# APPROCHES ET STRATEGIES POUR AMELIORER LA PROTECTION DE LA VIE PRIVEE DANS LE CONTEXTE DES INFOROUTES*

**TRUDEL Pierre et BENYEKHLEF Karim**

## INTRODUCTION

Ce mémoire aborde deux thèmes, évoqués par la Commission d'accès à l'information dans son Rapport sur la mise en oeuvre de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels et de la Loi sur la protection des renseignements personnels dans le secteur privé intitulé *Vie privée et transparence administrative au tournant du siècle*, à savoir la définition donnée à l'expression "renseignements personnels" et les moyens d'assurer la protection de la vie privée dans les réseaux électroniques décentralisés de communication, comme l'Internet.

Pour assurer avec plus d'effectivité le respect de la vie privée dans l'environnement virtuel qui émerge, il importe de cerner avec plus de précision les valeurs que l'on veut protéger et de revoir les techniques par lesquelles il sera possible d'actualiser efficacement les valeurs de protection de l'intimité des personnes. C'est dans cet esprit qu'il faut mener le processus d'adaptation des principes relatifs à la protection des renseignements personnels énoncés dans les législations québécoises, qui sont reconnus dans plusieurs pays, aux nouveaux contextes de communication. La notion de renseignements personnels devrait être revue dans le dessein d'accroître les garanties relatives aux informations qui sont vraiment relatives à la vie privée des personnes tout en libérant les autres informations personnelles qui, loin de concerner la vie privée, témoignent plutôt de leur participation à la vie sociale.

---

* MEMOIRE PRESENTE A LA COMMISSION DE LA CULTURE DE L'ASSEMBLEE NATIONALE DANS LE CADRE DE SON MANDAT SUR L'ETUDE DU RAPPORT QUINQUENNAL DE LA COMMISSION D'ACCES A L'INFORMATION, MONTREAL, CENTRE DE RECHERCHE EN DROIT PUBLIC, UNIVERSITE DE MONTREAL, 1997, 35 P.

Il est plus que jamais nécessaire de mettre en place les stratégies appropriées pour assurer la protection des données personnelles dans les réseaux décentralisés. Deux phénomènes ont connu un développement important depuis l'adoption des lois québécoisse sur la protection des renseignements personnels. Il s'agit du développement croissant du commerce électronique et du recours de plus en plus fréquent aux réseaux décentralisés dans le traitement de l'information.

Il convient donc d'aborder les questions relatives à l'efficience des règles actuelles de protection des données personnelles au regard des inforoutes, à la transmission transfrontière de ces données, aux modalités propres à assurer une protection effective aux données nominatives, aux efforts actuellement en cours afin de parvenir à une telle protection et aux actions qui pourraient être entreprises par le gouvernement du Québec afin de participer activement à ces efforts.

# 1- UNE DÉFINITION DE RENSEIGNEMENTS PERSONNELS PLUS RESPECTUEUSE DE LA VIE PRIVEE

La définition des notions de renseignements personnels des lois québécoises actuelles est trop large: elle empêche la circulation d'informations qui n'ont rien à faire avec la vie privée et du même coup, il en résulte une dilution de la protection des informations qui sont vraiment du domaine de la vie privée.

La définition de renseignements personnels qui est retenue dans l'actuelle législation québécoise est englobante. Dans la *Loi sur la protection des renseignements personnels dans le secteur privé*[†], la notion de renseignement personnel est définie largement. Elle vise tout renseignement, quel que soit le support ou la forme sur laquelle il est accessible, qui "concerne" une personne physique et permet de l'identifier. Il y a donc deux conditions à satisfaire. Premièrement, pour être en présence d'un renseignement personnel, le renseignement doit "concerner" une personne, c'est-à-dire y être relatif, y être rattaché d'une façon ou d'une autre.

Mais en plus, et c'est la seconde condition, il faut que le renseignement permette d'identifier la personne. C'est lorsque ces deux conditions sont réunies à l'égard d'une information que celle-ci devient un renseignement personnel. La loi reprend ici la définition de "renseignements nominatifs" de l'article 54 de la Loi d'accès. Mais contrairement à l'article 55 de la Loi d'accès, aucune distinction n'est faite entre un renseignement personnel à caractère public en vertu de la loi et un renseignement nominatif. Ici, tous les renseignements personnels ont le même statut et sont protégés de la même façon.

Ainsi, il faut et il suffit que le renseignement soit relatif à une personne physique et permette de l'identifier pour qu'il soit visé par la loi. La loi ne vise donc pas seulement les renseignements susceptibles de concerner la vie privé d'une personne mais la totalité des renseignements susceptibles de l'identifier. Cette protection au-delà des seules informations relevant de la vie privée s'explique présumément par le caractéère changeant des informations qui, une fois agglomérées par le truchement des possibilités rendues

---

[†] *Loi sur la protection des renseignements personnels dans le secteur privé*, L.R.Q., c. P-39.1.

disponibles par l'informatique pourraient révéler des informations relatives à la vie privée de certains. C'est donc un souci de commodité qui paraît avoir motivé ce recours à une définition si englobante de renseignements personnels.

La généralisation des environnements électroniques et surtout le fait que ceux-ci ont désormais vocation à constituer le théatre du déroulement de multiples activités que l'on considérait jusqu'ici comme étant l'apanage des lieux physiques impose une approche plus ciblée de la protection de la vie privée à moins de vouloir ériger cette valeur au-dessus de toutes les autres, et cela même au risque de méconnaître les autres droits essentiels à la vie démocratique.

Certaines données personnelles, liées aux traits les plus intimes de la personne humaine, se caractérisent par leur capacité à identifier une personne, à révéler des informations sur elle-même. De telles informations personnelles participent donc au domaine de la vie privée. Elles sont, en principe, assujetties à un pouvoir de maîtrise du sujet. Elles sont également des données à caractère social en ce que leur agglomération permet de produire des informations de grande valeur pour l'amélioration de la santé et du bien-être de l'entourage immédiat du sujet.

En raison de leur double caractère, les informations personnelles constituent l'archétype idéal pour tester les modèles et hypothèses en matière d'encadrement juridique et normatif de la production et de la circulation de l'information. Au plan des problèmes que pose son encadrement juridique, l'information personnelle se présente comme un objet qui préfigure les défis et difficultés qui confrontent ceux qui croient essentiel de s'assurer que l'encadrement juridique procure bien les protections essentielles aux individus pour leur assurer un contrôle effectif sur les informations relatives à leur intimité mais en même temps, laisse circuler l'information qui représente une valeur importante pour la collectivité.

### *1.1-Les deux volets de la vie privée*

L'on distingue deux volets à la notion de vie privée: le premier est le volet identificateur. Il réfère aux faits et aux aspects de la vie d'une personne qui sont inclus dans un domaine protégé. Il permet d'identifier les éléments généralement reconnus par la société comme étant inclus dans le domaine de la vie privée d'une personne, à une époque donnée. Mais le contenu concret de ce domaine varie suivant les personnes, la position qu'elles occupent dans la société et d'autres circonstances dont la plus importante est

l'existence d'une expectative raisonnable de vie privée. Ce volet contextuel met en relief le fait que la vie privée n'a pas un contenu défini au fil des sensibilités infiniment variables des individus mais constitue un droit dont le domaine s'harmonise aux exigences de la participation à la vie sociale. En revanche, les technologies de l'information offrent des possibilités inouies d'agglomération d'informations à tel point que des informations dont on peut convenir du caractère public peuvent connaître des traitements qui pourront s'avérer périlleux pour la vie privée de certaines personnes.

Pour établir s'il y a atteinte à la vie privée, il est nécessaire de déterminer si une divulgation d'information ou une intrusion porte sur un élément de la vie privée. D'où la nécessité de tenter de circonscrire le domaine de la vie privée. Le domaine de la vie privée regroupe certains types d'informations qui y sont, en principe, rattachées. Il connaît aussi des variations selon les qualités et la situation des personnes. Le domaine de la vie privée est aussi délimité. L'on peut prétendre au respect de sa vie privée lorsqu'on se trouve dans un contexte où il y a une expectative légitime de vie privée.

On identifie habituellement deux grands volets à la vie privée. Le premier se veut identificateur. Il réfère aux faits et aux aspects de la vie d'une personne qui sont inclus dans un domaine protégé. Il permet d'identifier objectivement les éléments traditionnellement reconnus par la société comme étant inclus dans le domaine de la vie privée d'une personne, à une époque donnée. Mais le contenu concret de ce domaine varie suivant les personnes, la position qu'elles occupent dans la société et d'autres circonstances. C'est le volet subjectif de la vie privée : celui qui prend en considération les personnes visées. Ce volet contextuel permet d'apprécier le contenu du domaine de la vie privée en fonction des circonstances, notamment la participation de l'individu à la vie de la Cité[‡].

**Le volet identificateur de la vie privée**

S'agissant du volet identificateur, on peut poser qu'*a priori*, la vie privée s'oppose à la vie publique. Si l'on s'accorde pour reconnaître que toute personne doit pouvoir sous-

---

‡ Patrick A. MOLINARI et Pierre TRUDEL, "Le droit au respect de l'honneur, de la réputation et de la vie privée: Aspects généraux et applications", dans BARREAU DU QUÉBEC, FORMATION PERMANENTE, *Application des chartes des droits et libertés en matière civile*, Cowansville, Éditions Yvon Blais, 1988, 197, 211.

traire sa vie privée aux ingérences et aux divulgations, l'on convient tout aussi bien pour dire que la vie publique des personnes doit être ouverte et transparente. Cela laisse deviner qu'il y a certains types d'informations référant à des aspects de la vie d'une personne qui sont inclus dans le «domaine» de la vie privée. Ce sont en quelque sorte des informations se rattachant à des aspects de la vie qui sont fréquemment associés à l'intimité. La plupart des décisions de justice ayant eu à déterminer ce qui fait partie du champ de la vie privée concernaient des vedettes ou des personnes ayant autrement défrayé la manchette. Dans son ouvrage sur la protection de la vie privée, Kaiser rappelle que"lorsqu'il a été décidé qu'une divulgation ou une recherche d'information est illicite, parce qu'elle a pour objet un élément de la vie privée, fût-ce d'une vedette, il en découle, à plus forte raison que ce type d'information fait partie de la vie privée des simples particuliers. [§] " La jurisprudence québécoise a énuméré plusieurs éléments de la vie privée d'une personne qui sont fréquemment rattachés à l'intimité par les tribunaux : l'intimité de son foyer[**], ses origines, son état de santé, son anatomie et son intimité corporelle, sa vie conjugale, familiale et amoureuse, ses opinions politiques, philosophiques ou religieuses[††], la vie professionnelle et l'orientation sexuelle[‡‡].

---

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

[**] *"C'est l'interdiction de pénétrer dans les lieux où habite une personne sans l'autorisation de cette personne, a fortiori contre son gré. Pour celui qu'elle protège, c'est le droit de défendre à autrui l'accès de sa maison, plus positivement le droit pour chacun de faire de sa demeure un lieu d'asile et de retraite où il puisse, s'il le désire, vivre seul et tranquille à l'abri des intrusions, immixtions et interventions. Aussi bien l'inviolabilité du domicile n'est-elle pas la protection d'une chose relevant du régime juridique d'un bien. Dans le droit des personnes, c'est un droit de la personnalité. [...] Ce qui est spécifique, c'est que la protection de [...] l'intimité prend ici un caractère géographique. Elle se manifeste par la reconnaissance d'un territoire aux frontières duquel s'arrête le pouvoir d'autrui et au sein duquel règne une petite souveraineté. Chacun chez soi, maître chez soi. [...] Il reste que la vie privée ne se confond pas avec la demeure privée. Si l'inviolabilité du domicile est une application particulière du droit au respect de la vie privée, spécifiquement concrétisée par la mise en défense d'un lieu, [...] la protection de la loi couvre la vie privée même en dehors de ce lieu et elle la couvre, en ce lieu , contre des atteintes autres que la pénétration physique des tiers. C'est un mode plus général de protection."* G. CORNU, *Droit civil. Introduction. Les personnes. Les biens*, 7e éd., Tome 1, Paris, Montchrestien, 1994, n° 506, pp. 189-190 et n° 516, pp. 193-194.

[††] Patrick A. MOLINARI et Pierre TRUDEL, "Le droit au respect de l'honneur, de la réputation et de la vie privée: Aspects généraux et applications", dans BARREAU DU QUÉBEC, FORMATION PERMANENTE, *Application des chartes des droits et libertés en matière civile*, Cowansville, Éditions Yvon Blais, 197, 212 et 214.

[‡‡] Martin MICHAUD, *Le droit au respect de la vie privée dans le contexte médiatique : de Warren et Brandeis à l'inforoute*, Montréal, Éditions Wilson & Lafleur, 1996, p. 40.

**Le volet contextuel de la vie privée**

S'agissant du volet contextuel, la protection accordée à la vie privée varie en fonction de certaines variables. Étant donné qu'*a priori* ce qui n'est pas du domaine de la vie privée relève du domaine de la vie publique, ce qui semble aujourd'hui faire partie du domaine de la vie privée d'une personne pourrait devenir, au fil des ans ou suivant un changement dans les moeurs, une information d'intérêt public. Le champ de protection de la vie privée varie principalement en fonction des personnes. En effet, comme les personnes ne jouent pas toutes le même rôle dans la société, ce qui est une information assimilable à un aspect de la vie privée pour l'une ne le sera pas forcément pour l'autre. En ignorant cela, la législation sur la protection des renseignements personnels devient un obstacle à la circulation d'informations qui sont pourtant revêtues d'un intérêt public manifeste.

Le volet contextuel de la vie privée se détermine aussi en tenant compte des nécessités de l'information publique de même que des autres valeurs qui sont forcément en cause dans la délimitation du droit à la vie privée. Ainsi donc, le volet contextuel de la définition de la vie privée ne peut être défini autrement que dans l'examen concret de la position occupée par le sujet au sein de la société, son rôle dans le déroulement des affaires publiques, l'intérêt que les membres du public (ou de l'entourage) ont à connaître certains aspects de son comportement et de ses moeurs susceptibles d'éclairer les décisions et choix qu'ils ont à faire à son sujet[§§]. Le droit au respect de la vie privée d'une personne trouvera ainsi ses limites dans l'intérêt que le public a à prendre connaissance de certains aspects de sa personnalité. L'intérêt du public à être informé est ainsi une notion de référence aidant à déterminer les limites entre ce qui doit être tenu secret au nom du respect de la vie privée et ce qui pêut être licitement révélé. Kayser constate que les tribunaux admettent que certaines divulgations concernant la vie privée de certaines personnes seraient néanmoins licites dans les circonstances où elles constituent des questions sur lesquelles le public a un intérêt légitime à être informé :

> *Comment expliquer la licéité des investigations et des divulgations relatives aux activités publiques et leur illécéité quand elles ont trait à la vie privée? Les*

---

[§§] Pierre TRUDEL, " Les dispositions sur la protection de la vie privée dans le nouveau code civil du Québec " «Les_dispositions_sur_la_protection_de_la_vie_privée_dans_le_nouveau_Code_civil_du_Québec», (1994) 111 *LEGIPRESSE* 6, 6-7.

*premières ressortissent <u>du domaine de la liberté de communication et d'expression parce que le public a un intérêt légitime à les connaître</u>.*[***]

Dans les sociétés démocratiques, l'on reconnaît que l'intérêt légitime du public à être informé est l'une des valeurs fondamentales permettant la délimitation du droit à la vie privée. C'est pourquoi l'on admet généralement que le domaine de la vie privée des personnes qui doivent représenter la collectivité et gérer les fonds publics est moins grand que celui du simple citoyen[†††]. En raison de la nature de leur participation aux activités de la société, les informations relatives à certains aspects de la vie de certains individus n'entrent pas d'emblée dans le domaine de leur vie privée, le public ayant un intérêt légitime à en être informé. Il en est ainsi pour les personnes publiques, ainsi que le soulignent Nicole Vallières et Florian Sauvageau[‡‡‡]. Par exemple, l'état de santé d'un simple citoyen

---

[***] Pierre KAYSER, *La protection de la vie privée par le droit. Protection du secret de la vie privée*, 3e éd., Paris, Economica, 1995, n° 135, p. 235.

[†††] Voir notamment S.H. ABRAMOVITCH, "Publicity Exploitation of Celebrities: Protection of a Star's Style in Quebec Civil Law", (1991) 32 *C. de D.* 301; Jean-Marie COTTERET et Claude EMERI, «Vie_privée_des_hommes_politiques» "Vie privée des hommes politiques", (1979-80) 14 *R.J.T.* 335 et Pierre TRUDEL, "Le rôle de la loi, de la déontologie et des décisions judiciaires dans l'articulation du droit à la vie privée et de la liberté de presse", dans Pierre TRUDEL et France ABRAN, *Droit du public à l'information et vie privée : deux droits irréconciliables?*, Montréal, Éditions Thémis, 1992, 181, 186. Voir également Louise POTVIN, *La personne et la protection de son image : étude comparée des droits québécois, français et de la common law canadienne*, Ottawa, McGill University, 1989, pp. 351 et suiv. Concernant le droit du simple citoyen à la protection de son image, voir : *L. Gilles c/ T.F.1 et autres*, Tribunal de Grande Instance de Nanterre (1re c., A), 18 janvier 1995, cité dans (octobre 1995) 125 *LEGIPRESSE* 145-147.

[‡‡‡] *"Le domaine de la vie privée des personnalités publiques est évidemment plus restreint que celui des individus n'ayant aucune responsabilité envers la collectivité. [...] À cet égard, les tribunaux ont dégagé un critère voulant que le comportement des personnes publiques dans leur vie privée ne puisse faire l'objet d'un reportage ou d'un commentaire à moins que cette conduite privée soit de nature à faire présumer qu'elle influencera l'exercice de leurs fonctions. Les faits relevant de la vie intime des personnalités publiques peuvent faire l'objet de divulgation dès lors qu'ils sont susceptibles de transparaître ou de déteindre à travers leurs activités publiques. Le droit à l'intimité cédera alors devant l'utilité sociale de la diffusion de l'information"*; dans Nicole VALLIÈRES, *La presse et la diffamation*, Montréal, Wilson et Lafleur, 1986, pp. 99 et suiv. ainsi que Nicole VALLIÈRES et Florian SAUVAGEAU, *Droit et journalisme au Québec*, Québec, Éditions GRIC - FPJQ, 1981, pp. 40 et suiv. Voir également, sur le domaine de la vie privée des personnalités publiques, *Bouchard* c. *Chartier*, [1907] 31 C.S. 535; *Vigeant* c. *Poulin*, [1890] 20 R.L. 567. Notons que le principe veut que toute personne, même célèbre, ait droit à la protection de sa vie privée. À cet égard, le Tribunal de la grande instance de Nanterre, écrit : *"Tout individu, fut-il célèbre, a droit au respect de l'intimité de sa vie privée et est fondé à en obtenir la protection en fixant lui-même les limites de ce qui peut être diffusé à ce sujet. Les mêmes droits doivent lui être reconnus quant à son image." Allégret c/ Edi 7.*, Tribunal de grande instance de Nanterre (1re ch., A), 15 février 1995, cité dans (octobre 1995) 125 *LEGIPRESSE* 91.

ne possède pas, *a priori*, le même intérêt aux yeux du public que celui d'une célébrité[§§§] ou d'une personne publique[****], comme l'a souligné la Cour supérieure dans l'affaire *Valiquette*[††††].

L'appréciation de l'intérêt public[‡‡‡‡] est donc une composante intrinsèque de la définition de la vie privée. Elle préside à la détermination de la portée de la vie privée en permettant le départage «contextué» entre les intérêts afférents à la préservation de l'intimité des personnes et les autres valeurs qui peuvent rendre légitimes les intrusions et les divulgations à propos d'une personne. C'est de cette façon que s'établit le nécessaire équilibre entre le droit à la vie privée et les autres valeurs qui doivent également être préservées.

Pour aider à apprécier l'intérêt public, les tribunaux ont dégagé le standard de l'expectative légitime de vie privée. Ce standard fait référence aux circonstances dans lesquelles se trouve une personne. Il contribue à délimiter le domaine la vie privée en fonction de la situation dans lequel se retrouve la personne. Par exemple, il est admis que certains lieux sont privés et une personne raisonnable est en droit de s'attendre au respect de sa vie privée lorsqu'elle s'y trouve. En revanche, il est des lieux où cette expectative est moins grande, voire inexistante: ainsi, une personne raisonnable ne s'étonnera pas d'être vue sur la rue en plein jour mais elle s'opposera avec raison à ce qu'on capte son image

---

§§§ La vie privée du simple citoyen pourra, dans certaines circonstances, être révélée, comme le souligne Nicole Vallières qui constate que la jurisprudence a adopté une conception large de l'intérêt public : *"Si dans son comportement privé, un individu touche à des intérêts relevant du domaine public tels la justice, la sécurité militaire, l'emploi de fonds publics ou porte atteinte aux droits d'un groupe social, alors ce comportement, devenu une affaire d'intérêt général, peut donner lieu à un débat public dans la presse."* Nicole VALLIÈRES, *La presse et la diffamation*, Montréal, Wilson et Lafleur, 1986, p. 98.

**** Pensons à la récente affaire concernant le défunt Président de la République Française François Mitterand. Voyant dans la publication du livre du docteur Gubler, *Le Grand Secret*, les éléments constitutifs de violation du secret professionnel et d'intrusion particulièrement grave dans l'intimité de la vie privée familiale du Président et dans celle de son épouse et de ses enfants, un tribunal français a fait défense à la diffusion du livre. *D. Mitterand, J.C. et G. Mitterand et M. Pingeot* c./*c. Gubler, G. de la Cité et S.A. Plon*, (Ordonnance de référé) 18 janvier 1996, cité dans (janvier-février 1996) 128 *LEGIPRESSE* 15-16. Notons au passage qu'en dépit de cette ordonnance, un individu a quand même publié l'ouvrage en cause sur le réseau Internet, ce qui a causé bien de l'émoi tant dans la communauté juridique que dans la société française en général.

†††† *Valiquette* c. *The Gazette*, [1991] R.J.Q. 1075, 1080.

‡‡‡‡ Lire Emmanuel DERIEUX, et Pierre TRUDEL (éd.), *L'intérêt public, principe du droit de la communication*, Paris, Éditions Victoires, 1996, 192 p.

lorsqu'elle se trouve dans une salle de toilette. Cette notion a d'abord été développée par la Cour suprême des États-Unis lors de cas d'intrusion dans l'intimité régie par le Quatrième Amendement[§§§§], disposition garantissant au citoyen une protection contre les fouilles, les saisies ou les perquisitions abusives de l'État. S'inspirant de cette approche, la Cour suprême du Canada, dans l'affaire *Hunter*[*****] et surtout dans l'affaire *Dyment*[†††††], tout en reconnaissant clairement dans ces arrêts une protection constitutionnelle à la vie privée[‡‡‡‡‡], a incorporé le standard d'expectative légitime de vie privée au droit canadien.

Un exemple tiré du quotidien d'Internet permet d'illustrer comment devrait fonctionner le régime de la protection des renseignements personnels si l'on tient à l'adapter aux contextes variés de la vie dans le cyberespace. Plusieurs internautes participent à des listes de discussions, il en existe des milliers sur Internet portant sur à peu près tous les sujets susceptibles d'intéresser les humains. La plupart des logiciels assurant le déroulement de ces discussions constituent une liste des participants aux discussion. Lorsque la liste est ouverte, c'est-à-dire accessible à tous ceux qui choisissent de s'y inscrire, elle est asssimilable à un lieu électronique public. Il est normal que les autres participants puissent prendre connaissance des coordonnées électroniques des autres participants. En revanche, celui qui s'aviserait de copier la liste des participants et l'utiliser à des fins différentes des finalités pour lesquelles elle est constituée commettra vraisemblablement une intrusion, portant ainsi atteinte au droit à la vie privée.

Il faut donc un régime juridique des renseignements personnels qui reconnaît à la fois le caractère éminement public de certains contextes de communication dans le cyberespace mais qui en même temps balise les traitements d'informations personnelles qui sont constitutifs d'atteintes à la vie privée.

---

§§§§ Voir notamment à cet égard *Katz* c. *United States*, 389 U.S. 347 (1967).

***** *Hunter* c. *Southam*, [1982] 2 R.C.S. 145.

††††† *La Reine* c. *Dyment*, [1988] 2 R.C.S. 417. L'arrêt *Dyment* a même reconnu une facette informationnelle au droit à la vie privée. Voir à cet égard Karim BENYEKHLEF, *La protection de la vie privée dans les échanges internationaux d'information*, Montréal, Éditions Thémis, 1992, p. 29.

‡‡‡‡‡ Voir à cet effet Martin MICHAUD, *Le droit au respect de la vie privée dans le contexte médiatique : de Warren et Brandeis à l'inforoute*, Montréal, Éditions Wilson & Lafleur, 1996, pp. 13 et suiv.

La notion de vie privée ne couvre pas toutes les informations qui touchent une personne. Comme nous vivons en société, il est des composantes de l'activité de chacun qui ont un caractère public. En ignorant cela et en persistant à promouvoir une définition englobante, telle la notion de " renseignements personnels ", on s'expose à inclure une kyrielle d'information dans le champ de la protection (en fait, tous les renseignements concernant une personne et permettant de l'identifier) et se retrouver dans l'obligation de multiplier les circonstances où il sera nécessaire, au nom du bien public, de déroger (par la multiplication des dispositions dérogatoires) aux protections pourtant essentielles à la préservation de la zone d'intimité de chaque personne.

**Les nouveaux contextes de communication**

La variété des contextes de communication susceptibles de prendre place dans les environnements électroniques comme Internet impose de fonder la qualification juridique des relations susceptibles d'exister dans le cyberespace en tenant compte du fait qu'il ne s'agit pas d'un espace homogène. André Bélanger relève que l'on compare souvent l'Internet à une ville "dont la fonction consiste à traiter de l'information"[§§§§§]. Certains quartiers plus anciens traitent les informations sans artifice comme le FTP et le WAIS tandis que d'autres zones plus modernes ont la capacité d'enrichir l'information avec de la vidéo, du son de l'image comme le World Wide Web[******] (WWW) et ses capacités hypertexte et multimédia. Des zones sont dévolues aux interactions comme le courrier électronique qui permet la communication entre des personnes déterminées ou les adhérents à des listes de discussions, les "newsgroups" ou les salons électroniques ("Internet Relay Chat") qui se présentent comme de véritables réunions virtuelles dans lesquelles interagissent des personnes pouvant être situées partout sur la planète[††††††].

---

§§§§§ André BÉLANGER, "Le cyberespace en bref", (13 octobre 1995) *La Presse* A8.

****** Paul DURIVAGE, "Planète WEB", (6 décembre 1995) *La Presse* D1.

†††††† Voici la définition de Usenet retenue par Gareth Sansom : "*USENET est un réseau coopératif de messagerie électronique qui permet à des millions de personnes de dialoguer sur des milliers de sujets (chaque sujet s'appelle un "groupe de news" (newsgroup)). Un observateur l'a décrit en ces termes : [TRADUCTION] "des bits, des tas de bits, des millions de bits chaque jour remplis d'inepties, de disputes, de discussions techniques sensées, d'analyses savantes et d'images lubriques"... USENET n'est pas la même chose qu'Internet. Le réseau Internet transmet toutes sortes de données et soutient toutes sortes de services : USENET est l'un de ceux-là. Inversement, les données USENET sont transmises par l'entremise de plusieurs autres réseaux qui ne font pas partie du réseau Internet proprement dit*"; dans Gareth SANSOM, *Le contenu illégal et offensant sur l'autoroute de*

Dans son ouvrage *Law in a Digital World*[‡‡‡‡‡‡], Katsh identifie trois contextes de communication sur les inforoutes : la communication par courrier électronique : *"de un vers un ou plusieurs usagers au choix de l'émetteur"*; les listes et les groupes de discussion : *"plusieurs usagers vers un serveur qui redistribue à plusieurs usagers (ou abonnés)"*; l'accès à des sites d'informations et des banques de données.

L'application de plusieurs règles de droit connaît des variations selon les différents contextes de communication que l'on retrouve dans les environnements électroniques[§§§§§§]. Par exemple, l'ampleur de l'expectative de vie privée à laquelle un internaute peut prétendre peut dépendre de l'auditoire, potentiel ou réel, du message véhiculé. Il importe donc, pour chacun des contextes que présente la communication électronique, d'en faire une qualification adéquate et d'évaluer les attentes des usagers et autres participants. Ces multiples contextes sont susceptibles de justifier des différences sur l'existence et l'ampleur des attentes des participants à la protection de leur vie privée de même que sur le caractère justifiable de certaines règles de conduite.

Une approche qui se voudrait respectueuse de la diversité des contextes de communication dans le cyberespace serait de délimiter la définition de renseignements personnels afin de ne viser dans la loi que ceux qui ont trait à la vie privée des personnes. Ainsi, la définition des renseignements personnels assujettis à la loi pourrait se lire ainsi:

" Est un renseignement personnel tout renseignement portant sur un élément de la vie privée d'une personne. "

ou encore:

" Est un renseignement personnel tout renseignement concernant une personne ou permettant de l'identifier mais qui n'a pas un caractère public. "

De cette façon, les renseignements concernant une personne mais qui ne relèvent pas du domaine de sa vie privée pourraient circuler librement.

---

*l'information*, Rapport préparé pour Industrie Canada, Ottawa, juin 1995, p. 5; aussi disponible à http://info.ic.gc.ca/ic-data/info-highway/general/offensive/offens_f.html.

‡‡‡‡‡‡ Ethan KATSH, *Law in a Digital World*, New York, Oxford University Press, 1995, pp. 35 et suiv.

§§§§§§ Voir notamment Pierre TRUDEL et France ABRAN, Karim BENYEKHLEF et Sophie HEIN, *Droit du cyberespace*, Montréal, Éditions Thémis, 1997, pp. 2-1 et suiv.

Il convient toutefois de préciser que les règles relatives au traitement de tous les renseignements concernant une personne devraient être ajustées de manière à éviter que des informations à caractère public soient agglomérées, accumulées ou traitées de manières à constituer une atteinte à la vie privée. C'est en effet au niveau du traitement de telles informations que se situent les dangers d'atteintes à la vie privée. Il faut donc intervenir à ce niveau et non pas interdire *a priori* toute circulation d'informations personnelles simplement parce que l'agglomération de ces données et informations pourrait éventuellement constituer une atteinte à la vie privée de certaines personnes.

Ainsi, par les balises ainsi imposées au traitement des informations relatives aux personnes, l'on obtient une protection plus ciblée de la vie privée tandis que les renseignements qui ne concernent pas la vie privée des personnes mais témoignent de la partipation des individus à la vie sociale redeviennent de libre parcours.

## 2- LA PROTECTION DES DONNEES PERSONNELLES DANS LE CONTEXTE DES INFOROUTES

La délocalisation et l'intangibilité de l'information numérique rend son contrôle difficile. On rappelle souvent le caractère territorial des règles législatives dont les États se sont dotés et le fait que l'efficacité de ces dernières soulève plus ou moins de perplexité au regard de l'éclatement du concept de territorialité dans le contexte des réseaux décentralisés. Comment, en effet, assurer une application effective des règles de protection des données personnelles lorsque l'usager est domicilié à Montréal et que le serveur, une entreprise commerciale, a sa place d'affaires à Singapour ou à Johanesbourg? Quelle autorité assurera l'application et la sanction de ces règles? Même si, par hypothèse, tous les pays du globe étaient dotés d'une loi de protection des données personnelles, le problème de l'intangibilité et de la délocalisation continuerait à se poser: quelle serait la loi applicable? quelle autorité serait compétente? comment assurer l'exercice des droits d'accès et de correction de la personne fichée? comment cette dernière pourrait-elle même déterminer l'existence d'un traitement automatisé la concernant? Toutes ces questions soulèvent finalement le problème de l'application et de l'applicabilité des règles législatives pertinentes. Nous y reviendrons.

### *2.1- La protection des données personnelles: sous-ensemble du droit à la vie privée*

Au préalable, il convient de préciser que les principes fondamentaux en matière de gestion de l'information personnelle, que l'on retrouve dans la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* et dans la *Loi sur la protection des renseignements personnels dans le secteur privé,* n'ont pas vocation à régir toutes les situations mettant en cause le droit à la vie privée dans le contexte des inforoutes. Il convient alors de faire une distinction entre le droit à la vie privée et la protection des données personnelles. La première notion englobe la seconde. Autrement dit, la protection des données personnelles n'est qu'un sous-ensemble du droit à la vie privée. La protection des données nominatives se rattache à l'aspect *informationnel* du droit à la vie privée[*******]. Les principes fondamentaux en matière de gestion de l'information personnelle traduisent en termes pratiques les préoccupations afférentes aux dimensions informationnelles du droit à la vie privée. Nous savons que ces principes établissent des procédures et des pratiques quant à la gestion de l'information nominative (*fair information practices*). Ces procédures et pratiques ont, entre autres, pour objet d'assurer à la personne fichée un certain contrôle sur les données la concernant. Ce corpus normatif s'applique au premier chef aux organismes publics et aux entreprises commerciales, c'est-à-dire aux organes qui détiennent une masse importante d'informations personnelles. En effet, il est bien clair que les dangers posés à la vie privée sont le fait de ceux qui font une grande utilisation des données nominatives dans l'accomplissement de leurs missions publiques et de leurs tâches commerciales. Par conséquent, les normes nationales et internationales en matière de protection des données personnelles s'appliquent, de prime abord, aux organismes publics et aux entreprises commerciales oeuvrant sur l'autoroute de l'information. Les données collectées par ces entités sur l'autoroute de l'information sont, en principe, soumises à ce corpus normatif.

Les organismes publics et les entreprises commerciales sont, sans aucun doute, les principaux détenteurs de renseignements personnels. Cette formidable accumulation de données constitue, en soi, une menace beaucoup plus importante au droit à la vie privée que les exactions de quelques individus. Toutefois, les organismes publics et les entreprises commerciales ne sont pas les seuls acteurs du théâtre télématique; il y a également les

---

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

usagers. Or les principes fondamentaux en matière de gestion de l'information personnelle ne s'appliquent pas aux individus dans l'exercice de leurs activités privées[†††††††]. Par conséquent, ces principes ne sont pas applicables à l'interception par un tiers du courrier électronique d'un utilisateur. Ces principes ne couvrent pas davantage les situations d'accès non autorisé à des sites pouvant contenir des données personnelles et la dissémination de ces données sur le réseau. Certaines lois pourvoient parfois à ce type de situation. Quoi qu'il en soit, ces situations mettent également en cause le droit à la vie privée ou, à tout le moins, un élément de celui-ci, le principe de confidentialité.

Les principes fondamentaux en matière de gestion de l'information personnelle n'ont pas vocation à régir toutes les situations soulevant le problème du droit à la vie privée dans le cyberespace. Ainsi, la possibilité d'échanger des messages électroniques sans faire l'objet d'une interception par un tiers ou même par l'État ou sans faire l'objet d'une surveillance par son employeur[‡‡‡‡‡‡‡], par exemple, s'inscrit dans une problématique certes associée au droit à la vie privée, mais tout de même distincte de celle relative aux principes afférents à la gestion de l'information personnelle. Il ne s'agit pas de déplorer l'inapplicabilité de ces normes à ces situations. Celles-ci n'ont pas été, en effet, élaborées pour répondre à ces interrogations. D'autres normes doivent être développées ou adaptées pour prévenir de telles atteintes au droit à la vie privée.

Mais notre propos se limitera ici aux questions relatives à la gestion des données personnelles dans le contexte des inforoutes.

### *2.2- L'application et l'applicabilité des normes relatives à la protection des données personnelles*

Le problème de la délocalisation et de l'intangibilité de l'information n'est pas vraiment nouveau. En effet, une lecture attentive des lois de protection des données personnelles, élaborées dans les années soixante-dix, permet de constater que les législateurs européens étaient conscients du fait que le mariage de l'informatique et des

---

[†††††††] Lire, par exemple, l'article 3(2) de la Directive de 1995 qui énonce: "Les dispositions de la présente directive ne s'appliquent pas aux traitements de données à caractère personnel: (...) effectués par une personne physique pour l'exercice d'activités exclusivement personnelles ou domestiques".

[‡‡‡‡‡‡‡] Voir, par exemple, Steven WINTERS, "The New Privacy Interest: Electronic Mail in the Workplace", [1993] 8 *High Technology Law Journal* 197.

télécommunications (télématique) pouvait faciliter le contournement de leurs législations. Il existe donc des dispositions législatives qui prohibent la transmission de données personnelles, à partir du territoire national, vers les pays dont le droit interne ne leur assure pas une protection satisfaisante.

La nouveauté du problème tient au fait qu'une masse toujours croissante d'utilisateurs, individus et personnes morales, ont aujourd'hui accès à la télématique. Il ne s'agit plus dès lors de contrôler simplement les flux informationnels entre de grandes entreprises ou des composantes de l'État. La décentralisation des réseaux entraîne une augmentation des acteurs et des usagers et, de ce fait, rend illusoire les prohibitions édictées dans les législations européennes. L'architecture de l'Internet, le nombre croissant d'usagers et le recours aux réseaux pour transiger et conclure tout type de transactions constituent autant de facteurs expliquant les difficultés d'appliquer les normes relatives au contrôle des transmissions d'informations personnelles.

Cette tension entre, d'une part, la nécessité de protéger les données personnelles et, d'autre part, le principe de la libre circulation de l'information, consacré en droit international, a rendu nécessaire l'élaboration d'instruments internationaux en la matière. C'est ainsi que l'OCDE adopte en 1980 les *Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel* et que le Conseil de l'Europe adopte en 1981 la *Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel*. De même, l'Union européenne adopte, en 1995, la *Directive du Conseil 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*. Ces instruments consacrent les principes fondamentaux en matière de gestion de l'information personnelle que l'on retrouve également dans les deux lois québécoises.

Ces principes fondamentaux constituent, en quelque sorte, l'architectonique des diverses lois nationales de protection des renseignements personnels. Bien que ces instruments puissent diverger au plan de leur structure et de leur portée, l'interprète peut remarquer qu'ils s'articulent, malgré tout, autour d'un ensemble de règles communes (noyau dur).

Ces règles communes sont-elles en adéquation avec le nouvel environnement électronique mis en place sur l'inforoute? Certes l’on peut convenir que les principes fondamentaux en matière de gestion de l'information personnelle sont en mesure de

répondre aux défis posés par le développement des inforoutes[§§§§§§§]. On peut noter, avec le Conseil de l'Europe, que "comme les garanties constitutionnelles ou internationales en matière de droits de l'homme, les principes pour la protection des données sont énoncés en des termes permettant une adaptation aux situations en évolution"[********]. Les principes fondamentaux constituent finalement des énoncés généraux qui identifient les enjeux en imposant des limitations. Ils sont donc appelés, à l'instar des garanties constitutionnelles, à évoluer et à s'adapter aux circonstances nouvelles.

Ce constat, bien que rassurant, ne règle pas les difficultés pratiques d'application suscitées par la délocalisation et l'intangibilité de l'information numérique. Une fois posés les principes fondamentaux en matière de gestion de l'information personnelle: quelle loi appliquer? quelle autorité est compétente? comment déterminer l'existence même d'un traitement d'information personnelle concernant un individu fiché? etc.

Il existe des instruments internationaux en la matière mais ceux-ci ne sont pas en mesure de répondre aux défis concrets et pratiques soulevés par la décentralisation des réseaux. La mise en oeuvre pratique des règles concacrées par les lois nationales et les instruments internationaux s'avère relativement aisé lorsqu'il s'agit de policer l'État et ses composantes ou des groupes industriels importants qui ont pignon sur rue dans les divers ressorts nationaux (sièges sociaux et filiales). Bien qu'il ne faille pas minimiser l'importance de l'effort consenti par les agences nationales de protection des données, il faut bien reconnaître qu'il apparaît plus facile de surveiller les activités informationnelles d'une poignée d'entreprises et de sociétés publiques ou parapubliques établies sur un territoire donné que de surveiller les activités d'une kyrielle de sites Web disséminés à travers le monde, dont on ne connaît pas toujours très bien la localisation exacte, et sur lesquels, bien souvent, aucun contrôle effectif n'apparaît possible. C'est donc bien l'architecture des réseaux qui complique la mise en oeuvre pratique des principes fondamentaux en matière de gestion de l'information personnelle. Cette architecture électronique a des conséquences

---

[§§§§§§§] Commission d'accès à l'information, *Vie privée et transparence administrative au tournant du siècle. Rapport sur la mise en oeuvre de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels et de la Loi sur la protection des renseignements personnels dasn le secteur privé*, Québec, Juin 1997, p.42 (ci-après "Rapport de la Commission").

[********] Conseil de l'Europe, *Les nouvelles technologies: un défi pour la protection de la vie privée?* (Étude préparée par le Comité d'experts sur la protection des données, CJ-PD), Strasbourg, Conseil de l'Europe, 1989, p.44-45.

sur les principes de territorialité et de juridiction autour desquels s'articule l'action législative classique. D'ailleurs, le droit de la protection des données personnelles n'est pas le seul secteur juridique à pâtir de l'éclatement des concepts de territorialité, de juridiction, d'espace et de temps[††††††††]

Cela signifie-t-il qu'il faille rester les bras croisés et déplorer l'inapplicabilité *pratique* de nos législations relatives à la protection des données? Certainement pas. D'autres moyens peuvent être mis en oeuvre afin de répondre aux défis de la numérisation de l'information et de l'architecture éclatée des réseaux électroniques. Il convient maintenant d'aborder ces moyens.

### *2.3- Les moyens susceptibles de faciliter la mise en oeuvre pratique des principes fondamentaux en matière de gestion de l'information personnelle*

On a tendance à opposer la régulation législative à la régulation par le marché[‡‡‡‡‡‡‡‡]. La pure régulation par le marché repose sur des incitatifs purement financiers. Une entreprise décidera de protéger la vie privée de ses clients si cela peut lui conférer un avantage concurrentiel et alors, elle agira seule. Cette approche n'est évidemment pas exempte de critiques; on ne peut manquer de noter que l'individu, avant de décider de faire affaire avec telle entreprise plutôt qu'une autre, devra se renseigner. Or, pour les particuliers, les coûts d'acquisition d'une telle information apparaissent importants. Comment peut-il, en effet, connaître les politiques relatives à la vie privée de toutes les entreprises d'un même secteur d'activité? Son pouvoir de négociation est tributaire de ses possibilités d'accéder à l'information pertinente. De même, l'individu devra pouvoir exercer un droit de regard sur le respect des politiques de l'entreprise avec laquelle il aura finalement choisi de faire affaire. Là encore, des coûts importants sont à prévoir. Comment, en effet, s'assurer que ladite entreprise respecte bel et bien les principes qu'elle s'est donnés?

---

[††††††††] Lire Ethan KATSH, *Law in a Digital World*, New York, Oxford University Press, 1995. Lire aussi Karim BENYEKHLEF, "L'Internet: un reflet de la concurrence des souverainetés", dans *Réglementer les inforoutes* (Actes du colloque d'octobre 1996), à paraître.

[‡‡‡‡‡‡‡‡] Sur ce sujet, lire Peter SWIRE, "Markets, Self-Regulation, and Government Enforcement in the Protection of Personal Information", disponible à l'adresse électronique suivante: <http://www.osu.edu/units/law/swire.htm>

La régulation législative présente également des inconvénients. Nous avons déjà décrit sommairement les difficultés pratiques d'application des règles que le législateur s'est données en matière de protection des données personnelles. Un plus haut niveau d'efficacité des règles, s'il s'avère possible, engendrera, par ailleurs, une augmentation substantielle des coûts d'application de la loi. Or, il est loin d'être sûr qu'un accroissement des dépenses publiques pourra se traduire par une effectivité accrue des normes de protection des données personnelles afin de répondre réellement aux défis sucsités par le cyberespace.

En cette matière, il faut se tenir loin de tout dogmatisme. Une approche unilatérale, qu'elle émane du marché ou du législateur, ne peut répondre adéquatement aux difficultés afférentes à la protection des données personnelles sur les inforoutes. Il convient alors de chercher des modèles qui empruntent aux deux approches. Il s'agit de l'approche fondée sur l'autoréglementation et des autres approches de protection des données personnelles.

**L'autoréglementation**

On a souvent parlé, dans le cadre des discussions entourant l'adoption de la *Loi sur la protection des renseignements personnels*, notamment, de l'autoréglementation. Peter Swire définit ainsi l'autoréglementation:

> *Self-regulation, like government regulation, can occur in the three traditional components of the separation of powers: legislation, enforcement, and adjudication. Legislation refers to the question of who should define appropriate rules for protecting privacy. Enforcement refers to the question of who should initiate enforcement actions. Adjudication refers to the question of who should decide whether a company has violated the privacy rules.*[§§§§§§§§]

Swire estime que l'autoréglementation ne relève pas de la pure approche de marché ou de l'approche législative. En effet, l'autoréglementation n'apparaît pas comme un simple avatar de la pure approche du marché, puisque que très souvent, les entreprises se coalisent afin d'élaborer des normes autoréglementaires dans leur secteur d'activités. Autrement dit, l'entreprise n'agit pas seule, à la recherche d'un pur avantage compétitif sur ses concurrents. Au surplus, l'autoréglementation produit des effets dès lors qu'elle dépasse les simples proclamations de bonnes intentions.

---

[§§§§§§§§] Ibid.

L'autoréglementation ne constitue cependant pas la panacée. Il importe, en effet, de développer d'autres modalités propres à parfaire cette approche qui, seule, ne saurait répondre, nous semble-t-il, aux défis posés par l'inforoute. Avant de décrire ces autres modalités, il convient de dire quelques mots sur l'approche autoréglementaire.

À certaines conditions, l'autoréglementation peut constituer une voie intéressante pour ce qui est des grandes et moyennes entreprises qui sont prêtes à se regrouper afin d'élaborer un code de pratiques équitables en matière de gestion de l'information personnelle. Il existe déjà au Canada des codes de conduite de cette nature. Pensons, par exemple, aux codes de l'Association des banquiers canadiens ou des assureurs de personne ou encore au code de conduite type de l'Association canadienne des normes. Toutefois, il ne s'agit pas là d'une approche autoréglementaire complète au sens où l'entend, notamment, Swire. En effet, ces codes ne prévoient pas généralement de mécanismes impartiaux et neutres de résolution ou d'adjudication des conflits. De même, on se heurte là aussi au caractère territorialement limité des normes autoréglementaires. En effet, ces normes ne s'adressent, en principe, qu'aux seules entreprises québécoises ou canadiennes. De plus, ces normes n'ont pas nécessairement été élaborées afin de tenir compte des particularismes des communications électroniques sur des réseaux décentralisés, de type Internet. Finalement, il existe toujours le risque que les règles élaborées par des associations d'entreprises ne fassent la part trop belle aux intérêts de celles-ci. En d'autres termes, les intérêts des personnes fichées risquent d'être négligés puisque ces dernières ne participent pas au processus d'élaboration des normes autoréglementaires.

Malgré ses limites, l'approche autoréglementaire présente des avantages. Il est possible de remédier aux écueils ci-haut énoncés. Tout d'abord, on peut favoriser le développement de cadres d'élaboration des normes autoréglementaires associant les usagers. Ces normes devraient évidemment tenir compte des particularités liées à la communication dans les réseaux décentralisés. Si la perspective d'associer des usagers apparaît trop problématique, il est également possible d'imaginer la participation de tiers neutre au processus d'élaboration des normes.

À cet égard, il convient de signaler les travaux de la Conférence sur l'harmonisation des lois du Canada (CHLC) qui a résolu qu'une loi uniforme provisoire sur la protection des données soit préparée par un groupe de travail et que celui-ci essaie de savoir s'il y a des mécanismes efficaces pour élaborer et ratifier des codes sectoriels ou d'autres mesures offrant des guides plus précis à la protection de la vie privée. Le groupe de travail a

justement pour tâche de déterminer la nécessité d'élaborer des codes industriels ou sectoriels de bonne conduite en matière de vie privée. Il fonde ses analyses notamment sur le code-type de l'Association canadienne des normes.

Les associations d'entreprises québécoises pourraient s'associer aux associations d'entreprises étrangères afin de participer à l'élaboration de codes de conduite de portée internationale. À ce propos, l'article 27 de la Directive européenne reconnaît la possibilité de développer des codes de bonne conduite. On y encourage les milieux professionnels à participer à l'élaboration de codes de conduite communautaires destinées à contribuer à la bonne application de la directive en fonction de la spécificité des secteurs. La coopération internationale, en la matière, s'avère primordiale. Il convient, par conséquent, que le secteur privé québécois soit associé étroitement à ces travaux afin de faciliter la mise en oeuvre de normes autoréglementaires propres à assurer une protection transfrontière des données personnelles. Il importe, en effet, d'assurer l'interopérabilité des codes nationaux.

Avec une telle approche, ce sont les entreprises et les autres groupes qui s'avèrent les premières responsables de la rédaction des normes de bonne conduite. Toutefois, ces entités peuvent bénéficier, dans cet exercice, des conseils judicieux et de l'appui des instances publiques détenant de l'expertise en la matière. Au bout du compte, ce sont les principes fondamentaux en matière de gestion de l'information personnelle, consacrés dans la législation, qu'il s'agit d'adapter et d'appliquer aux différents secteurs d'activités. La loi constitue donc un arrière-plan normatif qui inspire et guide les rédacteurs des codes de bonne conduite relatifs à la protection des données personnelles.

Il importe également d'assurer que ces codes puissent faire l'objet d'une sanction. Le contrat constitue, à ce propos, une voie intéressante. La plupart des juristes s'entendent pour dire que la voie contractuelle constitue sans doute l'approche la plus féconde dans le cyberespace[*********]. En effet, en l'absence de règles uniformes internationales et face aux formidables difficultés de mise en oeuvre et d'application de telles règles, si elles existaient, le contrat peut constituer un véhicule intéressant permettant à tous les acteurs du

[*********] Lire, entre autres, Joel R. REIDENBERG, "Setting Standards for Fair Information Practice in the U.S. Private Sector", (1995) 80 *Iowa L.Rev.* 497 et I. Trotter HARDY, "The Proper Legal Regime for Cyberspace", [1994] 55 *University of Pittsburgh L. Rev.* 993; BAKER, M. B., "Private Codes of Corporate Conduct: Should the Fox Guard the Henhouse?", (1993) 24 *University of Miami Inter-American Law Review* 399.

cyberespace d'assurer la protection et le respect de leurs droits[††††††††]. Il conviendrait alors d'élaborer un contrat-type ayant pour objet d'assurer la protection des données personnelles. Ce contrat-type reprendrait, en substance, les principes mis de l'avant dans les codes de conduite.

Certes, la conclusion d'un contrat ne convient pas à toutes les circonstances. La simple visite d'un site Web ou l'achat d'un bien matériel par voie électronique, par exemple, ne sauraient justifier la conclusion d'un contrat ayant pour objet d'assurer le respect des données personnelles. Il s'avère donc nécessaire de prévoir un mécanisme par lequel les atteintes aux normes autoréglementaires puissent être sanctionnées. On peut suggérer ici des mécanismes de médiation ou d'arbitrage électronique. À ce propos, ces mécanismes de médiation et d'arbitrage pourraient également servir dans les cas où un contrat-type a été conclu.

**Les démarches de standardisation**

Le phénomène de l'émergence des autoroutes de l'information demeure marqué par la technologie. C'est la technologie qui a rendu possible le concept d'environnement électronique et qui, par la force des choses, a introduit les problèmes de la protection des droits fondamentaux dans ces environnements. La technologie peut, en grande partie contribuer à réduire ou éliminer les problèmes qu'elle a engendrés. En offrant des techniques performantes pour classifier et canaliser l'information, le technologie peut aider les utilisateurs à exercer un contrôle approprié de la circulation des information[‡‡‡‡‡‡‡‡].

---

[††††††††] Le Conseil de l'Europe, conjointement avec la Commission européenne et la Chambre de commerce internationale, a élaboré un contrat-type applicable aux flux transfrontières de données à caractère personnel. L'objet essentiel de ce contrat est de faciliter la circulation internationale de données nominatives en assurant un degré de protection aux données, ainsi transmises, équivalent, en principe, à celui du pays exportateur. Cette exigence est bien-sûr la résultante des exigences à cet effet que l'on retrouve dans la plupart des lois européennes et dans les instruments internationaux. Lire Conseil de l'Europe, Contrat-type visant à assurer une protection équivalente des données dans le cadre des flux transfrontières de des et Rapport explicatif, Strasbourg, T-PD (92) 7 révisé, 2 novembre 1992. Pour la version anglaise, lire NOTE, "Transborder Data Flow Model Contract Agreed", (1992) *Privacy Laws & Business* 13.

[‡‡‡‡‡‡‡‡] David POST indiquait à cet égard : *"One can hardly imagine, to be sure, a rule regarding, say, fraudulent transactions that would be capable of digital embodiment in these engineering specifications. One can imagine, however, a digital embodiment of rules regarding other activities -for example, the transmission of anonymous messages, or encrypted files- that can be more easily expressed in digital form and thereby enforced at the level of the technical network specifications",*

Les politiques de soutien aux initiatives fondées sur la technologie de même qu'une implication active de l'expertise québécoise dans le développement et la formulation de normes techniques conçues afin d'améliorer la protection des droits des personnes dans les espaces cybernétiques devraient être envisagés comme des éléments centraux de toute politique québécoise en ces domaines.

Plusieurs initiatives ont été mises de l'avant afin de mettre la technologie au service de la protection des droits et valeurs sur les inforoutes. On n'a qu'à penser aux outils-censeurs comme le "V-chip" ou la puce anti-violence, au brouillage des émissions à caractère sexuel destinées aux adultes, à des programmes comme *Cyber Patrol* et *Net Nanny* s'appuyant sur le système de classification *Platform for Internet Content Selection* (P.I.C.S.), lequel permet de catégoriser l'information circulant sur l'Internet, donnant ainsi aux parents et aux enseignants la possibilité de bloquer certains sites particuliers[§§§§§§§§§] :

> *The choice of an interactive architecture, with header information, makes effective screening by the recipient possible. No longer will controversial material intrude into users' homes in the manner that, in Congress' view, required steps to aid parents in protecting children. Rather, users will request that particular information be delivered. These requests can be screened or controlled by parents if necessary to limit their children's access to certain kinds of information.*[**********]

Par ailleurs, Douglas Barnes évoquait la possibilité suivante :

> *Certain publications or information products might be available only to residents of certain countries, along the lines of the ftp sites used for distributing cryptography in the US. To be secure, this would require, for starters, a global standard for authenticating individuals as to their citizenship-- an electronic passport. Companies would then have to hire experts to screen materials, and only then could*

---

dans "Anarchy, State and the Internet : An Essay on Law-Making in Cyberspace" (1995) *J. Online L.* art. 3, http://warthog.cc.wm.edu/law/publications/jol/post.html, par. 24.

[§§§§§§§§§] Voir Marc CADEN et Stephanie LUCAS, "Accidents on the Information Superhighway : On-line Liability and Regulation", (1996) 2 *Rich. J.L. & Tech.* 3, http://www.urich.edu/~jolt/v2i1/caden_lucas.html.

[**********] Jerry BERMAN et Daniel WEITZNER, "Abundance and User Control : Renewing the Democratic Heart of the First Amendment in the Age of Interactive Media" (1995) 104 *Yale L.J.* 1619, 1621.

> *controversial materials be made available, based on the consumer's nationality.*[††††††††††]

Le législateur américain a reconnu le potentiel normalisateur de la technologie et a, à ce niveau, accordé à ceux qui l'exploiteront une très grande marge de manoeuvre. Le *Communications Decency Act* consacrait toute une disposition aux méthodes de filtrage et de blocage du contenu offensant. On y indique que le Congrès reconnaît que ces services *"[trad.] offrent un grand degré de contrôle aux usagers sur l'information qu'ils reçoivent, ainsi qu'un potentiel encore plus grand dans le futur, à mesure que la technologie se développera"*. La politique des États-Unis est donc *"[trad.] d'encourager le développement de ces technologies qui optimisent le contrôle, par les individus, les familles et les écoles qui utilisent l'Internet et les autres services informatiques interactifs, sur l'information qu'ils reçoivent"*[‡‡‡‡‡‡‡‡‡]. Le *National Information Infrastructure Advisory Council* avait d'ailleurs fait la recommandation suivante, en décembre 1995, à l'*Infrastructure Information Task Force* :

> *The government should not be in the business of regulating content on the Information Superhighway. It should defer to the use of privately provided filtering, reviewing and rating mechanisms, and parental supervision as the best means of preventing access by minors to inappropriate materials.*[§§§§§§§§§§]

Il convient également de rappeler que les différentes institutions gouvernementales des États disposent de pouvoirs réglementaires en ce qui a trait à la normalisation technique, ce qui leur permet d'orienter les travaux dans ces domaines vers la réalisation d'objectifs sociaux plus généraux. Bien qu'ils ne maîtrisent pas tous les leviers de la normalisation technique, tous les États semblent s'entendre sur la nécessité de participer à de tels travaux ou, à tout le moins, d'en promouvoir les aspects sociaux sous-jacents.

---

[††††††††††] Douglas BARNES, "The Coming Jurisdictional Swamp of Global Internetworking, (Or, How I Learned to Stop Worrying and Love Anonymity)" (16 novembre 1994), http://www.communities.com/paper/swamp.html.

[‡‡‡‡‡‡‡‡‡] La Loi oblige également les manufacturiers de télévision à installer des équipements qui permettront aux téléspectateurs de bloquer certaines émissions, en raison de leur qualification. La Loi accorde par ailleurs une protection de "bon samaritain" en accordant une immunité civile aux usagers et aux fournisseurs de services qui prendront, de bonne foi, des mesures en vue de restreindre l'accès ou la disponibilité de matériel qu'ils considèrent obscène, excessivement violent, ou autrement offensant.

[§§§§§§§§§§] Voir *NIIAC Recommendation (December 12, 1995) to Secretary Ron Brown Regarding Content Regulation*, http://www.niiac-info.org/~niiac/content.html.

La mise en place d'outils de contrôle n'est cependant pas qu'une opération technique; elle nécessite souvent l'exercice d'un jugement éditorial qui doit être entouré de garanties démocratiques. Il est donc essentiel de favoriser la mise en place de mécanismes collectifs afin de favoriser les contrôles à la réception dans une perspective pluraliste, notamment l'étiquetage des sites et des contenus, les mécanismes de filtres électroniques[**********] et les mécanismes propres à assurer la protection de la vie privée. La cryptographie est une autre technique de contrôle des contenus, visant notamment à en préserver la sécurité et la confidentialité.

La Commission d'accès à l'information mentionne, dans son rapport, la possibilité de recourir à des modalités technologiques susceptibles d'assurer la protection des renseignements personnels. Elle les regroupe sous l'acronyme anglais P.E.T. (Privacy Enhancement Technology)[††††††††††]. Voilà un exemple d'une voie à laquelle il importe de prêter l'attention nécessaire.

À cet égard, il convient de mentionner les travaux du World Wide Web Consortium (W3). Ce consortium regroupe diverses entreprises du secteur privé, des universités et des centres de recherche et a pour objectif de développer des protocoles et des standards communs à l'usage de l'Internet. Le W3 est justement en train de développer un projet propre à assurer la protection de la vie privée des internautes. Ce projet a pour nom "Platform for Privacy Preferences" (P3 Project). Le W3 décrit ainsi ce projet:

> *The Platform for Privacy Preferences is a project at the World Wide Web Consortium (...) P3 will enable computer users to be informed and to make choices about the collection, use and disclosure of their personal information on the Web. The P3 project will result in the specification and demonstration of the interaction between a site's privacy prcatices and a user's privacy preferences. Sites with practices that fall within a user's preference will be accessed "seamlessly", otherwise users will be notified of a site's practices and have the opportunity to agree to those terms, to be offered new terms, or to discontinue browsing that site. A result of such an "agreement" is that data from the user may be securely transferred to the site with the consent of the user. This aids users where they*

---

[**********] Sur ce sujet, voir Pierre TRUDEL et France ABRAN, Karim BENYEKHLEF et Sophie HEIN, *Droit du cyberespace*, Montréal, Éditions Thémis, 1997, chapitre 15 - *Les stratégies de contrôle des contenus indésirables*.

[††††††††††] Rapport de la Commission, p.40.

> *would otherwise have to repeatedly enter basic information, or in providing information to a site which may use it to offer customized service. P3 can be incorporated into browsers, or "proxy" products that sit between a user and the server*[‡‡‡‡‡‡‡‡‡‡].

Des entreprises comme Netscape, Microsoft, IBM, AT&T Labs, entre autres, sont associées à ce projet. Il ne s'agit pas ici de s'apesantir sur ce projet spécifiquement, mais bien plutôt de signaler l'importance pour le Québec de prendre une part active à ce type de travaux. La mise à contribution des solutions technologiques dans le but d'assurer la protection de la vie privée des citoyens et des citoyennes est une voie qui ne manquera pas d'être privilégiée par de nombreux intervenants. Si l'on souhaite que les valeurs et sensibilités québécoises se reflètent dans cette normativité à caractère essentiellement transnationale, il faut prendre les moyens de participer aux multiples processsus de son élaboration.

Cette normativité technique s'élabore en effet dans des forums différents des seuls lieux de rencontre de représentants gouvernementaux. Elle prend souvent ses racines au sein des organisations non gouvernementales voire même dans les congrès scientifiques. L'appui aux acteurs québécois susceptibles de faire progresser les valeurs que l'on cherche à préserver ici devient de ce fait une composante majeure de toute politique en ces matières.

Il conviendrait que les organismes publics et privés du Québec participent pleinement aux divers forums technologiques qui peuvent développer des solutions technologiques respectueuses des principes fondamentaux en matière de gestion de l'information personnelle.

Pour assurer l'efficacité de cette participation, il conviendrait également d'encourager les entreprises faisant affaires au Québec à se doter des instruments technologiques, comme le projet P3 ou d'autres qui pourront se développer à l'avenir. Un moyen pour ce faire serait peut-être d'octroyer des crédits d'impôt aux entreprises qui développent des solutions technologiques susceptibles d'assurer la protection de la vie privée des internautes.

---

‡‡‡‡‡‡‡‡‡‡ http//www.W3.org/P3/Overview.htm/

La cryptographie (ou le chiffrement) est une technique servant à transformer les messages électroniques de façon à les rendre illisibles pour ceux à qui ils ne sont pas destinés. Le décryptage étant la technique inverse, soit de rendre lisible un message crypté. L'intérêt principal de la cryptographie réside dans le fait qu'il protège le caractère privé et sécuritaire des communications électroniques. La technique de la cryptographie ne constitue pas en soi une activité illicite. Certes, son développement et son utilisation soulèvent des préoccupations importantes, notamment en matière de sécurité nationale mais cette technologie procure également des avantages.

La cryptographie a été développée dans les années 1970, au sein des administrations publiques, en raison des avantages que cela comportait en terme de sécurité et de confidentialité. La technique tend maintenant à être de plus en plus répandue, trouvant notamment de multiples utilisations dans les environnements électroniques. En effet, la cryptographie, qui peut reposer sur différents protocoles, certains plus puissants que les autres, permet aux usagers des environnements électroniques de communiquer entre eux et d'effectuer des transactions commerciales en toute sécurité et en toute confidentialité, deux éléments qui sont essentiels à la réalisation de nombreuses activités.

Toutefois, les avantages de la cryptographie peuvent être utilisés à mauvais escient, permettant aux malfaiteurs ou aux terroristes de camoufler leurs activités illicites sur l'inforoute. Ceux-ci pourraient, par exemple, déjouer toute tentative d'écoute électronique et ainsi éviter la détection de leurs activités criminelles[§§§§§§§§§§]. En raison de ce danger, le gouvernement Clinton a annoncé, le 16 avril 1993, l'initiative du standard Clipper Chip[**********]. Le but poursuivi par cette initiative était de :

---

[§§§§§§§§§§] L. DORMAN *et al.*, "Digital Privacy : The Ethics of Encryption", http://rescomp.standford.edu/~pweston/privacy.html. Il est intéressant de noter au passage qu'indépendamment des techniques d'encryptage, dans le contexte de réseaux de téléphonie, le remplacement des fils en cuivre par des fils en fibre optique compromet l'efficacité de l'écoute électronique. Puisque des milliers d'appels téléphoniques peuvent être transmis à travers un seul câble, il devient, pour des fins d'interception, extrêmement difficile de repérer une transmission unique. Voir Henry R. KING, "Big Brother, The Holding Company : A Review of Key-Escrow Encryption Technology", (1995) 21 *Rutgers Comp. & Tech. L.J.* 224, 227.

[**********] *Clipper Chip* serait la technique la plus sophistiquée de cryptographie. Clipper Chip contient un algorithme de cryptographie 64-bit à clé secrète unique appelée Skipjack. Le gouvernement américain prétend qu'il faudrait à un ordinateur super puissant plus d'un billion d'années pour découvrir le code de la clé. Le gouvernement américain propose de tenir en dépôt la clé spéciale de cryptage/décryptage pour chaque système de téléphonie muni du Clipper Chip. Pour tout Clipper Chip fabriqué, deux clés seraient créées; une insérée à Clipper Chip lui-même et une autre,

> [TRADUCTION] *réunir le gouvernement fédéral et l'industrie dans un programme volontaire visant à améliorer la sécurité et le caractère privé des communications téléphoniques, tout en rencontrant les besoins légitimes d'application de la loi.*[††††††††††]

En plus d'offrir aux usagers la technique la plus sophistiquée de cryptographie, le standard Clipper Chip a été conçu de façon à permettre aux agents de la loi d'intercepter les communications téléphoniques des citoyens et des organismes qui font usage de ce service. Bien que le gouvernement américain prétende que l'usage de ce standard se ferait sur une base volontaire, il aurait laissé sous-entendre qu'il encouragerait le développement de Clipper Chip comme standard unique pour l'industrie. Le 4 février 1994, l'Administration Clinton a approuvé le projet Clipper Chip, en précisant que son étendue serait limitée aux communications téléphoniques seulement. Toutefois, en butte à l'opposition de groupes défendant les libertés civiles, le gouvernement a dû retraiter, reformulant ultérieurement sa stratégie dans ce domaine. Le 20 mai 1996, la Maison Blanche déposait un document de travail destiné à exposer ses nouvelles propositions sur la question[‡‡‡‡‡‡‡‡‡‡‡]. On notera, à ce chapitre, que les dirigeants du G7, réunis le 30 juillet 1996 lors d'une conférence ministérielle sur le terrorisme, ont conclu un accord comportant 25 mesures qu'ils s'engagent à prendre. Parmi ces mesures, il y a les deux mesures suivantes qui invitent les États à :

---

identique, divisée en deux composantes. Pour décrypter un message, il faudrait recombiner ces deux composantes. Une personne qui aurait la connaissance d'une composante ne pourrait décoder un message sans la connaissance de l'autre composante. Ainsi, en confiant ces composantes à deux organismes gouvernementaux distincts (National Institute for Standards and Technology-NIST) et the Automated Systems Division of the Department of Treasury) le gouvernement américain prétend pouvoir garantir la sécurité des communications téléphoniques. Henry R. KING, "Big Brother, The Holding Company : A Review of Key-Escrow Encryption Technology", (1995) 21 *Rutgers Comp. & Tech. L.J.* 224; Serge PARISIEN, et Pierre TRUDEL, avec la collaboration de V. WATTIEZ-LAROSE, *L'identification et la certification dans le commerce électronique: Droit, sécurité, audit et technologies*, Cowansville, Éditions Yvon Blais, 1996.

[††††††††††] Henry R. KING, "Big Brother, The Holding Company : A Review of Key-Escrow Encryption Technology", (1995) 21 *Rutgers Comp. & Tech. L.J.* 224, 233.

[‡‡‡‡‡‡‡‡‡‡‡] Voir EXECUTIVE OFFICE OF THE PRESIDENT, OFFICE OF MANAGEMENT AND BUDGET, *Enabling Privacy, Commerce, Security and Public Safety in the Global Information Infrastructure*, 20 mai 1996, http://www.eff.org/pub/Privacy/Key_escrow/Clipper_III/HTML/960520_nist_clipper3_paper.draft.html. En bref, le gouvernement désire toujours mettre en place une infrastructure qui lui donnerait les outils nécessaires pour décrypter certains messages, comme ceux reliés au terrorisme ou au crime organisé.

> *6. Note the risk of terrorist using electronic or wire communications systems and networks to carry out criminal acts and the need to find means, consistent with national law, to prevent such criminality;*
>
> *11. Accelerate consultations, in appropriate bilateral or multilateral fora, on the use of encryption that allows, when necessary, lawful government access to data and communications in order to, inter alia, prevent or investigate acts of terrorism, while protecting the privacy of legitimate communications.*[§§§§§§§§§§§§]

Tout ce débat sur la cryptographie illustre très bien la nécessité d'aborder la question de la protection des droits dans le cyberespace en se tenant loin de tout dogmatisme. Les possibilités offertes dans cet espace virtuel comportent à la fois du bon et du mauvais: il est imprudent de décréter prématurément des approches trop catégoriques reposant sur un parti-pris trop rudimentaire en faveur d'une approche en particulier.

---

§§§§§§§§§§§§ MINISTERIAL CONFERENCE ON TERRORISM, *Agreement on 25 Measures* Paris, France, 30 juillet 1996, http://UTL1.library.utoronto.ca/www/g7/terror25.htm. En février 1996, le NATIONAL INFORMATION INFRASTRUCTURE ADVISORY COUNCIL avait indiqué dans son rapport final, *A Nation of Opportunity : Realizing the Promise of the Information Superhighway*, 1996, http://www.benton.org/KickStart/nation.home.html, que l'encryptage ne devait être autorisé que pour les communications légitimes : *"people should be able to encrypt all lawful communications, information and transactions on the Information Superhighway"*.

# CONCLUSION

L’univers des inforoutes est trop diversifié pour y entrevoir une modalité unique et exclusive de réglementation des échanges informationnels. En effet, il est bien difficile de prévoir la direction que prendra le développement du cyberespace. Il convient dès lors de rester à l'affût afin d'être au coeur des processus décisonnels qui auront une incidence sur l'architecture des réseaux et, de ce fait, sur le droit de la protection des données personnelles. Si l’on reconnaît désormais l’importance d’assurer des veilles technologiques comme composante centrale des politiques en ce domaine, les impératifs de la protection des droits fondamentaux sur les inforoutes appellent le maintien et la consolidation de veilles juridiques afin de promouvoir le développement et l’adoption des approches les plus efficaces pour assurer les équilibres plus que jamais nécessaires dans cet environnement planétaire dans lequel tous doivent avoir leur place.

Il faudrait dans cet esprit songer à la mise en place de mécanismes légers de veille juridique réunissant les différentes compétences situées aussi bien à la Commission d'accès à l'information que dans les secteurs privé et public et du monde universitaire. Un tel réseau pourrait contribuer à renforce la participation québécoise aux travaux d'organismes informels, comme le W3 Consortium, l'Internet Privacy Working Group ou l'Internet Law and Policy Forum, afin de pouvoir prendre part pleinement au processus de décision et aussi de tenir au courant le gouvernement des grandes orientations en matière de protection de la vie privée sur l'inforoute.