles du Web et la documentation qui s'y rattache. Ceci devait permettre à tous les entrepreneurs et chercheurs d'avoir accès à des données communes et à jour, ainsi qu'à encourager la création et le maintien des normes techniques. Par la suite, le W3C a entrepris de produire des logiciels, protocoles et références techniques pour distribution gratuite et

[27] Voir à ce sujet : http://www.cern.ch/Public/ACHIEVEMENTS/web_fr.html
[28] Voir la liste complète des membres sur le site du W3C, http://www.w3.org/Consortium/Member/List

d'encourager leur intégration dans les outils d'utilisation et de conception du Web, toujours aux mêmes fins de compatibilité et d'efficacité technique.

De façon plus concrète, le W3C est impliqué dans des projets comme le développement du langage HTML, du XML[29], ou encore certaines initiatives dans le domaine du commerce électronique, du paiement en ligne et de la signature électronique. Ses résultats les plus achevés dans le domaine technique ont sans doute été la finalisation de la norme HTML 4, les feuilles de style en cascade (*cascading Style Sheet, ou* CSS), et le langage XML. Avant P3P, le résultat le plus connu des travaux dans le domaine de la régulation technique du Web a été le projet d'étiquettage des contenus PICS (*Platform for Internet Content Selection*)[30].

Le projet P3P quant à lui, a été officiellement lancé par le W3C le 23 mai 1997 sous l'appellation initiale P3, acronyme bientôt remplacé par P3P.[31] Ce projet était l'héritier de deux projets antérieurs du W3C soit l'OPS (*Open Profiling Standard*) et le projet «*Web-privacy*».

L'OPS a été présenté sous le parrainage de Netscape en 1997. Il visait à assurer un échange sécuritaire de «profils» entre deux parties, ces profils étant définis comme étant l'ensemble des caractéristiques ou données concernant un usager ou un fournisseur de services sur le Web.[32] L'OPS visait également à fournir un cadre régissant le dévoilement préalable de l'usage projeté de ces informations par son récepteur. Selon ses concepteurs : « *This framework forms a basis for the further protection of privacy and usage through legal and social contracts and agreements as well as associated business processes*. »[33]

OPS se contentait de protéger et encadrer le seul processus de transmission des informations par l'usager et celui entourant la réception de la déclaration du site quant

[29] http://www.w3.org/MarkUp/Activity
[30] http://www.w3.org/PICS/
[31] Le choix de ce nouveau nom s'explique par la volonté du W3C de prévenir un litige potentiel de marque de commerce (voir à ce sujet: http://www.w3.org/P3P/Update.html)
[32] Proposal for an Open Profiling Standard. http://www.w3.org/TR/NOTE-OPS-FrameWork.html
[33] Proposal for an Open Profiling Standard. (abstract) http://www.w3.org/TR/NOTE-OPS-FrameWork.html

à l'usage prévu des données transmises. Il laissait ensuite la gestion de la relation entre les parties au contrat ou aux usages établis entre elles. Il lui aurait du coup été certainement plus difficile de régir globalement le domaine de la collecte et de l'usage des renseignements personnels.

Parallèlement à la présentation du projet OPS par Netscape, Microsoft présentait au W3C son propre projet dans le domaine de l'échange de renseignements personnels dans un document intitulé «*Privacy and Profiling on the Web*»[34]. L'objectif de ce projet, que nous désignerons sous le nom «*Web Privacy*», ignorait volontairement l'aspect légal ou social de la problématique pour se concentrer sur la recherche de solutions techniques aux problèmes pratiques liés à la gestion des informations personnelles. Ainsi la recherche d'un moyen d'éliminer l'obligation pour l'internaute de fournir des renseignements le concernant à de nombreuses reprises y est omniprésente. Cette situation était présentée comme un irritant pour les usagers et un frein à l'essor du commerce électronique. Le projet Microsoft cherchait donc à démontrer :

> *« [...] that it is possible to leverage existing Internet standards and proposals to provide sites access to demographic and other personal profile information while placing users in control of how this information is disclosed.»* [35] (nos soulignements)

Un aspect intéressant de ce projet «*Web Privacy*» consistait en la création dans l'ordinateur de chaque internaute d'un fichier contenant toutes les informations personnelles le concernant, et permettant leur transmission automatique subséquente sur son autorisation. Cette procédure cherchait à éviter à l'internaute la fastidieuse tâche de saisir ces informations à chaque fois qu'elles lui sont demandées, tout en lui réservant le privilège de les mettre à jour. Le projet prévoyait de plus la possibilité de permettre la conservation d'une copie de ces dépôts d'information dans une «banque de données corporative globale»? [36] Fallait-il y voir une manifestation des tendances

[34] "Privacy and Profiling on the Web. Submitted to W3C on 02 June 1997." http://www.w3.org/TR/NOTE-Web-privacy.html
[35] Id. , section 1
[36] " *This profile should be stored locally on the user's machine, but it may also be backed up remotely in a global corporate directory*." Privacy and Profiling on the Web. Submitted to W3C on 02 June 1997 http://www.w3.org/TR/NOTE-Web-privacy.html

«*Big Brother*» souvent attribuées à Microsoft? Nous laisserons ces conjectures à d'autres. Il n'en demeure pas moins que cet aspect du projet était peu rassurant. Il l'est encore moins depuis que nous avons été les impuissants témoins des cafouillages de cette compagnie dans le domaine de la sécurité des communications faites par le biais de son serveur «*Hotmail*».[37]

Le projet de Microsoft paraissait donc mettre l'accent sur la recherche d'un cadre apte à favoriser tant le «*one-click shopping*» pour l'usager que la collecte pré-autorisée d'informations sur les internautes. Il ne s'inscrivait pas dans une optique de protection du caractère confidentiel des informations et des volontés des usagers. Il y a lieu de se demander si le projet Microsoft ne cherchait pas simplement à apaiser les critiques qu'essuyait le Web en matière de confidentialité, en encadrant le tout d'une solution technique propre à maintenir l'accès pour les sites aux précieuses informations recueillies sur les internautes. Il ne fut pas retenu, alors nous ne le saurons probablement jamais. Mais il a fort probablement inspiré le service *Passport* lancé par Microsoft à l'automne 1999.[38] Notons au passage que ce service de Microsoft fait l'objet de nombreuses critiques quant à la sécurité entourant la conservation des informations qu'il entrepose[39], et qu'il a entraîné le dépôt d'une plainte[40] auprès de la *Federal Trade Commission* (FTC) par un groupe de défense de la vie privée des internautes (l'EPIC[41]). Microsoft ayant fait en sorte que les utilisateurs de son nouveau système d'exploitation Windows XP s'inscrivent de facto au service *Passport* lors de la mise à niveau de leur système, les forçant en quelque sorte à y transférer leurs données personnelles. La fermeture temporaire obligée de *Passport* au début du mois novembre 2001 provoquée par la menace d'un piratage imminent des

---

[37] *Watatatow! Hotmail a été piraté*!, Multimedium, http://www.mmedium.com/cgi-bin/nouvelles.cgi?Id=2577
ET *Hotmail piraté: ce n'est pas de notre faute, dixit Microsoft,* Multimedium, http://www.mmedium.com/cgi-bin/nouvelles.cgi?Id=2580

[38] Sur le site de Microsoft : *Microsoft Passport: Streamlining Commerce and Communication on the Web*, http://www.microsoft.com/PressPass/features/1999/10-11passport.htm ; ET page Web du service *Passport*: http://www.passport.com/Consumer/default.asp?PPlcid=1033

[39] Brian McWILLIAMS, *Stealing MS Passport's Wallet*, Wired news, Nov. 2, 2001, http://www.wired.com/news/technology/0,1282,48105,00.html

[40] *Privacy groups slam Windows XP*, Reuters, October 23, 2001, http://www.zdnet.com/zdnn/stories/news/0,4586,5098685,00.html

[41] http://www.epic.org/

numéros de carte de crédit conservée sur ses serveurs n'a rien de rassurant dans ce contexte[42].

Nous concluons cependant que, prises ensembles, ces propositions initiales présentées par Microsoft et Netscape contenaient la plupart des caractéristiques et fonctions principales de P3P. Elles allaient fournir au W3C les idées nécessaires à la conception de son projet et même, ironiquement, montrer la voie qu'il allait choisir, bien plus tard, pour sa mise en œuvre.

L'intérêt du W3C à créer un système cherchant à assurer le respect d'un niveau acceptable de vie privée sur le Web semble, de prime abord, manifeste. Il est en effet louable de vouloir protéger la confidentialité des renseignements et cet objectif semble avoir été le moteur de la création de quelques mouvements en ce sens à la fin de 1996 et au début de 1997 (dont TRUSTe et P3P). En poussant un peu la réflexion, nous découvrons cependant de multiples facettes à cette question. Dès l'automne 1997, Lorrie Faith Cranor et Joseph Reagle mentionnaient comme motivation la recherche de l'apaisement des craintes des usagers à l'égard de l'usage des données personnelles qu'ils sont appelés à transmettre dans le cours de leur navigation. L'usage secondaire des informations était particulièrement visé tant comme l'usage des adresses courriel à des fins de recoupement entre plusieurs banques de données et la transmission de renseignements par les enfants.

Bien que louable, il ne faut pas croire que l'initiative était entièrement altruiste ou spontanée puisqu'elle témoignait des préoccupations grandissantes de l'industrie et d'un questionnement pressant de la part de l'État américain, notamment par le biais du FTC[43]. Ainsi dès le printemps de 1995, le FTC organisait un atelier sous le thème de la protection du consommateur sur l'inforoute.[44] Lors de ce colloque, les représentants de la Commission abordèrent notamment la question de la protection des

[42] Brian McWILLIAMS, *Stealing MS Passport's Wallet*, Wired news, Nov. 2, 2001, http://www.wired.com/news/technology/0,1282,48105,00.html
[43] "Federal Trade Commission" http://www.ftc.gov
[44] "Consumer Protection and the Global Information Infrastructure.", http://www.ftc.gov/opp/trnscrpt.htm

renseignements personnels sur le Web. Ils eurent de ce fait l'occasion de manifester leurs inquiétudes en la matière aux représentants de l'industrie Web.

Peu de temps après, en juin 1995, une commission d'enquête du gouvernement américain[45] publie son rapport intitulé «*Privacy and the National Information Infrastructure: Principles For Providing and Using Personal Information*»[46], qui met en évidence certaines réalités du nouvel environnement Internet dans la gestion des renseignements nominatifs. Le rapport constate tout d'abord que le secteur privé devient, grâce au Web, aussi actif que l'État dans la collecte de renseignements personnels. Il prend également note que l'utilisation du Web par les individus génère des quantités énormes d'informations relatives tant aux transactions effectivement conclues qu'aux simples communications qui y ont cours. Le rapport relève par ailleurs que les réseaux participant à ces communications sont vulnérables en matière de sécurité. Finalement, la commission souligne que la rapidité d'évolution du réseau rend difficile la tâche d'y appliquer les normes éthiques traditionnelles, même celles qui sont bien reconnues et implantées.

Cette première réflexion de l'État américain était révélatrice à plusieurs égards. Tout d'abord elle montrait l'inquiétude de l'État américain face à la situation de la protection de la vie privée des internautes. La nouveauté du phénomène, la méconnaissance de la situation par les usagers, l'abondance des renseignements, la facilité d'y accéder pour les opérateurs des sites, tout comme l'absence de codes de conduite contribuant à créer un contexte de plus en plus propice aux abus :

> *«...as the NII evolves, more personal information will be generated and more will be done with that information. Here lies the increased risk to privacy. This risk must be addressed both to secure the value of privacy for individuals and society and to ensure that the NII will achieve its full potential. Unless this is done, individuals may not participate in the NII for fear that the costs to their privacy will outweigh the benefits.»* [47]

[45] " National Information Infrastructure Task Force", http://iitf.doc.gov/
[46] http://aspe.os.dhhs.gov/datacncl/niiprivp.htm
[47] PRIVACY WORKING GROUP INFORMATION POLICY COMMITTEE, INFORMATION INFRASTRUCTURE TASK FORCE *Privacy and the national information infrastructure: principles for providing and using personal information*, Washington, June 6, 1995, http://aspe.os.dhhs.gov/datacncl/niiprivp.htm (pages et paragraphes non-numérotés)

La commission d'enquête souhaitait d'ailleurs voir s'implanter, dès 1995, des codes de conduite inspirés de situations connues, mais adaptées au nouvel environnement du Web et tenant compte des buts et objectifs de chacun :

> *«Existing codes of fair information practice must be adapted to a new environment in which information and communications are sent and received over networks by users who have very different capabilities, objectives, and perspectives. [...] New principles must acknowledge that each party has a different relationship with the individual and has different uses for personal information.»*[48]

La commission d'enquête rend ainsi justice à la spécificité du Web et à sa situation. Elle constate du coup que la rapidité de son évolution technique et économique rend difficile l'appréciation des valeurs rattachées aux principes reconnus en matière de protection de la vie privée :

> *«The rapidly evolving information environment makes it difficult at times to know how to apply traditional ethical rules, even ones that are well understood and accepted when dealing with tangible records and documents. Consider, for example, how an individual who would never trespass into someone's home might rationalize cracking into someone's computer as an intellectual exercise. In addition, today's information environment may present questions about the use of personal information that traditional rules do not even address.»*[49]

La suggestion d'une solution auto-régulatrice, et possiblement même d'une solution technique, constitue le dernier élément original que nous retenons de ce rapport. La commission conclut en effet à la responsabilité de chaque membre de la société dans l'atteinte d'un niveau acceptable de respect des principes de protection de la vie privée sur le Web :

> *«New principles should not diminish existing constitutional and statutory limitations on access to information, communications, and transactions, [...] Such principles should ensure that access limitations keep pace with technological developments. [...] Moreover, the principles should recognize that the interactive nature of the NII can empower individuals to participate in protecting information about themselves. The new principles should also make clear that this responsibility can be exercised only with openness about the process, a commitment to fairness and accountability, and continued attention*

[48] Id.
[49] Id.

> *to security. Finally, the principles should recognize the need to educate all participants about the new information infrastructure and how it will affect their lives.»*[50] (nos soulignements)

Pendant la période qui a suivi, l'État américain semble avoir privilégié l'approche indirecte pour inciter les intervenants du Web à choisir la voie de l'auto-régulation et à mettre en place eux-mêmes des mécanismes assurant aux internautes le degré de confidentialité souhaité. La menace à peine voilée d'une intervention législative lancée par le vice-président Al Gore à l'été 1998 témoigne de cette stratégie de la carotte et du bâton. Ainsi, alors que le vice-président discourait sur les lois qu'il souhaiterait voir adoptées, notamment pour la protection des enfants et des dossiers médicaux ou bancaires, le FTC continuait de promouvoir la voie de l'auto-régulation tout en montrant son impatience. Vieille technique de négociation qui consiste à montrer à l'adversaire la porte de sortie que l'on souhaite le voir prendre... «*Gore recently warned computer industry executives that if self-regulation does not work, "we will be obliged to take action ourselves."* »[51] Le FTC renchérissait dans son rapport au Congrès de juin 1998 :

> «[...] *the question is what additional incentives are required in order to encourage effective self-regulatory efforts by industry. The Commission currently is considering this question in light of the survey results, monitoring self-regulation efforts since the survey was completed, and assessing the utility and effectiveness of different courses of action. This summer, the Commission will make recommendations on actions it deems necessary to protect online consumers generally.*»[52]

La FTC a maintenu cette attitude. Ainsi son rapport de 1999 repousse encore un peu l'adoption d'une solution législative :

> « *Based on these facts, the Commission believes that legislation to address online privacy is not appropriate at this time. [...] ...the present challenge is to educate those companies which still do not understand the importance of*

[50] Id.
[51] *E-Bill of Rights' Moves Forward* , ABC News, 31 juillet 1998, http://abcnews.go.com/sections/tech/DailyNews/netprivacy_kids980731.html
[52] FEDERAL TRADE COMMISSION *Privacy Online: A Report to Congress*, Extrait tiré de la conclusion du rapport: http://www.ftc.gov/reports/privacy3/conclu.htm

> *consumer privacy and to create incentives for further progress toward effective, widespread implementation.»*[53]

En octobre 2001 Timothy J. Muris, président de la FTC, maintenait le cap en résistant encore à la tentation de l'intervention législative. Il expose néanmoins que ses motifs pour ce faire relève plus du pragmatisme que d'une intime conviction que l'État ne doit pas intervenir dans ce domaine. Il déclare ainsi que la préparation d'une telle législation, si l'exercice devient un jour incontournable, sera une tâche très compliquée si l'État souhaite intervenir efficacement. Il souhaite plutôt utiliser l'arsenal législatif déjà en place pour contrôler les abus, notamment la violation des politiques de vie privée affichées sur les sites :

> *«I think there is a great deal we can do under existing laws to protect consumer privacy. That is what this privacy agenda is all about. At this time, we need more law enforcement, not more laws. Whether we ultimately need more laws requires further study. »*[54]

Mais la pression ne provient pas seulement des politiciens. Les usagers du Web, de plus en plus nombreux et avertis, sonnent l'alerte et manifestent leur inquiétude. Outre la multiplication d'articles de périodiques à grande diffusion ou de reportages dans les médias traitant des problèmes de vie privée sur le Web, ces craintes sont amplement documentés et quantifiées.

Par exemple un sondage mené par le *Center for Democracy and Technology (CDT)*[55]en 1998, montre que les problèmes liés à la protection de la confidentialité constituent le frein le plus important au développement du commerce électronique. Les résultats établissent en effet que leurs doutes sur le niveau de respect de la confidentialité de leurs agissements dans le cyberespace avaient poussé une majorité de répondants à s'abstenir de faire des achats en ligne (60%), à ne pas s'enregistrer lors de leurs visites sur certains sites (67,95%,) et à ne pas donner de renseignements

---

[53] FEDERAL TRADE COMMISSION *Self-regulation and privacy online: a report to congress,* July 1999, http://www.ftc.gov/os/1999/9907/privacy99.pdf

[54] FEDERAL TRADE COMMISSION , *Protecting Consumers' Privacy: 2002 and Beyond*, Remarks of FTC Chairman Timothy J. Muris, The Privacy 2001 Conference, Cleveland, Ohio, October 4, 2001, http://www.ftc.gov/speeches/muris/privisp1002.htm

[55] CENTER FOR DEMOCRACY AND TECHNOLOGY (CDT), *Privacy Not Price Keeping People Off The Internet*, http://www.cdt.org/privacy/survey/findings/surveyframe.html

personnels les concernant (86,75%). Fait intéressant, 42% des répondants à ce sondage croient que le problème le plus pressant dans le dossier de la confidentialité sur Internet réside au niveau de la vente d'informations personnelles, alors que 32% croient plutôt qu'il s'agit de la journalisation des navigations des internautes sur le Web.

Un autre sondage a été mené en avril 1998, soit à peu près à l'époque de l'introduction du projet P3P, par la firme américaine *Louis Harris and associates.* Intitulé «*E-Commerce Privacy Survey*»[56], il s'est attaché plus particulièrement à la problématique découlant du respect de certaines normes de confidentialité dans le domaine du commerce électronique. Il confirme le niveau d'inquiétude du public face à ces questions. Selon les résultats présentés, 86% des répondants se déclarent inquiets face à ces questions, y compris les 81% des répondants qui procèdent à des achats en ligne. Le nombre de personnes déclarant avoir été victimes de violations de leur vie privée reste par ailleurs limité, soit 6% du total des répondants et 9% des cyber-acheteurs. Par ailleurs, 72% des répondants à cette étude soulignent que la mise en circulation sur Internet d'informations personnelles sur des individus constitue un sujet d'inquiétude sérieux. Plus de 70% rendent le même jugement quant à la journalisation et au croisement d'informations sur des individus par la récupération des adresses de courriel, que cette récupération soit faite à la connaissance ou non de la personne concernée.

Ces réticences du public offrent une toile de fond plutôt révélatrice du contexte qui a précédé l'élaboration du projet P3P, et la naissance de plusieurs logiciels ou services visant à rendre le Web un peu plus discret et anonyme.

1.2 Le but recherché par P3P

Les contextes technique et politique qui viennent d'être brossés déterminent dans une bonne mesure les buts recherchés dans sa mise sur pied. Il vaut la peine de s'y attarder un peu.

[56] http://www.privacyexchange.org/iss/surveys/ecommsum.html

Le but le plus évident qui se dégage la lecture des documents cités jusqu'ici, et probablement le plus important, est bien sûr la protection de la vie privée des internautes. La motivation du W3C et de l'industrie du Web dans son ensemble, n'est toutefois pas entièrement désintéressée. Il faut bien comprendre la dichotomie de la problématique actuelle, issue de l'évolution rapide des moyens informatiques et de leur diffusion croissante dans le grand public. D'une part, les problèmes de protection de la vie privée inhérents aux échanges de données, et généralement méconnus du grand public, se trouvent exacerbés lorsqu'ils sont transposés sur le cadre offert par un réseau informatique planétaire. D'autre part, la médiatisation de ces problèmes et l'importante publicité qui leur est faite provoque un spectaculaire retour de balancier de l'opinion publique qui attache irrémédiablement l'évolution future du Web et du commerce électronique à leur résolution.

Soulignons aussi que malgré la croissance phénoménale du commerce électronique sur le Web, jusqu'en 1999[57], les internautes sont restés craintifs quand vient le temps de communiquer des renseignements nominatifs les concernant lors de leur navigation sur le Web, notamment en raison des usages secondaires possibles qui peuvent en être fait.

Les craintes des internautes face au manque de discrétion sur le Web sont très bien documentées. Selon plusieurs observateurs, l'évolution du commerce électronique, et par le fait même le développement futur du Web, pourrait voir sa course ralentie ou même arrêtée si la confiance du public n'est pas restaurée. Dans ce contexte, la décision d'élaborer et d'introduire un protocole technique capable de sécuriser le public est d'un grand intérêt pour l'ensemble de l'industrie. Elle fait écho à des intérêts économiques importants et l'enjeu de la partie se compterait donc sur la Terre en dollars et pas simplement au ciel en indulgences.

Cette analyse est largement confirmée par les interventions publiques des politiciens et régulateurs. Ainsi Christine Varney, commissaire au FTC, déclarait dès 1996 :

[57] LE JOURNAL DU NET, *E-commerce, le marché dans le monde*. http://www.journaldunet.com/cc/cc_ecommd.shtml

> *«The government's primary focus at this point should be to support the growth of self-regulatory efforts and online education for the public. Internet commerce won't really take off until consumer confidence in the system is established.»*[58]

Un autre enjeu économique qui pourrait motiver non pas la mise sur pied du projet P3P mais plutôt son adoption par l'industrie, tient au fait qu'il pourrait bien créer un standard technique de collecte et de gestion des renseignements personnels. Un tel dénominateur commun pourrait être perçu comme permettant aux systèmes et aux logiciels de mieux s'intégrer réduisant, par le fait même, leurs coûts de conception. Un protocole commun comme P3P, basé sur le langage XML ouvert à l'intégration et à la structuration d'éléments nouveaux ou propres à des systèmes plus localisés, pourrait offrir à l'industrie un standard technique propre à simplifier la gestion des renseignements personnels sur les usagers du réseau. En effet, l'échange d'informations relatives aux usagers du réseau est déjà une activité lucrative parce qu'elle rend possible la création de profils très précis des internautes. Or ces profils sont néanmoins fondés sur la consolidation d'informations contenues sur des bases de données hétéroclites, construites et élaborées selon des structures à peu près toutes différentes les unes des autres. La possibilité d'établir un standard au traitement de ces informations, en les balisant selon des normes communes appliquées dès leur collecte faciliterait encore plus l'opération et pourrait augmenter la quantité et la qualité des profils établis. L'industrie dans son ensemble ne pourrait qu'en bénéficier.

1.2.1 La « Platform for Privacy Preferences (P3P)

Encore aujourd'hui, même parmi nos collègues, P3P demeure assez mal connu. Il faut probablement mettre ce fait au compte du peu de publicité qui lui a été accordé pendant son développement, et à une certaine ambiguïté alimentée, peut-être volontairement, par ses initiateurs. Ainsi, Reagle et Cranor du W3C, définissent P3P comme :

> *« ... a framework for informed online interactions. The goal of P3P is to enable users to exercise preferences over Web sites' privacy practices. P3P*

[58] FEDERAL TRADE COMMISSION , *Consumer privacy in the information age: a view from the United States*, Remarks of Christine A. Varney, Commissioner , Before the Privacy & American Business National Conference, October 9, 1996 http://www.ftc.gov/speeches/varney/priv&ame.htm

> *applications will allow users to be informed about Web site practices, delegate decisions to their computer agent when they wish, and tailor relationships with specific sites. »*[59] (nos soulignements)

Leur définition procède donc ici par une description du but recherché, qui est de permettre aux usagers d'imposer leurs préférences en matière de confidentialité aux politiques correspondantes des sites qu'ils visitent, et par une description de la procédure employée pour y arriver. Les mêmes auteurs ont été un peu plus précis dans un autre texte, plus volumineux il faut bien dire :

> *P3P is a project of the W3C, an international industry consortium that specifies protocols that promote the evolution of an open and interoperable World Wide Web. [...] At a high level, P3P can be viewed simply as a protocol for exchanging structured data.*[60] (nos soulignements)

Roger Clarke, un chercheur australien indépendant du projet, définit pour sa part P3P comme un protocole visant à supporter la négociation dans divers contextes, comme la transmission volontaire d'information nominatives, la transmission volontaire d'informations relatives aux goûts et intérêts d'un internaute, ou la cueillette involontaire d'informations (comme les historiques de navigation, ou les questions posées aux moteurs de recherche, par exemple).[61]

Lisa Rein, du site XML.com, abonde dans le même sens lorsqu'elle décrit l'usage qui peut être fait de P3P :

> *End-users can use the protocol to indicate their privacy preferences, and those preferences will determine which content to highlight, filter, feature, censor, accept, or reject through a series of (eventually) automated negotiations between a server and an end user's browser client.*" (nos soulignements) [62]

Ces définitions permettent d'évacuer certains mythes entourant P3P :

---

[59] Joseph REAGLE et Lorrie Faith CRANOR, *P3P in a Nutshell*, version consultée: 25 juin 1999; http://www.w3.org/P3P/nutshell.html

[60] Joseph REAGLE et Lorrie Faith CRANOR, *The Platform for Privacy Preferences*. P3P Note 06-November-1998, http://www.w3.org/TR/NOTE-P3P-CACM/; également publié dans Communications of the ACM, Vol. 42, No. 2 (Feb. 1999), Pages 48-55

[61] Roger CLARKE , *Platform for Privacy Preferences: An Overview*. Version du 20 mai 1998, amendé le 12 mai 1999, http://www.anu.edu.au/people/Roger.Clarke/DV/P3POview.html

Tout d'abord, P3P n'est pas un logiciel. Un «logiciel», ou une «application», est un programme conçu pour remplir une fonction précise pour un utilisateur donné. [63] P3P ne comporte aucun programme et ne remplit aucune tâche précise. Il ne constitue pas une application qui peut être chargée et exécutée sur un ordinateur afin de remplir une tâche donnée pour son propriétaire. Il ne fait que permettre l'expression de paramètres et d'informations normalisées qui pourront être exploités par les logiciels qui voudront en faire usage. P3P n'est pas non plus un navigateur. Un navigateur est un logiciel dont la fonction est de décoder les informations circulant sur Internet et de les reconstituer à l'écran de façon intelligible. P3P ne sert pas ces fonctions, bien qu'il puisse s'intégrer à de tels logiciels de navigation.

P3P n'est pas non plus un langage informatique inédit et original. Il fait plutôt usage de langages informatiques connus, principalement le XML (Extensible Markup Language), évolution du langage SGML et du HTML qui est à la base du Web actuel. Le XML se distingue cependant du HTML en ce qu'il permet l'acheminement de données standardisées. Un fichier en langage HTML contient des balises («*markups*») indiquant au navigateur le recevant comment présenter à l'écran les données transmises selon certaines normes de présentation (couleur, taille...). Les balises XML vont beaucoup plus loin en permettant de définir la structure des messages qui sont échangés. Ces possibilités peuvent être utilisées, par exemple, pour indiquer le statut d'une information donnée au niveau de la politique de confidentialité du site concerné. XML offre donc un mode de balisage des messages et des échanges de politiques qui permettra le développement d'outils informatiques compatibles entre eux. C'est ce langage XML qui soutient P3P.

Le seul problème, d'ailleurs celui qui cause l'ambiguïté que nous mentionnions au départ quant à la qualification de P3P, est que le W3C n'utilise pas le terme «protocole» dans le nom du projet. En effet, P3P ne désigne pas «*Protocol for*

---

[62] Lisa REIN, *The Evolution of a Privacy Standard*, XML.com, 5 mai 1999 http://www.xml.com/pub/1999/05/p3pdraft.html

[63] "*What is : an application* ?" http://searchwebmanagement.techtarget.com/sDefinition/0,,sid27_gci211585,00.html

Privacy Preferences», mais bien «*Platform for Privacy Preferences*». Qu'est-ce donc qu'une *«platform»* dans ce contexte? Le site «*Whatis.com*» définit ainsi le terme :

> *With reference to computers, a platform is an underlying computer system on which application programs can run. On personal computers, Windows 95 and the Macintosh are examples of two different platforms. [...] A platform consists of an operating system, the computer system's coordinating program, and a microprocessor.*[64]

Le terme «*platform*» ne peut donc pas avoir été utilisé ici dans son sens informatique, P3P n'ayant rien à voir avec un système d'exploitation ou un système informatique. La définition de «*Whatis.com*» comporte cependant une deuxième partie «*A platform is any base of technologies on which other technologies or processes are built*.» [65] En étirant la réalité un peu, cette seconde définition pourrait coller à P3P.

Nous croyons plutôt que le W3C a utilisé le terme «*platform*» par analogie avec un de ses sens habituels dans le langage courant. Nous nous en remettons au dictionnaire Webster :

> «*platform: a statement of aims and policies in the program of a person or party seeking electoral support*»[66]

Les dictionnaires français donnent plusieurs sens au mot français équivalent, " plate-forme ". Le dictionnaire de la francophonie Hachette, disponible sur le Web :

> *plate-forme Programme, ensemble d'analyses et de revendications qui servent de point de départ à une politique commune. Plate-forme électorale.*[67]

Ainsi P3P peut être compris comme la solution politique, ou le programme, du W3C à titre d'organisme auto-régulateur d'Internet, dans le chaud dossier de la protection de la vie privée sur Internet. L'ambiguïté de l'appellation semble témoigner d'une démarche de relations publiques, et dénoter une volonté manifeste de ses concepteurs

---

[64] "*What is : a platform* ?" http://searchhp.techtarget.com/sDefinition/0,,sid6_gci212797,00.html
[65] Id.
[66] *The new Webster's encyclopedic dictionary of the English Langage*. Canadian Edition, Lexicon Publictions, New York. 1988
[67] http://www.francophonie.hachette-livre.fr/cgi-bin/hysearch2?V=plate-forme&E=1

d'utiliser le plus de précautions possibles pour le présenter aux intervenants du Web de la manière la plus propice à assurer un important ralliement. Le présenter comme un protocole aurait pu le reléguer au rang d'instrument technique classique, ce qui n'est pas le cas lorsqu'on considère ses implications sociales et légales, ou en choquer d'autres qui y auraient pu y voir un instrument imposé par voie technique, donc quasi incontournable, alors qu'il est en réalité d'application volontaire. Nous croyons que le choix d'appellation du projet par le W3C démontre à quel point le sujet de la protection de la vie privée est crucial et sensible chez nos voisins du Sud. Nous pourrions aussi y voir un rapprochement entre la technique et les principes de gouvernance qui, bien qu'il soit probablement involontaire dans le choix de cette dénomination, reste néanmoins présent dans toute cette aventure P3P.

Voyons donc si malgré son nom, P3P se qualifie pour faire partie de la catégorie des protocoles comme les auteurs cités, et nous-mêmes, semblent le croire. Un protocole se définit comme suit:

> *« In information technology, a protocol [...] is the special set of rules for communicating that the end points in a telecommunication connection use when they send signals back and forth. Protocols exist at several levels in a telecommunication connection.»*[68]

Cette définition semble convenir à P3P. En effet, il semble bien consister en un jeu de règles particulières de communication réglant des échanges entre les extrémités d'une connexion. Tel que présenté dans cette définition, les protocoles pouvant exister à différents niveaux de la communication, P3P se qualifie d'emblée comme étant le jeu de règles gouvernant la dimension confidentialité d'une communication sur le Web. Son originalité tient cependant à deux aspects.

Tout d'abord, P3P ne s'attaque pas seulement à un aspect technique d'une communication, mais bien au comportement des parties à l'égard du traitement des informations transmises par l'une à l'autre. Ainsi, il ne s'agit pas de règles rendues nécessaires au niveau technique pour assurer la transmission, mais bien de règles

[68] "*What is an internet protocol*?"
http://searchnetworking.techtarget.com/sDefinition/0,,sid7_gci212839,00.html

proposées par une instance externe afin de contrôler des comportements, soit ici l'utilisation de certaines informations obtenues dans le cadre d'une telle transmission. Le protocole quitte donc le domaine purement technique, pour entrer dans le champ légal et social. La seconde originalité du protocole P3P se rattache au fait qu'il gouvernera ces utilisations même après la fin de la transmission, fait rare dans le domaine technique puisqu'il prévoit que les déclarations doivent contenir des engagements des sites quant au règlement subséquent de problèmes nés lors de l'échange d'information.

P3P est donc un protocole qui vise à régler un problème social et légal par des moyens techniques. Il fera usage de langages de programmation et de protocoles de communications existants et il pourra être utilisé ou adopté par une foule de logiciels ou applications différents, existants ou à venir. Par exemple, les navigateurs pourront intégrer ses règles et s'y rendre compatibles afin de permettre aux usagers d'en bénéficier de façon transparente lors de leurs navigations. De même, les logiciels de gestion des sites Web pourront se conformer aux règles de ce protocole et les comprendre, afin de permettre aux usagers qui les visitent de vérifier leur conformité à leurs préférences de confidentialité. C'est de cette façon que le W3C souhaite voir P3P s'intégrer au quotidien du cyberespace et y favoriser un meilleur respect des règles de base en matière de protection de la vie privée. Le fait qu'il constitue un protocole à intégrer aux logiciels et outils communs du Web, plutôt qu'un produit qui viendrait les concurrencer, augmente à leurs yeux ses chances de succès.

Bien que techniquement exact, il peut cependant être réducteur de limiter P3P en le définissant comme étant un simple protocole technique. Tant par ses enjeux politiques et commerciaux que par l'implication sociale qu'il ne pourra éviter d'englober dans un pareil champ d'action, P3P dépasse les limites de la technique. C'est ici que le terme " platform " prend tout son sens. Les autres protocoles du Web ont généralement pour seul objet la normalisation de procédures purement techniques. Par exemple, la communication sur Internet (TCP/IP) ou la transmission de courrier électronique (POP3, SMTP...) entre des ordinateurs autrement incompatibles ou utilisant des logiciels différents. Dans le cas de P3P, nous avons vu que les objets dépassent le

simple cadre technique et visent à régler des enjeux légaux et sociaux, avec des objectifs politiques (la croissance du Web) et commerciaux (soutenir le commerce électronique). P3P comprend donc un protocole technique, mais il est, dans son ensemble, bien plus que ça.

La définition offerte par Reagle et Cranor[69] prend, dans ce contexte, tout son sens : *« (P3P) provides a framework for informed online interactions.»* Plutôt que *«protocol»* ces auteurs préfèrent utiliser le terme «*framework*», que nous pourrions traduire par «cadre». P3P constitue pour eux un «cadre» pour la poursuite du but recherché, permettre aux internautes d'imposer sur le Web leur préférences en matière de vie privée. Cette nuance, qui peut sembler anodine à première vue, est pourtant de taille. Elle implique en effet que pour ses principaux ténors, P3P dépasse la portée de ses seuls éléments techniques et comporte d'autres facettes et composantes, notamment sociales et légales. Le contexte législatif et contractuel entourant les négociations et les échanges entre usagers et sites visités pourraient faire partie de ce cadre d'intervention du projet. Le W3C l'affirme d'ailleurs directement dans le texte de la spécification P3P :

> *P3P is complementary to laws and self-regulatory programs that can provide enforcement mechanisms.* [70]

Il ne faudra jamais perdre cet élément de vue même si, pour alléger le texte, nous nous contenterons souvent de le désigner sous le terme «protocole» ou de «plate-forme».

1.2.2 P3P comme mode de régulation par l'architecture

À ce point, il est intéressant de revenir à la théorie proposée par Lawrence Lessig et revue par Graham Greenleaf, selon laquelle la régulation des activités humaines résulte d'une lutte d'influence entre quatre types de contraintes : la loi, le marché (contraintes économiques), les contraintes sociales et la nature. Nous avons également

---

[69] Lorrie Faith CRANOR, Joseph REAGLE, et Mark S. ACKERMAN *Beyond Concern: Understanding Net Users' Attitudes About Online Privacy,* 14 avril 1999*,* http://www.research.att.com/projects/privacystudy/

[70] W3C, *The Platform for Privacy Preferences 1.0 (P3P1.0) Specification,* December 2000, http://www.w3.org/TR/2000/CR-P3P-20001215/

vu que Lessig substitue le «code» à la «nature» lorsqu'il est question du cyberespace, notion que Greenleaf élargit à «architecture».

Nous croyons que P3P fournit un exemple intéressant de cette modélisation présentée par Lessig, tout en se qualifiant aisément comme mode de régulation par l'architecture tant dans son fonctionnement que dans le contexte général de la problématique qu'il cherche à résoudre. Tout d'abord, il est évident que P3P intervient sur le réseau par des moyens techniques. Cette plate-forme propose en effet, nous l'avons vu, d'automatiser les négociations et les échanges de consentements qui viendront encadrer la transmission d'informations personnelles et de renseignements nominatifs entre un individu et un site Web qu'il visite. La solution proposée n'est pas le fruit de législations adoptées par des structures étatiques connues et ne comprend aucune sanction ou mode d'exécution coercitif. P3P est un mode d'auto-régulation d'application volontaire qui doit offrir un cadre technique qui régira les relations qu'elles noueront sur le réseau.

L'absence même de sanction directe dans le projet P3P fournit un autre élément l'apparentant au modèle de Lessig. Nous avons vu en effet que les concepteurs du projet comptent sur la pression «sociale» et les contraintes du marché pour pousser les opérateurs de sites à se conformer à P3P et à respecter les politiques qu'ils s'imposeront. Ils souhaitent donc, dans un premier temps, que ce soit le jeu de la concurrence qui pousse les opérateurs de site à se conformer à P3P. Les craintes entourant la protection de la vie privée étant manifestement un frein au développement du commerce électronique, la possibilité d'apaiser ces inquiétudes par l'usage d'un protocole reconnu comme P3P devrait constituer un atout commercial pour les cyber-commerçants. Dans un deuxième temps, les retardataires pourraient être poussés à emboîter le pas pour éviter de perdre de la clientèle et/ou pour priver leurs compétiteurs respectant la norme de l'avantage qu'ils en retireraient face au public. À la limite, même les opérateurs de sites insensibles aux préoccupations du public en matière de protection de la vie privée pourraient apprécier la valeur commerciale de l'image qu'ils projetteraient en s'affichant comme site conforme à

P3P. Nous constatons aisément ici que ces arguments relèvent directement de la catégorie des contraintes économiques.

Quant à la pression sociale, elle est omniprésente dans la problématique de la vie privée. Aussi il n'est pas étonnant que les promoteurs de P3P comptent en partie sur elle pour pousser les fournisseurs de services du Web à adopter leur protocole. Nous avons déjà vu à quel point les interventions des groupes de pression sont rapides lorsque surviennent des atteintes à la vie privée sur le Web. Il faut donc prévoir que de telles réactions ne se feront pas attendre non plus advenant que certains sites ne respectent pas les engagements auxquels auraient publiquement souscrit dans leurs politiques de confidentialité P3P. Est-ce que la crainte de telles dénonciations publiques seront suffisantes pour assurer le respect des engagements et le succès du projet? La question reste ouverte et la situation sera intéressante à observer. Mais, chose certaine, un succès illustrerait l'analyse de Lessig quant à l'utilité des contraintes sociales dans la recherche du respect des normes. Les cyber-commerçants pourraient en effet fort bien choisir de respecter les règles du jeu de P3P simplement pour éviter le déshonneur ou la honte d'être accusés publiquement sur le Web d'avoir enfreint leurs propres politiques, même si les conséquences réelles de tels manquements étaient inexistantes.

Dernier élément qui nous motive à voir en P3P une illustration intéressante des théories de Lessig, le rôle de la «Loi», ou de l'État, dans le dossier de la vie privée. Nous y retrouvons les deux facettes des interventions étatiques : directes, et indirectes. Les interventions directes dans ce dossier sont connues, et nous aurons l'occasion de les aborder dans le prochain chapitre. Il s'agit en l'occurrence des lois existantes en matière de protection des renseignements personnels et de la vie privée. Ces lois existent depuis un certain temps et s'appliquent déjà aux échanges de données nominatives dans le monde dit «réel». Le problème est de voir à ce qu'elles conservent toute leur application sur le Web, au moins dans leurs principes généraux. La poursuite de ce but motive les États à toutes sortes de tentatives, qui se sont surtout manifestées jusqu'à maintenant par des approches auprès des intervenants de l'industrie et par certaines des déclarations publiques visant à faire pression sur elle.

Tous ces gestes constituent autant d'actions indirectes de l'État afin de pousser au respect des règles de protection de la vie privée.

L'intervention indirecte de l'État sur l'architecture reste assez marginale jusqu'à maintenant, quoiqu'elle puisse avant longtemps constituer une tendance lourde. Nous citerons d'abord en exemple que le projet d'amendement «Bloche», adopté par l'Assemblée Nationale française le 27 mai 1999. Cet amendement à la loi française en matière de responsabilité des fournisseurs d'accès sur les contenus circulant sur le Web, propose notamment l'article suivant :

> *Art 43-6-1 : Les personnes physiques ou morales dont l'activité est d'offrir un accès à des services en ligne autres que de correspondance privée sont tenues de proposer un moyen technique permettant de restreindre l'accès à certains services ou de les sélectionner.* (nos soulignements)

Le législateur français adopte ainsi cette voie en choisissant, plutôt que de légiférer sur le comportement comme tel, d'imposer l'obligation aux fournisseurs d'accès de mettre en place un cadre technique permettant le respect des objectifs de la Loi. Ils devront donc non seulement respecter les lois habituelles, mais offrir une solution technique au problème de la responsabilité sur les contenus.

Le Québec a adopté la même voie dans sa loi concernant le cadre juridique des technologies de l'information, en obligeant la personne chargée de l'accès à un document technologique qui contient des renseignements personnels à " *voir à ce que soient mis en place les moyens technologiques appropriés*. "[71]

Nous croyons que de telles interventions étatiques, indirectes, axées sur la désignation d'un cadre technique souhaité mettant à profit la structure et les possibilités techniques du Web, seront de plus en plus répandues. Dans ce contexte il semble donc fort à propos d'étudier P3P qui représente un des premiers cas de telles interventions de la technique à des fins de gouvernance.

[71] *Loi concernant le cadre juridique des technologies de l'information*, L.Q.2001, c.32, art. 25

1.3 Question de recherche et approche

La problématique de la vie privée sur Internet est vaste. Toute solution proposée pour la solutionner comportera de multiples facettes, et de nombreuses implications parfois insoupçonnées. P3P ne fait pas exception à cette règle et le fait qu'il constitue une solution technique ne fait que compliquer les choses.

Le choix d'une question de recherche est crucial ici, afin de mener nos travaux vers un résultat utile. Le but ultime de toute démarche dans ce domaine est facile à déterminer: régler la problématique de la vie privée sur Internet, en garantissant de façon raisonnable aux internautes que les renseignements recueillis sur eux dans leur usage du Web, qu'ils aient été fournis volontairement ou non, ne se transigeront pas en marge des normes qu'ils connaissent et acceptent. S'assurer que les échanges de données personnelles sur le Web respectent les lois en vigueur et/ou les politiques des gouvernants est également un objectif à rencontrer. La faculté d'adaptation de toute solution proposée aux divers cadres législatifs entrant en compétition sur Internet doit également être recherchée.

Est-ce que P3P offre, selon ces critères, une solution acceptable à la problématique? Ou, en d'autres termes, P3P peut-il permettre de répondre aux préoccupations des états et des individus en matière de protection de la vie privée sur Internet?

La réponse à une telle question est objective : oui ou non. Nous tenterons cependant de pousser la réflexion plus loin, en nous demandant comment P3P pourrait être utilisé dans une démarche régulatrice, et contribuer à rencontrer ces objectifs.

Notre question pourrait donc se formuler comme suit :

> *Comment P3P, à titre de mode d'auto-régulation technique, peut-il permettre de répondre aux préoccupations des états et des individus en matière de protection de la vie privée sur Internet et s'adapter aux différents cadres législatifs existants?*

Afin d'y répondre, nous nous proposons en premier lieu d'examiner le cadre législatif existant au Québec et au Canada en matière de protection de la vie privée, en encadrant la transmission de renseignements personnels. Nous chercherons ainsi à établir les rationalités de cette problématique, particulièrement dans le contexte du Web. Nous ne pourrons cependant complètement ignorer, Internet oblige, la situation prévalant dans les autres juridictions notamment la directive Européenne.[72]

Nous analyserons par la suite le projet P3P et son application, ce qui nous permettra en dernière étape de tirer nos conclusions et, de proposer certains éléments de réponse aux questions qui viennent d'être posées.

***

[72] 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 caractère personnel et à la libre circulation de ces données, http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=fr&numdoc=31995L0046&model=guichett

CHAPITRE 2 La vie privée et la protection des renseignements personnels

2.1 Rationalités, attentes et aperçu du cadre juridique international

> *" La société en vient rapidement à reconnaître les bienfaits indiscutables des systèmes d'information automatisés et à s'en prévaloir [...] Elle se rend moins bien compte, toutefois, de ses effets possibles sur les valeurs humaines. "*[73]

Ce passage aurait pu être écrit aujourd'hui. Il l'a cependant été en 1972 dans le rapport d'un groupe d'étude du gouvernement canadien. Le message qu'il veut transmettre est toujours criant d'actualité et de justesse : toute invention doit chercher à améliorer le sort de l'homme, mais sans le dénaturer ni altérer ses valeurs fondamentales.

L'humain est un animal bien étrange : autant il a besoin de socialiser avec ses semblables pour évoluer et se confronter à d'autres visions des choses, autant il doit périodiquement s'éloigner du groupe pour se ressourcer et faire le point. Le besoin de protéger sa vie privée tire sa source de ce besoin viscéral de l 'humain de se réserver une zone de confort où il pourra se retrouver quand il en sentira le besoin. Cette zone pourra se composer de divers éléments formant l'intimité : protection du domicile, de la liberté d'expression et de croyances d'un individu, de sa dignité et, bien entendu, de certaines informations personnelles le concernant.

Les revendications en matière de protection de la vie privée apparaissent principalement à partir de la fin du 19^{e} siècle. Faut-il relier ce phénomène à l'accroissement de la puissance des médias imprimés, et sa croissance à l'émergence des premiers médias radiophoniques ou télévisuels qui sont venus encore réduire les distances entre les individus? Cette influence a très certainement joué son rôle. Auparavant pourtant, protéger la vie privée en milieu rural était tout à fait illusoire. Tout le monde connaissait l'histoire de son voisin, la répandait et s'en souvenait longtemps. Celui qui était la proie du scandale ne pouvait y échapper qu'en s'exilant pour refaire sa vie dans un autre village. La concentration de la population dans de grandes cités anonymes avait en partie réglé ce problème et fait espérer à plusieurs

une vie plus discrète. Ces espoirs s'évanouirent rapidement à la faveur du développement des médias qui nous ont amenés vers le village global où chacun risque à tout moment de devenir le centre d'attention de tous. Plus d'issue possible, il n'y a pas d'autre village. Il fallait donc chercher à protéger la vie privée des individus d'une autre façon, le droit.

Mais que fallait-il donc protéger au juste? Westin[74] isole quatre composantes du besoin humain de vie privée. Le rapport du Groupe fédéral précité les résume bien :

> *" ... la solitude – pour que l'homme puisse réfléchir sur ce qui lui arrive; l'intimité avec la famille et les amis – pour permettre des relations plus étroites, plus attachantes; l'anonymat – pour permettre à l'homme d'exister en dehors du milieu où il évolue; et la distance – pour qu'il puisse suspendre les communications quand il en éprouve le besoin. "*[75]
> (nos soulignements)

La protection de la vie privée n'est pas un sujet monolithique, dont le cadre légal ne découle que d'une loi ni même d'une seule juridiction. Elle constitue plutôt une valeur fondamentale qui s'imbriquera dans plusieurs problématiques juridiques où elle affrontera ses éternels rivaux : liberté d'expression et droit à l'information. La protection de la vie privée constitue certes un exemple de choix de l'opposition classique voulant que la liberté de l'un s'arrête là où la liberté de l'autre prend naissance. Ses principes se traduiront pour l'individu en des droits différents, qui s'appliqueront selon les circonstances aux relations entretenues par les individus au niveau civil avec leurs pairs, ou au niveau public avec l'État : protection du domicile contre saisies et intrusions, interdiction d'intercepter les communications, protection de la dignité, encadrement de la collecte d'informations ou de la constitution de dossiers, et autres.

La protection de la vie privée figure également sur la courte liste des sujets d'inquiétude juridique sur les inforoutes.

---

[73] INFORMATION CANADA , *L'ordinateur et la vie privée*. Rapport du groupe d'étude établi conjointement par le ministère des Communications et le ministère de la Justice. Ottawa, 1972, p. 10
[74] Alan F. WESTIN, *Privacy and Freedom*. New York, Atheneum, 1970
[75] Id., p. 18-19

> *" Le mythe du Big brother, où l'État surveillerait la totalité des communications qu'un individu pourrait faire à partir de son ordinateur, joue pour beaucoup dans la place parfois démesurée, compte tenu du taux relativement faible d'incidents rapportés ou de violations effectives, que prennent les préoccupations au sujet de la vie privée. Certains croient de telles craintes tout à fait injustifiées puisque dans la réalité actuelle des réseaux de communication, il semble impossible, sinon par des moyens extravagants, de contrôler les flux d'informations. "*[76]

Mais est-ce toujours exact ? Le développement fulgurant des technologies rend aujourd'hui possible des opérations jugées impossibles ou démesurées il y a quelques années à peine. Nous n'avons qu'à penser aux systèmes *Carnivore*[77] ou *Echelon*[78] capables d'intercepter et d'analyser des centaines de millions de communications et messages électroniques pour comprendre à quel point les capacités de l'informatique de s'ingérer dans les affaires privées ne doivent pas être pris à la légère.

Les craintes de nombres d'internautes de voir s'instaurer, par le biais du Web, des infrastructures de surveillance systématiques de leurs moindres faits et gestes ont certes été exagérées au début. La découverte des systèmes américains de surveillance des communications électroniques aura cependant tôt fait de réveiller ces fantômes. La spectaculaire évolution technique des dix dernières années permet même maintenant de puiser des renseignements utiles et précis à même les masses d'information recueillies par le passé et alors jugées impossibles à traiter. Prenons par exemple la reconstitution rétroactive des archives de messages échangés sur les groupes de discussion. L'effet de masse de plus de 600 millions de messages amassés par le service *Déjà News* se retrouvant maintenant sur *Google*[79].

Mais l'évolution du Web nous a aussi montré que les cauchemars d'Orwell pourraient fort bien s'incarner dans des systèmes privés de cueillette d'information et, surtout, dans le commerce des données dont ils regorgent. Donc, même si les risques viennent

---

[76] Pierre TRUDEL et al, *Droit du cyberespace*, Montréal, Éditions Themis, 1997 , pages 1-19

[77] Associated Press, *FBI Gets Carnivore Approval*, Wired, 22 novembre 2000, http://www.wired.com/news/politics/0,1283,40335,00.html

[78] voir notamment http://www.echelonwatch.org/

[79] http://www.google.com sous l'onglet « groups », ou directement http://www.google.com/grphp?hl=en

d'une autre source que prévu, les craintes des internautes et des gouvernants à l'égard de la protection de la vie privée sur le Web sont tout à fait fondées.

Nous tenterons dans ce chapitre d'exposer brièvement la question de la vie privée et de son cadre juridique. Nous nous attarderons particulièrement à l'aspect de la protection des renseignements personnels, dimension incontournable pour notre analyse de la plate-forme P3P. À ce chapitre, nous traiterons plus en détails des législations canadienne et québécoise. Nous présenterons enfin le contexte général régissant cette question sur le Web aujourd'hui.

2.2 Cadre juridique canadien en matière de protection de la vie privée

Tout exposé de la problématique de la vie privée au Canada doit comprendre l'étude de deux périodes, soit celle qui a prévalu avant l'adoption des chartes des droits fédérales[80], et provinciales[81] et celle qui prévaut depuis. Sans prétendre approfondir de façon exhaustive ces notions, nous croyons important d'en dresser un portrait sommaire.

2.2.1 situation avant les chartes

Le droit de la vie privée en common law est quasi-inexistant. Le professeur Peter Burns de l'Université de Colombie-Britannique résume ainsi la question:

> *" In 1937[82] the Chief Justice of Australia, Latham C.J., was able to claim : " However desirable some limitation upon invasions of privacy might be, no authority was cited which shows that any general right to privacy exists. "* [83]

La solution du common law aux problèmes de vie privée consiste donc en l'application d'une série de principes généraux du droit, notamment en matière de

[80] *Charte canadienne des droits et libertés*, Édictée comme l'annexe B de la *Loi de 1982 sur le Canada*, 1982, ch. 11 (R.-U.), http://canada.justice.gc.ca/loireg/charte/const_fr.html
[81] *Charte des droits et libertés de la personne*, L.R.Q, c. C-12, http://www2.lexum.umontreal.ca/qclrq/fr/c12.html
[82] L'auteur cite un passage de l'arrêt *Victoria Park Racing and Recreation Grounds Co. Ltd v. Taylor et al* (1937), 58 C.L.R. 479
[83] Peter BURNS: *Privacy and the Common Law : a tangled skein unravalling*? dans Dale GIBSON (dir.) *Aspects of Privacy Law. Essays in Honour of John M. Sharp*, Butterwoths, 1980, page 21 et ss.

responsabilité (« *torts* »), qui seront appliqués à certains aspects des manquements à la confidentialité souhaitée.

> *" The right of privacy has not, so far, at least under that name, received explicit recognition by British courts. For one thing, the traditional technique in tort law has been to formulate liability in terms of reprehensible conduct rather that of specified interests entitled to protection. For another, our courts have been content to grope forward cautiously along the grooves of established legal concepts, like nuisance and libel, rather that make a bold commitment to an entirely new head of liability."*[84]

Ainsi, avant l'adoption des chartes, le droit à la vie privée au Canada n'était pas encadré par des textes généraux et il n'existait que par la somme de certains droits isolés reconnus par des lois ou introduits par la jurisprudence. Une première catégorie visait les intrusions dans l'intimité d'un individu[85]: violation de domicile (« *trespass to land* »), de personne (« *trespass to the person* ») protégeront par exemple contre l'espionnage ou le harcèlement. Une seconde regroupant la dissémination d'informations relativement à un individu : nuisance, libelle et diffamation, en sont de bons exemples. Et encore, ces protections étaient souvent différentes selon les traditions juridiques des provinces. Par exemple, le droit à la préservation de la réputation obéissait à des tests jurisprudentiels différents. En common law, plaider la véracité des faits répandus sur une personne suffisait à l'épandeur pour se dégager d'une action en libelle, alors qu'en droit civil québécois, la pertinence de dévoiler un fait par ailleurs véridique détermine le sort de l'action.

La codification de certains de ces droits a débuté à la fin des années soixante, à la faveur de la découverte de cas dérangeants pour l'opinion. Le développement des technologies de communication permettant d'empiéter plus facilement dans la vie privée des individus, tout autant que l'accroissement de la présence et de la puissance des médias ne sont certes pas étrangers à l'adoption de lois en la matière.

La Colombie-Britannique a ouvert la marche en 1968 en légiférant pour la première fois dans le Commonwealth pour interdire l'invasion déraisonnable et injustifiée de la

[84] FLEMING, The Law of Torts (5th ed.), 1977, cité par BURNS, op. cit. note 83.

vie privée d'un individu. Le Manitoba et la Saskatchewan devaient emboîter le pas peu après. Bien que leur effet reste discutable, le fait que des juridictions de common law aient décidé de légiférer en la matière était à l'époque un événement en soi.[86]

Au Canada, l'adoption du projet de loi C-176 en décembre 1974 constituait l'une des premières tentatives fédérales dans ce domaine. Cette loi, qui en réalité amendait le *Code Criminel* et la *Loi sur les secrets officiels,* fût surnommée " *Loi sur la protection de la vie privée*. "[87] Son but était principalement d'encadrer les activités d'écoute électronique pour tenir compte tant des besoins des forces policières que du droit du public à vivre privément. Elle interdisait donc l'interception de communications privées par tout moyen technologique, ainsi qu'on le dit aujourd'hui, en en faisant une offense pénale. La possession du matériel nécessaire à effectuer de telles interceptions était également prohibée. Par la suite, la loi ajoutait les cas d'exceptions où de telles opérations pouvaient être menées, notamment celles au bénéfice des forces de l'ordre sur autorisation du juge, ou celles où l'une des parties à la communication l'autorise. Ces dispositions ont subi quelques amendements depuis.

Au Québec, un peu de la même façon, les citoyens tiraient le plus clair de la protection de leur vie privée du droit civil général notamment au chapitre de la responsabilité civile. Ici aussi, les protections s'articulaient également autour de deux actions maîtresse, soit *l'intrusion* et la *diffusion*. La première étant utilisée pour protéger les individus contre les invasions de leur intimité et l'autre pour empêcher la dissémination d'informations les concernant.

Le *Code civil du Bas Canada*, alors en vigueur, ne comportait pourtant aucune disposition spécifique en matière de droit à la vie privée. Il revint aux tribunaux d'en établir les paramètres, ce qui fut fait sur les base des principes de droit civil généraux

---

[85]" *intrusion upon the plaintiff's seclusion and solitude* "

[86] Philip H. OSBORNE, The privacy Acts of British Columbia, Manitoba and Saskatchewan, dans Dale GIBSON (dir.) *Aspects of Privacy Law. Essays in Honour of John M. Sharp*, Butterwoths, 1980, page 73 et ss.

[87] David DEUTSCHER, *The protection of privacy Act :whose privacy is it protecting*?, dans Dale GIBSON (dir.) *Aspects of Privacy Law. Essays in Honour of John M. Sharp*, Butterwoths, 1980, page 141 et ss.

communs aux droits français et québécois, principalement autour des principes des droits inhérents à la personnalité.

Rappelons que le droit français, sous l'impulsion du droit allemand qui élevait en 1949 au rang de droit fondamental le droit au développement de sa personnalité[88], a reconnu la cristallisation d'un droit unique de protection de la personnalité issu de l'accumulation de droits épars accordés à l'individu par la loi et la jurisprudence : droit à l'image, droit à la voix, droit au respect de la vie privée… Ces éléments composant un droit de la personnalité protégeant tant la dignité que la tranquillité des individus. La Loi du 17 juillet 1970 consacrait ces principes en ajoutant l'article 9 au Code civil qui édicte que " *Chacun a droit au respect de sa vie privée.* " Ce concept a été repris au Code civil du Québec à l'article 35 :

> *35. Toute personne a droit au respect de sa réputation et de sa vie privée.*
>
> *Nulle atteinte ne peut être portée à la vie privée d'une personne sans que celle-ci ou ses héritiers y consentent ou sans que la loi l'autorise.*

Parallèlement, la sanction utilisée en droit québécois pour assurer le respect de ces règles fut fournie par les règles de droit commun en matière de responsabilité civile.[89] Ainsi la Cour supérieure reconnaissait dès 1874 le " droit à la solitude " et en sanctionnait le manquement en forçant au paiement de dommages l'importun qui avait ouvert le courrier d'autrui.[90] La célèbre affaire *Robbins c. CBC (Québec)*[91] tire également sa source de ces principes. La cour accordait alors des dommages au plaignant après que la lettre de plainte qu'il avait adressé à la CBC fût lue en ondes

---

[88] *Loi fondamentale allemande de 1949*, article 2, al 1 (version bilingue disponible au http://www.jura.uni-sb.de/BIJUS/grundgesetz/art2.htm): "*Chacun a droit au libre épanouissement de sa personnalité pourvu qu'il ne viole pas les droits d'autrui ni n'enfreigne l'ordre constitutionnel ou la loi morale.* "

[89] Patrick GLENN, *The right to privacy in Quebec Law*. dans Dale GIBSON (dir.) *Aspects of Privacy Law. Essays in Honour of John M. Sharp*, Butterwoths, 1980, page 41 et ss.

[90] *Cordingly c. Nield* (1875) 18 L.C.J. 204, cité par Glenn, voir note 88.

[91] (1958) C.S. 152, 12 DLR (2d) 35, également citée par Glenn, voir note 88.

avec une invitation faite au public de communiquer avec lui. Les protections civiles contre le harcèlement tirent leur source de ces solutions jurisprudentielles.

Les règles relatives au libelle et à la diffamation tombent également dans la catégorie du droit à la vie privée, plus particulièrement au chapitre de la protection de l'honneur et de la réputation. En cette matière aussi, la sanction juridique a été fournie par le droit de la responsabilité civile.

> *... dans la province de Québec, il nous faut cependant retenir que dans tous les cas c'est le droit civil qui s'applique et l'on devra faire appel à l'article 1053 du code civil pour apprécier l'existence et le degré de responsabilité, soit : injure, diffamation ou libelle. "*[92]

Le Code civil du Québec allait plus tard procéder à l'intégration de ces notions en codifiant quant à lui les notions générales du droit civil relatives au droit de la personnalité en stipulant ce qui suit :

> *3. Toute personne est titulaire de droits de la personnalité, tels 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.*

*2.2.2 **situation après les chartes***

L'adoption des chartes fédérale et québécoise devait venir codifier et assurer de façon plus définitive ces droits. Rappelons d'abord qu'aux termes de son article 32, la Charte canadienne des droits et libertés [93] s'applique :

> *a) au Parlement et au gouvernement du Canada, pour tous les domaines relevant du Parlement, y compris ceux qui concernent le territoire du Yukon et les territoires du Nord-Ouest;*
>
> *b) à la législature et au gouvernement de chaque province, pour tous les domaines relevant de cette législature.*

---

[92] Antoine TASCHEREAU, *Le libelle diffamatoire*. Dans MEREDITH MEMORIAL LECTURES : *Four lectures and one panel discussion on purchase and sale of business enterprise, jurimetrics, libel, estate planning. / Quatre conférences et une table ronde sur l'achat et la vente d'entreprises, jurimétrie, le libelle, planification successorale*. Montréal, Wilson et Lafleur, 1970

[93] *Charte canadienne des droits et libertés*, Édictée comme l'annexe B de la *Loi de 1982 sur le Canada*, 1982, ch. 11 (R.-U.), http://canada.justice.gc.ca/loireg/charte/const_fr.html

Elle ne trouve donc pas d'application aux litiges entre particuliers ou, par exemple, dans l'action des tribunaux[94]. Elle n'est pas très loquace non plus en matière de protection de la vie privée. La seule disposition pertinente à la vie privée se trouve à l'article 8 :

> *8. Chacun a droit à la protection contre les fouilles, les perquisitions ou les saisies abusives.*

Mais la Charte impose quand même son influence en matière de vie privée, à travers la jurisprudence qui a suivi son adoption. Ainsi dans l'arrêt *R. c. Dyment*[95], la Cour suprême du Canada précisait la notion de vie privée à travers la définition de trois domaines particuliers où elle doit être protégée: spatiaux, physiques et informationnels. Ces catégories s'inspirent des conclusions du rapport conjoint des ministères de la justice et des communications du Canada intitulé *L'ordinateur et la vie privée*[96].

Les protections rattachées à l'espace, issues du statut quasi sacré rattaché à la propriété du domicile dans la common law, reconnaissent l'importance de ce dernier dans la protection de la vie privée des individus qui y résident. Pour la cour cependant, cette protection dépasse maintenant le concept de propriété. Comme le dit le juge La Forest :

> *" En fait, il se peut que percevoir ces droits dont nous avons hérités comme visant essentiellement à protéger la propriété revienne à confondre les moyens et les fins. «Autrefois, la vie des gens était centrée autour du domicile [...] Bien que l'on ait tenté de le justifier en termes de propriété [...] le droit conféré par la common law de ne pas être soumis à des fouilles, à des perquisitions et à des saisies abusives, avait pour effet de protéger la vie privée des particuliers. [...] Quoi qu'il en soit, cette Cour, dans l'arrêt Hunter c. Southam Inc., a clairement jugé, pour reprendre les termes du juge Dickson, que l'art. 8 a pour objet «de protéger les particuliers contre les intrusions injustifiées de l'État dans leur vie privée» [...] et qu'il devait être interprété largement pour réaliser cette fin, sans que l'on soit inhibé par l'attirail historique qui lui a donné naissance. »*

---

[94] *SDGMR c. Dolphin Delivery ltd* (1986) 2 R.C.S. 598-603
[95] (1988) 2 R.C.S. 417 ; sur le Web http://www.canlii.org/ca/jug/csc/1988/1988csc84.html
[96] INFORMATION CANADA , *L'ordinateur et la vie privée*. Rapport du groupe d'étude établi conjointement par le ministère des Communications et le ministère de la Justice. Ottawa, 1972.

Le juge soutient les arguments additionnels suivants à l'appui de l'élargissement de cette protection :

> *« ...comme Westin*[97]*, précité, à la p. 363, le fait observer, [TRADUCTION] «protéger la vie privée au domicile seulement . . . revient à protéger ce qui n'est devenu, dans la société contemporaine, qu'une petite partie du besoin environnemental quotidien de vie privée de l'individu". L'arrêt Hunter c. Southam Inc*[98]*. a brisé les entraves qui limitaient ces revendications à la propriété. À la page 159, le juge Dickson a adopté à juste titre le point de vue avancé initialement par le juge Stewart dans l'arrêt Katz v. United States, 389 U.S. 347 (1967), à la p. 351, selon lequel ce qui est protégé, ce sont les personnes et non les lieux. »*[99]

On se rappellera que l'arrêt *Hunter* avait confirmé que l'article 8 précité protégeait les personnes et non les lieux. Le juge Dickson s'y était inspiré de l'arrêt *Katz* où la Cour Suprême américaine avait confirmé que l'expectative de vie privée qu'attribue l'individu moyen à une conversation téléphonique ne variait pas selon le lieu d'où est effectuée la conversation. L'interception d'une conversation faite à partir d'une cabine téléphonique avait donc été jugée comme constituant une atteinte à la vie privée même s'il n'y avait pas eu de perquisition au domicile de l'individu visé.

Le second domaine de protection de la vie privée retenu par la cour a trait à la *personne*, et vise spécifiquement à garantir l'intégrité physique des individus contre des fouilles abusives ou des prélèvements abusifs et leur dignité.[100] Ce concept de dignité et d'intégrité de la personne est par la suite étendu au traitement de *l'information* relative à un individu. Le juge La Forest cite ici directement le rapport précité *L'ordinateur et la vie privée* pour ensuite confirmer l'importance de la protection des renseignements privés dans nos sociétés modernes :

> *« Comme l'affirme le groupe d'étude (à la p. 13): «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*

[97] Le juge La Forest cite : Alan F. WESTIN, *Privacy and Freedom*. New York: Atheneum, 1970.
[98] Le juge La Forest cite : *Hunter c. Southam Inc,* [1984] 2 R.C.S. 145
[99] *R. c. Dyment ,* précité, paragraphe 20
[100] *R. c. Pohoretsky*, [1987] 1 R.C.S. 945

> *spécialement, la conservation de renseignements à notre sujet revêt une importance accrue.*
>
> *[...] 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 utilisés que pour les fins pour lesquelles ils ont été divulgués. Tous les paliers de gouvernement ont, ces dernières années, reconnu cela et ont conçu des règles et des règlements en vue de restreindre l'utilisation des données qu'ils recueillent à celle pour laquelle ils le font»*[101]

Cette jurisprudence sur la définition du concept de protection de la vie privée sous-jacent à la Charte canadienne des droits et libertés démontre l'importante évolution qu'a connu ce domaine du droit au cours du dernier siècle. Elle cristallise les notions qui se sont dégagées pour former une certaine notion d'expectative de vie privée. Cette notion, prise ici dans un contexte de droit public, trouve son pendant dans plusieurs autres juridictions incluant le droit civil québécois. Elle apparaît fondamentale à toute étude des questions relatives à la protection de la vie privée.

Si nous avons vu que les textes fédéraux accordent de façon accessoire une certaine protection de la vie privée, le droit québécois aborde la question de façon beaucoup plus directe en la traitant explicitement au nouveau Code civil du Québec, aux articles 35 et suivants. Par exemple :

> ***35.*** *Toute personne a droit au respect de sa réputation et de sa vie privée.*
>
> *Nulle atteinte ne peut être portée à la vie privée d'une personne sans que celle-ci ou ses héritiers y consentent ou sans que la loi l'autorise.*

Comparons au passage l'article 35 à ce passage de la C*onvention Européenne de sauvegarde des droits de l'homme et des libertés fondamentales*[102] :

> *Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance.*

Revenons au Code civil du Québec :

---

[101] *R. c. Dyment* , précité, paragraphe 22
[102] http://www.justice.gouv.fr/textfond/europ1.htm

36. *Peuvent être notamment considérés comme des atteintes à la vie privée d'une personne les actes suivants:*
1° Pénétrer chez elle ou y prendre quoi que ce soit;
2° Intercepter ou utiliser volontairement une communication privée;
3° Capter ou utiliser son image ou sa voix lorsqu'elle se trouve dans des lieux privés;
4° Surveiller sa vie privée par quelque moyen que ce soit;
5° Utiliser son nom, son image, sa ressemblance ou sa voix à toute autre fin que l'information légitime du public;
6° Utiliser sa correspondance, ses manuscrits ou ses autres documents personnels.

Le Code civil inclut également dans ce chapitre certaines dispositions relatives aux renseignements sur les individus, à savoir celles contenues à ses articles 37 à 40. Ces règles de base relatives à la cueillette et à la gestion d'informations sur un citoyen seront reprises et complétées par la *Loi sur la protection des renseignements personnels dans le secteur privé*[103] à son entrée en vigueur le 1er janvier 1994. Ensemble, ces règles déterminent le droit québécois en matière de protection de la vie privée, le Code civil du Québec le plaçant au chapitre des droits de la personne.

Les applications des éléments du droit à la vie privée reconnus par le Code civil font du droit québécois l'un des plus complets en la matière au Canada. Il s'en dégage par exemple un droit à l'anonymat (ex. droit à l'image[104]) ou à l'autonomie (ex. libre choix du lieu de résidence[105]). Ces droits sont appelés à un riche avenir en jurisprudence en ce début de règne de *little brother*, notamment en milieu de travail. Mais là n'est pas notre sujet.

Il faut noter que la Cour suprême consacre le test de l'homme raisonnable dans l'évaluation de manquements présumés aux droits découlant de la protection de la vie privée. Ainsi, la cour reconnaîtra que les règles de protection de la vie privée invoquée par un individu dans une instance donnée trouveront application si un homme raisonnable pourrait s'attendre à en bénéficier dans les mêmes circonstances. Nous y voyons la confirmation de l'importance de la notion d'expectative de vie privée, tant aux niveaux civil que pénal.

---

[103] *Loi sur la protection des renseignements personnels dans le secteur privé* LRQ c. P-39.1 ; sur le Web http://www.canlii.org/qc/loi/p39.1/
[104] *Aubry c. Éditions Vice-Versa inc,* [1998] 1 R.C.S. 591; sur le Web http://www.canlii.org/ca/jug/csc/1998/1998csc31.html

La place de la charte québécoise[106] dans le droit québécois de la vie privée est également fondamentale puisqu'à la différence de la charte fédérale, elle ne s'applique pas seulement à l'État et à ses représentants, mais également aux individus. Ses règles sont donc opposables aux individus, entreprises, commerçants. Elle force donc le respect des grands principes de protection de la vie privée des individus dans les relations privées. On y retrouve par exemple, à ses articles 5 et suivants :

> *5. Toute personne a droit au respect de sa vie privée.*
>
> *6. Toute personne a droit à la jouissance paisible et à la libre disposition de ses biens, sauf dans la mesure prévue par la loi.*
>
> *7. La demeure est inviolable.*
>
> *8. Nul ne peut pénétrer chez autrui ni y prendre quoi que ce soit sans son consentement exprès ou tacite.*

La charte québécoise confirme également que l'exercice du droit à la vie privée doit respecter la liberté des autres et l'ordre public :

> ***9.1.*** *Les libertés et droits fondamentaux s'exercent dans le respect des valeurs démocratiques, de l'ordre public et du bien-être général des citoyens du Québec.*
>
> *La loi peut, à cet égard, en fixer la portée et en aménager l'exercice.*

L'intérêt de ces dispositions est très grand en matière de protection de la vie privée sur Internet. Les protections en matière de surveillance, d'interception de communications ou d'invasion de " domicile " (au sens large du mot, tel qu'exposé plus haut) ont en effet historiquement permis de protéger les citoyens contre les abus des représentants de l'État. Le contexte qui prévaut en cette ère de révolution technologique, et tout particulièrement sur le Web, met à la portée d'à peu près n'importe qui les moyens nécessaires pour empiéter dans l'intimité de son voisin. Il peut s'agir de l'obtention de renseignements, d'interception de courriels, de surveillance électronique, de l'utilisation de caméras miniatures et ainsi de suite.

---

[105] *Godbout c. Longueuil (Ville),* [1997] 3 R.C.S. 844; sur le Web http://www.canlii.org/ca/jug/csc/1997/1997csc97.html

Nous n'avons qu'à penser aux technologies de surveillance en milieu de travail pour réaliser que la limite entre l'intimité des employés et le droit de surveillance de l'employeur est mince et difficile à tracer.

Le domaine de la protection de la vie privée est tout aussi passionnant que diversifié. Faut-il y voir l'existence dans nos sociétés contemporaines de multiples menaces à la tranquillité de leurs citoyens et à leur droit de vivre en paix? Sans sombrer dans la paranoïa, force est de constater que la vie moderne impose toutes sortes de limites et de contraintes à la vie privée des individus, qui se reflètent dans le secteur du droit qui les régit : menaces découlant de l'administration de la justice (règles pénales), de l'exercice des fonctions gouvernementales (droit public) et de l'activité commerciale (droit privé). Mais nous constatons sans grande surprise que les solutions apportées à chacune de ces menaces sont proches parentes : droit à l'intimité, protection du domicile, de l'intégrité de la personne et, surtout, analyse fondée sur le niveau d'intimité auquel le citoyen est en droit de s'attendre ou, si vous préférez, sur son expectative de vie privée.

Nous abordons maintenant plus spécifiquement un autre aspect tout aussi important du domaine du droit de la vie privée, qui s'est développé de façon indépendante et a provoqué l'adoption de nombreuses lois particulières pour le gouverner. La protection des renseignements personnels est en effet par essence appelée à être au cœur de toute démarche d'encadrement juridique des technologies informatiques. Ces dernières permettent, nous l'avons vu, la mise sur pied de processus de cueillette, de gestion et d'accumulation d'informations atteignant des niveaux d'efficacité sans précédent. L'importance d'encadrer la gestion d'informations nominatives sur des individus dans un tel contexte n'est plus à démontrer. Voyons quel cadre juridique s'applique actuellement en cette matière.

---

[106] *Charte des droits et libertés de la personne*, L.R.Q, c. C-12, http://www.canlii.org/qc/loi/c12/

2.3 Cadre juridique général en matière de protection des renseignements personnels

La protection des renseignements personnels, ou données nominatives comme elles sont parfois désignées outre Atlantique a pris beaucoup d'ampleur depuis quelques décennies, au rythme de l'augmentation des moyens informatiques de la société. Désormais, on ne peut se contenter de réglementer la cueillette volontaire et ostensible de renseignements d'un individu. Les informations peuvent se recueillir et s'accumuler de bien des façons.

Le Conseil de l'Europe définissait la problématique en 1989[107] sous les deux catégories " *médias interactifs* "et " *télémétrie* ". Ces termes, qui n'ont pas vraiment survécu à la redéfinition des rôles et des techniques survenue depuis l'arrivée du Web, ont quand même initié la réflexion sur l'impact de l'évolution des technologies de l'information sur la confidentialité des informations véhiculées sur les individus.

Par exemple, au sujet de la télémétrie qui visait à l'époque les systèmes de surveillance à distance (compteurs d'eau, systèmes relevant les numéros de plaque des véhicules, etc...), le professeur Benyekhlef notait :

> *" Les dangers posés par la télémétrie sont simples à identifier . La télémétrie instaure un véritable régime de surveillance et de contrôle de l'individu. Des données ne sont-elles pas collectées à l'insu de la personne? On recueille ainsi des informations à distance hors la connaissance de l'individu sans assurance d'une non-utilisation secondaire de celles-ci. Il faut en effet éviter de permettre l'utilisation de telles informations à des fins détournées, c'est-à-dire à des fins étrangères à celles pour lesquelles ces données ont été recueillies. "*[108]

Il est intéressant de constater que si nous voulons utiliser le terme du Conseil de l'Europe, le Web constitue un formidable outil télématique. Son taux de pénétration dans la population fait en sorte de fournir à ses intervenants techniques une masse

[107] COMITÉ D'EXPERTS SUR LA PROTECTION DES DONNÉES, *Les nouvelles technologies: un défi pour la protection de la vie privée*?, Strasbourg, Conseil de l'Europe, 1989. cité par Karim BENYEKHLEF, *La protection de la vie privée dans les échanges internationaux d'informations*, Montréal, Thémis, 1992

[108] Karim BENYEKHLEF, *La protection de la vie privée dans les échanges internationaux d'informations*, Montréal, Thémis, 1992, p.361

phénoménale d'information. Ces intervenants étant souvent eux-mêmes des commerçants, il ne leur faut pas longtemps pour réaliser leur valeur :

> *" Les entreprises télématiques deviennent dès lors le reposoir d'une formidable masse de renseignements à caractère personnel. Il devient possible de dresser un profil de l'utilisateur grâce à une analyse des données personnelles qu'il communique : type de produits achetés, opinions politiques ou autres (sondages), nature des films sélectionnés, objet des interrogations aux banques de données, etc. [...] Ce profil peut alors devenir l'objet de transactions commerciales ou servir à exercer une surveillance et un contrôle de la personne fichée. "*[109]

Car si l'informatisation de masse de la population dite civile est un phénomène relativement récent, les grandes entreprises disposent depuis très longtemps des moyens techniques nécessaires à la compilation d'énormes banques de renseignements sur leurs clients actuels et potentiels. La valeur commerciale de telles banques de données a toujours été reconnue, l'informatisation n'ayant fait qu'aider à leur constitution et au développement de ramifications de plus en plus profondes dans la vie des personnes qui se cachent derrière ces fiches.

Le commerce de listes par ou pour des compagnies de publipostage, les échanges trans-frontaliers d'informations, le risque de voir des informations erronées disséminées sans contrôle, l'impossibilité d'accéder aux contenus se trouvant dans ces banques de données constituées le plus souvent à l'insu des principaux intéressés, ont donc créé une pression sur les gouvernements pour qu'ils encadrent ces pratiques.

Certains États ont légiféré sur la question, en réponse aux préoccupations du public. Deux tendances importantes se dégagent des positions législatives ou jurisprudentielles.

Tout d'abord, le courant d'inspiration américaine se contente d'envisager la question sous l'angle du droit public ou administratif. Pour les américains en effet, les seuls abus à sanctionner, les plus graves selon eux, proviennent de l'État et de ses créatures. Il est exclu pour eux de régir le traitement réservé aux données nominatives dans le secteur privé.

Les américains n'ont donc pas procédé à l'adoption de lois englobantes sur la protection des renseignements personnels. Le droit américain en la matière découle plutôt du *right of privacy*, constitutionnalisé par la U.S. Supreme Court suite à un courant doctrinal de droit public mené par Warren et Brandeis[110]. Cette doctrine est générale, et ne se limite pas à protection des renseignements personnels comme tels puisqu'elle englobe divers aspects de la protection de la vie privée, notamment le droit à l'anonymat, le droit au secret des opinions et au secret des communications. La protection offerte aux États-Unis en matière de protection des renseignements personnels semble donc un peu émiettée à première vue. La FTC américaine en venait récemment au même constat :

> «*Current American privacy law can best be described as sectoral, consisting of a handful of disparate statutes directed at specific industries that collect personal data [...] Pursuant to the Supreme Court's decision in United States v. Miller, 425 U.S. 435 (1976), individuals have no Fourth Amendment interest in personal information they voluntarily have conveyed to another. Consequently, any privacy protections for personal information must be legislatively grounded.*»[111]

Donc pour les citoyens américains, des lois sectorielles d'application limitée, et pas de protection générale quant à la gestion des renseignements personnels. Ils doivent s'en remettre au bon vouloir de leur législateur la protection de la constitution leur étant refusée.

L'autre courant, que nous pourrions qualifier d'européen, perçoit la notion de protection des renseignements personnels comme faisant partie des droits fondamentaux des individus.

Les lignes directrices de l'OCDE de 1980 sur la protection de la vie privée et les flux trans-frontaliers de données personnelles[112], l'affirment noir sur blanc :

---

[109] Id., p.362

[110] Samuel D. WARREN, Louis D. BRANDEIS, *The Right to Privacy*, 4 Harvard L.R. 193 (1890). Sur le Web: http://www.lawrence.edu/fac/boardmaw/Privacy_brand_warr2.html

[111] FEDERAL TRADE COMMISSION, *Privacy Online: A Report to Congress*, note de fin # 16, http://www.ftc.gov/reports/privacy3/endnotes.htm

[112] OCDE, *Lignes Directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel*, http://www.oecd.org/dsti/sti/it/secur/prod/priv-fr.html

> *" ... des législations relatives à la protection de la vie privée ont été adoptées ou le seront prochainement[...]en vue de prévenir des actes considérés comme constituant des violations des droits fondamentaux de l'homme, tels que le stockage illicite de données de caractère personnel qui sont inexactes, l'utilisation abusive ou la divulgation non autorisée de ces données. "* (nos soulignements)

Ce renvoi aux droits de l'homme et aux libertés fondamentales fait en sorte d'imposer la protection de la loi à toutes les sphères d'activité. La protection est donc issue de textes de loi spécifiques et elle fournit par conséquent un cadre très strict à toute activité de cueillette ou d'usage de renseignements personnels.

La plupart des lois adoptées par les pays ayant souscrit à cette philosophie juridique, s'inspirent de principes communs régissant les diverses étapes d'un tel type d'activité, que nous pouvons classer sous les trois catégories *cueillette*, *accès* et *dissémination*. Ces principes ont été cristallisés dans la partie 2 des lignes directrices de l'OCDE adoptées le 23 septembre 1980. En voici l'essence :

1) Principe de la limitation en matière de collecte : toutes données de caractère personnel devraient être obtenues par des moyens licites et loyaux, après en avoir informé la personne concernée ou avec son consentement.

2) Principe de la qualité des données : Les données recueillies devraient être pertinentes aux finalités de la collecte et, devraient être exactes, complètes et tenues à jour.

3) Principe de la spécification des finalités : Les finalités de la collecte des données devraient être déterminées au plus tard au moment de la collecte des données. Les données ne devraient être utilisées que pour atteindre ces finalités.

4) Principe de la limitation de l'utilisation : Les données de caractère personnel ne devraient pas être divulguées, ni fournies, ni utilisées à des fins autres que celles spécifiées sauf avec le consentement de la personne concernée ou lorsqu'une règle de droit le permet.

5) Principe des garanties de sécurité : Les données de caractère personnel devraient être protégées grâce à des garanties de sécurité raisonnables, contre la perte ou leur accès, destruction, utilisation, ou divulgation non autorisés.

6) Principe de la transparence : La transparence des pratiques et politiques, ayant trait aux données de caractère personnel doit être assurée.

> 7) Principe de la participation individuelle
>
> Toute personne physique devrait avoir le droit :
>
> a) obtenir confirmation du fait que le maître du fichier détient ou non des données la concernant ;
>
> b) obtenir communication des données la concernant, dans un délai raisonnable, moyennant, éventuellement, une redevance modérée, selon des modalités raisonnables et sous une forme qui lui soit aisément intelligible ;
>
> c) être informée des raisons pour lesquelles une demande qu'elle aurait présentée conformément aux alinéas (a) et (b) est rejetée et de pouvoir contester un tel rejet ; et
>
> d) contester les données la concernant et, si la contestation est fondée, de les faire effacer, rectifier, compléter ou corriger.
>
> 8) Principe de la responsabilité Tout maître de fichier devrait être responsable du respect des mesures donnant effet aux principes énoncés ci-dessus.

Le droit québécois en la matière s'inscrit résolument dans ce courant dit européen, notamment par sa *Loi sur la protection des renseignements personnels dans le secteur privé*[113], et les dispositions pertinentes du Code civil. La loi fédérale de 2000, *Loi visant à faciliter et à promouvoir le commerce électronique en protégeant les renseignements personnels recueillis, utilisés ou communiqués dans certaines circonstances, en prévoyant l'utilisation de moyens électroniques pour communiquer ou enregistrer de l'information et des transactions et en modifiant la Loi sur la preuve au Canada, la Loi sur les textes réglementaires et la Loi sur la révision des lois,* que nous préférerons nommer C-6 pour des raisons évidentes, respecte également cette philosophie. Ce n'est pas un hasard, car ils sont tous deux inspirés des dispositions du *Code type pour la protection des renseignements personnels*[114] de l'Association canadienne de normalisation, qui s'abreuve lui-même à la source des lignes directrices de l'OCDE en matière de protection des renseignements personnels[115].

---

[113] *Loi sur la protection des renseignements personnels dans le secteur privé* LRQ c. P-39.1; sur le Web : http://www.canlii.org/qc/loi/p39.1/

[114] CSA, *Code type pour la protection des renseignements personnels*, http://strategis.ic.gc.ca/SSGF/sf03281f.html

[115] OCDE, *Lignes Directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel*, http://www.oecd.org/dsti/sti/it/secur/prod/priv-fr.html

Mais jusqu'à l'adoption de cette loi C-6, successeur du défunt projet de loi 54, nous notons que l'intervention fédérale se limitait à la *Loi sur la protection des renseignements personnels*[116], qui ne visait qu'à régir la gestion des renseignements personnels colligés par l'État canadien dans la poursuite de ses activités. Il semble donc que le gouvernement fédéral canadien passe progressivement d'une approche américaine à une approche davantage inspirée par les conceptions européennes en la matière.

Nous utiliserons notre étude du droit québécois et canadien, pour examiner de plus près ces principes généraux.

2.4 La protection des renseignements personnels en droit québécois et canadien

Passons sans plus tarder à notre survol du cadre législatif général régissant la protection des renseignements personnels au Canada (niveau fédéral) et au Québec. Nous ferons d'une pierre deux coups. Nous examinerons les principes de base en matière de protection des renseignements personnels en définissant d'abord la notion pour en dégager par la suite les principes fondamentaux.

Le domaine de la protection des renseignements personnels, faisant partie de l'ensemble des règles régissant la protection de la vie privée des citoyens, se qualifie d'emblée comme étant un élément tenant à leurs droits et libertés. Dans le contexte constitutionnel canadien, la compétence sur les libertés publiques n'est pas attribuée exclusivement à l'un ou l'autre des paliers de gouvernement. Les grands principes des libertés publiques volent au-dessus de chaque secteur d'activité et peuvent s'y appliquer sans contrainte. La compétence d'édicter des règles relatives à l'une de ces libertés, la protection de la vie privée par exemple, à un champ d'activité humaine, s'appréciera en regard de la compétence constitutionnelle sur ledit champ d'activité :

> *" ... a law's impact on civil liberties has not been treated by the courts as the leading characteristic in determining the law 's classification. The courts have instead relegated the impact of a law on civil liberties to an*

[116] *Loi sur la protection des renseignements personnels* L.R.C. 1985, c. P-21 ; sur le Web : http://www.canlii.org/ca/loi/p-21/

> *incidental or subordinate position. The effect of this approach to classification is that the power to affect civil liberties is distributed between the two levels of government, depending upon which level of government has jurisdiction over the activities regulated by the law."*[117]

Cette affirmation ne ferme cependant pas le débat, loin de là. Quelques études relatives à la compétence constitutionnelle en matière de protection des renseignements personnels ont été menées par le passé, principalement avant leur adoption. L'adoption récente de la loi C-6 par le gouvernement fédéral et ses dispositions quant à l'existence de règles provinciales équivalentes ont cependant remis le débat à l'ordre du jour. Reste à voir si les gouvernements décideront de l'amener au niveau judiciaire. Nous n'aborderons pas cette question plus en détails dans le cadre limité de cette étude. [118]

Passons sans plus tarder en revue les législations fédérales et québécoises en la matière. Nous regrouperons ci-dessous les références à ces lois ainsi que les abréviations que nous utiliserons pour les désigner dans le reste de cette étude, afin de faciliter la lecture de cette section.

Lois encadrant la cueillette publique. Les deux niveaux de gouvernements ont adopté dans un premier souffle des lois visant à encadrer la cueillette, la gestion et l'accès aux informations sur les citoyens recueillis par leurs appareils publics respectifs :

Juridiction	Année	Titre	Abréviation utilisée
Canada	1983	*Loi sur la protection des renseignements personnels*[119]	**LPRP**
Québec	1982	*Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*[120]	**Loi sur l'accès**

[117] Peter W. HOGG, *Constitutional Law of Canada*,, (2e edition), Toronto, Carswell, 1985; cité par Karim BENYEKHLEF, *La protection de la vie privée dans les échanges internationaux d'informations,* Montréal, Thémis, 1992, à la page 386.
[118] Nous vous référons à l'ouvrage de Karim BENYEKHLEF, *La protection de la vie privée dans les échanges internationaux d'informations*, Montréal, Thémis, 1992, aux pages 383 et suivantes pour une étude fort intéressante de l'aspect constitutionnel de la question de la vie privée au Canada.
[119] *Loi sur la protection des renseignements personnels* L.R.C. 1985, c. P-21 ; sur le Web : http://www.canlii.org/ca/loi/p-21/
[120] *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* L.R.Q, c. A-2.1 Sur le Web : http://www.canlii.org/qc/loi/a2.1/

Lois encadrant la cueillette privée. Par la suite, les gouvernements ont adopté des lois encadrant le même type d'activités dans le secteur privé. Le Québec fera sa première incursion dans le domaine lors de l'adoption du Code civil du Québec en 1991 et complétera l'exercice en 1993. Le fédéral quant à lui, adopte la loi C-6 en l'an 2000 :

Juridiction	Année	Titre	Abréviation utilisée
Canada	2000	*Loi sur la protection des renseignements personnels et les documents électroniques*[121]	**C-6**
Québec	1991	*Code civil du Québec*	**CcQ**
Québec	1993	*Loi sur la protection des renseignements personnels dans le secteur privé*[122]	**Loi québécoise**

Mais avant de débuter notre étude de ce cadre juridique, il importe de se questionner sur le sens accordé par les différents législateurs à la notion de renseignement personnel ainsi que les principes fondamentaux couverts par ce type de législation.

2.4.1 Définition

Comment le *droit québécois* définit-il le renseignement personnel? Ou, si vous préférez, quels sont les renseignements personnels qui bénéficient de sa protection?

Le Code civil ne contient pas de définition précise du terme «renseignement personnel». Le législateur y utilise le terme général de « renseignement » dans le cadre d'articles traitant de la constitution de dossiers sur un individu. En revanche la *loi québécoise* comble cette lacune à l'article 2 :

> *Renseignement personnel.*
>
> *2. Est un renseignement personnel, tout renseignement qui concerne une personne physique et permet de l'identifier.*

Il y a ici abandon de l'expression «*renseignement nominatif*» utilisé auparavant dans la *Loi sur l'accès* de 1982. Celle-ci semblait être volontairement plus limitative,

[121] *Loi sur la protection des renseignements personnels et les documents électroniques*. L.C. 2000 c. 5. Sur le Web: http://www.canlii.org/ca/loi/p-8.6/ .
[122] *Loi sur la protection des renseignements personnels dans le secteur privé* LRQ c. P-39.1 ; sur le Web http://www.canlii.org/qc/loi/p39.1/

probablement à cause de la portée publique de certaines informations recueillies et conservées par l'État. Elle énonce ainsi :

> *Dans un document, sont nominatifs les renseignements qui concernent une personne physique et permettent de l'identifier.*
>
> *55. Un renseignement personnel qui a un caractère public en vertu de la loi n'est pas nominatif.*
>
> *56. Le nom d'une personne physique n'est pas un renseignement nominatif, sauf lorsqu'il est mentionné avec un autre renseignement la concernant ou lorsque sa seule mention révélerait un renseignement nominatif concernant cette personne.*

Nous concluons donc, a contrario, que la *Loi sur l'accès* visait à encadrer la cueillette et l'usage de renseignements permettant d'identifier une personne physique autre que son nom, à moins que celui-ci ne soit ajouté à d'autres renseignements le concernant, et tout renseignement de nature publique répondant aux critères de l'article 57 de la même loi[123]. La notion de *renseignement personnel qui a un caractère public* venait également limiter la définition, ce qui peut sembler inévitable dans le contexte gouvernemental. La *loi québécoise* adopte donc une position plus générale en encadrant tout renseignement qui permettrait d'identifier une personne physique, sans restriction quant à la qualification des informations.

La *Directive Européenne en matière de protection des données à caractère personnel*[124] fournit quant à elle la définition suivante à son article 2 :

> *«données à caractère personnel», toute information concernant une personne physique identifiée ou identifiable («personne concernée»); 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.*

---

[123] Il s'agira principalement ici de renseignements sur des personnes faisant partie ou faisant affaires avec des organismes publics, selon les critères très précis établis par l'article 57.

[124] *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 caractère personnel et à la libre circulation de ces données*.
http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=fr&numdoc=31995L0046&model=guichett

Cette définition est tout à fait comparable à la définition simplifiée proposée par la LPRP. Nous relevons aussi au passage le débat qui a lieu outre-Atlantique sur les définitions différentes apparaissant à la Directive Européenne et dans la *Loi Informatique et Liberté* du 6 janvier 1978. Citons pour ce faire Mme Cynthia Chassigneux :

> *Nous remarquons que la Directive 95/46/CE emploie l'expression " données à caractère personnel "125[14], là où la Loi Informatique et Liberté utilise celle d'" informations nominatives ". Cette distinction, qui peut sembler anodine, est à l'origine de nombreux débats doctrinaux, la définition de la Directive 95/46/CE englobant un trop grand nombre de données et risquant, par conséquent, d'affaiblir la protection elle-même. Quoi qu'il en soit, ces deux notions ont pour vocation de protéger les renseignements identifiant ou permettant d'identifier une personne physique et, ce, quel que soit le support utilisé.*[126]

Qu'en est-il du *droit fédéral canadien* quant à la définition de la notion de renseignement personnel? La LPRP qui, à la manière de la Loi sur l'accès encadre le secteur public fédéral dans sa gestion des informations sur les citoyens, fournit à son article 2 une définition détaillée de l'expression. Cette définition procède différemment en incluant expressément certains éléments.

Constituerait un renseignement personnel aux fins de la LPRP tout renseignement concernant un individu identifiable relatif à sa personne (race, origine nationale ou ethnique, couleur, religion, âge situation familiale, dossier médical, groupe sanguin), à son passé (éducation, casier judiciaire, antécédents professionnels, opérations financières antérieures), à son identification (tout numéro ou symbole, ou toute autre indication identificatrice, qui lui est propre, adresse, empreintes digitales), ses opinions, ses correspondances avec une institution fédérale (implicitement ou explicitement, privée ou confidentielle), les opinions d'autrui sur lui. Son nom tomberait également dans cette définition lorsqu'il est mentionné avec d'autres renseignements personnels le concernant ou lorsque sa seule divulgation révélerait des renseignements à son sujet.

---

[126] Cynthia CHASSIGNEUX, *La protection des données personnelles en France*, Lex Electronica, vol. 6, n°2, hiver 2001, http://www.lex-electronica.org/articles/v6-2/chassigneux.htm

Le projet de loi C-54, prédécesseur non-adopté de C-6, s'insérait dans la nouvelle tendance à la simplification et à l'élargissement de la définition de «renseignement personnel». Sa définition simple et englobante le définissait comme étant « *Tout renseignement concernant un individu identifiable, quelle que soit sa forme.* »[127] Cette définition a été un peu restreinte dans le projet de loi C-6 qui mentionne plutôt qu'un renseignement personnel est :

> *Tout renseignement concernant un individu identifiable, à l'exclusion de nom et du titre d'un employé d'une organisation et des adresse et numéro de téléphone de son lieu de travail.*

Nous notons aussi au passage que la définition utilisée dans la LPRP a inspiré certaines législations d'autres provinces canadiennes, comme par exemple en Ontario dans la *Loi sur l'accès à l'information et la protection de la vie privée*.[128]

2.4.2 Les principes fondamentaux

Trois catégories fondamentales de situations à encadrer se dégagent par elles-mêmes en matière de protection des renseignements personnels: la cueillette, l'accès (et mise à jour) et la dissémination des renseignements. La *cueillette* vise les processus de collecte d'informations par les intervenants et encadre leurs relations avec les individus sur lesquels ils souhaitent se renseigner. Cette catégorie fait appel aux principes de transparence quant à la cueillette elle-même et aux raisons qui la motivent, ainsi qu'à la question cruciale du consentement du sujet. *L'accès* réfère à l'encadrement de la conservation des informations. Elle implique également la transparence du processus au niveau du droit de consultation de l'individu et à la possibilité de demander la correction d'informations erronées ou révolues. La *dissémination* touche parallèlement à la conservation des informations et à la durée de vie des dossiers. Faisant appel à une notion de contrôle de l'individu sur le dossier constitué à son sujet, elle implique l'interdiction d'utiliser les informations à des fins

---

[127] *Loi sur la protection des renseignements personnels et les documents électroniques*, Projet de Loi C-54, 1ière lecture, 1re session, 36e législature, (Can.), art. 2; sur le Web : http://www.parl.gc.ca/36/1/parlbus/chambus/house/bills/government/C-54/C-54_1/90052bF.html#1

[128] *Loi sur l'accès à l'information et la protection de la vie privée.* L.R.O. 1990, chap F.31; Sur le Web: http://192.75.156.68/DBLaws/Statutes/French/90f31_f.htm

autres que celles initialement déclarées tout comme la transmission des données collectées à des tiers. De façon implicite, elle introduit aussi l'obligation de destruction du dossier une fois que l'objectif de sa constitution a été atteint. La constitution d'un dossier et la collecte d'informations ne doivent donc durer que tant que la finalité initiale subsiste.

L'examen de ces principes de base en matière de protection des renseignements personnels permet un examen éclairé des législations québécoises et fédérales en la matière.

Au Québec les règles de protection des renseignements personnels découlent principalement du code civil et de deux lois : la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* («*loi sur l'accès*»), adoptée en 1982 pour régir l'accès aux documents publics et l'usage fait par l'État des renseignements personnels qu'il recueille, et la *Loi sur la protection des renseignements personnels dans le secteur privé* («*loi québécoise*») adoptée suite à l'entrée en vigueur du nouveau Code civil pour préciser certaines des dispositions qui y étaient déjà stipulées dans ce domaine. Il ne faut pas non plus oublier la *Loi sur le cadre juridique des technologies de l'information*, ou loi 161. Adoptée en juin 2001[129], elle comporte quelques dispositions applicables en la matière. De plus, son impact général viendra potentiellement faciliter l'application du droit québécois en matière de protection des renseignements personnels au médium électronique en confirmant et assurant la valeur juridique des documents conservés sur support électronique. Bases de données, dossiers ou documents, la valeur des documents s'apprécie selon 161 au niveau du contenu, pas de la forme ou du support technologique. L'effet des règles générales relatives à la cueillette et à la gestion des renseignements personnels ne peuvent donc nullement être limitées par le support technologique utilisé pour les recueillir ou les utiliser. Voyons maintenant ces règles générales qui s'appliquent aux renseignements.

[129] *Loi concernant le cadre juridique des technologies de l'information*, L.Q. 2001, c. 32

Nous avons vu que le Code civil du Québec intègre à ses articles 35 à 41 certaines dispositions tenant au respect de la vie privée[130]. Sauf les deux premiers, tous les articles de ce chapitre du Code traitent de la protection des renseignements personnels. Les règles se retrouvent dans le chapitre de la vie privée, qui se trouve lui-même dans le titre deuxième, *«De certains droits de la personnalité»*. L'inclusion de ces dispositions à cet endroit est tout à fait révélatrice. Nous y voyons la confirmation que l'État québécois souscrit au courant de pensée dit européen en matière de vie privée et qu'il considère que cette notion fait partie des droits fondamentaux de la personne.

Nous retrouvons à ce chapitre la plupart des éléments de base autour desquels s'articulent à peu près toutes les lois en la matière. Il y a lieu de les présenter :

- nécessité d'un intérêt sérieux et légitime pour constituer un dossier sur un individu et déclaration du motif de sa constitution (art 37. CcQ) ;
- droit de consultation de l'information accumulée accordé à la personne concernée (art. 38 et art. 39 CcQ) ;
- obligation de correction ou de mise à jour de l'information sur demande de l'intéressé (art. 40 CcQ) ;
- interdiction de communication non-autorisée des informations détenues (art. 37 CcQ).

La table était mise pour un élargissement du champ d'application des principes imposés à l'État par l'adoption en 1982 de *Loi sur l'accès*. Adoptée quant à elle après l'entrée en vigueur du Code Civil du Québec, la *loi québécoise* vient compléter et préciser ces articles pour les fins des activités des entreprises privées. Les principes énoncés au Code civil du Québec se retrouvent donc dans cette loi. Nous l'utiliserons pour les décrire un peu plus en détails.

La *loi québécoise* utilise les mêmes critères d'intérêt sérieux et légitime pour justifier la collecte que ceux proposés par l'article 37 du Code civil. Elle ajoute que l'entreprise qui créé le dossier doit y inscrire son objet, déclaration qui est réputée en faire

[130] CcQ, art. 35 à 41; sur le Web : http://www.droit.umontreal.ca/doc/ccq/fr/l1/t2/c3/0035a0041.html

partie.[131] Nous remarquons que la directive Européenne précise que les données à caractère personnel doivent être « [...] *collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement de manière incompatible avec ces finalités*.»[132] Le principe d'un lien entre la collecte et le but déclaré de l'exercice apparaît donc de façon claire. Nous pourrons parler d'une obligation de transparence, ou d'intégrité dans l'exercice de l'activité de collecte.

La loi québécoise précise par ailleurs ce critère de transparence, en ajoutant une obligation de s'adresser directement à l'intéressé pour recueillir les informations le concernant :

> *6. La personne qui recueille des renseignements personnels sur autrui doit les recueillir auprès de la personne concernée, à moins que celle-ci ne consente à la cueillette auprès de tiers.*

Toute cueillette d'informations auprès d'un tiers ne doit se faire qu'avec l'autorisation de l'intéressé, sauf en application des exceptions spécifiques de la loi, ou si l'entreprise peut justifier d'un intérêt sérieux et légitime et de l'application de l'une des conditions suivantes :

> *- les renseignements sont recueillis dans l'intérêt de la personne concernée et ils ne peuvent être recueillis auprès de celle-ci en temps opportun ;*
>
> *- la cueillette auprès d'un tiers est nécessaire pour s'assurer de l'exactitude des renseignements*[133]

Le législateur exclut donc toute possibilité de collecte occulte de renseignements personnels sur un individu. L'exercice doit en conséquence être mené au grand jour, à la connaissance du sujet.

---

[131] *Loi sur la protection des renseignements personnels dans le secteur privé* LRQ c. P-39.1; sur le Web : http://www.canlii.org/qc/loi/p39.1/

[132] Directive 95/46/CE , *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 caractère personnel et à la libre circulation de ces données*. http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=fr&numdoc=31995L0046&model=guichett, article 6

[133] *Loi sur la protection des renseignements personnels dans le secteur privé* LRQ c. P-39.1; sur le Web : http://www.canlii.org/qc/loi/p39.1/, art 12

Ainsi les règles établies au Code civil correspondent parfaitement aux trois grandes catégories de règles gouvernant les renseignements personnels que nous avions identifiées, soit : cueillette (accumulation), accès (mise à jour) et dissémination (distribution et utilisation). Ces principes de base inspirés des politiques de l'OCDE se reflètent aussi dans les dispositions de la Directive Européenne.

Au chapitre de la *cueillette* des informations, le droit québécois impose aux organismes l'obligation d'assurer la confidentialité des dossiers qu'ils maintiennent.

> *10. Toute personne qui exploite une entreprise et recueille, détient, utilise ou communique des renseignements personnels sur autrui doit prendre et appliquer des mesures de sécurité propres à assurer le caractère confidentiel des renseignements.*[134]

Cette confidentialité survit même à la transmission hors-Québec des informations, puisque le législateur impose au détenteur des dossiers l'obligation de s'assurer de l'usage qui en sera fait et de la possibilité pour l'individu concerné d'exercer un certain droit de veto sur la sortie des informations.[135] Nous retrouvons ici une préoccupation comparable à celle de la directive européenne relativement à la destination des dossiers qui sortent de son territoire.

La deuxième catégorie de règles, soit *l'accès* et la mise à jour, a comme toile de fond le principe que les informations personnelles doivent toujours être à jour avant d'être utilisées, tout en mettant en pratique le principe général de transparence dans la collecte et l'usage des données. Les organismes collecteurs doivent donc s'assurer en tout temps de l'exactitude et de l'actualité des informations qu'ils utilisent.[136]

À cet égard, le Code civil et la loi québécoise confirment tant l'obligation de laisser à l'individu concerné l'accès gratuit et sur demande aux informations le concernant, que son droit de requérir qu'elles soient corrigées en cas d'inexactitude.[137] Il peut de plus demander qu'une information par ailleurs exacte soit retirée de son dossier si sa collecte n'était pas autorisée par la loi (art 28) ou demander qu'y soit ajoutés certains

[134] Id., art 10 ss.
[135] Id., art 17
[136] Id., art 11

commentaires de sa part (CcQ art 40). Tout refus de communication des renseignements doit être motivé par un intérêt sérieux et légitime, par un risque de causer préjudice à un tiers (CcQ art 40) ou par une exception spécifique de la Loi. Le Code, et surtout la loi québécoise, contiennent plusieurs exceptions de cet ordre se rattachent plus particulièrement à des questions de santé, d'enquêtes judiciaires.

La loi québécoise fait découler les restrictions imposées à la *dissémination* des renseignements personnels du principe de confidentialité devant gouverner la conservation des données. Celles-ci devant à défaut demeurer confidentielles, leur usage et leur distribution ne peuvent donc être autorisés que par consentement ou exception. Ainsi, le consentement préalable de l'individu à la distribution d'informations le concernant demeure la clef de voûte de cette partie de l'équation. Elle découle en droit québécois de l'article 37 du Code civil, et notamment des articles 12 à 15 de la loi québécoise. Nous reviendrons plus tard sur la question de la qualité du consentement.

La loi québécoise énonce par ailleurs à son article 18 certaines situations où la communication d'informations peut se faire sans cette autorisation. Il s'agit principalement de cas découlant de l'administration de la justice (al 1° à 4°, 6° et 9°), d'une communication à un organisme public lui-même tenu au respect des termes de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (al 5°), à une situation d'urgence mortelle (al 7°) ou pour des fins d'étude scientifique ou statistique au sens de l'article 21 de la loi (al 8°). L'alinéa 10 permet par ailleurs la communication de listes nominatives sous les conditions spécifiques de l'article 22. Outre ces cas d'exception, le consentement de l'individu sera requis.

2.4.3 Les principes fondamentaux et le droit fédéral canadien

Au niveau fédéral, rappelons que la *LPRP* offre un équivalent à la *Loi sur l'accès* au Québec pour régir l'usage étatique des informations recueillies sur les citoyens. Le volet privé de l'usage des renseignements personnels a récemment été complété par

[137] Id., art 27 et ss. ; CcQ art 38 à 41

l'adoption et la mise en vigueur du controversé projet de loi C-6, introduit dans le contexte de l'essor des inforoutes. Ce projet est le successeur du projet de loi C-54 mort au feuilleton en 1999.

Cette loi fédérale[138] introduit donc en droit fédéral canadien des principes directement puisés à la conception dite européenne de la protection des renseignements personnels. Elle implique même l'inclusion de ces principes dans le droit des différentes provinces et territoires par l'application *a contrario* des dispositions de l'article 30(1) :

> *30. (1) La présente partie ne s'applique pas à une organisation à l'égard des renseignements personnels qu'elle recueille, utilise ou communique dans une province dont la législature a le pouvoir de régir la collecte, l'utilisation ou la communication de tels renseignements, sauf si elle le fait dans le cadre d'une entreprise fédérale ou qu'elle communique ces renseignements pour contrepartie à l'extérieur de cette province.*

Ainsi, C-6 trouve application dans toute province qui n'a pas déjà légiféré dans le domaine de la protection des renseignements personnels tel qu'il y est défini. Dans le cas contraire, elle n'y affecte que les entreprises qui utilisent les renseignements dans le cadre d'activités extra-provinciales et, bien entendu, les entreprises fédérales. Ces exceptions font en sorte d'offrir un arrimage quasi parfait entre C-6 et une loi provinciale régissant le domaine de la protection des renseignements personnels produisant de ce fait un cadre juridique satisfaisant dans une province donnée. Ainsi, les législateurs provinciaux qui voudront légiférer sur la question dans la foulée de l'adoption et de la mise en vigueur de C-6 ne pourront pas beaucoup déroger à ses principes de base. Le droit déjà en vigueur au Québec se rapprochant déjà pas mal de la nouvelle législation fédérale, puisqu'il s'inspire du même courant, les ajustements qui devront y être apporté par parfaire l'ajustement ne seront que mineurs. C'est dans les autres provinces que l'impact de C-6 se fait sentir et suscite le plus de débats.

---

[138] *Loi sur la protection des renseignements personnels et les documents électroniques*. L.C. 2000 c. 5. Sur le Web: http://www.canlii.org/ca/loi/p-8.6/

De façon générale, C-6 codifie par son article 5(1) les principes élaborés dans le *code type sur la protection des renseignements personnels*[139] et oblige toute organisation à s'y conformer.

> ***5.*** *(1) Sous réserve des articles 6 à 9, toute organisation doit se conformer aux obligations énoncées dans l'annexe 1.*

Ce code du CSA, qui est d'ailleurs repris textuellement à l'annexe 1 de la loi[140], s'inspire des lignes directrices de l'OCDE[141] qu'il reprend textuellement à sa propre annexe 1. Le Canada avait déjà adhéré à ces principes en 1984. Le lien de parenté entre ces documents est fermement établi puisque ces mêmes principes de l'OCDE ont également inspiré les lois québécoises en matière de protection des renseignements personnels, ainsi que la *Directive Européenne en matière de protection des données à caractère personnel*[142]. Il ne faut donc pas se surprendre de retrouver dans la loi C-6 à peu près les mêmes principes généraux que nous avons abordés dans notre étude du droit québécois. Aussi nous contenterons-nous de les survoler rapidement.

Les principes du CSA codifiés par C-6 reprennent la nécessité déterminer les fins de la collecte, et de les documenter afin de se conformer aux obligations de transparence imposées à la gestion des informations. Les principes imposent également d'informer le sujet des fins de la collecte au moment où elle se réalise, ainsi que d'un usage postérieur motivé par des fins non-déclarées initialement.

Ces obligations ouvrent la voie à l'adoption du principe du consentement préalable du sujet à la collecte d'informations le concernant, le tout sujet aux quelques exceptions

---

[139] CSA, *Code type pour la protection des renseignements personnels*, http://strategis.ic.gc.ca/SSGF/sf03281f.html

[140] Le code se retrouve également sur le site du CSA à l'adresse http://www.csa.ca/standards/privacy/code/

[141] OCDE, *Lignes Directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel*, http://www.oecd.org/dsti/sti/it/secur/prod/priv-fr.html

[142] *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 caractère personnel et à la libre circulation de ces données*. http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=fr&numdoc=31995L0046&model=guichett

prévues à la loi. Cette législation précise aussi que le consentement peut être retiré à tout moment, confirmant le droit du citoyen au « *opt-out* »[143].

Les principes mènent par la suite aux obligations relatives à la collecte elle-même, à savoir le fait qu'elle doit se limiter à ce qui est nécessaire pour rencontrer les fins déclarées, tant en termes de quantité que dans la nature des informations.

L'usage des informations recueillies est également abordé dans ces principes du CSA codifiés par C-6 :

> *Les renseignements personnels ne doivent pas être utilisés ou communiqués à des fins autres que celles auxquelles ils ont été recueillis à moins que la personne concernée n'y consente ou que la loi ne l'exige. On ne doit conserver les renseignements personnels qu'aussi longtemps que nécessaire pour la réalisation des fins déterminées.*

C-6 confirme également le droit d'un individu d'avoir accès au dossier d'informations recueillies à son sujet, d'en contester l'exactitude et d'en obtenir la correction et de porter plainte en cas de non-respect des principes.

Nous nous permettrons une petite disgression pour noter en terminant que le procédé employé par C-6 d'imposer ses principes par la reprise intégrale en annexe du code type de la CSA nous semble donner des effets plutôt bizarres. En effet, ce dernier a été adopté initialement pour encourager la mise en pratique des lignes directrices de l'OCDE, qui avaient elles-mêmes un objectif d'incitation à l'égard des pays membres de l'organisation. La rédaction du texte est en conséquence prudente et se présente souvent sous forme de conseils, d'exemples ou de commentaires faisant amplement usage du conditionnel (pourrait, devrait, etc...) plutôt que sous forme de règles de droit classiques ordonnées selon la présentation habituelle d'un texte de loi. Par exemple, l'article 4.3 contient une « note », ce qui est déjà inhabituel, comportant des phrases comme celles-ci :

---

[143] *Loi sur la protection des renseignements personnels et les documents électroniques*. L.C. 2000 c. 5. Sur le Web: http://www.canlii.org/ca/loi/p-8.6/, Annexe 1, *Principes énoncés dans la norme nationale du canada intitulée code type sur la protection des renseignements personnels*, CAN/CSA-Q830-96, article 4.3.8

> *Il peut être impossible ou inopportun de chercher à obtenir le consentement d'un mineur, d'une personne gravement malade ou souffrant d'incapacité mentale.*

Ou encore :

> *Par exemple, il peut être peu réaliste pour une oeuvre de bienfaisance ou une entreprise de marketing direct souhaitant acquérir une liste d'envoi d'une autre organisation de chercher à obtenir le consentement des personnes concernées.*

Par exemple aussi, l'article 4.3.6 :

> *4.3.6 La façon dont une organisation obtient le consentement peut varier selon les circonstances et la nature des renseignements recueillis. En général, l'organisation devrait chercher à obtenir un consentement explicite si les renseignements sont susceptibles d'être considérés comme sensibles. Lorsque les renseignements sont moins sensibles, un consentement implicite serait normalement jugé suffisant. Le consentement peut également être donné par un représentant autorisé (détenteur d'une procuration, tuteur).*

Cette situation explique probablement pourquoi le législateur a stipulé qu'une organisation doit : se conformer : « *...aux obligations énoncées dans l'annexe 1* » plutôt que carrément respecter les termes de l'annexe 1. Il est intéressant de constater que la résultante est une obligation pour les organisations de consulter les principes énoncés au code type de la CSA afin d'en dégager les obligations qui en sont l'essence avant de les appliquer. Il faut que le législateur ait eu bien peur des réactions négatives de la part des provinces anglaises réfractaires à l'introduction de lois dans le domaine de la protection des renseignements personnels pour qu'il ait senti le besoin de se reposer sur le code CSA au point de l'intégrer carrément dans C-6 sans lui-même dégager clairement les obligations à respecter.

Il faut espérer que la détermination de la limite entre les obligations et les conseils contenus au code type fera toujours l'unanimité et que ce mode de rédaction législative à rabais n'aura pas trop de conséquences juridiques.

2.5 L'arrimage Europe/Etats-Unis : les accords de Safe Harbour

Nous avons vu précédemment l'existence de courants de pensée en matière de protection des renseignements personnels. Le courant européen, qui prône l'adoption de lois générales pour régir le domaine de la collecte et de la gestion des informations personnelles, et le courant américain qui favorise plutôt l'application de solutions jurisprudentielles issues du droit commun et la génération de règles particulières à chaque domaine d'activité par la voie de l'auto-régulation.

Les grandes disparités législatives, dans le cas de la protection des renseignements personnels qui nous occupe, posent problème dans un environnement global comme le Web. Avant qu'Internet ne soit largement utilisé comme infrastructure de communication, et surtout avant l'invention du Web, les données recueillies par voie électronique étaient surtout destinées à circuler sur des réseaux privés, à valeur ajoutée, établis par les entreprises concernées. Leur échange, bien que grandement facilité par l'utilisation de l'informatique, était beaucoup plus ponctuel. Autrement dit, les échanges survenaient surtout entre les entreprises ayant procédé à la cueillette des informations, dans des circonstances précises. L'échange trans-frontalier d'informations entre entreprises, bien qu'aussi inquiétant pour les individus, était donc un phénomène plus facile à isoler et, à la limite, plus facile à encadrer.

Plus la technologie se développe et fait usage de réseaux ouverts comme le Web, plus la situation se complique. Les informations recueillies sur tout internaute, qu'il en soit conscient ou non, peuvent circuler instantanément entre plusieurs pays. Leur cueillette et leur échange peut donc enjamber les juridictions à la vitesse de l'éclair. Ce phénomène, lié à la mondialisation du commerce fait en sorte d'abattre les contraintes des échanges commerciaux et pourrait mener à la globalisation des banques d'informations sur les individus.

> *«Telematics being by its nature international, the multinational companies in particular have taken advantage of these new technological developments. The extended possibilities to transmit information almost without reference to distance, time or volume has given rise to a*

> *spectacular growth in transborder data flow through the use of the international telecommunication networks. Already in 1985 the volume in Europe alone stood at around 12 million transborder data transactions per day. Gradually the world economy is transforming itself from an industrial-based economy to an information-based economy, in which the free exchange of information has become the life-blood of modern business life.»*[144]

Par définition, tout échange d'information sur le Web aujourd'hui est susceptible d'acquérir un caractère international, tant directement qu'indirectement. Le commerce électronique international, l'hébergement des sites ou la localisation des serveurs à l'étranger, la gestion de l'information par des compagnies mandataires situées dans d'autres pays ou encore le partage d'information entre compagnies d'un même groupe multinational sont autant de facteurs pouvant permettre de telles situations.

On peut comprendre, dans un tel contexte, l'importance d'en arriver à un traitement juridique, sinon identique, au moins compatible entre les différentes juridictions. Le contraire équivaudrait à créer des conflits de lois encore plus dommageables qu'un vide juridique. L'arrimage entre les normes des différents États est donc ici fondamental.

Le désaccord entre ces deux philosophies d'intervention juridique s'est cristallisé de façon plus particulière depuis l'adoption de la directive européenne,[145] et surtout autour de son article 25. Voyons-en le principe général à l'alinéa 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*

---

[144] A.C.M. NUTGER, *Transborder Flow of Personal Data Within the EC*, Deventer, Kluwer, 1990, p.1; cité par Karim BENYEKHLEF, Les *normes internationales de protection des données personnelles et l'autoroute de l'information,* http://www.canada.justice.gc.ca/fr/cons/jae/karim.html#recueillies

[145] "*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 caractère personnel et à la libre circulation de ces données*. http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=fr&numdoc=31995L0046&model=guichett

> *application des autres dispositions de la présente directive, le pays tiers en question assure un niveau de protection adéquat.*

La portée de la directive se trouvait donc augmentée de manière presque planétaire, ce qui devait causer problème en matière de transfert de données vers les États-Unis qui étaient dépourvus de lois gouvernant la protection des renseignements personnels.

La directive précise également des critères pour déterminer le caractère adéquat du niveau de protection offert par un pays tiers donné. Elle stipule que : « toutes les circonstances relatives à un transfert ou à une catégorie de transferts de données; en particulier, sont prises en considération », notamment : « les règles de droit, générales ou sectorielles, en vigueur ». L'absence d'une législation générale en matière de protection des données personnelles aux États-Unis causait donc problème et pouvait à la limite handicaper sérieusement les transactions commerciales des entreprises américaines sur le marché européen.

Le compromis intervenu entre la communauté européenne et le département du commerce des États-Unis sous la désignation de « *Safe Harbour Principles* »[146] consiste en l'établissement de règles de base en matière de gestion des renseignements personnels, auxquelles les entreprises américaines ont la possibilité de souscrire sur une base volontaire[147]. Ces principes peuvent ensuite faire l'objet d'une déclaration d'approbation en vertu de l'article 25.6 de la Directive Européenne, permettant aux entreprises qui y auront souscrits de montrer patte blanche quant à leur traitement adéquat des informations personnelles auprès des autorités européennes. La décision de la communauté Européenne entérinant cette entente a été rendue[148], reconnaissant que ces principes de Safe-Harbour fournissent un niveau de protection adéquat aux termes de la Directive et permettant les transferts de renseignements personnels vers les entreprises américaines qui y souscrivent. Nous voyons donc ici un arrimage osé entre les tenants de l'imposition d'un cadre législatif

[146] http://www.export.gov/safeharbor/
[147] CONSEIL DE L'EUROPE, *US safe harbour arrangement, draft discussion documents*, 19 November 1999, http://europa.eu.int/comm/internal_market/en/dataprot/news/harbor2.htm
[148] CONSEIL DE L'EUROPE, Décision de la Commission des communautés Européennes, http://europa.eu.int/comm/internal_market/en/dataprot/news/decision_fr.pdf

et les défenseurs de l'auto-régulation. En effet l'adhésion est volontaire, mais les principes s'inspirent directement de ceux défendus par la Directive.

Aux termes du *Safe Harbour*, les entreprises devront en effet s'astreindre aux obligations suivantes :

- informer les individus faisant l'objet de la cueillette de renseignements de la finalité de l'opération, de la façon de contacter les responsables et d'acheminer de splaintes et de fournir la liste des tiers vers lesquels ces informations pourraient éventuellement être transférées;

- l'obligation d'obtenir le consentement préalable de l'individu au transfert de ses données personnelles ou à leur usage à des fins autres que celles déclarées initialement (« *opt-in* »), ainsi que de leur donner le droit de retirer subséquemment leur consentement (« *opt-out* »);

- accorder aux individus l'accès à leur dossier, ainsi que le droit sous certaines conditions de requérir que soit corrigées, amendées ou détruites les informations inexactes;

- entourer la gestion des dossiers de mesures de sécurité raisonnables garantissant leur protection et leur intégrité;

- se prêter à des mesures de contrôle permettant de sanctionner les manquements à ces engagements, et fournir annuellement à cet effet une attestation émanant d'un organisme de vérification indépendant[149].

Le pari apparaît risqué, mais intéressant. À ce jour, environ cent-trente entreprises américaines ont adhéré au programme[150]. Rien n'est encore joué. Nous relevons aussi l'obligation qui résulte pour le consommateur européen de vérifier le statut d'une entreprise américaine avec laquelle il veut transiger au chapitre des principes *Safe Harbour*[151]. Reste à voir l'effet réel qu'il aura sur les échanges internationaux de données personnelles ayant cours sur le Web.

***

[149] US DEPARTMENT OF COMMERCE, *Safe Harbor Overview*, http://www.export.gov/safeharbor/sh_overview.html
[150] http://web.ita.doc.gov/safeharbor/shlist.nsf/webPages/safe+harbor+list
[151] Yves POULLET, *Les Safe Harbor Principles - Une protection adéquate?,* Juriscom.net, 17 juin 2000, http://www.juriscom.net/uni/doc/20000617.htm

CHAPITRE 3- Analyse et critique de la norme P3P

3.1 Présentation générale de P3P

P3P veut être une solution auto-régulatrice à la problématique de la vie privée sur le Web. Pour ce faire, ses concepteurs ont choisi de créer une plate-forme devant encadrer globalement tous les échanges d'informations sur les internautes. P3P dépasse donc l'encadrement de la simple cueillette d'informations, car il fournit un cadre technique commun et normalisé au sein duquel les informations pourront être comprises et traitées par les systèmes à l'aide des divers logiciels et applications qui s'y conformeront.

Daniel J. Weitzner, directeur des activités du domaine « technologie et sociétés » du W3C[152], exposait de façon précise les objectifs du projet P3P devant la conférence des procureurs généraux des Etats-Unis. Voici ce qu'il en disait d'après le contenu des ses diapositives de présentation[153] disponibles sur le Web :

> The Goal of P3P -- Meet Increasing User Privacy Demands
>
> *Use the power of the Web to:* *enhance notice*
>
> *enable choice*
>
> *Streamline ecommerce transactions*
>
> *Framework for global privacy*

Ces énoncés impliquent que l'implantation de P3P permettra non seulement, si les objectifs sont remplis, de protéger la vie privée des internautes en poussant l'usage d'un cadre technique pour la cueillette et l'usage de renseignements personnels. Il contribuerait à faire aussi en sorte d'éviter que le règlement de cette épineuse question nuise à la convivialité du Web, au développement du commerce électronique et à la liberté de navigation dans le cyberespace par l'encadrement automatique et transparent des échanges d'informations et l'usage d'une solution technique intégrée à

[152] http://www.w3.org/TandS/

[153] Daniel WEITZNER'S P3P: *User Empowerment Tools for Web Privacy*, http://www.w3.org/P3P/naag-p3p.ppt, slides presented at 23 April 2001 National Association of Attorneys General meeting [PowerPoint slides]

la structure même du réseau. Les notes de Weitzner suggèrent aussi que P3P veut proposer une structure globale à la protection de la vie privée dans le cyberespace, à laquelle pourront s'intégrer d'autres composantes.

L'implantation d'un protocole normalisé pour l'organisation de l'information accumulée sur les internautes entraîne des conséquences plus grandes qu'on pourrait l'imaginer à prime abord. En effet le commerce des renseignements personnels glanés sur le Web a réussi à devenir à ce point florissant qu'il a attisé les inquiétudes des internautes et attire l'attention des gouvernements, et cela même si les données ont été accumulées selon des formats et des structures variant d'un système à l'autre. L'implantation d'une structure normalisée pour ces données, qui implique l'organisation des renseignements personnels selon un même schéma d'une banque de données à l'autre, ne pourra que faciliter leur partage. Dans le meilleur des mondes, un tel état de fait pourra alimenter le développement du Web, encourager la croissance du commerce électronique et faciliter l'accès aux nouvelles technologies par une plus grande convivialité. Il faut néanmoins garder à l'esprit qu'une telle normalisation pourra rendre la situation encore plus dangereuse si le cadre juridique entourant les échanges n'est pas rendu plus étanche,. Cet aspect est à notre avis capital pour comprendre la stratégie de mise en oeuvre du projet adopté par le W3C.

Afin de mettre en évidence les aspects les plus pertinents à l'analyse légale de la situation engendrée, nous axerons l'analyse sur les fonctions recherchées par P3P plutôt que sur une description élaborée de tous ses aspects techniques. Nous présenterons donc les principales fonctions que P3P se propose de remplir en expliquant les moyens techniques utilisés. Ceci permettra de mettre en relief les motivations et la stratégie de mise en vigueur de P3P.

L'idée générale ayant guidé la formation du projet P3P est que l'ordinateur de l'internaute et le serveur qu'il visite pourraient, au moment où le contact s'établit entre eux, vérifier automatiquement si les pratiques du site quant à la cueillette et l'usage d'informations personnelles correspondent aux désirs du visiteur. La cueillette et l'usage de renseignements sur les individus nécessitant généralement l'obtention du

consentement de l'intéressé, les concepteurs du projet P3P cherchaient à permettre que ce consentement puisse être fourni par son ordinateur après vérification automatique de la politique de vie privée du site visité. En plus de permettre l'automatisation et idéalement la normalisation de ce processus de négociation et de consentement dans le cas de cueillette d'informations personnelles sur le Web, ce cadre devait aussi éviter à l'internaute la fastidieuse tâche de saisir à tout moment ses coordonnées personnelles. Par cet élément, P3P cherchait à encourager le développement du Web commercial en facilitant et en accélérant la conclusion des transactions.

Nous verrons que le W3C a finalement choisi d'implanter P3P par étapes. Pour les fins de cette recherche, et afin également de mieux voir venir les conséquences qui pourraient découler de la mise en oeuvre des fonctions laissées en suspens, nous prendrons en considération le projet original tel qu'il a été conçu par ses artisans.

Les détails de cette plate-forme P3P, telle que mise en vigueur par le W3C, se retrouvent dans le document " *The Platform for Privacy Preferences 1.0 (P3P1.0) Specification* " du 15 décembre 2000[154], et dans un document de corrections mis à jour périodiquement intitulé " *Updates to the 15 December 2000 P3P1.0 Candidate Recommendation* " dont la dernière version date du 23 août 2001. Ces documents contiennent la description des éléments de P3P adoptés et en vigueur à l'été 2001. Les corrections contenues au deuxième document, ainsi que certaines autres corrections mineures ont fait l'objet d'une version refondue en date du 28 septembre 2001[155]. Pour alléger notre texte, nous référerons désormais à ces documents et à ces éléments par le terme P3P 1.0 et continuerons de faire référence au document existant au jour de la mise en vigueur, à moins des changements importants ne soient apparus à la version subséquente.

Nous pouvons isoler cinq fonctions principales que P3P doit remplir afin de se conformer à la vision initiale de ses créateurs : information, négociation, entente, transmission des informations, vérification des pratiques. Chacune de ces fonctions

[154] http://www.w3.org/TR/2000/CR-P3P-20001215/

doit être remplie en faisant appel à des éléments techniques ou architecturaux précis du protocole. Nous procéderons à l'examen de ces éléments au fur et à mesure où les fonctions principales du projet entrent en scène dans la procédure proposée.

Les principales problématiques relatives à la protection de la vie privée sur le Web ont pris naissance dès les débuts du réseau, sans même que le public n'y prête vraiment attention. Bien peu de gens en dehors des cercles d'initiés connaissaient par exemple l'existence des témoins, leur véritable rôle, et encore moins les fonctions nouvelles qui leurs ont été confiées dans la construction d'empires du renseignement comme celui bâti par le courtier publicitaire *Doubleclick*.

Les efforts menés par plusieurs instances gouvernementales comme la FTC[156], de nombreux groupes de pression ainsi que l'attention des médias qui s'est tournée vers ce phénomène à la faveur de la croissance du nombre d'internautes a cependant fait en sorte de forcer les opérateurs de sites à se sensibiliser à la question. La multiplication des cas problèmes a finalement nourri dans l'opinion publique le sentiment que quelque chose ne tournait pas rond sur le Web et qu'il valait peut-être mieux être prudent avant d'y inscrire son pedigree.

Les opérateurs de sites Web sérieux ont donc souhaité montrer patte blanche afin de sécuriser leurs clients quant à la cueillette et à l'usage de renseignements personnels les concernant et de préserver ou même augmenter leur chiffre d'affaires. La plupart, sinon tous, se sont donc pliés de bonne grâce à la suggestion de la FTC qui souhaitait voir l'apparition de codes de bonne conduite en matière de traitement des informations personnelles sur le Web. La préparation et la publication sur les sites de politiques de vie privée venait donc incarner cette volonté du réseau de s'auto réglementer afin de rassurer les clients et de satisfaire les gouvernements.

Cette façon de faire s'inscrivait dans la logique de la position traditionnelle américaine de favoriser l'adoption de normes auto-régulatoires. Il est cependant intéressant de souligner que bien que de nombreux sites opérés dans des pays

[155] http://www.w3.org/TR/2001/WD-P3P-20010928/
[156] Federal Trade Commission, http://www.ftc.gov

s'inscrivant plutôt dans la tradition européenne ont également emboîté le pas malgré le fait qu'ils restaient de toutes façons régis par leurs lois nationales spécifiques. Globalisation, effet d'entraînement, goût du jour... allez donc savoir. Le fait demeure que la période d'absence totale d'intervention en matière de vie privée qui a caractérisé les débuts du Web a été suivie par une période d'affichage frénétique de politiques de vie privée.

Mais ce n'était pas suffisant, car même si un site affiche ses intentions dans de telles politiques, encore faut-il qu'elles respectent la loi et qu'elles soient mises en pratique par leur auteur. De plus, ces documents ne sont pas vraiment utiles si les internautes ne les consultent pas ou n'y comprennent rien. Il faut d'ailleurs constater que la présence d'une politique de vie privée n'a pas entièrement fait disparaître les cas problèmes, La facilité et le peu de scrupules qu'ont eues certains sites à modifier unilatéralement leurs dites politiques témoigne de façon éloquentes des faiblesses de ce système. Pensons par exemple à *Ebay*[157] qui modifiait unilatéralement sa politique de vie privée au printemps 2001, pour permettre désormais le partage des informations recueillies advenant la vente de la compagnie[158]. De telles situations inquiètent, notamment la FTC qui compte voir au respect des politiques de vie privée affichées sur les sites, surtout dans les cas de vente ou de faillite des entreprises qui les opèrent :

> *"Problems that arise in bankruptcy or reorganization are of particular concern. Companies that promise confidentiality may decide to sell or transfer personal information they have collected. If confidentiality promises are to be meaningful, then they must survive when the company is sold or reorganized.*[159]*"*

P3P a donc comme première fonction d'informer les usagers sur les pratiques de confidentialité en vigueur sur les sites qu'ils visitent. Nous pourrions aussi dire que P3P cherche tout d'abord à établir entre les sites et leurs visiteurs un mode de

[157] http://www.ebay.com/
[158] Jeffrey BENNER, *EBay Alters Privacy Policy*, Wired News, http://www.wired.com/news/business/0,1367,42778,00.html
[159] MURIS, Timothy J. (Chairman Federal Trade Commission), *Protecting Consumers' Privacy: 2002 and Beyond*, The Privacy 2001 Conference, Cleveland, Ohio, October 4, 2001, http://www.ftc.gov/speeches/muris/privisp1002.htm

communication commun et reconnu par tous comme préalable à toute transmission d'information. Pour ce faire, la plate-forme se fonde sur le langage XML, dernière évolution des langages de balisage de données, afin de structurer les échanges d'information en des séquences normalisées comprises et organisées de la même façon par tous les intervenants.

3.1.1 Vocabulaire, syntaxe et procédure

Pour aspirer au degré d'efficacité essentiel à son succès, P3P doit reposer sur un vocabulaire et une syntaxe adéquats. À cet égard, la documentation de P3P 1.0 énonce :

> *The P3P1.0 specification defines the syntax and semantics of P3P privacy policies, and the mechanisms for associating policies with Web resources. P3P policies consist of statements made using the P3P vocabulary for expressing privacy practices. P3P policies also reference elements of the P3P base data schema -- a standard set of data elements that all P3P user agents should be aware of. The P3P specification includes a mechanism for defining new data elements and data sets, and a simple mechanism that allows for extensions to the P3P vocabulary.*[160]

Nous y retrouvons les caractéristiques fondamentales du XML, soit la définition d'un vocabulaire commun servant à exprimer les politiques de vie privée dans un langage compréhensible aux ordinateurs, l'établissement d'un schéma de données standardisé ainsi que la possibilité d'ajouter au vocabulaire de base afin de tirer profit au maximum des possibilités offerte par le langage. Nous passerons en revue les principaux termes de ce vocabulaire en examinant la politique de P3P dans la section « *Politiques P3P»* ci-dessous

La première étape de la procédure générale du protocole est la vérification de la présence d'une politique P3P sur le site auquel le visiteur souhaite accéder. Il s'agit, nous le verrons, d'un document équivalent à une politique de vie privée, mais qui est cette fois exprimé en langage XML de façon à pouvoir être lu, compris et analysé par un programme d'ordinateur.

[160] http://www.w3.org/TR/P3P/#P3P1.0

Cette politique devra être accessible selon une des trois voies offertes par le protocole :

- dans un endroit prédéterminé bien connu (“ *predefined well-known location* ”)
- dans un répertoire indiqué au moyen d’une balise HTML *link*
- dans une entête de page sous HTTP.

Les agents logiciels installés sur les ordinateurs des usagers devront néanmoins supporter les trois modes de recherche des politiques afin de se conformer à la norme. Dans le premier cas, l’endroit prédéterminé sera simplement un document nommé *p3p.xml*, placé dans un répertoire nommé *W3C* du répertoire général du site. Cette façon de faire, bien qu’elle ne soit pas obligatoire, constitue la façon la meilleure d’assurer que la politique P3P soit accessible aux ordinateurs des usagers. Elle offre de plus une excellente flexibilité aux opérateurs de sites, en leur permettant de conserver des politiques différentes pour chacun des sites qu’ils exploitent.

Dans le cas des entêtes HTTP et des balises HTML *link*, il s’agit de deux façons différentes permettant de rediriger les agents logiciels des usagers vers le répertoire où ils trouveront la politique P3P qu’ils recherchent. Elles permettent, par exemple, aux concepteurs de sites de diriger les visiteurs de tous les sites exploités par un opérateur vers une politique P3P commune conservée et mise à jour en un seul endroit. Elles ne se distinguent entre elles que par des éléments informatiques particuliers qui ne changent rien à l’application de la norme pour nos fins.

Le système utilise, pour permettre de retracer les politiques applicables, des fichiers de référence nommés “ *policy reference file* ”. En fait, c’est ce type de document qui sera retracé au départ. Il fournira les informations suivantes :

- L’adresse exacte du répertoire où la politique comme telle est conservée;
- Les URI (*Uniform Ressource Identifier*) ou les parties d’URI qui sont couverts ou exclus de l’application des termes de cette politique qu’ils se trouvent sur le même serveur ou sur le serveur d’une tierce partie ;

- Les témoins qui sont couverts ou exclus de l'application des termes de cette politique ;
- Les moyens d'accéder à la politique ;
- La période de temps pendant laquelle les engagements contenus dans la politique restent valides.

Le protocole appelle par la suite à la lecture de la politique P3P par l'agent logiciel installé sur l'ordinateur de l'usager, et à sa comparaison au document préparé par l'usager pour contenir son profil de préférences quant à la collecte et l'usage de ses renseignements personnels. Cet agent logiciel peut être tout simplement faire partie d'un navigateur habituel compatible au protocole P3P (comme Internet Explorer 6.0 par exemple) et permettre d'interpréter les politiques des sites. Il peut s'agir également d'un logiciel indépendant ne servant qu'à ces fonctions spécifiques, comme *IDcide* par exemple.[161] L'usager pourra donc théoriquement choisir entre divers produits pour le " représenter " dans la lecture et l'analyse des politiques P3P.

3.2 Politiques P3P

Le terme *policy* est ainsi défini par le W3C :

> ***Policy*** *A collection of one or more privacy statements together with information asserting the identity, URI, assurances, and dispute resolution procedures of the service covered by the policy.*[162]

La politique sera donc composée d'un ou plusieurs « *privacy statements* » et informations qui permettront d'identifier et de localiser le « service » visité, ses garanties (« *assurances* ») quant à ses engagements au niveau de la résolution des conflits potentiels. Qu'est-ce donc qu'un « *privacy statements* »? Il faut consulter deux définitions contenues dans la spécification pour le découvrir :

> ***Statement*** *A P3P statement is a set of privacy practice disclosures relevant to a collection of data elements.*[163]

[161] www.idcide.com
[162] http://www.w3.org/TR/P3P/#Terminology, sous « policy »
[163] Id., sous « statement »

> ***Practice*** *The set of disclosures regarding data usage, including purpose, recipients, and other disclosures.*[164]

Les « *privacy statements »* constituent donc une déclaration relative aux pratiques du service quant à l'usage des données, notamment quant aux buts de l'opération et aux destinataires de l'information, applicables à une collection donnée d'éléments d'information. Une politique pourra donc être composée d'une ou plusieurs telles déclarations, s'appliquant chacune à une collection d'informations. Pour simplifier la lecture de ce texte, notons que nous ferons fi de cette distinction à moins qu'elle n'entraîne une conséquence particulière. Nous nous contenterons d'utiliser simplement le terme « politique ».

Nous retrouvons dans cette définition de *« policy »* certains éléments de base de P3P. Les engagements principaux qui intéresseront l'usager se retrouvant dans les déclarations d'identité et de localisation du site, celles relatives aux informations recueillies et à leur gestion (« *assurances* »), ainsi que dans la référence à un mode de résolution de conflits.

Cette dernière mention préfigure d'ailleurs l'épineuse question de la vérification du respect des engagements. Le reproche principal qui a été formulé envers P3P tient au fait qu'il ne prévoit aucun mécanisme obligatoire de vérification du respect effectif des engagements pris par les sites tels que déclarés dans les politiques P3P. Faut-il voir ici une suggestion quasi-subliminale du W3C aux services Web de traiter de la question du contrôle des engagements par l'inclusion de déclarations relatives au règlement des conflits? Nous aurons l'occasion d'y revenir.

3.2.1 « Service »

Nous devons maintenant préciser la notion de « service » apparaissant à la définition du W3C. Nous avons jusqu'à présent fait référence aux obligations des sites ou de leurs opérateurs dans le cadre du protocole P3P. Il importe ici de nuancer cette notion en regard des définitions exactes fournies par le W3C, afin de bien cerner ceux qui

[164] Id.sous « practise »

seront tenus à ces obligations. Nous devons ici examiner deux définitions, celles de « *service*» et de « *service provider* ».

> ***Service*** *A program that issues policies and (possibly) data requests. By this definition, a service may be a server (site), a local application, a piece of locally active code, such as an ActiveX control or Java applet, or even another user agent.*
>
> ***Service Provider (Data Controller, Legal Entity)*** *The person or legal entity which offers information, products or services from a Web site, collects information, and is responsible for the representations made in a practice statement.*

En utilisant le terme "*service*" pour désigner l'objet qui doit soumettre une politique P3P à l'examen d'un usager, le W3C cherche à élargir le plus possible l'application du protocole et à lui conférer le plus de souplesse possible. Les conditions et engagements pourront en effet varier d'un service à un autre sur un même site Web. Un « *service* » pourra donc s'entendre d'un site Web, d'un logiciel ou d'un code secondaire comme des *Applets Java* ou des contrôles *ActiveX*, ou d'autres agents. Le W3C fait ici preuve de neutralité technologique en refusant de fermer son énumération de façon trop précise.

Il est évident qu'au niveau juridique, seul le fournisseur de tels services peut s'engager dans des obligations envers le visiteur, et encourir une quelconque responsabilité contractuelle envers ce dernier. Nous sommes donc justifiés de rechercher si le lien de responsabilité entre le service et son fournisseur est suffisamment bien établi selon le W3C. Ce lien et cette responsabilité du fournisseur face aux déclarations faites et aux engagements pris par son « *service* » aux termes des politiques P3P apparaît clairement, bien qu'un peu maladroitement, dans les définitions préliminaires contenues au document relatant la spécification P3P 1.0.

Ainsi, la définition de « *policy* » donne l'obligation de déclarer l'identité du service ainsi que son URI (*Uniform Resource Identifier* qui permet de retracer les ressources sur le Web). Elle n'exige pas que la politique identifie et fournisse les coordonnées du fournisseur de service qui en est responsable, ce qu'un juriste serait très intéressé à retrouver non seulement afin de pouvoir retracer le fournisseur, mais pour en déduire

une déclaration claire et non équivoque de sa responsabilité face aux engagements souscrits par le « service » qu'il a mis en ligne. Ce lien de « paternité » entre le fournisseur et son service se retrouve donc ailleurs, notamment dans la définition de fournisseur de service (« *service provider* »).

Il importe au départ d'éviter toute confusion entre ce fournisseur de service au sens de P3P, et l'expression générale " fournisseur de service Internet " qui réfère dans le langage commun à un fournisseur d'accès. Il est évident que P3P ne vise pas à rendre responsable les entreprises qui n'offrent que des connexions au réseau, sauf en ce qui concerne leur propre collecte et usage de renseignements personnels par le biais des services qu'elles pourraient par ailleurs offrir sur le Web.

Réexaminons maintenant la définition de « *service provider* » proposée par le W3C :*"The person or legal entity which offers information, products or services from a Web site [...]"* Il s'agit donc bel et bien de toute personne (morale ou physique si nous nous référons à notre droit civil) qui offre de l'information, des produits ou des services sur le Web. L'utilisation du mot « services » à ce stade-ci s'avère malheureuse puisqu'il ne s'agit manifestement pas seulement des « services » tels que définis par P3P 1.0, mais bien du terme général utilisé dans le langage commun. En effet, le contraire reviendrait à définir le fournisseur de service (au sens de P3P) comme une personne qui fournit des services au sens de P3P... Le mot « services » doit donc ici être compris dans son sens le plus large (ex. vente de biens et services).

Cette personne, dans le cadre de ces activités, doit également recueillir de l'information (« *collects information »).* Il semble un peu superflu de préciser que si aucune collecte d'information n'a lieu, l'application de P3P n'a pas d'utilité. Pourtant, il faut garder à l'esprit que la simple opération d'un site Web implique nécessairement la collecte d'un minimum d'information sur les visiteurs, ne serait-ce que pour établir et maintenir la connexion. Ce qui ne veut pas dire que ces informations seront conservées une fois la session terminée, ni qu'elles seront accumulées, partagées ou même revendues à des tiers. De plus, le fait qu'un site donné ne s'adonne pas à de telles pratiques ne sera pas connu du visiteur si le fait

n'est pas déclaré. Il ne faut donc pas se surprendre de voir cette condition « ...collects information... » être applicable à tous les sites ou presque.

Finalement, nous touchons au but avec la troisième caractéristique déclarée du fournisseur de service dans la définition du W3C : « *... and is responsible for the representations made in a practice statement. »*" Le fournisseur de service est donc la personne qui se porte responsable des déclarations intégrées à la politique. Ainsi, si la responsabilité du fournisseur quant aux engagements souscrits par son « service » apparaît clairement dans cette définition, il y a quand même un problème quant à l'identification de ce fournisseur. En effet, rien ne semble obliger un fournisseur à déclarer son identité ou sa « paternité » face à un service donné.

Le lien entre le fournisseur et son service, essentiel pour obtenir le respect des engagements souscrits envers un usager, n'est pas établi de façon suffisamment claire à la face même des documents du W3C. Il est clair qu'en droit un « service » tel que défini par le W3C ne peut exister par lui-même et que son propriétaire devrait normalement être tenu responsable de ses agissements et tenu de respecter ses engagements. L'usager devra probablement avoir recours aux règles générales du droit civil pour y parvenir, car P3P semble être dépourvu d'engagements clairs à cet égard. Il est dommage que les définitions contenues aux documents décrivant P3P 1.0 ne soient pas aussi claires que lorsqu'elles définissent le lien entre l'agent logiciel de l'usager et ce dernier :

> ***User*** *An individual (or group of individuals acting as a single entity) on whose behalf a service is accessed and for which personal data exists.*
>
> ***User Agent*** *A program whose purpose is to mediate interactions with services on behalf of the user under the user's preferences. A user may have more than one user agent, and agents need not reside on the user's desktop, but any agent must be controlled by and act on behalf of only the user. The trust relationship between a user and his or her agent may be governed by constraints outside of P3P. For instance, an agent may be trusted as a part of the user's operating system or Web client, or as a part of the terms and conditions of an ISP or privacy proxy.* (nos soulignements)

3.2.2 Contenu

Voyons maintenant ce que devra contenir cette politique, et comment ses éléments seront structurés. Tout d'abord, il est important de noter que les éléments de contenu des politiques doivent être lus et analysés dans un ordre prédéterminé. Ainsi, non seulement les seuls éléments de la politique P3P reflètent-ils la politique de vie privée du service, mais l'ordre dans lequel ils y sont placés pourra jouer un rôle déterminant dans la traduction en langage informatique des choix de l'opérateur du service.

Les politiques P3P s'articulent autour d'une série d'éléments qui définissent les choix pris par le service visé dans sa gestion des renseignements personnels recueillis sur ses visiteurs. Les différentes actions qu'un service peut poser à l'égard de renseignements personnels ainsi que les autres informations requises pour décoder sa politique de vie privée sont donc décortiquées en éléments uniformisés. L'ajout entre les balises de ces éléments d'un sous-élément définissant la pratique du service à ce sujet ou fournissant l'information requise, vient compléter la politique. Par exemple l'insertion du sous-élément *none* entre les balises de l'élément *access :*

```
<ACCESS> <NONE/><ACCESS/>
```

signifiera que le service n'offre pas à ses visiteurs la possibilité d'accéder aux renseignements colligés sur eux, alors que le sous-élément *all* :

```
<ACCESS> <ALL/><ACCESS/>
```

aurait signifié que l'usager pouvait consulter toutes les informations le concernant.

De tels éléments peuvent se classer au chapitre de la politique (*policy*) générale du service, ou des déclarations (*statements*) particulières relatives à certaines catégories de données. Voyons-les plus en détails.

3.2.3 Éléments de politiques

Les éléments de politiques sont les suivants : <POLICY>, <POLICIES>, <TEST>, <ENTITY>, <ACCESS>, <DISPUTES>, et <REMEDIES>.

<POLICY> : Élément fondamental s'il en est un, il contient des informations obligatoires comme le nom de l'opérateur et ses coordonnées, la règle de base régissant le droit d'accès aux informations recueillies et des éléments optionnels comme une liste des déclarations (*statements*) qui s'y rattachent, la durée de validité de la politique, la référence à un schème de données (*data schema*) particulier à ce service ou des extensions qui y sont utilisées. Cet élément <POLICY> est obligatoire et doit fournir à lui seul la politique de base du service :

> *The <POLICY> element contains a complete P3P policy. Each P3P policy MUST contain exactly one <POLICY> element.*[165]

Certaines des stipulations tombant dans cet élément <POLICY> sont elles-mêmes définies en tant qu'*attributs* :

> L'attribut **`discuri`** **(***obligatoire***)** fournit l'URI de la politique de vie privée traduisant en langage naturel le contenu de la politique P3P;

L'attribut **`opturi`** dirige vers l'URI contenant les instructions à suivre pour un usager qui souhaite se prévaloir d'un choix (« *opt-in » or « opt-out »*) qui lui est offert à l'égard de certains usages de ses renseignements personnels. Cet attribut ne sera obligatoire que si un élément <PURPOSE> exigeant un tel choix de l'usager est inclus à la politique.

> L'attribut **`name`** donne le nom qui est donné à la politique afin de faciliter son identification. Cet attribut ne sera obligatoire que si plusieurs politiques sont en place et identifiées dans un élément <POLICIES>.

<POLICIES> : servira le cas échéant au regroupement de plusieurs politiques en une, par exemple dans des cas où plusieurs services sont opérés par un même opérateur.

---

[165] http://www.w3.org/TR/P3P/#POLICY

L'agent logiciel qui lira la politique pour le compte du visiteur saura, par la présence et le contenu d'un tel élément, que plusieurs politiques doivent être obtenues et combinées pour fournir le portrait global.

< ENTITY > : Cet élément contient des déclarations relatives aux nom et adresse de la personne qui fait les affirmations contenues dans la politique. On pourrait interpréter cet élément comme constituant la signature de l'opération du service.

<ACCESS> *:* Cet élément servira à fournir les règles gouvernant l'accès des usagers aux informations accumulées à leur sujet.

Pour être plus précis, le protocole fait ici référence à la notion de *Identifiable Information*. C'est donc l'accès à ce type d'informations qui est régi par l'élément <ACCESS>. Le juriste est tenté de traduire d'emblée ce terme par " information nominative ", en faisant référence au concept juridique de renseignement personnel. Nous savons de façon générale qu'un tel renseignement est défini dans la loi québécoise[166] comme étant tout renseignement qui concerne une personne physique et permet de l'identifier. Le protocole, bizarrement, ne fournit pas de définition formelle de *Identifiable Information*, son glossaire définissant plutôt *Personally Identifiable Data*.

> ***Personally Identifiable Data*** *: Any information relating to an identified or identifiable individual.*

Présumons donc que ces notions sont équivalentes et interchangeables dans l'esprit du W3C. Nous constatons alors que l'élément <ACCESS> régit le droit d'accès à toutes informations relatives à un individu identifié ou identifiable, et non pas aux seules informations qui pourraient permettre d'identifier une personne physique. Cette notion semble donc dépasser la notion de renseignement personnel fournie par la loi québécoise. Nous notons de plus une similarité entre cette définition et celle de C-6, qui englobe sauf quelques exceptions " *Tout renseignement concernant un individu identifiable,...* ". Nous emploierons donc dans ce texte l'expression *information identifiable* afin de marquer la distinction entre les différents concepts.

---

[166] *Loi sur la protection des renseignements personnels dans le secteur privé* LRQ c. P-39.1; sur le Web : http://www.canlii.org/qc/loi/p39.1/, article 2

Cet élément <ACCESS> est obligatoire, les services devant déclarer s'ils consentent un tel droit d'accès ou non, qui peut en bénéficier et à quel type d'information il aura accès. Ces déclarations sont faites en utilisant un des sous-éléments suivants :

> **<nonident/>** : Le site ne recueille aucune information identifiable, rendant superflue l'octroi d'un droit d'accès;
>
> **<all/>** : L'Usager peut accéder à la totalité des informations le concernant;
>
> **<contact-and-other/>** : L'usager peut consulter les informations relatives à ses coordonnées physiques (adresse, téléphone, etc...) et virtuelles (courriel, URI, etc...) ainsi qu'aux autres informations identifiables le concernant;
>
> **<ident-contact/>** : L'usager ne peut consulter que les informations relatives à ses coordonnées physiques et virtuelles;
>
> **<other-ident/>** : L'usager ne peut consulter que certaines informations identifiables le concernant, par exemple leur dossier d'achat avec le service en question;
>
> **<none/>** : Le service ne permet l'accès à aucune information sur les usagers.

< DISPUTES >[167] Cet élément est lui aussi obligatoire, c'est-à-dire que le service devra statuer sur le mode de règlement des conflits qui pourront naître de ses relations avec ses visiteurs dans le domaine de la confidentialité ou en cas de violation des protocoles. En réalité, la politique devra contenir un groupe nommé <DISPUTES-GROUP>, qui contiendra au moins un élément < DISPUTES >.

Cette façon de faire permettra aux services de se doter de règles plus ou moins détaillées en la matière, selon le type d'activité qu'ils exercent et, pourquoi pas, selon les juridictions où leurs activités sont exercées. À première vue, l'observateur pourrait voir ici une première façon d'introduire dans l'application de P3P des éléments particuliers à un système de droit national donné.

Le premier sous-élément de l'élément < DISPUTES > est obligatoire. Il s'agit de l'élément <**resolution-type**>, qui semble avoir pour but de procéder à un choix de mode de résolution des conflits potentiels entre le service et ses usagers. La politique devra donc obligatoirement fournir une réponse à cet élément, par l'insertion de l'une des quatre valeurs suivantes : [service], [independent], [court] ou [law]. Contentons-

[167] http://www.w3.org/TR/P3P/#DISPUTES

nous de résumer l'usage qui semble être réservé à chacun par le W3C, ou du moins l'intention qui semble se dégager de leur description contenue au texte de la plate-forme, avant de les commenter en bloc. Pour ce faire nous choisissons d'utiliser le texte anglais décrivant ces valeurs dans la description de la plate-forme, afin de vous permettre de l'apprécier à sa juste valeur :

> `[service]` Individual may complain to the Web site's customer service representative for resolution of disputes regarding the use of collected data. The description MUST include information about how to contact customer service. (Note: la description devra alors contenir le sous-élément <service> qui fournira les coordonnées du service à la clientèle.)
>
> `[independent]` Individual may complain to an independent organization for resolution of disputes regarding the use of collected data. The description MUST include information about how to contact the third party organization. (Note : la description devra alors contenir le sous-élément <service> qui fournira les coordonnées de l'organisme indépendant.)
>
> `[court]` Individual may file a legal complaint against the Web site.
>
> `[law]` Disputes arising in connection with the privacy statement will be resolved in accordance with the law referenced in the description.[168]

De façon générale, la rédaction de cette section est extrêmement décevante, car elle ne réussit pas à clairement rencontrer son objectif d'établissement du mode de résolution des conflits. Premièrement, la structure générale de la première phrase des trois premiers paragraphes est très confuse : « *Individual may complain to [...] for resolution of disputes regarding the use of collected data.* » Elle nous dit que

[168] http://www.w3.org/TR/P3P/#DISPUTES

l'individu peut se plaindre à l'un ou l'autre des endroits prévus pour la résolution des conflits. Une telle phrase nous laisse l'idée générale d'un destinataire pour les plaintes des usagers, mais semble faible lorsque comparée à ce qu'un juriste aurait pu rédiger à ces fins.

Ensuite, cette phrase sous-entend que l'individu ne pourrait adresser de plaintes qu'en matière d'usage des informations recueillies. Ne pourrait-il pas le faire dans d'autres circonstances comme par exemple la cueillette non autorisée de données ou leur conservation après la disparition des objectifs de la cueillette? Cette mention contredit la description générale plus large de l'élément disputes : « *... procedures that may be followed for disputes about a services' privacy practices, or in case of protocol violation*. » Ceci dénote une faiblesse de rédaction certaine, qui porte tout particulièrement à conséquence dans le domaine du choix d'un mode alternatif de résolution de conflits.

La première valeur, `[service]`, est assez déroutante : "*Individual may complain to the Web site's customer service representative for resolution of disputes regarding the use of collected data*". Il nous semble en effet un peu risqué de référer la résolution des conflits aux représentants du service à la clientèle du site impliqué. Le W3C fait-il preuve de pensée magique en permettant de se fier à l'une des parties à un litige pour le régler, ou s'agit-il plutôt d'une manière politiquement correcte de permettre aux opérateurs de site de déclarer qu'aucun mode de résolution des conflits n'est prévue dans leur politique? À moins que la conception du concept même de résolution de conflits qu'ont les rédacteurs du protocole soit beaucoup plus floue que celle qui existe dans le monde juridique.

Par ailleurs l'individu conservant de toute façon, ne serait-ce que par son droit à la liberté d'expression, le droit de contacter le bureau du service à la clientèle pour se plaindre, n'aurait-il pas été plus clair de prévoir plutôt une valeur `[none]` puisque le résultat risque fort d'être le même dans bien des cas?... D'un point de vue juridique cette valeur `[service]` est donc à notre avis parfaitement inutile.

Les deux valeurs suivantes `[independent]` et `[court]`, laissent à penser que la plate-forme permet aux services d'opter pour un mode alternatif de règlement des différends, comme l'arbitrage virtuel ou traditionnel par exemple, pour solutionner les litiges à naître. En ne lisant que la description de la valeur `[court]`, l'usage du verbe « *may* » peut en effet faire référence à l'absence de l'exclusion préalable du recours aux tribunaux, condition fondamentale à l'établissement de tout arbitrage qui aurait découlé du choix de l'autre option, `[independent]`. L'arbitrage étant exclu par le choix de `[court]` les parties « peuvent » s'adresser aux tribunaux.

En effet, nous savons que par l'application des règles du droit de l'arbitrage, notamment de l'article 2638 du Code civil du Québec, la convention d'arbitrage impose aux parties à un litige actuel l'exclusion absolue du recours tribunaux. Cette exclusion est une condition fondamentale de toute convention d'arbitrage et son absence entraînera la nullité de la clause compromissoire.

Mais malheureusement le W3C utilise le verbe « *may* » dans tous ses paragraphes, ce qui nous empêche d'interpréter la description de la valeur `[court]` en ce sens. Il est certain que la description que fait la plate-forme de ces deux valeurs capitales aurait dû être beaucoup plus précise pour qu'un tribunal puisse en inférer l'existence d'une clause compromissoire.

La dernière valeur, `[law]`, équivaut à la notion de droit international privé que les juristes connaissent bien sous le nom de « choix du droit applicable ». Ces clauses permettent en effet aux parties à une transaction internationale, ou inter-provinciale, de choisir le droit qui régira leurs relations. La décision des parties à cet égard régira donc le choix du tribunal compétent à entendre un litige, ou le déroulement de l'arbitrage si une clause compromissoire à été insérée au contrat. Le choix du droit applicable pourra donc se faire en toutes circonstances.

En revenant à notre point de départ, nous restons cependant perplexe sur le fait que l'élément <**`resolution-type`**> ne devra prendre que l'une des quatre valeurs que nous venons de survoler. Il ne pourra donc pas contenir la valeur `[law]` s'il contient

l'un ou l'autre des valeurs `[independent]` ou `[court]`. Comment alors faire le choix du droit applicable?

Nous notons aussi que ce groupe d'éléments <DISPUTES> contient des sous-éléments qui permettent de référer à un service de vérification externe pour l'audit des pratiques du service, ainsi qu'une description courte ou longue en langage compréhensible à l'humain (« *human readable* ») des déclarations faites dans ce groupe d'éléments. Je ne peux m'empêcher de badiner un peu en arguant que certains usagers risquent de ne pas plus croire au caractère " *human readable* " des textes que les avocats des services insèreront à cet endroit, qu'à celui que leurs informaticiens auront préparé. Mais voilà une question tout à fait différente...

<REMEDIES>[169] Cet élément devrait, selon la spécification, être compris dans tout groupe d'élément <DISPUTES>. Il servira à déclarer le type de réparation offert en cas de violation des termes de la politique d'un service donné. Il devra contenir l'un des trois sous-éléments suivants :

> <CORRECT/> Errors or wrongful actions arising in connection with the privacy policy will be remedied by the service.
>
> <MONEY/> If the service provider violates its privacy policy it will pay the individual an amount specified in the human readable privacy policy or the amount of damages.
>
> <LAW/> Remedies for breaches of the policy statement will be determined based on the law referenced in the human readable description.

La première valeur, <CORRECT/>, indique que le service s'engage à remédier aux situations problématiques qui pourraient se présenter dans la gestion des informations. Cet engagement semble plutôt général, car il ne précise pas outre mesure la nature du remède. C'est en l'examinant par opposition à la seconde, <MONEY/>, que nous comprenons qu'il s'agira dans le premier cas de corrections et

rectifications aux dossiers et pratiques, et de dédommagements monétaires dans le second. La rédaction laisse aussi présumer qu'il s'agit en fait de l'établissement de dommages fixes en cas de problème, alors que la troisième, <LAW/>, fait plutôt référence à un recours aux tribunaux pour le règlement du différend. La rédaction de ce troisième sous-élément aurait néanmoins pu être plus habile.

3.2.4 Éléments de déclarations

Avant d'aborder en détails les éléments formant une déclaration, rappelons qu'une politique peut comporter plus d'une déclaration qui consiste en une série de pratiques déclarées par un service relativement à une collection particulière d'informations[170]. De façon technique, la déclaration est elle-même formée des éléments «*purpose*», «*recipient*», «*retention*», «*data-group*» et «*data*» ainsi que, lorsque nécessaire, l'élément «*consequence*». Par ailleurs, la déclaration peut comporter l'élément «*non-identifiable*» que nous décrirons sommairement. Nous présenterons également ici l'élément «*categories*» servant à décrire les informations recueillies ainsi que les éléments qui peuvent eux-mêmes apparaître sous «*categories*».

Une politique peut contenir une ou plusieurs déclarations, pour tenir compte de catégories ou d'ensembles d'informations différents. Chacune de ces déclarations peut faire usage des éléments <STATEMENT>, <CONSEQUENCE>, <NON-IDENTIFIABLE>, <PURPOSE>, <RECIPIENT>, <RETENTION>, <DATA-GROUP> et <DATA>.

Le premier de ces éléments, **<STATEMENT/>,** est en fait un groupe d'éléments, un « contenant » dans les termes du W3C, qui contient obligatoirement les éléments <PURPOSE>, <RECIPIENT>, <RETENTION> et <DATA-GROUP> et au besoin un élément <CONSEQUENCE>. C'est de cette façon, c'est-à-dire en préparant différentes déclarations (« *statements* ») qui contiendront ces éléments de base assorties de valeurs différentes, que les services pourront prévoir plusieurs catégories de données régies par des règles différentes.

---

[169] http://www.w3.org/TR/P3P/#REMEDIES
[170] http://www.w3.org/TR/P3P/#Terminology, sous « statement »

Le premier élément obligatoire du groupe « STATEMENT », **<PURPOSE/>,** fait référence aux finalités de la collecte et de l'usage d'informations, composante fondamentale du droit applicable en matière de protection des renseignements personnels. Il représente l'un des éléments les plus complexes du protocole, puisqu'il se précise en pas moins de douze sous-éléments.

Sous-élément	Finalités de la cueillette
<CURRENT/>	aux seules fins de compléter l'opération en cours, soit immédiatement soit plus tard (recherche sur le Web, transmission d'un courriel ou d'une commande);
<ADMIN/>	pour les besoins d'administration du site Web ou de son système informatique, par exemple pour la génération de statistiques sur les visites;
<DEVELOP/>	aux fins d'évaluer le site Web et les produits qui y sont offerts et de permettre leur développement;
<TAILORING/>	pour ajuster le contenu offert au visiteur sur le site au cours d'une même visite;
<PSEUDO-ANALYSIS/>	pour créer un profil de visiteur ou d'ordinateur qui ne sera pas relié à un individu nommé ou déterminé, le tout pour des fins d'études et de statistiques;
<PSEUDO-DECISION/>	pour créer un profil de visiteur ou d'ordinateur qui ne sera pas relié à un individu nommé ou déterminé, mais cette fois-ci pour ajuster le contenu présenté au visiteur lors de visites subséquentes;
<INDIVIDUAL-ANALYSIS/>	pour créer un profil de visiteur ou d'ordinateur qui sera relié à un individu nommé ou déterminé, le tout pour des fins d'études et de statistiques;
<INDIVIDUAL-DECISION/>	pour créer un profil de visiteur ou d'ordinateur qui sera relié à un individu nommé ou déterminé, mais cette fois-ci pour ajuster le contenu présenté au visiteur lors de visites subséquentes;
<CONTACT/>	pour permettre de contacter subséquemment un individu, par d'autres moyens que par téléphone, à des fins promotionnelles;

<TELEMARKETING/>	pour permettre de contacter subséquemment un individu par téléphone, à des fins promotionnelles;
<HISTORICAL/>	aux fins d'archiver des informations relatives à la visite ou aux opérations effectuées (« *social history* ») conformément au droit applicable où aux termes de la politique en vigueur;
<OTHER-PURPOSE/>	pour d'autres fins qui doivent être précisées dans la version textuelle (« *human readable* ») de la politique

Les valeurs qui sont associées à chacun de ses éléments seront placées en rapport avec l'attribut <**required**> :

> <**always**> indiquera qu'un type d'usage associé est obligatoire relativement à la catégorie d'informations visées et que l'usager ne peut choisir de ne pas s'y soumettre,
>
> <**opt-in**> ou <**opt-out**> , indiquera l'usager peut avoir à accepter chaque type de collecte ou, à l'inverse, qu'il y sera inscrit d'office à moins d'instruction contraire. Les détails de ces options, si l'une ou l'autre est choisie, doivent être décrits dans le document proposé à l'adresse *opturi* (décrit plus haut, à la section 2.3).

Le deuxième élément obligatoire du groupe « STATEMENT », <**RECIPIENT**>, précise la destination des données recueillies et leur partage éventuel. La déclaration peut préciser que les données sont conservées uniquement sur les ordinateurs du service d'origine ou de ses agents (<OURS>), sont confiées à des intermédiaires oeuvrant à l'acheminement des données (<DELIVERY>), à des services appliquant les mêmes politiques quant à la gestion des informations personnelles (<SAME>).

Trois autres sous-éléments abordent la question du partage des données. Il s'agit tout d'abord de <OTHER-RECIPIENT> qui indique si les informations sont partagées avec des tierces parties appliquant éventuellement des politiques différentes mais tout en demeurant responsables de leurs actions face à l'organisme collectant les données. Il

ne s'agirait pas ici d'entités contrôlées par l'organisme opérant le service concerné, mais qui entretiendraient avec lui des relations d'affaires pouvant laisser croire qu'ils lui doivent des comptes sur leurs agissements. La possible transmission des informations à un organisme tiers échappant à toute forme de contrôle direct ou indirect de la part de l'organisme opérant le service sera plutôt indiquée par le sous-élément <UNRELATED> . Finalement, le sous-élément <PUBLIC> indiquera que les données recueillies sont mises à disposition du public par exemple par le biais de bottins ou de babillards électroniques.

À nouveau, le statut de ces éléments est déterminé en utilisant les valeurs **<required>,<opt-in>** ou **<opt-out>.**

L'élément <RETENTION>, nous informe sur la politique en vigueur quant à la conservation des informations par le service, ne pose pas trop de problèmes. Soit que l'organisme ne les conserve pas (<NO-RETENTION/>), qu'il ne les conserve que pour remplir le but déclaré pour la collecte (<STATED-PURPOSE/>), qu'il les conserve en respect des normes juridiques en vigueur dans sa juridiction (<LEGAL-REQUIREMENT/>) au quel cas la politique devra fournir une description du calendrier prévu de destruction, ou encore, qu'il les conserve indéfiniment (<INDEFINITELY/>).

Quatrièmement, la déclaration doit contenir au moins un élément obligatoire <DATA-GROUP/> qui contiendra lui-même au moins un élément <DATA/> dont le but est de fournir une description du type d'information qui sera recueilli par le service en question. Tout d'abord, il est intéressant de noter que le W3C a mis en ligne[171] une description du schéma d'informations de base qu'un site peut être appelé à collecter. Le service pourra donc y référer en bloc en activant le sous-élément <BASE>. Cette description sera utilisée par défaut en l'absence d'une description préparée par le service en un élément <DATA REF> qui pourra spécifier directement les informations recueillies ou carrément référer à l'adresse d'une description plus étoffée. Notons qu'il est ici possible d'inclure plus d'une description de types de données recueillies, afin de leur associer des politiques différentes.

[171] http://www.w3.org/TR/P3P/base

Finalement, en plus de ses quatre éléments obligatoires, l'élément <STATEMENT> peut contenir un élément <CONSEQUENCE> qui servit à indiquer à l'usager les conséquences pratiques d'un refus qu'il pourrait éventuellement opposer à une activité de collecte ou de conservation d'informations. Par exemple, le site peut utiliser ce moyen pour indiquer à son visiteur qu'un refus de la collecte d'un type d'information pourrait l'empêcher d'accéder à certains produits ou services offerts sur le site. Cet élément est toutefois optionnel. On peut facilement déduire qu'il aurait joué un rôle dans le processus de négociation (offre et contre-offre) qui devait initialement faire partie du projet P3P.

Finalement, l'élément <NON-IDENTIFIABLE/> viendra affirmer que le service ne procède à la collection d'aucune information pouvant être reliée à un individu identifié. Une telle affirmation doit être supportée dans tous les cas par une description des moyens employés pour assurer qu'un tel lien avec un individu est impossible. Cette description doit être contenue dans la version textuelle de la politique (« *human readable* »).

Un élément est traité séparément dans la spécification, c'est à dire qu'il est abordé en dehors des séries d'éléments de politiques ou de déclarations, puisqu'il peut être utilisé dans n'importe quel contexte. L'élément <CATEGORIES>[172] a pour objet de décrire plus précisément le type d'informations recueillies. Voici la liste des sous-éléments prévus à la spécification à pour permettre cette description :

<*physical*>	Coordonnées de l'individu dans le « monde réel »;
<*online*>	Coordonnées de l'individu dans le « monde virtuel »;
<*uniqueid*>	Numéros identificateurs uniques autres qu'officiels (émis par le site par exemple) ;
<*purchase*>	Informations recueillies lors d'une transaction électronique, comme les coordonnées bancaires;
<*financial*>	Coordonnées financières telles que soldes de comptes, historiques d'achats;

[172] http://www.w3.org/TR/P3P/#Categories

<*computer*>	Informations sur l'ordinateur utilisé (adresse IP, etc…);
<*navigation*>	Données dynamiques recueillies lors des navigations ;
<*interactive*>	Données recueillies au cours des interractions de l'individu avec le site, tel que l'historique des recherches effectuées ou des options choisies sur les pages ;
<*demographic*>	Données démographiques, incluant les informations socio-économiques : âge, sexe, tranches de revenus, etc...
<*content*>	Le contenu de textes émanant de l'usager, tels que le texte de ses courriels, des messages laissés sur un babillard électronique ou dans une salle de clavardage ;
<*state*>	Informations requise pour maintenir une communication continue avec l'usager, incluant les témoins;
<*political*>	Appartenance de l'individu à un parti politique, une association ou un regroupement quelconque ;
<*health*>	Information relative à l'état de santé physique ou mentale de l'individu, son orientation sexuelle, son usage de certains services de santé, les interrogations qu'il a formulées à ce sujet ou l'historique de ses achats de produits ou services de santé ;
<preference>	Préférences personnelles : couleurs préférées, goûts personnels en matière de musique, cinéma, etc...
<location>	Information permettant de retracer un individu, dont ses coordonnées sous le système GPS ;
<government>	Identificateurs stables de l'individu, émanant d'une autorité gouvernementale (numéro d'assurance sociale par exemple);
<other-category>	Autre catégorie d'information détaillée dans la version textuelle de la politique de vie privée.

Il est important de souligner que ces sous-éléments servent à identifier le ou les types d'informations recueillies par un service et par suite ils permettent de préciser le sort réservé à chacune. Ces éléments servent aussi à l'usager dans l'élaboration de ses préférences. Il pourra ainsi accepter le partage de certains types d'informations

(comme ses coordonnées physiques ou virtuelles) mais pas l'échange de renseignements liés à son état de santé ou ses coordonnées financières. Il importe cependant de garder à l'esprit que le fait que la spécification contienne des sous-éléments consacrés à des sujets aussi personnels ne signifie pas automatiquement que les sites qui adopteront P3P collecteront des informations sur l'état financier ou médical des individus. Leur présence permettra aux sites qui le feront de le déclarer et de spécifier les conditions qui entoureront ces opérations, ce qui fournira aux usagers la possibilité d'inclure à leurs profils qu'elles seront leurs instructions dans de telles situations.

3.3 Mise en œuvre et autres composantes

Nous abordons dans cette section les autres composantes qui entrent en jeu dans le déploiement et le fonctionnement de P3P. Nous utiliserons pour ce faire le cadre offert par la stratégie de mise en vigueur adoptée par le W3C puisqu'elle fait en sorte de reporter l'implantation de certains aspects de la plate-forme originale.

Au départ, P3P cherchait à mettre en place un contexte global encadrant la collecte et l'échange d'informations sur les internautes, en chapeautant la négociation et la conclusion d'une entente avec l'entité procédant à la collecte. Le but moins ambitieux recherché par la version 1.0 de P3P est décrit comme suit dans la description de la spécification :

> *The goal of P3P version 1.0 is twofold. First, it allows Web sites to present their data-collection practices in a standardized, machine-readable, easy-to-locate manner. Second, it enables Web users to understand what data will be collected by sites they visit, how that data will be used, and what data/uses they may « opt-out» of or « opt-in» to.*[173]

La politique de mise en vigueur de la plate-forme décidée par le W3C y est par ailleurs décrite ainsi :

> *Significant sections were removed from earlier drafts of the P3P1.0 specification in order to facilitate rapid implementation and deployment of a P3P first step. A future version of the P3P specification might*

[173] http://www.w3.org/TR/P3P/#goals_and_capabs

> *incorporate those features after P3P1.0 is deployed. Such specification would likely include improvements based on feedback from implementation and deployment experience as well as four major components that were part of the original P3P vision but not included in P3P1.0:*
>
> > *a mechanism to allow sites to offer a choice of P3P policies to visitors*
> >
> > *a mechanism to allow visitors (through their user agents) to explicitly agree to a P3P policy*
> >
> > *mechanisms to allow for non-repudiation of agreements between visitors and Web sites*
> >
> > *a mechanism to allow user agents to transfer user data to services*

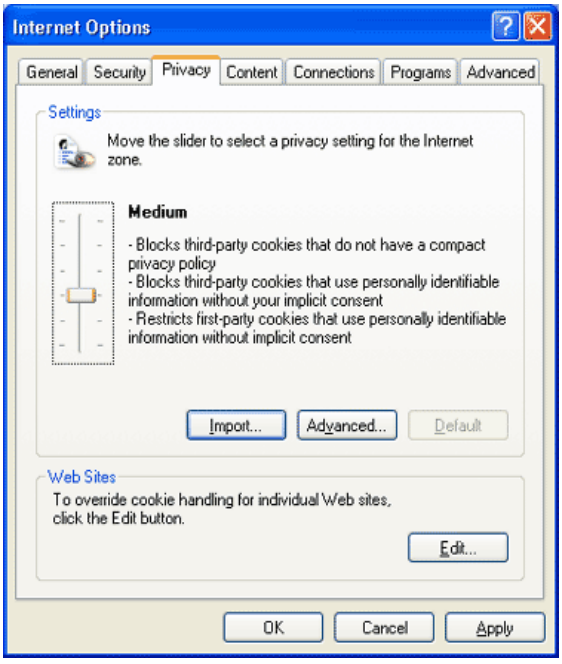
La mise en vigueur de P3P n'est donc que partielle, sa version 1.0 se limitant à exiger des services qui s'y conforment de rédiger une politique de vie privée à l'aide des conventions établies, des logiciels des usagers (incluant les navigateurs) de récupérer les politiques et de les analyser afin d'informer leur propriétaire sur leur conformité. Rappelons les cinq fonctions de base de P3P que nous avons isolées en début de chapitre : information, négociation, entente, transmission des informations, vérification. Nous nous rendons compte que P3P 1.0 ne s'attaque qu'à la première, l'information. Toutes les fonctions relatives à la formation de l'entente et à la transmission des informations ont disparu au fil du temps et de l'évolution des travaux du W3C.

Dans le cas particulier de la vérification, elle n'a jamais vraiment fait partie de la plate-forme puisque le W3C a toujours laissé l'option aux services de se soumettre ou pas à de telles procédures. Elle ne comporte que les éléments nécessaires pour référer aux procédures de vérification éventuellement adoptées par les services, mais n'en impose aucune en particulier.

L'établissement des préférences des usagers n'est pas vraiment abordé en détails dans la spécification. Elle ne fait à ce chapitre que souligner en moins de deux lignes que l'agent logiciel de l'usager (comme le logiciel de navigation) devra être en mesure

d'importer et d'exporter des profils de préférence[174]. Il reviendra donc aux entreprises qui élaboreront des agents logiciels pour les internautes de leur donner les fonctions de leur choix. La marge de manœuvre des usagers dans l'établissement de leurs choix et préférences en matière de protection de leurs renseignements personnels pourra donc varier grandement selon les produits utilisés.

L'exemple le plus connu au moment de cette étude est certes celui offert par la version 6.0 du navigateur Internet Explorer, qui s'affiche ouvertement comme étant compatible avec P3P[175]. L'arrivée d'un joueur aussi important que Microsoft pour supporter le projet P3P a toujours été considéré comme un facteur déterminant de sa réussite. L'intégration de P3P dans Explorer 6.0 s'avère pourtant relativement limitée, quand on connaît les possibilités plus étendues offertes par la plate-forme. Ainsi, le produit Microsoft permet de retrouver et lire une politique P3P rattachée à un site, mais ne s'en servira que dans la gestion (acceptation ou refus) des témoins.



L'usager dispose d'une catégorie supplémentaire, sous l'onglet « *privacy* », dans la panoplie d'options Internet offertes par Explorer. Il pourra y choisir le protection dont il veut disposer dans la gestion des témoins. Pour ce faire, il choisira entre six niveaux

[174] spécification, section 3.6 http://www.w3.org/TR/P3P/#PREFERENCES

prédéterminés de protection allant de l'acceptation au refus pur et simple de tous les témoins, en passant par des niveaux intermédiaires détaillant les cas d'acceptation ou de refus de témoins selon qu'ils proviennent du serveur d'origine ou d'un serveur tiers par exemple.

Explorer 6.0 permet aussi de modifier à la pièce les détails de ces niveaux, et de passer outre aux réglages choisis pour certains sites déterminés. La présence d'un icône () au coin inférieur droit de la fenêtre principale n'indiquera donc seulement que certains témoins ont été bloqués en application des réglages programmés par l'usager. La déclaration des finalités de la collecte d'informations, les conséquences d'un défaut du site à ses engagements, le choix d'un mode de règlement d'un conflit éventuel et toutes les autres données contenues dans la politique de vie privée présentée en format conforme à P3P sont totalement évacuées.

La première impression laissée par Explorer 6 à sa sortie, était que la conformité de la politique P3P affichée par le site était vérifiée et que les cas problématiques étaient signalés par un icône sur le navigateur même. En l'absence d'icône, le site serait donc conforme aux paramètres programmés par l'usager. Il ne s'agissait que d'une demi vérité puisque seule la problématique des témoins fait l'objet de vérifications et d'alertes. IE6 ne fait donc que pousser un peu plus loin son système traditionnel de gestion des témoins par le biais de P3P. Même sa fonction d'importation de profils de préférences est limitée à ce contexte :

> *Also, you can import a file of custom preferences to work with P3P for handling cookies*[176]. (nos soulignements)

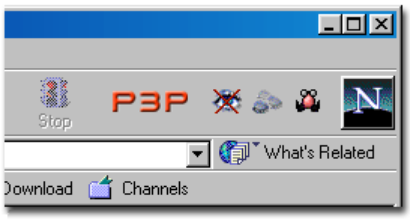
Il est un peu difficile de soutenir dans ce contexte qu'Internet Explorer 6.0 utilise P3P à son maximum pour protéger la vie privée des internautes. Cet exemple révèle aussi l'importance de l'agent logiciel dans la mise en œuvre de P3P. L'absence de résultats concrets ou de rapports précis sur la question des renseignements personnels ne pourra certes pas générer l'intérêt nécessaire chez les usagers pour donner à la plate-

[175] http://www.microsoft.com/windows/ie/evaluation/overview/privacy.asp
[176] http://www.microsoft.com/windows/ie/evaluation/overview/privacy.asp

forme le second souffle dont elle aura besoin pour passer à la deuxième phase de son implantation.

À titre de comparaison, nous avons visité les sites de deux compagnies offrant des agents logiciels compatibles à P3P. Tout d'abord le « *Privacy companion* » celui de *Idcide*[177] *(*prononcé *« I decide »)* qui englobe déjà plusieurs fonctionnalités en matière de protection de la vie privée. Il permet en effet de détecter les activités de repérage ou de « filature » mises en place par les sites pour reconnaître les visiteurs. Il indiquera ainsi que le site visité tente de détecter l'usager ou si de telles opérations se font par partage d'informations avec d'autres serveurs. Il permettra alors de bloquer ces opérations et de brouiller les pistes.

Idcide a présenté récemment un prototype de la prochaine mouture de son produit, qui sera compatible avec la plate-forme P3P[178]. Ce lien sera opéré par l'ajout d'un indicateur additionnel qui changera du vert au rouge selon que la politique du site est conforme ou non aux préférences de l'usager :



Le logiciel n'est cependant pas encore disponible et le site de la compagnie ne donne pas de détails sur la configuration du profil de préférences de l'usager. Il nous est donc impossible à ce stade-ci d'évaluer sa portée ni sa facilité d'utilisation. Notons cependant que l'entreprise *Privacy council*[179], qui conseille et fournit des solutions aux entreprises en matière de protection de la vie privée, annonçait cet automne son intention d'utiliser la technologie *Idcide* [180]pour les analyses de la conformité des

[177] http://www.idcide.com/
[178] http://www.idcide.com/pages/res_best.htm#p3p
[179] http://www.privacycouncil.com/index.php
[180] YAHOO FINANCE, *Privacy Council Selects IDcide PrivacyWall Product for Remote Diagnosing Of Website Privacy Gaps and P3P Compliance Program,* 27 septembre 2001, http://biz.yahoo.com/prnews/010927/dcth023_1.html

sites Web faites dans le cadre de son programme « *privacy scan* »[181]. Ce service permet aux entreprises de connaître l'état de la situation quant à leurs propres sites afin de recevoir conseils et recommandations.

Le dernier produit dont nous discuterons montre un peu mieux comment un usager pourrait mieux prendre le contrôle de la gestion de ses informations personnelles en utilisant P3P. Il s'agit en l'occurrence du *WorldNet Privacy Tool*[182] présentement en élaboration chez AT&T. Notons que AT&T supporte le projet P3P depuis ses débuts, ce qui se traduit notamment par l'implication de l'une de ses chercheurs à titre de directrice du projet[183].

Cet agent logiciel récupérera et analysera lui aussi la politique P3P du site visité par l'usager. Il l'informera de sa conformité à ses préférences au moyen d'un signal visuel. Le logiciel présentera également un icône signalant un conflit entre les préférences de l'usager et la politique.

Cependant le *WorldNet Privacy Tool* semble beaucoup plus flexible dans la détermination des préférences d'un utilisateur. Il permettra tout d'abord à l'usager de choisir entre trois profils types représentant des attentes basses, moyennes ou élevées quant aux pratiques en question. Ces profils sont également modifiables au gré de l'usager. Ce dernier pourra également créer son propre profil de préférences ou en importer un. Ces choix concordent par ailleurs beaucoup mieux avec les objectifs de départ du W3C quant à la préparation du profil de préférences de l'usager, et devraient permettre de se rapprocher plus de la philosophie qui l'a vu naître. Par exemple, il semble faire usage des sous-éléments `<CATEGORIES>` pour permettre à l'usager de distinguer ses préférences en matière de gestion des renseignements financiers ou médicaux. Il permettra aussi de visualiser séparément les exigences du site relativement à l'exercice d'options sur les renseignements (« *opt-in* » ou « *opt-out* »).

[181] http://www.newmediagateway.com/privacycouncil/privacy_scan.php
[182] http://privacy.att.net/
[183] Mme Lorrie Faith Cranor pour être plus précis.

A ce chapitre, il est aussi très intéressant de constater que ce produit permettra également de visualiser un sommaire de la politique de vie privée du site rédigée en langage naturel à partir du document XML qui la contient[184].

Voici donc les traits principaux de la spécification P3P 1.0 mise en vigueur par le W3C au bout d'un long effort de rédaction et, on s'en doute, de négociation. Nous n'avons pas cherché à résumer ici toute la technique qui sous-tend la plate-forme, mais plutôt à indiquer les parties principales qui devraient intéresser le juriste. Nous croyons maintenant disposer de suffisamment de données pour pouvoir synthétiser et formuler une opinion sur le projet du W3C.

***

[184] http://privacy.att.net/tour/example-w3c.html . Voir aussi l'exemple : http://privacy.att.net/tour/example-w3c.html

CHAPITRE 4 – Synthèse

4.1 Questions préliminaires

Notre étude nous a permis d'aborder sous trois angles différents les efforts récents du W3C. Nous sommes tout d'abord remontés aux origines du projet afin d'isoler ses buts initiaux et d'examiner le contexte qui l'a inspiré. Nous avons ensuite résumé le droit existant en matière de protection de la vie privée et des renseignements personnels, pour tenter de dégager les principes fondamentaux qui s'appliquent au domaine et qui devraient être traités de manière satisfaisante par tout protocole dont l'objectif est de fournir une solution technique à une telle problématique. Finalement, nous avons examiné plus en détails la façon dont le W3C a donné vie à son projet en posant un regard juridique sur la rédaction de certaines parties stratégiques du protocole technique.

Beaucoup de questions sont apparues au fil de ces analyses, tant sur des points particuliers que sur les fondements mêmes du projet. En fait, beaucoup de questions demeurent sans réponse, comme autant d'invitations à poursuivre ce type d'étude. Il importe donc ici de faire un tri dans ces questionnements et d'isoler les plus pertinents dans notre quête d'une réponse générale à notre question de recherche.

Cette question de recherche a été formulée comme suit : comment P3P, à titre de mode d'auto-régulation technique, peut-il permettre de répondre aux préoccupations des États et des individus en matière de protection de la vie privée sur Internet et s'adapter aux différents cadres législatifs existants?

Avec le recul nous croyons qu'il faut, avant de répondre à cette question, se demander carrément *si* P3P peut répondre à ces préoccupations et s'adapter aux différents cadres législatifs. Nous pouvons en effet facilement envisager maintenant la possibilité que le projet ait été trop ambitieux et que le pari qu'un protocole technique puisse régler de façon satisfaisante une problématique aussi complexe et si finement imbriquée dans le tissu même de nos sociétés ne puisse être entièrement gagné.

Peut-on donc estimer raisonnable de régler globalement la problématique de l'échange de renseignements personnels sur le Web au moyen d'un protocole technique et que l'objectif de mettre sur pied un mécanisme technique capable de représenter un individu pour consentir à la divulgation de ses renseignements personnels ait été une utopie ? Autrement dit le projet P3P, même s'il était mis en vigueur selon la conception initiale qu'en avait le W3C, pourrait-il apporter une solution satisfaisante aux préoccupations parfois contradictoires des différents intervenants en cause?

Nous aborderons cette question en présumant que P3P est, ou sera incessamment, mis en vigueur dans sa totalité selon le plan initial de ses concepteurs. Ceci nous permettra de le confronter tout d'abord au droit, et par la suite au Web. Le résultat de ces confrontations devrait nous permettre de suggérer des pistes de solutions dans la poursuite de ce projet.

Rappelons en deux mots que le concept d'origine prévoyait l'encodage des politiques de vie privée par les sites et des préférences personnelles par les individus, l'inscription des données personnelles dans un dépôt de données sur l'ordinateur de l'usager, la récupération et analyse des politiques par l'agent logiciel de l'usager, la négociation et la conclusion automatique d'une entente encadrant la remise des données et le transfert automatique de celles-ci entre les ordinateurs, sans intervention humaine.

4.2 P3P face au droit

Comment ce projet est-il être perçu lorsque observé à travers le spectre du droit ? Analysons donc P3P face aux principes fondamentaux en matière de protection des renseignements personnels. En effet, les principes de l'OCDE fournissent un excellent dénominateur commun. Nous formulerons donc quelques commentaires sur notre appréciation de P3P en regard de chacun d'eux.

1) *Principe de la limitation en matière de collecte : toutes données de caractère personnel devraient être obtenues par des moyens licites et*

> *loyaux, après en avoir informé la personne concernée ou avec son consentement.*

Deux aspects retiennent ici notre attention : le caractère licite et loyal des moyens employés ainsi que l'obtention du consentement de la personne concernée. Par essence, P3P cherche à normaliser la façon dont sont présentées et structurées les politiques de vie privée. Cet aspect est d'ailleurs, tout compte fait, le seul a avoir survécu jusqu'à la première mise en vigueur de la spécification. Il n'est donc pas faux de prétendre que P3P cherche justement à instaurer un cadre loyal et licite pour la collecte des informations.

La loyauté de l'opération, si menée avec bonne foi bien entendu, peut certes figurer au nombre des objectifs rencontrés par P3P. Il est raisonnable de croire qu'un site qui prendra la peine d'engager les coûts et les efforts nécessaires au déploiement d'une politique P3P pour encadrer ses activités de cueillette d'informations ne cherchera pas à duper ses visiteurs. D'ailleurs, la seule présence d'une politique P3P constituera déjà un dévoilement important des conditions entourant l'opération. À condition bien sûr que l'usager dispose des outils nécessaires pour la retrouver et la décoder, des outils qui iront plus loin que la simple gestion des témoins offerte par IE 6.0, et que son profil de préférences soit configuré pour correspondre à ses désirs.

La noblesse des intentions du service se manifestera également par l'existence ou non d'une procédure de vérification chapeautée par un organisme de vérification externe. Car la politique P3P pourra bien prévoir toutes les déclarations ou garanties possibles, encore faudra-t-il s'assurer qu'elles soient conformes à la réalité et à la réelle nature du processus. Dans l'ensemble, nous croyons pouvoir quand même décerner une bonne note à P3P quant à l'établissement des conditions de la collecte.

Le caractère licite de l'opération se mesurera par ailleurs en regard de la loi applicable dans chaque juridiction, et reviendra à faire à peu près le même exercice que ce que nous faisons présentement. Un élément important de cette évaluation est justement la question du consentement de l'individu à la collecte d'informations le

concernant. Le concept original de P3P permettait-il vraiment d'obtenir un consentement valide ?

Nous utiliserons la *loi québécoise*[185] pour analyser le type de consentement que P3P permettrait d'obtenir d'un internaute. Elle décrit ainsi le consentement à obtenir :

> ***14.*** *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.*
>
> *Un consentement qui n'est pas donné conformément au premier alinéa est sans effet.*

« Manifeste » : Le consentement devra donc être indiscutable à sa face même et, idéalement, être fourni par écrit. Si nous nous limitons à ce simple point, nous pouvons dire que le consentement fourni selon les règles du concept P3P d'origine peut se qualifier. En effet, les projets antérieurs de spécification prévoyait en effet la conclusion d'une entente entre les ordinateurs de l'usager et du service, qui serait constaté dans un fichier informatique nommé *agreementID* devant être conservé sur le serveur.

Face au droit québécois, la simple validité d'un tel fichier électronique comme manifestation du consentement ne pose pas vraiment problème, surtout depuis l'entrée en vigueur de la *Loi concernant le cadre juridique des technologies de l'information*[186]. Celle-ci prévoit en effet que :

> ***2.*** *À moins que la loi n'exige l'emploi exclusif d'un support ou d'une technologie spécifique, chacun peut utiliser le support ou la technologie de son choix, dans la mesure où ce choix respecte les règles de droit, notamment celles prévues au Code civil.*
>
> *Ainsi, les supports qui portent l'information du document sont interchangeables et, l'exigence d'un écrit n'emporte pas l'obligation d'utiliser un support ou une technologie spécifique.*

[185] *Loi sur la protection des renseignements personnels dans le secteur privé* LRQ c. P-39.1; sur le Web : http://www.canlii.org/qc/loi/p39.1/
[186] *Loi concernant le cadre juridique des technologies de l'information*, L.Q. 2001, c. 32

La loi québécoise n'exigeant pas l'emploi d'un support en particulier pour l'obtention et la conservation d'un consentement, rien n'empêcherait donc que celui-ci soit fourni et conservé sur support électronique.

« Donné à des fins spécifiques » : nous vous référons à notre examen du principe de spécification des finalités de la collecte abordé dans la section 4.2 ci-dessus. Disons seulement que le fait que P3P vise particulièrement à fournir les raisons motivant la demande de renseignements nous permet de conclure au respect de cette condition si nous l'abordons dans son sens le plus restreint.

« libre, éclairé » : C'est sur ce point que le consentement de type P3P est le plus interpellé par les réalités du monde juridique. En effet, pouvons-nous dire qu'un internaute qui configure son profil de préférences pour permettre à son ordinateur de négocier avec celui du service pour en venir à la conclusion d'une entente automatisée fournit vraiment un consentement libre et éclairé à la collecte d'informations le concernant et à leur usage selon les termes stipulés dans la politique du site visité?

Les auteurs Beaudoin et Jobin abordent la question de l'existence et de l'intégrité du consentement dans leur traité des obligations. Leur description de la notion de consentement est utile à notre analyse :

> *« Le consentement est la condition la plus importante du contrat, car s'engager c'est consentir par acte de volonté non équivoque à assumer certaines obligations. Il est indispensable que le consentement existe. On ne saurait admettre, en effet, qu'une personne se trouve liée par un contrat dont elle ignore l'existence ou qu'elle n'a pas voulu. L'expression du consentement doit, en outre, représenter aussi la volonté réelle du contractant. Ce dernier doit donc donner un consentement libre et éclairé et non déterminé par une erreur [...] une fraude [...] ou une crainte. »*[187]

Dans le cas de P3P, nous pouvons raisonnablement écarter de l'analyse le cas de la crainte. En effet, mis à part la crainte de ne pouvoir accéder à certains services, qui ressemble beaucoup plus à un intérêt personnel ou économique, il est bien peu

[187] Jean-Louis BAUDOUIN, Pierre-Gabriel JOBIN, *Les obligations*, 5e éd, Cowansville, Québec : Éditions Y. Blais, c1998, parag. 157

probable de voir un service forcer un internaute à lui donner ses renseignements personnels. Quant aux cas de fraude, ou de dol, ils font généralement référence au fait de provoquer l'erreur de l'autre au moyen de promesses ou de fausses déclarations. Cette situation reste théoriquement possible dans la préparation de politiques P3P et elle ne pourrait être évitée que par la mise sur pied de cadres de vérification ou par des interventions législatives pour encadrer le processus. Il reste néanmoins que la fraude ou la crainte sont des situations assez isolées dans le contexte qui nous intéresse. En effet, le système étant d'application volontaire, il est à prévoir que ceux qui emboîteront le pas le feront de bonne foi pour se démarquer de la concurrence et pour éviter la survenance de scandales suite à de mauvais usages de renseignements personnels.

La situation qui risque de se présenter plus souvent et de poser problème relève plutôt de l'erreur. Cette problématique est double dans le cas de P3P. Nous pourrions tout d'abord discourir longuement sur la validité du consentement intervenu par ordinateur interposé. Le Code civil du Québec nous dit que « *le contrat se forme par le seul échange de consentement entre des personnes capables de contracter* [...][188] » et relie la notion de « personne » à la possession d'un patrimoine[189]. Qui plus est, si un ordinateur n'est manifestement pas une personne physique, il ne peut non plus être considéré comme une personne morale puisque le Code prévoit que « *Les personnes morales sont constituées suivant les formes juridiques prévues par la loi, et parfois directement par la loi*. [190]»

Une autre avenue serait de considérer l'ordinateur comme le mandataire de son propriétaire. Ici aussi, cette théorie se heurte à la réalité du Code civil qui définit ainsi le mandat :

> *«Le mandat est le contrat par lequel une personne, le mandant, donne le pouvoir de la représenter dans l'accomplissement d'un acte juridique*

[188] art. 1385
[189] art. 2
[190] art 299

> *avec un tiers, à une autre personne, le mandataire qui, par le fait de son acceptation, s'oblige à l'exercer.* [191]*»*

Il a été aussi suggéré de considérer l'ordinateur comme un simple moyen de communication comme un système téléphonique par exemple. Il ne servirait donc qu'à transmettre la volonté de l'humain qui le possède :

> *«Le fait de considérer les actes perpétrés par un ordinateur au même titre qu'une conversation téléphonique relève donc d'une véritable fiction théorique. [...] Le risque est indéniable : si les juges adoptent cette théorie, l'acteur juridique devra irrémédiablement supporter les conséquences désastreuses qui pourraient survenir d'un bug informatique, d'une erreur de calcul ou d'un défaut de programmation. Il sera tenu de l'ensemble des termes contractuels réorganisés ou « décidés » par la machine comme si ceux-là émanait directement de sa propre volonté»*[192]

P3P est d'ailleurs un exemple éloquent de tels systèmes autonomes qui agissent non pas en fonction des volontés réelles de leur propriétaire, mais qui appliquent plutôt de manière totalement implacable la traduction que ce dernier en a faite dans un langage informatique donné. L'équivalence de ces deux réalités est loin d'être garantie car il reste possible qu'une erreur ou un vice de programmation entraîne l'application de préférences techniques qui ne concordent pas avec les véritables volontés de la personne physique qui les a élaborées. Il est aussi possible que l'encodage de la politique de vie privée ne corresponde pas tout à fait, pour les mêmes motifs, à la politique de vie privée appliquée par le site ou aux pratiques de l'entreprise en question. Est-il, dans ce contexte, raisonnable d'accepter qu'une « entente » ainsi conclue soit imposée entre les parties et reconnue par le droit?

Il y a fort à parier de toutes façons qu'une telle situation soit un jour utilisée par l'une des parties pour invoquer un vice de consentement sur la base d'une erreur sur un élément essentiel ayant déterminé le consentement. En effet, selon l'article 1400 du Code civil du Québec :

> ***1400. CcQ*** *L'erreur vicie le consentement des parties ou de l'une d'elles lorsqu'elle porte*

[191] art.2130
[192] Lionel THOUMYRE, *L'échange des consentements dans le commerce électronique*, Juriscom.net, 15 mai 1999 http://www.juriscom.net/uni/doc/19990515.htm

> *sur la nature du contrat, sur l'objet de la prestation ou, encore, sur tout élément essentiel qui a déterminé le consentement.*
> *L'erreur inexcusable ne constitue pas un vice de consentement.*

À cela, Beaudoin et Jobin ajoutent :

> *« En utilisant l'expression « erreur sur tout élément essentiel qui a déterminé le consentement, le Code civil du Québec, à l'article 1400, regroupe sous un seul et même vocable, plus général, ce qui était connue, dans le droit antérieur, comme l'erreur sur les qualités substantielles, l'erreur sur la considération principale et l'erreur sur la cause de l'obligation.. [...] Assez souvent d'ailleurs, les juges, depuis la réforme, ne précisent pas le type d'erreur [...] pour lequel ils prononcent la nullité. »*[193]

Pour clore cette question, pouvons-nous croire que P3P sera un jour un système si répandu, si fiable techniquement et si facile à utiliser qu'il pourrait devenir inexcusable d'invoquer une erreur dans la programmation de son profil ou de ses politiques ? Cette éventualité serait plutôt étonnante à court terme. Il faudrait pour ce faire que la rédaction de la plate-forme ne laisse place à aucune interprétation, que les agents logiciels élaborés pour les usagers et les sites soient très abordables et permettent, au moyen de processus de validation très serrés, d'arriver à un résultat final par essence toujours libre d'erreurs. Autrement dit, P3P devrait devenir un standard incontournable sur le Web. Tout ceci nous amène à conclure que pour le moment, nous croyons que la possibilité qu'une entente fondée sur un consentement obtenu à travers un protocole technique comme P3P soit reconnu sans problème par un tribunal reste utopique. En l'absence d'un consentement valide en droit, il apparaît donc difficile de soutenir que P3P puisse permettre de satisfaire au principe de limitation en matière de collecte.

> *2) Principe de la qualité des données : Les données recueillies devraient être pertinentes aux finalités de la collecte et, devraient être exactes, complètes et tenues à jour.*

Dans le cas du deuxième principe aussi, la bonne foi et la vérification jouent un rôle primordial. Rien en effet dans ce que nous avons vu de la plate-forme P3P ne permet d'assurer ces critères de pertinence, d'exactitude, d'exhaustivité et d'actualité des

données. Le système repose donc sur l'acceptation préalable de la véracité des déclarations faites par un service dans sa politique P3P et, le cas échéant, sur la vérification externe qui, nous l'avons vu, n'est pas obligatoire :

> *Although P3P provides a technical mechanism for ensuring that users can be informed about privacy policies before they release personal information, it does not provide a technical mechanism for making sure sites act according to their policies. Products implementing this specification MAY provide some assistance in that regard, but that is up to specific implementations and outside the scope of this specification.*[194]

L'analyse n'est donc pas vraiment concluante sur ce principe.

> *3) Principe de la spécification des finalités : Les finalités de la collecte des données devraient être déterminées au plus tard au moment de la collecte des données. Les données ne devraient être utilisées que pour atteindre ces finalités.*

P3P passe plus facilement la barre dans le cas du troisième principe puisqu'il permet de spécifier beaucoup plus précisément les finalités justifiant la collecte des données, et même d'établir des règles différentes selon les types de données recueillies. Le lecteur se souviendra des douze sous-éléments de l'élément <PURPOSE>, et de la possibilité de créer des règles différentes dans l'un ou plusieurs des dix-sept sous-éléments de données prévus par l'élément <CATEGORIES>. Un service qui voudra implanter une politique P3P n'aura donc pas beaucoup d'excuses pour se justifier de déclarations insuffisantes à ce chapitre.

Quant à l'utilisation des données dans le seul cadre de la poursuite des finalités, comprenant par interprétation leur destruction une fois les finalités atteintes, P3P l'introduit dans son élément <RETENTION> qui encadre leur conservation. La plate-forme prévoit que si elles doivent être conservées, elles ne le seront que pendant la poursuite des fins déclarées de la collecte, ou qu'en conformité avec les lois et règlements en vigueur. On se souviendra aussi qu'en pareil cas, la politique doit

---

[193] Jean-Louis BAUDOUIN, Pierre-Gabriel JOBIN, *Les obligations*, 5e éd, Cowansville, Québec : Éditions Y. Blais, c1998, parag. 206

[194] http://www.w3.org/TR/P3P/#Introduction

fournir un calendrier de destruction dans sa version textuelle (*human readable*). Nous pouvons donc conclure que la plate-forme passe bien le test de ce troisième principe.

> *4) Principe de la limitation de l'utilisation : Les données de caractère personnel ne devraient pas être divulguées, ni fournies, ni utilisées à des fins autres que celles spécifiées sauf avec le consentement de la personne concernée ou lorsqu'une règle de droit le permet.*

Encore une fois, sujet à la conformité des déclarations avec la situation réelle et à nos commentaires sur la vérification des pratiques, nous pouvons dire que P3P permettrait au moins de bien connaître le sort réservé aux données recueillies après la collecte. Du moins, sous l'onglet « partage » de ce vaste dossier. L'élément <RECIPIENT> , obligatoire d'ailleurs, précisant quel seront les organismes qui auront accès aux dossiers.

Il est donc raisonnable de conclure que P3P permettrait au moins de recevoir une déclaration à ce sujet, qui pourra ici aussi être précisée selon les catégories d'informations. P3P se comporte bien face à ce principe, bien que le doute qui subsiste quant à la vérification des pratiques nous retient de lui accorder un score parfait.

> *5) Principe des garanties de sécurité : Les données de caractère personnel devraient être protégées grâce à des garanties de sécurité raisonnables, contre la perte ou leur accès, destruction, utilisation, ou divulgation non autorisés.*

Ici aussi, P3P est volontairement muet dans la rédaction de la spécification technique :

> *In addition, P3P does not include mechanisms for transferring data or for securing personal data in transit or storage. P3P may be built into tools designed to facilitate data transfer. These tools should include appropriate security safeguards.*[195]

Il ne permet donc pas d'assurer un quelconque niveau de sécurité dans la conservation des données recueillies.

[195] Id.

> *6) Principe de la transparence : La transparence des pratiques et politiques, ayant trait aux données de caractère personnel doit être assurée. Principe de la participation individuelle.*

P3P est un projet dont la philosophie est justement d'assurer la transparence des politiques et de favoriser la conclusion d'ententes préalables à toute collecte d'information. Les objectifs qui ont inspiré ce principe semblent donc biens englobés par la plate-forme.

> *7) Droits de la personne physique :*
>
> *a) obtenir confirmation du fait que le maître du fichier détient ou non des données la concernant ;*
>
> *b) obtenir communication des données la concernant, dans un délai raisonnable, moyennant, éventuellement, une redevance modérée, selon des modalités raisonnables et sous une forme qui lui soit aisément intelligible ;*
>
> *c) être informée des raisons pour lesquelles une demande quelle aurait présentée conformément aux alinéas (a) et (b) est rejetée et de pouvoir contester un tel rejet ; et*
>
> *d) contester les données la concernant et, si la contestation est fondée, de les faire effacer, rectifier, compléter ou corriger.*

Deux éléments de la syntaxe P3P peuvent nous aider dans notre appréciation de sa performance face à ces droits des usagers : <ACCESS>, et <REMEDIES>. Tout d'abord <ACCESS>, qui balise le droit d'accès de l'individu à son dossier. Nous remarquons que la plate-forme prévoit la possibilité de refuser tout accès de l'individu aux données le concernant, ce qui est contraire aux principes de l'OCDE, et même aux dispositions de la *Loi québécoise :*

> ***27.*** *Toute personne qui exploite une entreprise et détient un dossier sur autrui doit, à la demande de la personne concernée, lui en confirmer l'existence et lui donner communication des renseignements personnels la concernant.*[196]

[196] *Loi sur la protection des renseignements personnels dans le secteur privé* LRQ c. P-39.1; sur le Web : http://www.canlii.org/qc/loi/p39.1/, art. 27

La loi fédérale C-6 reprend aussi cette règle par le biais de son adoption du neuvième principe du code type CSA[197].

L'inclusion d'une telle option dans la spécification de P3P est tout à fait stupéfiante puisqu'elle permet en quelque sorte de stipuler des politiques qui seront carrément contraires aux lois en vigueur dans plusieurs pays et aux principes fondamentaux en matière de protection des renseignements personnels. L'arrimage souhaité entre P3P et les lois existantes, notamment dans le contexte des accords de Safe Harbour ne semble donc pas avoir été tellement pris en considération dans la rédaction de la plate-forme. Il faut espérer que les services qui élaboreront leurs politiques P3P qu'ils respectent les lois en vigueur dans leur juridiction et que, dans l'ensemble, peu d'entre eux auront recours à l'option <NONE>...

Nous constatons par ailleurs que l'élément <REMEDIES> se comporte un peu mieux, puisqu'il comprend un choix de valeurs prévoyant que le service s'engage à corriger les erreurs ou l'inclusion par référence des règles de droit en vigueur dans la juridiction concernée. Mais dans l'ensemble, l'effet négatif découlant de la possible exclusion de tout droit d'accès aux informations est suffisant pour nous faire douter de la capacité de P3P de protéger adéquatement l'usager à ce chapitre, et à se modeler aux différents systèmes juridiques.

Nous nous permettrons une parenthèse à ce sujet. Dès les débuts de notre étude de P3P, la possibilité d'interaction entre usagers et sites grâce au Web et à sa technologie nous a semblé constituer un terreau propice au développement d'interfaces interactives de gestion des renseignements personnels. Cette réflexion nous apparaissait particulièrement pertinente au chapitre de l'accès et de la correction des informations, la possibilité d'une connexion directe de l'internaute au site de l'organisme concerné constituant une occasion en or de lui donner accès à son dossier et d'en arriver à une gestion quasi-instantanée des demandes de correction. Nous constatons que la plate-forme reste relativement faible sur ce sujet ou, à tout le moins,

[197] *Loi sur la protection des renseignements personnels et les documents électroniques*. L.C. 2000 c. 5, art. 4.9 et ss.; Sur le Web http://www.canlii.org/ca/loi/p-8.6/partie74947.html,

qu'elle ne cherche pas à tirer profit de la situation pour faciliter cet aspect capital de la gestion des renseignements personnels.

Nous pouvons aussi inclure au chapitre de la protection des droits des usagers, bien que cette possibilité ne figure pas directement aux principes de l'OCDE ou aux lois relatives à la protection des renseignements personnels, la section de P3P exigeant l'indication à la politique P3P d'un mode de règlement des conflits. L'individu pourrait en effet utiliser ce moyen pour faire prévaloir ses droits. L'élément < DISPUTES > vient donc obliger le service à dévoiler dès le départ ses couleurs en la matière, ce qui est très positif. Un usager pourra ainsi connaître la marche à suivre pour se plaindre ou obtenir réparation si un problème survient, et prendre en conséquence la décision de transmettre ou non ses informations. Sans revenir sur les faiblesses juridiques de cette section, rappelons quand même la bizarre possibilité du recours au « service à la clientèle », nos interrogations sur la valeur juridique du choix de l'arbitrage et sur le problème posé par la présence du choix de juridiction dans cette partie de l'encodage.

L'obligation faite par P3P d'inclure un mode de résolution des différends améliore un peu à nos yeux sa performance vis à vis des principes de protection des droits de l'individus. Mais des amendements à cette partie du protocole restent quand même fort souhaitables dans la prochaine version afin de resserrer un peu les faiblesses de rédaction de la spécification à ce chapitre.

> *8) Principe de la responsabilité Tout maître de fichier devrait être responsable du respect des mesures donnant effet aux principes énoncés ci-dessus.*

Ici aussi, sujet à nos remarques formulées au chapitre 3 relativement à la clarté de la rédaction de ces sections de la spécification, nous constatons que la plate-forme cherche bien à identifier l'entité qui opère le service d'où origine la politique P3P. Les objectifs du huitième et dernier principe seraient donc rencontrés.

Dans l'ensemble, nous constatons que le score de P3P face aux grands principes du droit de la protection des renseignements personnels est loin d'être égal. P3P réussit

relativement mal dans les aspects demandant une intervention (négociation, entente, accès, correction, etc…) alors qu'il semble bien meilleur pour s'acquitter de fonctions relevant de l'information. Si l'absence de procédures de vérification rendent difficile le respect de quelques-uns des principes de l'OCDE comme celui de la qualité des données, d'autres comme celui de la transparence et de la responsabilité y trouvent un traitement beaucoup plus avantageux. De la même façon, si nous avons pu toucher du doigt les aléas du concept de négociation et d'entente du plan d'origine, nous avons quand même pu mettre en valeur les possibilités offertes par l'encodage normalisé des politiques de vie privée, tout particulièrement au chapitre de la déclaration des finalités de la collecte.

4.3 P3P face au Web

Toutefois, le projet P3P devra passer un test encore plus critique avant d'espérer atteindre ses objectifs : s'intégrer aux us et coutumes des internautes. En effet, c'est en gagnant de la popularité qu'il pourra atteindre une masse critique d'utilisateurs, tant commerciaux que privés, et justifier son développement ultérieur. Essayons d'évaluer ses chances de succès en quelques mots, en tentant de voir comment il peut espérer se faire une place dans le merveilleux monde du Web.

Nous devons malheureusement émettre de sérieux doutes à ce chapitre. Tout d'abord au niveau de la complexité du plan général d'intervention et de la rédaction de ses termes techniques. Le Web compte des dizaines de millions d'usagers qui, il faut l'admettre, disposent d'un bagage de connaissances en informatique très variable. La convivialité grandissante du réseau et des technologies récentes permettant de naviguer sans vraiment savoir comment fonctionne la mécanique, nombre d'internautes n'ont donc pas plus connaissance des réglages de leurs ordinateurs et navigateurs qu'ils ne connaissent les principes de l'OCDE en matière de protection de leurs renseignements personnels. S'ils sont généralement mal à l'aise au moment de répondre à des questions indiscrètes en ligne ou de fournir leurs coordonnées bancaires, l'idée qu'ils se font des risques réels de l'opération et de son contexte légal est plutôt floue. P3P ne vient pas vraiment simplifier la chose, au contraire. Comment

en effet amener les usager à finement configurer leurs préférences pour refléter leurs désirs réels, par exemple au niveau de leur droit d'accès, et respecter les lois en vigueur dans leur juridiction s'ils ne savent même pas qu'il leur est possible de bloquer les témoins ? Plusieurs ne sachant même pas ce qu'est un témoin, il y a vraiment loin de la coupe aux lèvres.

Les différences marquées entre les applications P3P destinées aux internautes pourraient ici entrer en ligne de compte. L'usage très limité qu'a fait Explorer de P3P, et à un degré moindre l'absence totale de Netscape du tableau, pourraient bien avoir engagé le projet sur une voie de garage car sa meilleure chance de s'insérer dans la fibre du Web résidait en son intégration aux navigateurs les plus connus. Il est en effet malheureusement à prévoir que bien peu d'internautes poseront le geste de rechercher, télécharger et installer un agent logiciel P3P .

La complexité de la rédaction, dont nous avons pu voir quelques exemples au chapitre précédent, pourrait aussi constituer un obstacle à l'adhésion des opérateurs de sites Web. Il faudra espérer l'apparition d'outils et de conseillers en la matière, comme le *Privacy Council*[198] par exemple, pour leur offrir le support technique et juridique requis et s'assurer que leurs politiques correspondent à leurs pratiques réelles.

La mise en œuvre de P3P comporte de plus plusieurs risques. Tout d'abord au niveau de sa rédaction qui emprunte au droit sans véritablement l'englober de façon satisfaisante. Si les faiblesses et imprécisions de la plate-forme relevées par un regard de juriste sont malheureuses dans la phase 1, elles pourraient devenir inquiétantes ou même carrément catastrophiques dans une deuxième phase qui mettrait en place des processus de conclusion d'ententes autorisant de réels échanges d'informations. Le portrait ne s'améliore pas lorsqu'on réalise l'effet obtenu en combinant de possibles ententes boiteuses conclues sur la base de consentements viciés avec des processus automatisés d'échange d'informations structurées selon un mode normalisé. Les informations y gagneront beaucoup de vélocité puisqu'elles pourront s'échanger plus rapidement et être utilisées avec une efficacité redoutable, sans que le consentement

[198] http://www.privacycouncil.com/p3p_compliance.php

de l'internaute ne puisse être considéré ni fiable ni basé sur une connaissance réelle des usages projetés. Ajoutons à l'équation l'absence de l'obligation de souscrire à des procédures de vérification externes et nous obtenons une situation potentiellement très instable et peut-être même pire que la problématique actuelle que le W3C cherche à résoudre.

L'illusion de sécurité conférée par un système défaillant peut être plus dangereuse que l'absence totale de normes. D'ailleurs, si on examine la question sous un autre angle, les racines du projet en font justement un système axé vers l'autorisation de la collecte de renseignements sur les usagers du Web plutôt que vers la protection de la vie privée des individus. Dès le départ l'optique adoptée par les initiateurs a été de mettre en place un mécanisme qui permettrait aux sites d'obtenir le consentement des internautes à la collecte d'informations les concernant par le dévoilement des pratiques des sites. C'était là une façon de satisfaire les gouvernements en démontrant la rectitude des pratiques ayant cours sur Internet par l'apposition du sceau d'approbation des usagers eux-mêmes. La plate-forme n'avait pas pour but d'empêcher ou de limiter la collecte pour une meilleure protection des individus. C'est l'optique adoptée par une critique de P3P :

> *«Essentially, privacy practices are not the same as privacy as in "the right to be left alone." Privacy preferences are exercised within the context of a data exchange; the user gives more or less information based on a set of factors. Nowhere do the authors of P3P suggest that less information should be exchanged between users and Web sites. If your definition of privacy includes anonymous Web surfing, then P3P will not help you achieve that goal. »*[199]

Rappelons-nous les composantes de la vie privée telles que définies par Westin, et repris dans le rapport d'une commission d'enquête fédérale au début des années soixante-dix, déjà citées au chapitre 2 :

> *" ... la solitude – pour que l'homme puisse réfléchir sur ce qui lui arrive; l'intimité avec la famille et les amis – pour permettre des relations plus étroites, plus attachantes; l'anonymat – pour permettre à l'homme*

[199] Karen COYLE *P3P: Pretty Poor Privacy? A Social Analysis of the Platform for Privacy Preferences (P3P),* June 1999, http://www.kcoyle.net/p3p.html

> *d'exister en dehors du milieu où il évolue; et la distance – pour qu'il puisse suspendre les communications quand il en éprouve le besoin. "*[200]

Il faut admettre que P3P ne cherche pas vraiment à satisfaire à ces attentes bien qu'il donne l'impression de vouloir régler la problématique de la vie privée sur Internet, d'où l'illusion.

Ce qui ne veut pas dire que P3P soit totalement inutile par ailleurs, loin de là. Ses meilleures chances de succès résident dans la définition objective de ses forces et de ses faiblesses. Le W3C pourra alors espérer qu'il soit vraiment efficace dans les domaines où son intervention risque le plus d'être bénéfique.

4.4 Que faire alors ?

Quel rôle P3P peut-il jouer pour apporter une contribution significative à l'effort de normalisation des échanges de renseignements personnels sur les internautes? En bout de piste, notre analyse nous amène à conclure que P3P aurait tout avantage à éviter de s'immiscer dans des processus où il ne peut réussir, comme la conclusion d'une entente par exemple, à moins de pouvoir proposer une solution tout à fait sécuritaire et étanche. Par ailleurs, il faut constater que P3P a été présenté il y a bientôt quatre ans, une éternité sur le Web. Il faut aussi remarquer qu'il a fait l'objet de dilutions successives qui l'ont édulcoré au point de lui retirer le plus clair de sa saveur originale. Ceci peut nous indiquer que ses fonctions de négociation, de conclusion d'ententes et de transmission d'informations, suscitent de réelles résistances dans les milieux concernés. Ce qui confirmerait que nos craintes quant à la formation intempestive de consentements d'une fiabilité douteuse sont partagées.

Les fonctions relevant de l'information sur les pratiques, où les règles de P3P ont plus de succès et permettent de mieux rencontrer les objectifs généraux ayant cours dans le domaine de la protection des renseignements personnels, étant pour la plupart déjà en vigueur, le W3C pourrait se concentrer sur l'inclusion de normes plus précises quant

[200] INFORMATION CANADA , *L'ordinateur et la vie privée*. Rapport du groupe d'étude établi conjointement par le ministère des Communications et le ministère de la Justice. Ottawa, 1972, p. 18-19

à la vérification des pratiques des services et sur l'amélioration de la rédaction de certaines parties de sa spécification.

De cette manière, tout en laissant la négociation des ententes, la confirmation du consentement et la transmission des informations aux usagers eux-mêmes, P3P pourrait apporter une excellente contribution en normalisant la façon dont les politiques de vie privée sont présentées et structurées, en favorisant l'élaboration d'interfaces permettant de décoder les politiques et de les présenter aux usagers de façon plus compréhensible. En encourageant, finalement, le développement de mesures de contrôle qui ne pourront que bénéficier à tous. P3P se voulant déjà complémentaire aux différentes lois en vigueur, il pourrait du même souffle contribuer à renseigner les usagers sur les situations qu'ils rencontrent à travers des interfaces familières, sans prétendre se substituer à eux pour la prise de décision ni être le génie qui viendra trancher le nœud gordien de l'application de lois divergentes. Le professeur Graham Greenleaf lui-même a d'ailleurs mesuré l'ampleur d'une telle tâche :

> *« P3P could develop as one of many useful forms of privacy protection, but it will be of little value unless it meshes with law and organizational practices. P3P is therefore an instance of where law is necessary to make protections offered by cyberspace architecture meaningful. Until law does that, P3P could be little more than a framework for deception.*[201] *»*

La meilleure contribution de P3P serait donc selon nous de mieux éclairer le consentement que l'internaute sera appelé à donner lui-même, selon l'ordre normal des choses.

Dans la même foulée, il serait beaucoup plus facile pour un État d'avoir prise sur le réseau en imposant à ses ressortissants faisant affaires sur le Web de déclarer leurs politiques de vie privée sous le format P3P, que de tenter de conférer par la loi un statut juridique aux ententes produites par le projet d'origine. Les risques potentiels de l'application d'ententes ne reflétant pas nécessairement les volontés des usagers pourraient en effet constituer un frein suffisant pour dissuader les États d'agir en ce

[201] Graham GREENLEAF, *An endnote on regulating cyberspace:architecture vs Law*,

sens, alors que l'adoption du standard P3P pour le simple encodage des politiques pourrait au contraire présenter une avenue d'intervention intéressante.

Si nous nous référons simplement à notre Code civil, nous constatons à ce niveau l'imposition d'une obligation générale d'information aux parties à un contrat, afin de favoriser la formation d'un consentement éclairé :

> *« Peu de temps avant l'entrée en vigueur du nouveau code, la Cour suprême est venue consolider cette tendance et faire de l'obligation d'information, à certaines conditions, une obligation générale ; l'existence de cette obligation a été reconnue à la formation du contrat et en cours de contrat.* [202] *Dans certaines circonstances, donc, une partie ne peut plus se contenter de répondre honnêtement aux questions de l'autre partie : elle doit prendre l'initiative de lui divulguer tous les faits qui sont normalement susceptibles d'influencer son consentement de façon importante. »*

L'intérêt d'utiliser ainsi P3P apparaît intéressante dans ce contexte.

Pour terminer, pouvons-nous conclure que notre examen emporte un constat d'échec du projet P3P et, de façon plus large, des théories de régulation par l'architecture avancées notamment par Lessig et Greenleaf ? Dans le premier cas, la constatation se doit d'être plus finement stipulée car rien ne permet de croire que P3P ne pourra jamais rencontrer tous les objectifs de ceux qui l'ont conçu au départ. Il faut plutôt conclure que le W3C devra s'assurer que la technologie, les internautes et les cyber-commerçants sont vraiment prêts avant de s'aventurer dans d'autres fonctions que celles relevant de la simple organisation de l'information. Il est dans ce contexte difficile de conclure à l'échec. Disons plutôt que le développement du projet a montré que ce type d'intervention doit mesurer avec précision le domaine d'intervention qu'il peut raisonnablement espérer occuper. Adopter une attitude réaliste n'équivaut certes pas pour nous à un échec.

Par ailleurs, P3P a souvent été cité comme constituant un exemple de choix de l'application des théories de régulation par l'architecture. Pouvons-nous invoquer les

---

http://www.austlii.edu.au/au/other/unswlj/thematic/1998/vol21no2/greenleaf.html

[202] *Banque de Montréal c. Bail ltée*, (1992) 2 R.C.S. 554. Disponible sur le Web au http://www.canlii.org/ca/jug/csc/1992/1992csc68.html

aléas de l'élaboration de P3P et des résultats obtenus pour conclure à la faillite de ces théories ? Nous ne le croyons pas. Si le constat d'échec pour P3P quant à sa capacité à régler la problématique de la vie privée dans le cyberespace devait se matérialiser, la résultante devrait plutôt être la recherche d'un meilleur exemple aux théories de Lessig plutôt que leur rejet pur et simple. D'un autre côté, l'expérience de P3P permettra peut-être de confirmer que la technique permet bel et bien une certaine prise sur le réseau, mais que son intervention est limitée dans la réalisation de certains gestes juridiques.

En d'autres mots, P3P pourrait nous donner de précieuses informations autant sur le potentiel que sur les limites du concept de l'utilisation de la technique dans l'application de normes juridiques, ce qui ne pourrait qu'être utile dans la conception de ses successeurs.

* * *

Conclusion

La création, l'échange et le partage d'informations est à la base de toute communication sur un réseau informatique. L'arrivée de centaines de millions de visiteurs sur le Web a généré une masse gigantesque d'informations contenant très souvent des renseignements personnels sur des individus et leur agissements. Dans un tel contexte il n'est pas étonnant qu'un important marché de l'information sur les usagers du Web se soit développé très tôt dans l'histoire du réseau. La valeur des informations échangées et des profils établis ayant justifié tous les stratagèmes susceptibles d'alimenter les banques de données.

L'émergence de solutions techniques à ces problèmes n'étonne pas non plus, le potentiel régulateur de la technique sur le Web semblant prometteur aux yeux de plusieurs observateurs. Cette avenue ne pouvait d'ailleurs qu'intéresser les institutions américaines en quête d'une piste de solution mettant de côté toute intervention étatique. P3P apparaît donc comme la conséquence logique de ces événements. Mais ceci ne veut pas dire qu'il faut pour autant en arriver à une solution qui retire tout contrôle à l'individu sur ses choix en le livrant pieds et poings liés au tout puissant dieu de la technique.

Le W3C aura bientôt des choix déterminants à faire quant à sa plate-forme P3P. Poursuivra-t-il sa recherche d'une solution innovatrice substituant la technique au libre arbitre humain dans la conclusion d'une entente sur la transmission de renseignements personnels? Préférera-t-il plutôt consolider la première mouture de son projet, se contentant d'établir un mode normalisé de communication des politiques de vie privée?

L'informatique comporte bien sûr des avantages qu'il faut exploiter. Elle permet notamment de mieux gérer, organiser et présenter l'information. Pour l'usager d'un réseau compatible à P3P 1.0, ceci pourrait se traduire par plus de clarté dans la présentation de politiques de vie privée qu'avant seuls certains initiés pouvaient espérer comprendre. De bons outils P3P pourraient fort bien retracer, lire, et décoder ces documents pour lui afin de les lui rendre plus accessibles.

Peu importe la façon dont les sites les auront élaborées et où ils les auront affichées sur leur site, l'usager pourrait alors en voir la teneur dans un format qui lui sera familier, le rendant du coup mieux en mesure de prendre une décision éclairée. Lui est-il vraiment nécessaire de pouvoir « *mandater* » son système pour négocier et conclure à sa place une entente avec le site qu'il visite? La technologie est-elle suffisamment fiable aujourd'hui pour qu'elle ose se substituer au jugement du principal intéressé et produire des ententes fidèles à sa volonté qui lieront juridiquement les parties? Le développement d'outils techniques et juridiques permettant l'implantation d'un tel cadre est-il vraiment réaliste, ou même prioritaire? Il faudra un jour se demander si de telles fonctions sont vraiment conçues dans l'intérêt de l'usager. À première vue, elles semblent beaucoup plus compatibles avec ceux des opérateurs de sites qui aimeraient multiplier les consentements au rythme de leurs cueillettes d'information pour montrer patte blanche aux gouvernants.

Nous croyons personnellement que l'implantation intempestive d'un protocole technique générateur d'ententes contestables ne peut être avantageuse pour personne et apportera plus d'incertitude que de sécurité sur le réseau. À l'opposé, l'établissement d'un mode normalisé de communication informant mieux les usagers renforcerait la valeur des consentements qu'ils doivent fournir et pourrait contribuer à assainir la situation..

Nous croyons que c'est à l'individu que revient la prise de décision finale sur la transmission de ses renseignements personnels. Pousser plus loin le développement technologique est certes important, mais pas au risque d'ébranler la sécurité que le droit impose dans un domaine aussi important. Car finalement, la sagesse consiste souvent à savoir où s'arrêter.

***

Sources documentaires

I - Doctrine

a) Monographies et recueils

ARIÈS P., *Histoire de la vie privée*. Paris : Éditions du Seuil, 1985.

BAUDOUIN, J.-L., P-G JOBIN, *Les obligations*, 5e éd., Cowansville, Québec : Éditions Y. Blais, 1998

BEIGNIER, B., *Le droit de la personnalité*, Paris, Presses universitaires de France, 1992.

BÉLIVEAU P., *Les garanties juridiques dans les chartes des droits*, 2e ed., Montréal, Éditions Themis, 1995.

BENYEKHLEF, K., *La protection de la vie privée dans les échanges internationaux d'informations*., Montréal, Thémis, 1992.

CHOLEWINSKI, R.I., *Les Droits de la personne au Canada : dans les années 1990 et au-delà.* Ottawa : Centre de recherche et d'enseignement sur les droits de la personne, Université d'Ottawa, 1990.

CÔTÉ, R., *Vie privée sous surveillance : la protection des renseignements personnels en droit québécois et comparé*. Cowansville, Éditions Y. Blais, 1994.

GAUCH, P., F WERRO, J-B ZUFFEREY (dir), *La Protection de la personnalité : bilan et perspectives d'un nouveau droit ; contributions en l'honneur de Pierre Tercier pour ses cinquante ans* , Fribourg : Éditions universitaires, 1993.

G.R.I.D. , *L'identité piratée*, Montréal, Soquij, 1986

HOGG, P. W., *Constitutional Law of Canada*.., (2e edition), Toronto, Carswell, 1985

KATSH, E., *Law in a digital world*, New York, Oxford university Press, 1995

LAMARCHE, L., *Le régime québécois de protection et de promotion des droits de la personne.,* Montréal, Éditions Yvon Blais, 1996

LESSIG, L., *Code and other laws of cyberspace*, NewYork, Basic Books, 1999.

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

TRUDEL, P. et al, *Droit du cyberespace*, Montréal, Éditions Themis, 1997

WACKS, R., *Personal Information / Privacy and the law*, Oxford, Clarendon Press, 1993

WESTIN, A.F., *Privacy and Freedom*. New York, Atheneum, 1970

WESTIN, A.F., M. A. BAKER, *Databanks in a free society: computers, record-keeping and privacy*, New York, Quadrangle , 1972

b) Articles et sondages

ADAR, E., et B HUBERMAN, *Free Riding on Gnutella*, http://www.firstmonday.dk/issues/issue5_10/adar/index.html

BENYEKHLEF, K., *Les normes internationales de protection des données personnelles et l'autoroute de l'information*, http://www.canada.justice.gc.ca/fr/cons/jae/karim.html#recueillies

BURNS, P.: *Privacy and the Common Law : a tangled skein unravalling*? dans : GIBSON, D. (dir.) *Aspects of Privacy Law. Essays in Honour of John M. Sharp*, Butterwoths, 1980, page 21 et ss.

CADOUX, L., *Analyse de la position européenne concernant le Safe Harbor* . http://www.delis.sgdg.org/menu/donneesperso/safeharbour.htm

CENTER FOR DEMOCRACY AND TECHNOLOGY (CDT), *Privacy Not Price Keeping People Off The Internet*, http://www.cdt.org/privacy/survey/findings/

CHASSIGNEUX, C., *La protection des données personnelles en France*, Lex Electronica, vol. 6, n°2, hiver 2001, http://www.lex-electronica.org/articles/v6-2/chassigneux.htm

CLARKE, R., *Platform for Privacy Preferences: An Overview*. Version du 20 mai 1998, amendée le 12 mai 1999, http://www.anu.edu.au/people/Roger.Clarke/DV/P3POview.html

COYLE, K., *P3P: Pretty Poor Privacy? A Social Analysis of the Platform for Privacy Preferences (P3P).,* June 1999, http://www.kcoyle.net/p3p.html

CRANOR, L.F., J REAGLE, et M. S. ACKERMAN *Beyond Concern: Understanding Net Users' Attitudes About Online Privacy.,* 14 avril 1999, http://www.research.att.com/projects/privacystudy/

DESJARDINS, L., *Responsabilité civile et Internet: Le médium utilisé importe peu*. Le journal du Barreau, 15 juin 1997, http://www.barreau.qc.ca/journal/vol29/no11/responsabiliteinternet.html#note2

DEUTSCHER, D., *The protection of privacy Act :whose privacy is it protecting*?, dans Dale GIBSON (dir.) *Aspects of Privacy Law. Essays in Honour of John M. Sharp*, Butterwoths, 1980, page 141 et ss.

GAUTRAIS, V., G. LEFEBVRE et K. BENYEKHLEF, *Droit du commerce électronique et normes applicables : l'émergence de la lex mercatoria*, (1997) 5 RDAI/IBLJ 547, 550 et ss.

GLENN, P., *The right to privacy in Quebec Law*. dans Dale GIBSON (dir.) *Aspects of Privacy Law. Essays in Honour of John M. Sharp*, Butterwoths, 1980, page 41 et ss.

GREENLEAF, G., *An endnote on regulating cyberspace:architecture vs Law*, http://www.austlii.edu.au/au/other/unswlj/thematic/1998/vol21no2/greenleaf.html

LOUIS HARRIS AND ASSOCIATES, *E-Commerce Privacy Survey*, avril 1998, http://www.privacyexchange.org/iss/surveys/ecommsum.html

LABBÉ, E., *La technique dans la sphère de la normativité : aperçu d'un mode de régulation autonome*, Juriscom.net, 8 novembre 2000, http://www.juriscom.net/uni/doc/20001108.htm

LESSIG, L., *The Law of the Horse: What Cyberlaw Might Teach*, http://cyber.law.harvard.edu/works/lessig/finalhls.pdf

LESSIG, L., *Reading the Constitution in Cyberspace* (1997) 45 Emory L. J. 869-910

OSBORNE, P.H., *The privacy Acts of British Columbia, Manitoba and Saskatchewan*, dans : GIBSON, D. (dir.) *Aspects of Privacy Law. Essays in Honour of John M. Sharp*, Butterwoths, 1980, page 73 et ss.

PÉLADEAU, P., *Looking Beyond Privacy*., http://www.lex-electronica.org/articles/v3-2/peladeau.html

POST, D.G., *Anarchy, State, and the Internet: An Essay on Law-Making in Cyberspace (Article 3),* 1995, http://www.cli.org/DPost/X0023_ANARCHY.html

POULLET, Y., *Les Safe Harbor Principles - Une protection adéquate ?,* Juriscom.net, 17 juin 2000, http://www.juriscom.net/uni/doc/20000617.htm

RACICOT, M., M. S. HAYES, A. R. SZIBBO, P. TRUDEL, *L'espace cybernétique n'est pas une terre sans loi : étude des questions relatives à la responsabilité à l'égard du contenu sur Internet*, http://strategis.ic.gc.ca/pics/itf/1603118f.pdf

REAGLE , J.et L.F. CRANOR, *The Platform for Privacy Preferences*. P3P Note 06-November-1998, http://www.w3.org/TR/NOTE-P3P-CACM/ ; Également publié dans Communications of the ACM, Vol. 42, No. 2 (Feb. 1999), Pages 48-55

REIDENBERG, J. R., *Governing networks and rule-making in cyberspace*, 45 Emory Law Journal 911 (1996); sur le Web: http://www.law.emory.edu/ELJ/volumes/sum96/reiden.html

REIDENBERG, J. R., *The Use of Technology to Assure Internet Privacy : Adapting Labels and Filters for Data Protection* , http://www.lex-electronica.org/articles/v3-2/reidenbe.html

REIN, L., *The Evolution of a Privacy Standard*, XML.com, 5 mai 1999 http://www.xml.com/pub/1999/05/p3pdraft.html

SANDBOTHE, M., *Interactivity - hypertextuality - transversality: A media-philosophical analysis of the Internet*.. http://www.uni-jena.de/ms/tele/e_top.html

STANDLER, R.B., *Privacy Law in the USA*. http://www.rbs2.com/privacy.htm

TASCHEREAU, A., *Le libelle diffamatoire*. Dans *MEREDITH MEMORIAL LECTURES : Four lectures and one panel discussion on purchase and sale of business enterprise, jurimetrics, libel, estate planning. / Quatre conférences et une table ronde sur l'achat et la vente d'entreprises, jurimétrie, le libelle, planification successorale*. Montréal, Wilson et Lafleur, 1970

THOUMYRE, L., *L'échange des consentements dans le commerce électronique*., Juriscom.net, 15 mai 1999 http://www.juriscom.net/uni/doc/19990515.htm

TILMAN, V., *Arbitrage et nouvelles technologies : Alternative Cyberdispute Resolution*, Revue Ubiquité, 1999, n° 2, p. 47-64. Sur le Web : http://www.droit.fundp.ac.be/textes/ADR.pdf

VARTANIAN, T.P., *In and Out of Court: The Legal Perspective on Privacy & Commerce,* http://www.ffhsj.com/bancmail/bmarts/priv_spch.htm

WARREN, S. D., L. D. BRANDEIS, *The Right to Privacy*, 4 Harvard L.R. 193 (1890). Sur le Web: http://www.lawrence.edu/fac/boardmaw/Privacy_brand_warr2.html

c) Médias d'information (imprimés et électroniques)

ABC News, *Internet Companies Sign on to Self-Regulation Sealing Your Online Privacy Fate* , 24 juillet 1998, *http://more.abcnews.go.com/sections/tech/dailynews/truste980722.html*

ABC NEWS, *E-Bill of Rights' Moves Forward* , 31 juillet 1998, http://abcnews.go.com/sections/tech/DailyNews/netprivacy_kids980731.html

ABC NEWS, *Intel Looks Into Reported Flaw*, 23 février 1999 http://www.abcnews.go.com/sections/tech/DailyNews/pentiumflaw990223.html

Associated Press, *FBI Gets Carnivore Approval*, Wired, 22 novembre 2000, http://www.wired.com/news/politics/0,1283,40335,00.html

BENNER, J., *EBay Alters Privacy Policy*, Wired News, 2 avril 2001, http://www.wired.com/news/business/0,1367,42778,00.html

EPICALERT, *Microsoft Tracks Users, But Watchdog is Mute*, Volume 6.05, March 25, 1999, http://www.epic.org/alert/EPIC_Alert_6.05.html , 4e article

KREBS, B., *FTC Urged To Go Public On Privacy Investigations*, Newsbytes, 17 juillet 2001, http://www.newsbytes.com/news/01/168047.html

LE JOURNAL DU NET, *E-commerce, le marché dans le monde*. http://www.journaldunet.com/cc/cc_ecommd.shtml

McCULLAGH, D., *Forbes, the Privacy Candidate*, 17 décembre 1999, http://www.wired.com/news/print/0,1294,33049,00.html

McWILLIAMS, B., *Stealing MS Passport's Wallet*, Wired news, Nov. 2, 2001, http://www.wired.com/news/technology/0,1282,48105,00.html

MULTIMÉDIUM, *Québec: la loi sur le commerce électronique sera adoptée au printemps*. 10 septembre 1999 http://www.mmedium.com/cgi-bin/nouvelles.cgi?Id=2604

MULTIMÉDIUM, *Plus de sécurité avant d'acheter en ligne, disent les québécois*., 13 septembre 1999, http://www.mmedium.com/cgi-bin/nouvelles.cgi?Id=2608

MULTIMÉDIUM, *Québec, Watatatow! Hotmail a été piraté*!, 30 août 1999, http://www.mmedium.com/cgi-bin/nouvelles.cgi?Id=2577

MULTIMÉDIUM, *Hotmail piraté: ce n'est pas de notre faute, dixit Microsoft*, 30 août 1999, http://www.mmedium.com/cgi-bin/nouvelles.cgi?Id=2580

REUTERS, *Privacy groups slam Windows XP*, October 23, 2001, http://www.zdnet.com/zdnn/stories/news/0,4586,5098685,00.html

ROSE, L., *FTC seeking to regulate online privacy*, Washington Legal Foundation, 24 février 1996, http://www.webcom.com/lewrose/article/ftcprivacy.html

SPRENGER, P., *Intel on Privacy: 'Whoops*!' Wired, 25 janvier 1999, http://www.wired.com/news/news/politics/story/17513.html

WHATIS.COM, *What is: an internet protocol*?

http://searchnetworking.techtarget.com/sDefinition/0,,sid7_gci212839,00.html

WHATIS.COM, *What is : OPS* ?

http://searchwebmanagement.techtarget.com/sDefinition/0,,sid27_gci214208,00.html

WHATIS.COM, *What is : XML* ?

http://searchwebservices.techtarget.com/sDefinition/0,,sid26_gci213404,00.html

WHATIS.COM, *What is : an application* ?

http://searchwebmanagement.techtarget.com/sDefinition/0,,sid27_gci211585,00.html

WHATIS.COM, *What is : a platform* ?

http://searchhp.techtarget.com/sDefinition/0,,sid6_gci212797,00.html

WHATIS.COM, *What is a program* ?

http://whatis.techtarget.com/definition/0,,sid9_gci212834,00.html

YAHOO FINANCE*, Privacy Council Selects IDcide PrivacyWall Product for Remote Diagnosing Of Website Privacy Gaps and P3P Compliance Program.*, 27 septembre 2001, http://biz.yahoo.com/prnews/010927/dcth023_1.html

ZDNET, *Gore says laws needed to protect privacy*, 31 juillet 1998, http://www.zdnet.com/zdnn/stories/news/0,4586,2124342,00.html

d) communiqués et documents divers

FEDERAL TRADE COMMISSION, *FTC sues failed Website, Toysmart.com, for deceptively offering for sale personal information of Website visitors*., Washington, 10 juillet 2000, http://www.ftc.gov/opa/2000/07/toysmart.htm

GOOGLE, *Google Acquires Deja's Usenet Archive*., 2001, http://groups.google.com/googlegroups/deja_announcement.html

MICROSOFT, *Microsoft Passport: Streamlining Commerce and Communication on the Web*, 11 octobre 1999, http://www.microsoft.com/presspass/features/1999/10-11passport.asp

TRUSTE, *Microsoft Statement of Finding*, Watchdog #1723, http://www.truste.org/news/padvisories/users_w1723.html

WEITZNER'S, D., P3P: User Empowerment Tools for Web Privacy, slides presented at 23 April 2001 National Association of Attorneys General meeting [PowerPoint slides], http://www.w3.org/P3P/naag-p3p.ppt

II- Documents et rapports officiels

AUTOROUTE DE L'INFORMATION (QUÉBEC), *L'autoroute de l'information, au cœur du développement du Québec*., notes pour l'allocution de M. David Cliche, à l'occasion d'un déjeuner-causerie organisé par la Fédération de l'informatique du Québec, Section de Montréal, Montréal, Le 18 février 1999, http://www.tresor.gouv.qc.ca/ministre/disenjeu.htm

CANADA. Ministère des communications, *Principes de protection de la vie privée dans les télécommunications*.,Ottawa, Communications Canada, 1992.

COMMISSION DES DROITS DE LA PERSONNE ET DES DROITS DE LA JEUNESSE, *Mémoire à la commission de la culture de l'assemblée nationale dans le cadre de l'examen du rapport sur la mise en œuvre des lois sur l'accès à l'information et la protection des renseignements personnels*, Québec, septembre 1997. http://www.cdpdj.qc.ca/htmfr/pdf/pdf_repertoire/acces.pdf

COMMISSION EUROPÉENNE, Groupe Sur La Protection Des Personnes À L'égard Du Traitement Des Données À Caractère Personnel, *Une approche européenne intégrée sur la protection des données en ligne* , 21 novembre 2000, http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp37fr.pdf

CONFÉRENCE POUR L'HARMONISATION DES LOIS AU CANADA *La protection des données dans le secteur privé: Options en vue d'une loi uniforme*., 1996, http://www.law.ualberta.ca/alri/ulc/96pro/f96c.htm

COMMISSION EUROPÉENNE, *Protection des données dans l'union européenne* , 1999, http://europa.eu.int/comm/internal_market/en/dataprot/news/guide_fr.pdf

CONSEIL DE L'EUROPE, *Convention Européenne de sauvegarde des droits de l'homme et des libertés fondamentales*, , Rome, 4.XI.1950, http://www.justice.gouv.fr/textfond/europ1.htm

CSA, *Code type pour la protection des renseignements personnels*., http://strategis.ic.gc.ca/SSGF/sf03281f.html

FEDERAL TRADE COMMISSION , *Consumer privacy in the information age: a view from the United States*., Remarks of Christine A. Varney, Commissioner , Before the Privacy & American Business National Conference, October 9, 1996 http://www.ftc.gov/speeches/varney/priv&ame.htm

FEDERAL TRADE COMMISSION, *Privacy Online: A Report to Congress*., June 1998 http://www.ftc.gov/reports/privacy3/toc.htm

FEDERAL TRADE COMMISSION *Self-regulation and privacy online: a report to congress*, July 1999, http://www.ftc.gov/os/1999/9907/privacy99.pdf

INFORMATION CANADA , *L'ordinateur et la vie privée*., Rapport du groupe d'étude établi conjointement par le ministère des Communications et le ministère de la Justice. Ottawa, 1972

INSTITUT DE LA STATISTIQUE DU QUÉBEC , *Enquête sur les transactions et l'identification dans un contexte d'inforoute*., mai 1999 http://www.autoroute.gouv.qc.ca/publica/pdf/isq.pdf

MURIS, Timothy J. (Chairman Federal Trade Commission), *Protecting Consumers' Privacy: 2002 and Beyond*, The Privacy 2001 Conference, Cleveland, Ohio, October 4, 2001, http://www.ftc.gov/speeches/muris/privisp1002.htm

NATIONAL ACADEMY OF SCIENCES (États-Unis). Project on Computer Databanks, *Databanks in a free society: computers, record-keeping and privacy*., New York, Quadrangle Books, 1972.

OCDE, *Lignes Directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel*., http://www.oecd.org/dsti/sti/it/secur/prod/priv-fr.html

OCDE, *Privacy Protection on Global Network*, 23 juin 1999, http://www.oecd.org/dsti/sti/it/secur/act/privnote.htm

PRIVACY WORKING GROUP INFORMATION POLICY COMMITTEE, INFORMATION INFRASTRUCTURE TASK FORCE , *Privacy and the national information infrastructure: principles for providing and using personal information*, June 6, 1995, http://aspe.os.dhhs.gov/datacncl/niiprivp.htm

US DEPARTMENT OF COMMERCE, *Safe Harbor Overview*, http://www.export.gov/safeharbor/sh_overview.html

W3C, *Proposal for an Open Profiling Standard*., 2 juin 1997 http://www.w3.org/TR/NOTE-OPS-FrameWork.html

W3C, *Privacy and Profiling on the Web*., 2 juin 1997 http://www.w3.org/TR/NOTE-Web-privacy.html

W3C, *P3P and Privacy on the Web FAQ* http://www.w3.org/P3P/P3FAQ.html

III- Sites Web (sélection)

Commissaire à la protection de la vie privée du Canada
http://www.privcom.gc.ca/

Commission d'accès à l'information (Québec)
http://www.cai.gouv.qc.ca/

Echelon Watch
http://www.echelonwatch.org/

Federal Trade Commission
http://www.ftc.gov

IDCide, the Internet security company
www.idcide.com

MSPassport
http://www.passport.com/Consumer/default.asp?PPlcid=1033

OCDE
http://www.oecd.org

Organisation Européenne pour la Recherche Nucléaire (CERN)
http://public.web.cern.ch/Public/Welcome_fr.html

Privacy Council
http://www.privacycouncil.com/index.php

PrivacyExchange
http://www.privacyexchange.org/

Privacy Security Network
http://www.privacysecuritynetwork.com/

TRUSTe
http://www.etrust.org/

W3C
www.w3c.org/

***

Table de la Législation

a) Textes fédéraux

Charte canadienne des droits et libertés, Édictée comme l'annexe B de la *Loi de 1982 sur le Canada*, 1982, ch. 11 (R.-U.), http://canada.justice.gc.ca/loireg/charte/const_fr.html

Loi sur la protection des renseignements personnels L.R.C. 1985, c. P-21 ; sur le web : http://www.canlii.org/ca/loi/p-21/

Loi sur la protection des renseignements personnels et les documents électroniques. L.C. 2000 c. 5. Sur le Web: http://www.canlii.org/ca/loi/p-8.6/

Loi sur la protection des renseignements personnels et les documents électroniques. Projet de Loi C-54, 1ière lecture, 1re session, 36e législature, (Can.), art. 2; sur le Web : http://www.parl.gc.ca/36/1/parlbus/chambus/house/bills/government/C-54/C-54_1/90052bF.html#1

b) Textes québécois

Charte des droits et libertés de la personne, L.R.Q., c. C-12, http://www2.lexum.umontreal.ca/qclrq/fr/c12.html

Code civil du Bas-Canada, S.Q. 1865, c. 41

Code civil du Québec, L.Q., 1991, c. 64; sur le Web : http://www.canlii.org/qc/loi/ccq/tout.html

Loi concernant le cadre juridique des technologies de l'information, L.Q. 2001, c. 32.

Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels L.R.Q., c. A-2.1 Sur le Web : http://www.canlii.org/qc/loi/a2.1/

Loi sur la protection des renseignements personnels dans le secteur privé, L.R.Q. c. P-39.1 ; sur le Web http://www.canlii.org/qc/loi/p39.1/

c) Textes d'autres provinces canadiennes

Loi sur l'accès à l'information et la protection de la vie privée. L.R.O. 1990, chap F.31; Sur le Web: http://192.75.156.68/DBLaws/Statutes/French/90f31_f.htm

c) Textes Européens

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 caractère personnel et à la libre circulation de ces données. http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexapi!prod!CELEXnumdoc&lg=fr&numdoc=31995L0046&model=guichett

Loi fondamentale allemande de 1949, article 2, al 1 ; version bilingue disponible sur le Web au http://www.jura.uni-sb.de/BIJUS/grundgesetz/

***

Table des jugements

a) Jurisprudence canadienne

Aubry c. Éditions Vice-Versa inc., [1998] 1 R.C.S. 591
http://www.canlii.org/ca/jug/csc/1998/1998csc31.html

Banque de Montréal c. Bail ltée, (1992) 2 R.C.S. 554
http://www.canlii.org/ca/jug/csc/1992/1992csc68.html

Cordingly c. Nield (1875) 18 L.C.J. 204

Godbout c. Longueuil (Ville), [1997] 3 R.C.S. 844
http://www.canlii.org/ca/jug/csc/1997/1997csc97.html

Hunter c. Southam Inc., [1984] 2 R.C.S. 145

R. c. Dyment (1988) 2 R.C.S. 417
http://www.canlii.org/ca/jug/csc/1988/1988csc84.html

R. c. Pohoretsky, [1987] 1 R.C.S. 945
http://www.canlii.org/ca/jug/csc/1987/1987csc34.html

Robbins c. CBC (Québec), (1958) C.S. 152, 12 DLR (2d) 35

SDGMR c. Dolphin Delivery ltd, (1986) 2 R.C.S. 598-603
http://www.canlii.org/ca/jug/csc/1986/1986csc68.html

b) Jurisprudence américaine

ACLU c. Reno, http://www.aclu.org/court/renovacludec.html § 55 et 56

FTC c. Toysmart.com, (District of Massachusetts) (Civil Action No. 00-11341-RGS).

Katz c. United States, 389 U.S. 347 (1967)

c) Jurisprudence européenne

CONSEIL DE L'EUROPE, Décision de la Commission des communautés Européennes,
http://europa.eu.int/comm/internal_market/en/dataprot/news/decision_fr.pdf

***