DROIT À LA VIE PRIVÉE:

DEUXIÈME DOCUMENT DE TRAVAIL

Mai 1998

TABLE DES MATIÈRES

PROTECTION DE LA VIE PRIVÉE : DEUXIÈME DOCUMENT DE TRAVAIL

RÉSUMÉ

Il s'agit du deuxième document de travail sur la vie privée que le ministère de la Justice a rédigé récemment. Le premier, qui a été rendu public en juillet 1996, contenait des propositions de mesures législatives visant à protéger les renseignements personnels en possession du gouvernement du Nouveau-Brunswick. Ce document a été soumis au Comité de modification des lois en vue de la tenue d'audiences publiques. Après celles-ci, le comité a approuvé les propositions contenues dans le document et il a recommandé que le ministère prépare un second document de travail afin d'examiner la possibilité d'appliquer des mesures législatives sur la protection de la vie privée dans le secteur privé.

Le présent document de travail fait suite à cette recommandation. Il a pour objectif de déterminer si la vie privée des Néo-Brunswickois doit être protégée davantage qu'elle ne l'est par les lois actuelles et, si oui, par quels moyens. Plutôt que des recommandations, le document contient des propositions pour les fins de la discussion. Comme le précédent document, il sera soumis au Comité de modification des lois qui en fera l'étude et qui permettra à la population de contribuer à l'élaboration des politiques à cet égard.

Le document se divise en deux parties. La première porte sur la *Protection des données dans le secteur privé*. La « protection des données » concerne la mise en oeuvre de règles qui guident le traitement des renseignements personnels qu'un organisme recueille et utilise dans le cadre de ses activités. La *Loi sur la protection des renseignements personnels* du Nouveau-Brunswick, qui vient tout juste d'être adoptée, est un ensemble de mesures législatives assurant la protection des données dans le secteur public. Le document examine le bien-fondé de l'adoption de mesures législatives pour le secteur privé et il en étudie le contenu possible.

Dans la deuxième partie, on discute de la question de *La vie privée en général*. La protection des données est l'un des éléments de la protection de la vie privée dans son sens large; l'examen du bien-fondé d'une loi sur la protection des données et de son contenu doit aborder la question de savoir ce qui existe ou ce qui pourrait être mis en oeuvre en matière de législation sur la protection de la vie privée en général. Il existe aussi un lien important en ce qui concerne les grandes orientations des diverses mesures législatives susceptibles d'être adoptées dans le but de protéger la vie privée. La protection des données est-elle la seule ou la plus urgente des préoccupations? L'examen de la législation en matière de la vie privée en général ainsi que de son sous-élément assurant la protection des données permettra de soumettre des questions de ce genre aux discussions publiques.

Au sujet de la protection des données, le document suggère, compte tenu de l'état actuel des choses au Canada, que l'on s'inspire du *Code type sur la protection des renseignements personnels* de l'Association canadienne de normalisation (le code de la CSA) pour préparer une loi applicable au secteur privé. Le code de la CSA constitue déjà le

fondement de la *Loi sur la protection des renseignements personnels* que le Nouveau-Brunswick vient d'adopter.

Le document décrit la portée et le contenu possibles des mesures législatives inspirées du code de la CSA. Leur portée pourrait être vaste. Le code de la CSA est conçu de sorte à trouver une application dans tous les organismes commerciaux et non commerciaux, y compris chez les particuliers qui recueillent et utilisent des renseignements personnels à des fins commerciales ou à d'autres fins non personnelles. Dans le code de la CSA, l'expression renseignement personnel désigne un renseignement concernant un individu identifiable, enregistré sous quelque forme que ce soit. Cette définition englobe les renseignements sensibles ainsi que l'information ordinaire. Tous les organismes recueillent et utilisent des renseignements personnels, ne serait-ce que sous forme de listes de données sur leurs membres ou leurs clients ou de dossiers sur leurs employés.

Le document suggère que les principaux éléments du code de la CSA à retenir en vue de la préparation de mesures législatives sont ses dix principes. Ces principes sont énoncés en termes généraux pour tenir compte de la grande diversité des situations auxquelles ils pourraient s'appliquer.

Premier principe - Responsabilité
Un organisme est responsable des renseignements personnels dont il a la gestion et doit désigner une ou des personnes qui devront s'assurer du respect des principes énoncés ci-dessous.

Deuxième principe - Détermination des fins de la collecte des renseignements
Les fins pour lesquelles des renseignements personnels sont recueillis doivent être déterminées par l'organisme avant ou au moment de la collecte.

Troisième principe - Consentement
Toute personne doit être informée et consentir à toute collecte, utilisation ou communication de renseignements personnels qui la concernent, à moins qu'il ne soit pas approprié de le faire.

Quatrième principe - Limitation de la collecte
L'organisme ne peut recueillir que les renseignements personnels nécessaires aux fins déterminées et doit procéder de façon honnête et licite.

Cinquième principe - Limitation de l'utilisation, de la communication et de la conservation
Les renseignements personnels ne doivent pas être utilisés ou communiqués à des fins autres que celles auxquelles ils ont été recueillis à moins que la personne concernée n'y consente ou que la loi ne l'exige. On ne doit conserver les renseignements personnels qu'aussi longtemps que nécessaire pour la réalisation des finalités déterminées.

Sixième principe - Exactitude
Les renseignements personnels doivent être aussi exacts, complets et à jour que l'exigent les fins pour lesquelles ils sont utilisés.

Septième principe - Mesures de sécurité
Les renseignements personnels doivent être protégés au moyen de mesures de sécurité correspondant à leur degré de sensibilité.

Huitième principe - Transparence
Un organisme doit mettre à la disposition de toute personne des renseignements précis sur ses politiques et ses pratiques concernant la gestion des renseignements personnels.

Neuvième principe - Accès aux renseignements personnels
Un organisme doit informer toute personne qui en fait la demande de l'existence de renseignements personnels qui la concernent, de l'usage qui en est fait et du fait qu'ils ont été communiqués à des tiers, et lui permettre de les consulter. Il sera aussi possible de contester l'exactitude et l'état complet des renseignements et y faire apporter les corrections appropriées.

Dixième principe - Possibilité de porter plainte contre le non-respect des principes
Toute personne doit être en mesure de se plaindre du non-respect des principes énoncés ci-dessus en communiquant avec le ou les individus responsables de les faire respecter au sein de l'organisme concerné.

On passe en revue ces principes dans le document. On suggère dans certains cas d'apporter de légères modifications à leur formulation pour les fins législatives, mais la partie la plus importante de l'étude porte sur la signification de la détermination des fins de la collecte dont parle le deuxième principe, sur celle du consentement et de l'expression « à moins qu'il ne soit pas approprié de le faire » du troisième principe ainsi que sur les exigences du neuvième principe en ce qui concerne le droit à l'information. Le code de la CSA aborde ces points dans les commentaires qui accompagnent les principes. Dans le document, on indique que la loi devrait aussi régler certaines de ces questions.

On pose parfois dans ce document la question de savoir si ces principes se prêtent aussi bien aux petits qu'aux grands organismes. Le code de la CSA est conçu de sorte à trouver une application peu importe l'échelle, mais certains de ses principes sont formulés dans des termes qui conviennent mieux aux grands organismes qu'aux petites organisations. Pour les fins de la discussion, le document est fondé sur la même hypothèse que le code de la CSA, à savoir que la loi devrait s'appliquer à tous, et il examine les questions qui semblent problématiques du point de vue des petits organismes. L'une des questions que l'on doit se poser est celle de savoir si une loi sur la protection des données dans le secteur privé (si elle est adoptée) doit avoir une portée aussi vaste que le code de la CSA ou si une approche plus ciblée convient mieux à la situation.

Le document examine en outre l'application des possibles mesures législatives sur la protection des données axées sur le code de la CSA, et il analyse le caractère opportun des recours pénaux (poursuite et amende), des recours civils (dommages-intérêts, jugement déclaration et injonction) et des recours administratifs (qui peuvent être de natures diverses et qui seraient dispensés par un organisme administratif plutôt que par un tribunal). Contrairement à ce que l'on entend souvent au sujet des mesures législatives sur la protection des données, le document conclut que les recours administratifs ne sont pas essentiels à la loi. Il s'agit cependant d'un choix politique. Voici les principales questions que pose l'adoption possible de recours administratifs en matière de protection des données : Quels pouvoirs de contrainte, le cas échéant, devrait-on accorder à l'organisme administratif aux fins de la protection des renseignements? Le traitement des plaintes doit-il être la seule fonction de l'organisme?

La partie II du document, qui s'intitule *La vie privée en général,* porte sur les deux principales avenues législatives qui s'offrent à la province si elle décide de renforcer aux protections législatives générales dont bénéficie la vie privée des Néo-Brunswickois. La première consiste à créer un délit civil d'atteinte à la vie privée (un délit civil est un acte fautif qui donne droit à la personne lésée de s'adresser aux tribunaux afin d'exercer les recours ordinaires en jugement déclaratoire, en dommages-intérêts ou en injonction). L'autre avenue consiste à créer des recours non judiciaires de violation de la vie privée qui seraient dispensés par un organisme autre que les tribunaux.

En ce qui a trait à la création d'un délit civil, le document décrit brièvement les recours judiciaires actuels qui permettent d'assurer le respect de la vie privée, et il examine en profondeur la *Loi uniforme sur la protection de la vie privée* préparée par la Conférence sur l'harmonisation des lois au Canada. Le document conclut que le délit civil qui pourrait être créé au Nouveau-Brunswick en cas d'atteinte à la vie privée ressemblerait en grande partie à la loi uniforme. Plusieurs provinces ont déjà adopté des lois de ce genre. Le document examine la loi uniforme comme modèle possible et il soumet les trois grandes questions suivantes à la discussion publique : La violation de la vie privée devrait-elle être un délit civil? Des mesures législatives fondées sur la *Loi uniforme sur la protection de la vie privée* pourraient-elles décrire adéquatement la violation de la vie privée sans menacer des activités désirables? La prudence dicte-t-elle de confier aux tribunaux, plutôt qu'au législateur, le soin d'élaborer le délit civil de violation de la vie privée?

Le document examine enfin la possibilité de créer des recours non judiciaires en cas de violation de la vie privée. On indique d'abord qu'il existe une marge entre une conduite qui serait qualifiée de délit civil, soit un acte fautif donnant ouverture aux recours en jugement déclaratoire, en dommages-intérêts et en injonction, et une violation moins grave de la vie privée. Le document mentionne des questions comme la surveillance vidéo ainsi que les tests et la surveillance pratiqués en milieu de travail qui, de l'avis de bien des gens, sont symptomatiques d'une perte graduelle d'intimité dans la société contemporaine. Il s'agit de savoir si l'on peut trouver des réponses non judiciaires à certaines des questions qui se posent en matière de protection de la vie privée.

Les opinions pourront diverger à ce sujet. L'intimité, que chacun chérit, concernerait strictement les relations sociales, de l'avis de certains. Les tenants de cette position soutiennent que les normes appropriées en matière de respect de l'intimité émergent de façon naturelle des interactions sociales. Il y aura toujours des activités qui soulèveront des questions au sujet des normes acceptables, mais à longue échéance, la seule indication de ce qui est acceptable est la persistance. Certaines personnes pourront penser aussi qu'il est incongru d'envisager des recours administratifs -- la bureaucratie, diraient-elles -- pour protéger et promouvoir le droit à la vie privée.

Il existe toutefois des organismes qui ont le mandat de protéger la vie privée. On en trouve des exemples dans le document, où on indique aussi qu'un organisme doté d'un mandat élargi dans le domaine de la protection de la vie privée pourrait s'occuper aussi de la protection des données. Le document conclut que les principales questions qui devraient être soumises à la discussion publique au sujet des recours non judiciaires en cas de violation de la vie privée en général sont semblables à celles qui se posent dans le cas précis de la protection des renseignements. A-t-on vraiment besoin de recours non judiciaires? L'organisme se contenterait-il de traiter les plaintes? Devrait-il avoir des pouvoirs de contrainte? Bien sûr, les réponses à ces questions pourront être différentes dans le contexte particulier de la protection des données et dans celui plus global de la protection de la vie privée en général.

Les questions examinées dans le document sont à la fois indépendantes et potentiellement interdépendantes. L'une des approches, une combinaison de deux de celles-ci ou même les trois ensemble pourraient constituer le fondement d'une législation visant à promouvoir la protection de la vie privée des Néo-Brunswickois. Par contre, on peut aussi soutenir qu'il est superflu de légiférer à cet égard.

Le document a pour but de donner lieu à un débat public complet sur les choix politiques qui s'imposent en la matière.

Introduction

En juillet 1996, le ministre de la Justice a déposé à l'Assemblée législative, en vue de l'étude par le Comité permanent de modification des lois, un document de travail intitulé *Loi sur la protection des renseignements personnels au Nouveau-Brunswick.* Celui-ci renfermait des recommandations au sujet du contenu des mesures législatives visant la protection et la confidentialité des renseignements personnels qui se trouvent en possession du gouvernement du Nouveau-Brunswick.

Le Comité permanent de modification des lois a tenu des audiences publiques en octobre et en novembre 1996, et il a présenté son rapport en février 1997. Ce rapport renfermait deux recommandations. La première approuvait en principe le document de travail. Des mesures législatives fondées sur ce document, à savoir la *Loi sur la protection des renseignements personnels,* ont été promulguées en février 1998; les préparatifs en vue de la proclamation vont débuter bientôt. L'expression *« Loi visant le secteur public »* servira à désigner ces mesures législatives dans les pages qui suivent.

La deuxième recommandation du Comité permanent de modification des lois se lisait comme suit :

> RECOMMANDATION 2
> Le comité recommande fortement que le gouvernement prépare un document de travail sur-le-champ, en vue d'audiences publiques, pour ce qui est d'étendre au secteur privé l'application de la mesure législative sur la protection des renseignements personnels.

Pour expliquer cette recommandation, le comité s'est exprimé de la façon suivante :

> Le comité entend, dans diverses interventions, que la mesure législative sur la protection des renseignements personnels ne devrait pas seulement s'appliquer aux organismes gouvernementaux mais aussi au secteur privé. Il est avancé que, peu importe si l'organisme ayant la surveillance des données personnelles se trouve dans un ministère ou dans une entreprise du secteur privé, les renseignements personnels sur les particuliers doivent quand même être protégés contre un accès préjudiciable.

Le présent document de travail a été préparé pour faire suite à la recommandation 2 du Comité permanent de modification des lois.

La première question que soulève cette recommandation est celle de savoir si le nouveau document de travail doit être fondé sur une définition plus restreinte ou plus large de son objet. Le document de 1996 se penchait sur ce que l'on appelle « la protection des données », c'est-à-dire l'établissement de règles qui régissent le traitement des renseignements personnels dont les organismes font la collecte dans le cadre de leurs activités. Si on adopte un point de vue restrictif, il suffirait de discuter ici des mesures législatives sur la protection des données dans le secteur privé qui seraient comparables à la *Loi visant le secteur public.*

Si on adopte une approche plus large, par contre, on s'aperçoit que la protection des données ne constitue qu'une partie de la question plus vaste de la protection de la vie privée. La définition que l'on donne souvent à la vie privée de nos jours comporte trois principales facettes : la protection de l'intégrité physique (le respect du corps de la personne), la protection de l'espace personnel (l'intimité spatiale) et la protection des renseignements personnels (qui sait quoi à votre sujet et que fait-on de ce qu'on sait?). La protection des données appartient en grande partie au domaine de la protection des renseignements personnels, n'étant par conséquent qu'une facette de la protection de la « vie privée » dans son sens large. Dans certains documents, comme le rapport intitulé *La vie privée : Où se situe la frontière?* qui a été rendu public en 1997 par le Comité permanent des droits de la personne et de la condition des personnes handicapées de la Chambre des communes, on avance que la protection de la vie privée dans son ensemble – et non seulement celle des renseignements personnels – soulève des préoccupations sociales et devrait faire l'objet de mesures législatives.

Bien qu'on pourrait ne s'en tenir dans ce document qu'aux mesures législatives visant précisément la protection des données, il est opportun d'examiner parallèlement le contexte global des lois assurant la protection de la vie privée. Il existe un lien évident entre les deux, surtout du point de vue des recours qui pourraient être créés par les mesures législatives sur la protection des données. Ce qui s'imposerait dans ce contexte serait en partie tributaire des recours que prévoient ou pourraient établir les lois relatives à la protection de la vie privée. Il existe aussi un lien important au chapitre de la portée de toute mesure législative qui pourrait être adoptée en vue de promouvoir la protection de la vie privée. La protection des données est-elle la seule ou la plus pressante des préoccupations? L'examen de la législation sur la protection de la vie privée dans son ensemble de même que les mesures auxiliaires sur la protection des données permettra de soumettre ces questions à un débat public.

Le présent document abordera donc la législation sur la protection de la vie privée entendue dans son sens large. Le document est divisé en deux parties. La première traite de la *Protection des données dans le secteur privé*. Il s'agit du prolongement logique et inéluctable du document de travail de 1996 et de la *Loi visant le secteur public*. Dans cette partie, on s'interrogera sur l'opportunité d'adopter des mesures législatives relatives à la protection des données dans le secteur privé; pour orienter la discussion, on y a décrit le contenu possible d'une loi portant sur cette question. Le modèle tracé est fondé sur le *Code type sur la protection des renseignements personnels* de l'Association canadienne de normalisation (appelé ci-après le « code de la CSA ») et sur la *Loi visant le secteur public* qui s'inspire en grande partie du code de la CSA.

Dans la deuxième partie, intitulée *La vie privée en général*, les recours judiciaires qui s'offrent actuellement au Nouveau-Brunswick en cas d'atteinte au droit à la vie privée seront examinés. On s'interrogera sur la nécessité de légiférer davantage à ce sujet. À cet égard, deux questions seront abordées. La première consiste à savoir si le Nouveau-Brunswick devrait suivre l'exemple de plusieurs (mais pas toutes) provinces canadiennes et légiférer afin de faire de l'atteinte à la vie privée un « délit civil » en bonne et due forme. Le délit civil est un acte fautif dont la victime peut demander réparation aux tribunaux dans le cadre de recours comme l'action en dommages-intérêts, le jugement déclaratoire et l'injonction. La deuxième question consiste à savoir si des recours pourraient être exercés devant des organismes autres

que les tribunaux en cas de violation du droit à la vie privée. Diverses possibilités seront étudiées, notamment celle qui consiste à élargir le mandat de la Commission des droits de la personne du Nouveau-Brunswick de sorte à lui permettre de jouer un rôle en matière de protection de la vie privée, en plus de son travail actuel de lutte à la discrimination. S'ils étaient adoptés, les recours judiciaires et extrajudiciaires examinés dans la partie II s'appliqueraient à tous les cas, qu'ils proviennent du secteur public ou du secteur privé.

Dans le présent document on ne présente pas de recommandations précises au sujet des diverses questions abordées. On présente plutôt des propositions en vue d'alimenter la discussion. Bon nombre de ces propositions ont été formulées de façon détaillée et pourraient servir de base à des mesures législatives si l'on concluait, à la suite des consultations, qu'une démarche semblable s'impose. Aucune décision n'a cependant été prise à ce sujet jusqu'à maintenant. Il est toujours possible de ne pas promulguer de loi, de légiférer à la pièce au sujet de l'une ou l'autre ou de plusieurs des questions examinées, ou d'adopter des mesures législatives qui aborderaient toutes les facettes de la question. Le présent document de travail a pour but d'aider à établir, au plan de la politique, les choix les plus appropriées dans les circonstances.

I. Protection des données dans le secteur privé

Dans la présente partie du document, on posera les deux questions suivantes : « Des mesures législatives sur la protection des données s'imposent-elles dans le secteur privé? »; « Dans l'affirmative, quel pourrait en être le contenu? » Les deux questions sont étroitement reliées. Plus on pourra préciser la teneur possible de la loi, plus on pourra argumenter à son sujet de façon éclairée.

Heureux effet du hasard, le présent document de travail a été préparé au moment même ou un document en particulier, le code de la CSA, domine les débats touchant la protection des données dans le secteur privé. Ce code a été préparé à l'intention de l'Association canadienne de normalisation par un comité technique composé de représentants du gouvernement fédéral, de l'industrie, des commissariats à la protection de la vie privée et des groupes de pression. De la façon dont il a été conçu, le code n'a pas force obligatoire; les organismes du secteur privé peuvent donc l'adopter intégralement s'ils le désirent ou même le modifier en fonction de leur situation particulière s'ils le jugent à propos. Mais on a peu à peu commencé à y voir le fondement d'une loi plutôt qu'une simple mesure d'autoréglementation. Le gouvernement fédéral est en faveur d'un tel point de vue. Il a fait connaître son intention d'adopter d'ici l'an 2000 des mesures législatives sur la protection des renseignements personnels dans les industries du secteur privé qui relèvent de sa compétence; le document de consultation qu'il a récemment rendu public et qui est intitulé *La protection des renseignements personnels : Pour une économie et une société de l'information au Canada* (janvier 1998) fait porter le débat sur le code de la CSA. Un certain nombre de commissaires à la protection de la vie privée au Canada se sont exprimés de manière favorable sur l'utilisation du code de la CSA comme base de la loi.

Cependant, on ne voit pas encore se dégager aucun consensus clair quant à l'intégration de la substance du code de la CSA dans une loi dont il serait le fondement. Même si certaines industries représentées au sein du comité technique de la CSA ont déjà adopté leur propre code sectoriel inspiré de celui de la CSA, rares sont celles qui préconisent de rendre le code obligatoire en le transformant en loi. Même ceux qui appuient en principe l'adoption de mesures législatives axées sur le code de la CSA veulent savoir *comment* celui-ci serait transformé en loi avant de concrétiser leur appui.

C'est ce besoin de clarté qui rend tout à fait opportun la *Loi visant le secteur public* du Nouveau-Brunswick. Cette loi, qu'on trouvera à l'annexe B, est carrément fondée sur le code de la CSA; elle constitue donc un exemple possible de la façon d'élaborer une loi en s'inspirant du code de la CSA. Par surcroît, ce modèle pourrait facilement trouver application dans le secteur privé, si les consultations actuelles indiquent qu'il s'agit de la voie à suivre.

Voilà précisément la question qui sera posée dans la première partie du présent document : *convient-il* d'appliquer des mesures législatives comparables dans le secteur privé? Il existe une marge entre le fait pour le gouvernement d'adopter des règles juridiques pour régir sa propre conduite et celui d'imposer à autrui des règles semblables. De nombreuses lois néo-brunswickoises créent des règles particulières qui s'appliquent au fonctionnement du secteur public. Celles-ci portent par exemple sur des questions comme les méthodes

d'embauche ou d'achat, les finances publiques ou l'équité salariale. Bon nombre de ces lois établissent des règles qui n'ont pas à être édictées sous forme législative; le fait de les intégrer à des mesures législatives donne cependant un poids additionnel à un engagement politique. On pourrait soutenir que les règles sur la protection des données se classent dans cette catégorie. On pourrait aussi avancer que des facteurs particuliers inhérents aux activités du secteur public et absents de celles du secteur privé rendent d'autant plus importante l'adoption de lois, plutôt que de règles, dans le secteur public dans le but de régir l'utilisation des renseignements personnels. Le fait que la *Loi visant le secteur public* pourrait être appliquée au secteur privé ne signifie pas nécessairement qu'elle *devrait* l'être. Les choix politiques et législatifs qui conviennent dans le secteur privé peuvent fort bien être différents de ceux qui réussissent dans le secteur public.

A. Doit-on légiférer dans le secteur privé?

Les mesures législatives visant la protection des données font en grande partie écho à l'informatisation croissante de notre société. Comme il est de plus en plus facile d'accumuler et de manipuler des renseignements, des préoccupations ont été soulevées sur la quantité de données dont disposent les organismes sur les particuliers et sur le peu de mesures de contrôle qui sont exercées relativement à leur utilisation. Ces préoccupations s'expriment de diverses façons selon le moment et le contexte. Le récent document de consultation du gouvernement fédéral, qui met l'accent sur le commerce électronique en vue de faire du Canada « le pays le plus branché du monde » (p.1), énonce ce qui suit :

> Le défi de l'ère électronique est qu'à chacune de nos transactions, nous laissons des données retraçables qui, combinées, peuvent révéler des détails personnels et nos préférences. À cause de la numérisation des dossiers médicaux, des dossiers scolaires, des dossiers d'emploi et de consommation, il devient possible, en combinant des renseignements, de tracer le profil d'un consommateur, et ce, à partir de données que la plupart d'entre nous estiment très personnelles. Ces renseignements peuvent être transmis d'une province à l'autre, voire d'un pays à l'autre, être vendus, réutilisés ou intégrés dans d'autres bases de données sans que nous le sachions ou y consentions. (p. 2)

D'autres descriptions pourraient élargir les perspectives pour englober d'autres formes de collectes de renseignements en plus des méthodes électroniques ainsi que d'autres utilisations possibles des renseignements en plus de l'élaboration de profils de consommateurs.

C'est pour répondre à ces préoccupations que les lois sur la protection des données tentent d'établir une panoplie de « méthodes équitables de gestion des renseignements personnels » que les organismes doivent adopter. Les règles portent sur le genre de renseignements personnels que les organismes peuvent recueillir, sur la durée de leur conservation ainsi que sur leur utilisation. Elles accordent aussi aux particuliers le droit d'avoir accès aux organismes qui les concernent et d'en demander la correction. Ces règles ont pour objet global de faire valoir l'intérêt continu qu'ont les particuliers à l'égard des renseignements que les organismes obtiennent à leur sujet et de ce qu'elles en font. Elles ont pour but d'établir que les renseignements n'appartiennent pas uniquement aux organisations pour en disposer comme bon leur semble.

La plupart des États européens ont adopté des lois qui s'appliquent à la fois au secteur privé et au secteur public en matière de protection des données. La Directive 95/46/CE (la « Directive de l'Union européenne ») oblige les membres de l'Union européenne à se doter de telles mesures législatives.

À l'extérieur de l'Europe, toutefois, la législation en matière de protection des données en général est moins bien établie, particulièrement dans le secteur privé. Pour les fins de la rédaction du présent document, les lois de Hong Kong et de la Nouvelle-Zélande qui s'appliquent au secteur privé ainsi qu'au secteur public ont été passées en revue. Le ministère de la Justice a aussi appris que Taiwan et Israël se sont dotés de lois en la matière. Les autres pays qui ont adopté des mesures législatives relatives à la protection des données (p. ex. : le Japon, l'Australie et les États-Unis) ont surtout mis l'accent sur le secteur public.

Au Canada, seul le Québec a adopté des mesures législatives visant à la fois le secteur privé et le secteur public. Ailleurs (sauf à Terre-Neuve et à l'Île-du-Prince-Édouard), il existe des lois portant sur le secteur public, bien que celui-ci soit défini de façon plus large par certaines administrations que par d'autres. En Colombie-Britannique, par exemple, la loi s'applique à des organisations comme les organismes d'autoréglementation des professions. Le Manitoba a récemment promulgué une loi traitant spécifiquement de l'utilisation des renseignements relatifs à la santé, que ce soit par le secteur public ou par le secteur privé.

De son côté, le gouvernement fédéral s'est engagé à adopter d'ici l'an 2000 une loi sur la protection des données dans les industries du secteur privé qui relèvent de sa compétence, et il incite les provinces à élaborer des lois correspondantes en ce qui concerne les activités de compétence provinciale. Le récent document de travail du gouvernement fédéral mentionne que des tribunes comme les rencontres des ministres responsables de l'autoroute électronique de l'information et des ministres de la Consommation servent de lieux de débats à ce sujet. Il indique aussi que la Conférence sur l'harmonisation des lois du Canada prépare une loi uniforme sur la protection des données; cette conférence permet aux représentants des diverses autorités canadiennes de tenter d'élaborer des modèles de lois dans des domaines où il serait souhaitable d'harmoniser les lois provinciales.

La Directive de l'Union européenne a été l'un des éléments qui ont incité le gouvernement fédéral à agir dans ce domaine. La Directive, qui a été adoptée en octobre 1995, exige que tous les pays membres de l'Union européenne mettent en vigueur, d'ici octobre 1998, des mesures législatives sur la protection des données qui satisfont aux critères énoncés. En vertu de l'un de ces critères, les pays membres doivent interdire le transfert de renseignements personnels vers des pays non-membres, à moins que ceux-ci assurent un « niveau de protection adéquat » des renseignements (art. 25) ou, en l'absence d'un « niveau de protection adéquat », à moins que « le responsable du traitement offre des garanties suffisantes au regard de la protection (des renseignements personnels transférés); ces garanties peuvent notamment résulter de clauses contractuelles appropriées » (art. 26). Voici ce qu'on pouvait lire à ce sujet dans le récent document de consultation du gouvernement fédéral : « Cette directive peut faire de la protection des renseignements personnels un obstacle non tarifaire majeur au commerce avec le Canada » (p. 8).

Un discours prononcé à Ottawa par Allan Rock alors qu'il était procureur général du Canada, en septembre 1996, devant la Conférence internationale des commissaires à la protection des données, résume de façon commode les arguments qui militent en faveur de l'application au secteur privé des mesures législatives sur la protection des données. Il a fait remarquer à l'audience que lorsque le gouvernement fédéral a promulgué la première loi sur la protection des données, il ne l'a fait que pour le secteur public; à l'époque, le gouvernement était de loin le principal agent de collecte, de conservation et d'utilisation des renseignements concernant les particuliers. Par la suite, le gouvernement a choisi d'inciter le secteur privé à prendre des mesures de protection des données dans le cadre de mécanismes d'autoréglementation. Mais depuis, le gouvernement a conclu que l'autoréglementation n'était pas suffisante dans le secteur privé.

(trad.) Notre position antérieure est devenue désuète. Les technologies de l'information modernes facilitent infiniment l'accumulation et l'échange de données par les entreprises et les organismes privés à l'intérieur et à l'extérieur des frontières. Les progrès des ordinateurs et des réseaux ont multiplié et accru les risques pour la vie privée.

Parallèlement, le Canada est passé rapidement d'une économie basée sur les ressources à une société axée sur l'information et le savoir. Dans ce contexte, un nombre sans cesse croissant d'établissements privés amassent, utilisent et échangent des renseignements au sujet de nos habitudes de consommation et des services que nous utilisons.

Compte tenu de la situation, le gouvernement du Canada est d'avis que la protection des renseignements personnels ne peut plus être tributaire du fait que les renseignements sont en possession d'un organisme public ou d'un organisme privé. Cela ne signifie pas que les règles régissant la collecte, l'utilisation, la communication et la destruction des renseignements personnels doivent être identiques quelle que soit la personne ou l'organisme. Mais cela signifie qu'elles doivent être fondées sur une série de principes communs, et cela signifie que les renseignements personnels dont le secteur privé est dépositaire doivent être protégés par la loi.

Mais les opinions divergent à ce sujet. En Australie, le ministère du Procureur général du Commonwealth (fédéral) a rendu public un document de travail, en septembre 1996, dans lequel il examine l'application au secteur privé des lois sur la protection des données. En 1997 cependant, le ministère a décidé de ne pas aller de l'avant. Il se préoccupait surtout des coûts que devraient assumer les entreprises, petites ou grandes, et de la nécessité de réduire le fardeau réglementaire, plutôt que de créer de nouveaux régimes obligatoires. Depuis cette décision, on a organisé en Australie des consultations au sujet d'un mécanisme national d'autoréglementation qui a donné lieu à la publication par le commissaire à la protection de la vie privée du Commonwealth des *National Principles for the Fair Handling of Personal Information,* en février 1998.

Aux États-Unis, les discussions qui ont eu lieu jusqu'à maintenant à l'échelon fédéral n'ont apparemment pas permis de conclure là non plus que l'adoption de mesures législatives généralisées s'imposait. Dans *Options for Promoting Privacy on the National Information*

Infrastructure, un document de consultation rendu public en avril 1997 par le comité sur la politique de l'information du groupe de travail sur l'infrastructure nationale de l'information, la protection des données par voie législative était seulement l'une des nombreuses possibilités examinées. Le document faisait aussi place à l'opinion de ceux qui constataient une évolution satisfaisante dans les critères et les pratiques du marché et qui voulaient laisser cette évolution se poursuivre; il mentionnait aussi l'alternative de continuer, comme on l'a fait dans le passé, de faire appel aux solutions législatives pour régler des problèmes ponctuels, le cas échéant, plutôt que d'adopter une loi de portée générale. L'adoption de mesures législatives d'application générale dans le secteur privé en matière de protection des données semble peu probable aux États-Unis à l'heure actuelle.

Voilà donc le contexte dans lequel s'inscrit la première question, c'est-à-dire doit-on légiférer dans le secteur privé? D'une part, compte tenu de la technologie de l'information moderne, on se préoccupe du fait qu'une trop grande quantité de renseignements personnels circule entre les mains d'intervenants trop nombreux qui en font une utilisation assujettie à trop peu de mesures de contrôle. On souhaite établir au moins un cadre composé de principes fondamentaux qui traduiraient l'intérêt continu qu'ont les particuliers à l'égard des renseignements que les organisations possèdent à leur sujet, et on juge que la voie législative est la façon la plus efficace de mettre sur pied un cadre commun qui serait respecté par tous.

Par contre, on s'inquiète non seulement du contenu des règles proposées, mais aussi de leur incidence pratique sur les organisations qui devront s'y conformer. Quant au contenu, on se préoccupe du fait que les mesures législatives pourraient faire obstacle à des activités désirables. En ce qui concerne leurs incidences pratiques, on craint que la loi impose un fardeau administratif excessif et qu'elle entraîne d'autres coûts. On se demande aussi si le problème est suffisamment grave pour justifier le recours à la solution législative.

Voilà les questions au sujet desquelles l'opinion du public et des intéressés devra être recueillie. Il y aura probablement peu de désaccords sur les grands principes qu'une telle loi sur la protection des données dans le secteur privé aurait pour objectif de promouvoir : les renseignements personnels ne doivent être ni recueillis ni utilisés à mauvais escient et, sous réserve de limites raisonnables, les particuliers doivent être en mesure de prendre connaissance de ce que les organismes savent d'eux et d'y apporter les corrections nécessaires. Cependant, les opinions vont certes diverger quant aux questions de savoir si l'adoption de mesures législatives est la bonne façon de faire valoir ces principes, si la loi atteindrait vraiment ses objectifs et si les avantages l'emportent sur les inconvénients. Il est facile d'inclure des expressions comme « à mauvais escient » ou « sous réserve de limites raisonnables » dans d'abstraits énoncés de principes. Elles peuvent cependant susciter la controverse lorsqu'on se pose réellement la question de savoir ce qui est fait ou n'est pas fait « à mauvais escient » ou ce qui constitue ou ne constitue pas une « limite raisonnable ».

Proposition 1

Les objectifs généraux des initiatives en matière de protection des données sont louables. Les grandes questions à être examinées dans le cadre des consultations publiques sont les suivantes:

a) L'adoption d'une loi est-elle la bonne façon de réaliser ces objectifs?

b) La loi atteindrait-elle ses objectifs?

c) Les avantages de l'adoption d'une loi justifient-ils les coûts et les restrictions qui en découleraient?

B. Quel pourrait être le contenu des mesures législatives sur la protection des données ?

La simple mention de certaines questions comme l'efficacité de la loi de même que ses coûts et ses avantages fait ressortir l'importance d'examiner en détail les mesures législatives proposées, ne serait-ce qu'à titre indicatif, de sorte à fournir un point de départ solide aux intervenants qui voudront réagir au présent document. Heureusement, la combinaison du code de la CSA et de la *Loi visant le secteur public* nous fournit un bon cadre pour la discussion du contenu possible de la loi sur la protection des données dans le secteur privé. Dans l'état actuel du débat au Canada, le code de la CSA est le point de départ tout indiqué pour l'élaboration d'une loi.

Proposition 2

La possible loi sur la protection des données dans le secteur privé devrait s'inspirer du *Code type sur la protection des renseignements personnels* de l'Association canadienne de normalisation.

Jusqu'à quel point, toutefois, les mesures législatives sur la protection des données devraient-elles s'inspirer du code de la CSA? Il conviendrait ici d'expliquer la structure du code. Celui-ci se compose de dix principes et de six définitions; un commentaire explicatif accompagne chacun des principes, et deux de ceux-ci font l'objet d'une note. Ces deux notes ont leur importance, puisqu'elles décrivent l'application des principes fondamentaux relatifs au consentement et à l'accès aux renseignements personnels lorsque des impératifs opposés comme la protection de la santé ou de la sécurité publique sont en cause. Dans les mots mêmes du code, la note à la suite d'un principe fait partie intégrante de ce principe (paragraphe 3.1.2).

L'une des façons d'élaborer une loi sur la protection des données qui s'inspire du code consiste, comme le suggèrent certains, à adopter intégralement celui-ci. D'après une communication qui a été présentée lors de l'assemblée de 1997 de la Conférence sur l'harmonisation des lois du Canada, il semble que cette position rallie certains participants aux consultations. Si on optait pour cette solution, on pourrait probablement procéder au moyen d'un renvoi législatif, comme on le fait parfois avec les normes techniques de la CSA.

Toutefois, cette façon de procéder ne semble pas convenir à l'élaboration d'une loi de portée générale en matière de protection des renseignements personnels. Si cette question doit faire l'objet de mesures législatives, c'est qu'il faut protéger d'importantes valeurs sociales; dans ce cas, le législateur devrait l'exprimer directement, plutôt que par renvoi à un code qui n'a pas valeur de loi. D'autant plus que l'un des avantages que présenterait l'adoption par renvoi du code de la CSA, comme le prétendent certains des partisans de cette façon de faire,

serait de faciliter la mise à jour des normes relatives à la protection des renseignements personnels, à mesure que le code de la CSA sera passé en revue et mis à jour à la lumière de l'expérience. Cette position sous-entend que le jugement de la CSA, quant aux critères convenables en matière de protection des renseignements personnels, ferait jurisprudence avec le temps. Il y a lieu de douter du bien-fondé de cette façon de voir les choses.

S'il n'est pas question que les mesures législatives renvoient simplement au code, quel devrait donc en être le contenu? Il ne semble pas possible de simplement transposer intégralement le texte du code dans la loi, notamment parce que la plupart des commentaires se présentent sous formes d'explications, de descriptions et d'exemples qui seraient déplacés dans un texte législatif. Par conséquent, si on veut s'inspirer du code de la CSA pour élaborer une loi sur la protection des données, on doit le faire de façon sélective et ne transposer dans la loi que les parties du code qui y sont à leur place.

Les principales caractéristiques du code de la CSA, soit ses dix principes, qui constituent son énoncé des pratiques équitables en matière de traitement des renseignements, peuvent être adoptées pratiquement telles quelles comme base de la loi. C'est ce que l'on a fait dans le cas de la *Loi visant le secteur public.* Si on se conforme étroitement à la formulation des principes de la CSA, c'est qu'ils sont le résultat d'un consensus apparemment fragile qui n'a pas été facile à faire. La communication présentée lors de l'assemblée de 1997 de la Conférence sur l'harmonisation des lois du Canada laissait entendre que ce consensus pourrait se désintégrer si les mesures législatives adoptées étaient formulées de façon différente. Le code de la CSA a aussi été adopté comme Norme nationale du Canada par le Conseil canadien des normes. Il faudrait probablement apporter *certaines* modifications à leur formulation si on intégrait les dix principes à la loi, mais il s'agirait de détails. On trouvera des précisions et des explications à ce sujet dans les pages qui suivent.

Les commentaires, les notes et les définitions pourront servir de matériel de référence lorsqu'on déterminera ce qui doit être ajouté aux principes énoncés par la CSA en matière de protection des renseignements personnels afin de bien guider l'interprétation et l'application des principes. Dans la *Loi visant le secteur public,* les principes sont énoncés à l'annexe A sous la rubrique « Code de pratique statutaire », et l'annexe B porte sur l'interprétation et l'application de ce Code de pratique statutaire. La loi touchant le secteur privé pourrait suivre le même modèle.

Proposition 3

Une loi sur la protection des données devrait adopter dans la mesure du possible les dix principes de la CSA tels que formulés dans le code. Les définitions, les notes et les commentaires du code de la CSA devraient être utilisés comme matériel de référence pour l'élaboration de la loi sur la protection des données, mais leurs éléments essentiels pourraient être adoptés en tout état de cause.

B.1 La portée d'une loi sur la protection des données

Comme on le faisait remarquer à la page 1 du document de consultation rendu public par le Ministère en 1996, deux questions préliminaires déterminent la portée d'une loi sur la

protection des données : « À qui la loi s'applique-t-elle? » et « Qu'entend-on par renseignements personnels? ».

a. À qui la loi s'applique-t-elle?

Il était relativement simple de répondre à la même question posée dans le document de travail de 1996, puisque celui-ci ne portait que sur le gouvernement provincial; il suffisait simplement de définir le gouvernement provincial. On a alors choisi de dresser une liste d'organismes gouvernementaux. Toutefois, lorsqu'on sort du secteur public, les choses se compliquent. Une loi sur la protection des données dans le secteur privé est susceptible de s'appliquer à toute une panoplie d'organismes, notamment aux organisations commerciales. Toutefois, des organisations à but non lucratif, comme les organismes de bienfaisance, les églises, les partis politiques et les syndicats, peuvent aussi recueillir et utiliser des renseignements personnels. Elles possèdent à tout le moins une liste de membres et des dossiers sur leurs employés qui sont constitués de renseignements personnels qui doivent être conservés conformément aux principes relatifs à la protection des données. Même dans le secteur strictement commercial, on peut se poser des questions sur la possibilité d'appliquer la loi sur la protection des données à de petites entreprises familiales ou aux professionnels qui exercent seuls.

Le code de la CSA décrit ce que les « organismes » doivent faire, et il définit le terme « organisme » de façon très générale en indiquant qu'il comprend « les associations, les entreprises, les œuvres de bienfaisance, les clubs, les organismes gouvernementaux, les institutions, les ordres professionnels et les syndicats » (paragraphe 2.1). Placée dans son contexte, cette définition a une importance plutôt secondaire. Le code de la CSA est une norme *volontaire*; il ne s'applique donc qu'aux organismes qui acceptent d'y être assujettis. Néanmoins, une définition générale de ce genre semble convenir, même dans le contexte d'une loi qui *impose* des obligations à quiconque est visé par la définition. La plupart des organismes, même les plus petits, possèdent des renseignements personnels, et même dans les plus petites organisations, certains de ces renseignements sont vulnérables et peuvent être utilisés à mauvais escient. Les professionnels qui exercent seuls, notamment les médecins, possèdent eux aussi des renseignements personnels comme des dossiers médicaux. Les petites entreprises comme le dépanneur du coin peuvent aussi conserver des renseignements tels les registres des locations de vidéos, dont l'utilisation à des fins détournées a entraîné l'adoption de la *Video Privacy Protection Act 1988* aux États-Unis. Une loi sur la protection des données ne doit pas imposer aux petites entreprises des obligations dont elles ne pourraient vraisemblablement pas s'acquitter. (On reviendra périodiquement sur cette question dans les pages qui suivent). Cependant, à l'étape actuelle des discussions, il serait préférable d'envisager que des organismes de tous les genres et de toutes les tailles pourraient être assujettis à la loi.

L'une des réserves dignes de mention que contient la Directive de l'Union européenne énonce que les mesures législatives sur la protection des renseignements personnels ne s'appliquent pas aux « traitements effectués par une personne physique pour l'exercice d'activités exclusivement personnelles ou domestiques ». Il faudrait prévoir une réserve de ce genre si l'on songe à assujettir à la loi les particuliers lorsqu'ils agissent dans le cadre d'une activité commerciale. Dans un tel cas, il faudrait établir une distinction entre les activités

commerciales de la personne, qui seraient assujetties à la loi, et ses activités personnelles, qui ne le seraient pas. La Directive de l'Union européenne fait la distinction qui s'impose.

Proposition 4

Une loi sur la protection des données pourrait s'appliquer à tous les organismes constitués ou non en personnes morales ainsi qu'aux particuliers lorsqu'ils recueillent et utilisent des renseignements personnels à des fins autres que leurs fins personnelles ou domestiques.

La Directive de l'Union européenne contient une autre réserve. En effet, les mesures législatives doivent s'appliquer à toutes les formes de traitement « automatisé » (c.-à-d. informatisé) de renseignements personnels, mais elles ne doivent s'appliquer au traitement « manuel » que si les renseignements personnels font partie d'un « système de classement », c'est-à-dire tout « ensemble structuré de données à caractère personnel accessibles selon des critères déterminés, que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique ». La loi du Québec contient une disposition semblable qui fait de l'établissement d'un dossier sur une personne l'élément déclencheur de l'application de la loi.

Le code de la CSA ne fait aucune distinction entre le traitement manuel et le traitement informatisé et il ne contient aucun critère explicite relatif à l'établissement d'un dossier sur une personne. À cet égard, le présent document s'inspirera du code de la CSA. Étant donné que le but de l'exercice consiste à examiner l'utilité du code de la CSA comme fondement d'une loi sur la protection des données dans le secteur privé, il semble tout naturel d'emprunter la voie du code pour voir où elle conduit. Si l'exercice donne des résultats trop vagues auxquels il serait possible de remédier en intégrant la notion « d'établissement d'un dossier sur une personne », celle-ci pourrait probablement être incluse.

b. Qu'entend-on par renseignements personnels?

Le code de la CSA contient une définition assez lapidaire, que voici : enregistrement de renseignements concernant un individu identifiable, quelle que soit sa forme (paragraphe 2.1). L'article 1 de la *Loi visant le secteur public* est substantiellement identique et contient la précision suivante au paragraphe 1(3) :

> Un particulier est identifiable aux fins de la présente loi si des renseignements
>
> a) comprennent son nom,
>
> b) rendent évidente son identité, ou
>
> c) ne comprennent pas son nom ou ne rendent pas évidente son identité mais sont susceptibles dans les circonstances d'être adjoints à d'autres renseignements qui comprennent son nom ou rendent son identité évidente.

Il convient de s'attarder à deux attributs d'une définition de cette nature. En premier

lieu, les renseignements personnels n'ont pas à être de nature sensible ou particulièrement privée. Il suffit qu'on soit en présence de « renseignements concernant un individu identifiable ». À cet égard, la définition est vaste, comme l'est, par voie de conséquence, la portée de la loi.

Toutefois, l'exigence selon laquelle il doit s'agir de renseignements enregistrés sous quelque forme que ce soit restreint la portée de la loi. Les renseignements personnels ne sont donc pas assujettis à la loi s'ils ne sont pas enregistrés sous une forme quelconque. Bien sûr, la portée de la loi pourrait être plus large. La partie III de la *Loi sur l'accès à l'information et la protection de la vie privée* de l'Ontario (secteur public), à titre d'exemple, applique les principes de la protection des données aux renseignements qui n'existent pas sous forme enregistrée. La portée de la loi serait élargie si on adoptait cette approche. Par contre, la mention de « dossier » dans la Directive de l'Union européenne et dans la loi du Québec qui ont été abordées auparavant semble avoir un effet légèrement restrictif. Pour les fins de l'exercice, cependant, la définition de la CSA semblant s'approcher de la norme, c'est celle qui sera utilisée dans les pages qui suivent.

Proposition 5

Une loi sur la protection des données pourrait s'inspirer de la définition que donne le code de la CSA des renseignements personnels; elle traiterait donc des renseignements concernant un individu identifiable enregistrés sous quelque forme que ce soit.

B.2 Les principes de la CSA

Dans les pages qui suivent, on retrouvera une analyse des principes de la CSA à titre de composantes possibles du Code de pratique statutaire. Pour ce faire, chacun des principes sera examiné individuellement. Dans certains cas, de légères modifications à leur formulation sera suggérée, mais surtout on s'interrogera sur la nécessité d'étoffer, dans la loi sur la protection des données, chaque principe au moyen de dispositions régissant son interprétation et son application. Lorsque chaque principe aura été passé en revue, d'autres éléments importants d'un programme législatif fondé sur le code de la CSA seront examinés, notamment en ce qui concerne l'application de la loi. Contrairement à une loi, le code de la CSA n'a pas à tenir compte de cet aspect, puisqu'il est de la nature d'une norme volontaire.

Dans l'examen des principes, il sera important de se reporter au sens large des expressions « organisme » et « renseignements personnels ». Les principes sont conçus de sorte à s'appliquer à tous les organismes, qu'ils soient petits ou grands, aux petits et aux gros utilisateurs de renseignements personnels ainsi qu'à tous les genres de renseignements personnels, qu'ils soient ou non de nature confidentielle. Les principes établissent donc un cadre général susceptible de s'appliquer à un vaste éventail de situations. Pour les appliquer à des cas précis, les organismes devront s'en remettre à leur jugement.

Premier principe de la CSA – Responsabilité

Un organisme est responsable des renseignements personnels dont il a la gestion et doit désigner une ou des personnes qui devront s'assurer du respect des principes énoncés ci-dessous.

Ce principe a pour objet d'énoncer la responsabilité qu'a chaque organisme d'assurer le fonctionnement de la loi et de faire en sorte qu'une personne est chargée de cette tâche au sein de l'organisme. Toutefois, la formulation de ce principe soulève certaines difficultés d'ordre pratique. Tout d'abord, le principe ne prévoit rien en cas de vacance au poste de « responsable » si l'organisme néglige ou omet de désigner une ou des personnes. En second lieu, on peut prétendre que le principe s'applique mieux dans une grande société que dans un petit organisme. Dans le cas d'une petite organisation (il peut même s'agir d'une seule personne selon la formulation de la proposition 4), il sera parfois bizarre de voir « l'organisme » désigner une personne qui devra s'assurer du respect des dispositions du code.

Dans le cas de la *Loi visant le secteur public,* on a réglé le problème en modifiant la formulation du premier principe de la CSA afin de rendre « le directeur exécutif de l'organisme public et ses représentants » responsables du respect de la loi. Le second problème ne se présentait pas, puisque les organismes publics – même les plus petits d'entre eux – sont tous dotés d'une structure organisationnelle dans laquelle on peut facilement identifier le directeur exécutif, peu importe son titre.

Dans le secteur privé, où les formes d'organismes sont plus diversifiées, on devra faire appel à une légère variante de cette approche. La loi devrait prévoir un poste de « responsable par défaut », à moins que l'organisme ne prenne les dispositions nécessaires pour confier à une personne la responsabilité d'assurer le respect de la loi. Si le poste de chef de la direction existe au sein de l'organisme, son titulaire devrait être d'office responsable d'assurer le respect de la loi. Dans le cas des organismes qui sont dotés d'une structure organisationnelle plus nébuleuse, on pourrait confier d'office la responsabilité d'assurer la conformité de l'organisme à la loi sur la protection des données à la personne ou aux personnes qui en dirigent les activités. L'identité du responsable sera assez facile à établir dans la plupart des cas, mais moins évidente dans d'autres cas. On peut penser aux sociétés constituées de trois associés ayant chacun un droit de vote. Dans un tel cas, les trois associés dirigeraient collectivement les activités de l'organisme. En vertu de la règle proposée de la responsabilité par défaut, les associés seraient collectivement responsables d'assurer le respect de la loi, à moins qu'ils désignent une autre personne.

Proposition 6

À moins qu'une personne soit désignée conformément au premier principe de la CSA, la personne responsable d'assurer le respect de la loi au sein d'un organisme devrait être :

a) le chef de la direction, si ce poste existe au sein de l'organisme; ou

b) la ou les personne(s) qui dirigent les activités de l'organisme, si le poste de chef de la direction n'existe pas au sein de celui-ci.

Deuxième principe de la CSA –
Détermination des fins de la collecte des renseignements

Les fins pour lesquelles des renseignements personnels sont recueillis doivent être déterminées par l'organisme avant ou au moment de la collecte.

L'idée selon laquelle les fins pour lesquelles les renseignements personnels sont recueillis doivent être déterminées est l'un des principes essentiels du code de la CSA et d'autres documents relatifs à la protection des données. Les fins déterminées jouent un rôle pivot dans les décisions prises en vertu des quatrième et cinquième principes de la CSA en ce qui concerne les renseignements qu'un organisme peut recueillir et ce qu'il peut faire des renseignements qu'il a recueillis. Toutefois, la détermination des fins présente certains défis conceptuels et opérationnels.

L'un des détails qui peut être rapidement réglé concerne la question de savoir s'il y a des limites aux fins pour lesquelles les organismes peuvent recueillir des renseignements personnels. Le code de la CSA est tout à fait muet à ce sujet. Par contre, la *Loi visant le secteur public* (annexe B, paragraphe 2.1) et les mesures législatives comparables des autres provinces canadiennes prévoient qu'un organisme public ne peut recueillir des renseignements personnels que pour des fins se rattachant directement à ses activités. Une restriction semblable devrait aussi être acceptable dans le secteur privé.

Proposition 7

Les fins pour lesquelles un organisme recueille des renseignements personnels doivent être licites et se rattacher directement à une de ses activités existantes ou proposées.

Certaines des questions relatives à la détermination des fins sont plus complexes. Si on examine le code de la CSA, la détermination des fins désigne deux réalités. D'une part, l'organisme formule *pour lui-même,* dans le cadre de ses procédés internes, les motifs pour lesquels il désire recueillir des renseignements personnels. D'autre part, dans le cadre d'un mécanisme externe, il détermine ce qu'il dira au particulier au sujet des fins de la collecte. En apparence, le deuxième principe de la CSA trouve son application principale dans la seconde facette de l'exercice. Le commentaire brouille cependant les choses. Il ajoute que l'organisme doit « documenter » ses fins, mettant ainsi l'accent sur l'aspect *interne* de la détermination des fins. Par contre, il est moins catégorique lorsqu'il aborde le genre d'explications qui doivent être données au particulier (procédé *externe).* En effet, le paragraphe 4.2.3 se lit comme suit : « Il faudrait préciser à la personne auprès de laquelle on recueille des renseignements, avant ou au moment de la collecte, les fins auxquelles ils sont destinés ». Mais l'emploi des mots « il faudrait » est délibéré et important. Le paragraphe 3.1.3 précise en effet que l'emploi de termes de cette nature dénote une recommandation, par opposition à une obligation.

Dans la *Loi visant le secteur public,* le deuxième principe de la CSA (qui équivaut au deuxième principe du code figurant à l'annexe A) est globalement considéré comme une explication à l'externe des fins, pas nécessairement de façon formaliste. Dans le cours normal des affaires, la collecte de renseignements personnels sera généralement accompagnée d'au moins une indication quelconque des raisons pour lesquelles l'organisme veut recueillir les renseignements en question. Cet énoncé se fait parfois brièvement lors d'une entrée en matière d'une conversation ou d'une lettre. De ce point de vue, l'obligation de déclarer les fins pour lesquelles les renseignements sont recueillis ne semble donc pas exagérée.

L'annexe B de la *Loi visant le secteur public* prévoit aussi l'obligation pour l'organisme de « documenter, relativement à tout système d'enregistrement des renseignements personnels, la ou les fins pour lesquelles les renseignements personnels sont conservés dans le système » (paragraphe 2.2). Le système d'enregistrement des renseignements personnels est défini comme étant « un système d'enregistrement informatisé ou manuel qui contient des renseignements sur des particuliers et qui est organisé de manière à donner facilement accès à des renseignements sur des particuliers spécifiques » (paragraphe 2.3). Selon cette définition, pratiquement tout registre structuré de renseignements conservé au sujet de particuliers peut être considéré comme un système d'enregistrement des renseignements personnels. Le fait de documenter les fins pour lesquelles les renseignements sont conservés dans le système lie en pratique les fins à l'utilisation des renseignements qui se trouvent dans le système.

Une telle obligation de « documenter les fins » pourrait-elle trouver application dans le secteur privé? Elle présente l'avantage d'assurer une certaine clarté administrative, en particulier dans les grands organismes qui pourraient ainsi s'assurer que tous les intervenants connaissent les renseignements qui peuvent être recueillis ainsi que les fins auxquelles ils seront utilisés. Toutefois, l'obligation générale de documenter les fins pourrait en fait imposer aux petits organismes un fardeau administratif qui ne contribuerait en rien à assurer la protection de la vie privée des particuliers. Est-il vraiment utile, par exemple, d'exiger d'un petit organisme (comme un commerçant indépendant) qu'il documente les fins pour lesquelles il recueille des renseignements personnels lorsque celles-ci sont évidentes et lorsqu'il est seul à utiliser les renseignements? Certains affirmeront que même dans les grands organismes la documentation des fins aura lieu en pratique sans que la loi ne les y force.

Proposition 8

Le deuxième principe de la CSA pourrait être accompagné d'une obligation pour l'organisme de documenter les fins pour lesquelles il tient un système d'enregistrement des renseignements personnels; dans ce cas, cette obligation ne s'appliquerait pas lorsque le fait de documenter les fins ne serait d'aucune utilité au contrôle administratif.

Par ailleurs, le code de la CSA ne répond pas à la question suivante : Qu'arrive-t-il lorsque les fins, telles que documentées à l'interne, ne correspondent pas aux explications qui sont données au particulier? Dans un tel cas, l'explication donnée au particulier doit prévaloir. L'utilisation qui pourrait être faite des renseignements ne dépend pas des fins documentées que l'organisme a fait défaut d'expliquer de façon convenable, mais bien de l'explication qui a été donnée et de ce à quoi la personne a consenti (au sens décrit dans le troisième principe de la CSA, qui figure ci-dessous) à la lumière de ladite explication.

Cela ne signifie pas que l'organisme qui recueille des renseignements personnels est tenu de réciter machinalement chaque fois les fins telles qu'elles sont décrites dans ses documents internes. Cette façon de procéder pourrait convenir dans certains cas et pas dans d'autres. Ainsi, on peut s'attendre à ce que la version documentaire des fins de certains organismes soit énoncée dans des termes généraux, voire dans un langage bureaucratique. Le fait de la réciter n'aidera pas beaucoup à l'expliquer. Dans d'autres cas, l'indication des fins ne fera que confirmer l'évidence, notamment lorsque le fait pour la personne de s'adresser à

l'organisme explique en soi le contexte dans lequel les renseignements sont demandés et fournis. Mais la plupart du temps, les fins qui font l'objet de la documentation interne pourront être accompagnées d'une explication mieux adaptée au contexte de la relation entre la personne et l'organisme. Différentes explications peuvent mieux convenir à certains moments ou en rapport avec certains éléments d'information. Cela signifie toutefois que l'organisme a le fardeau de s'assurer que les fins déterminées « à l'interne » sont expliquées convenablement à la personne de la manière que choisit l'organisme, de façon que ses fins « documentées » correspondent à ce que le consentement de la personne l'autorise à faire.

Proposition 9

Si les fins documentées de l'organisme ne correspondent pas aux explications qu'il fournit à la personne, ces dernières prévaudront conformément au troisième principe de la CSA relatif au consentement.

Troisième principe de la CSA – Consentement

Toute personne doit être informée et consentir à toute collecte, utilisation ou communication de renseignements personnels qui la concernent, à moins qu'il ne soit pas approprié de le faire.

Ce principe soulève trois grandes questions. La première a trait à sa formulation; la seconde porte sur l'opposition entre le consentement implicite et le consentement exprimé. La troisième question consiste à déterminer les cas où l'obligation d'obtenir le consentement ne serait pas appropriée.

a) Formulation

Selon le troisième principe de la CSA, l'obligation d'informer la personne et d'obtenir son consentement ne s'applique pas seulement à la collecte, mais aussi à l'utilisation et à la communication. Le paragraphe 4.3.2 montre clairement que l'expression « être informée et consentir » a été employée sciemment. Cette formulation est toutefois incohérente par rapport à celle du cinquième principe, qui traite aussi de l'utilisation et de la communication, mais qui comporte la simple obligation d'obtenir le consentement, par opposition à celle d'informer la personne et d'obtenir son consentement.

On devrait éviter les incohérences de la sorte dans un texte législatif. La meilleure façon d'y parvenir consisterait à éliminer les termes « être informée et » du troisième principe de la CSA. Du point de vue de la collecte, on ne semble pas amoindrir la portée de l'exigence, puisque « consentir » a un sens plus large. On voit mal, en effet, comment la personne pourrait donner son consentement à une collecte de renseignements si elle n'en a pas été informée. Par contre, la situation serait plus complexe du point de vue de « l'utilisation » et de la « divulgation » si les mots « informée » et « consentir » devaient être interprétés comme deux critères distincts. On peut supposer qu'il est possible de consentir à une utilisation sans savoir si elle a véritablement été faite. Si l'obligation d'informer la personne constituait un critère *additionnel,* le principe imposerait une obligation dont il pourrait être difficile de s'acquitter.

Proposition 10

Le troisième principe de la CSA porte essentiellement sur le consentement. Une loi sur la protection des données ne doit pas faire de l'obligation d'informer la personne un critère distinct et indépendant auquel devraient satisfaire les organismes.

b) Consentement exprimé et consentement implicite

Le code de la CSA établit clairement que le consentement peut être exprimé ou implicite (paragraphe 2.1). Voici la suite de cette disposition :

> Le consentement exprimé se donne de façon explicite, de vive voix ou par écrit. Le consentement explicite est non équivoque et n'oblige pas l'organisme qui demande le consentement de la personne à l'inférer. Le consentement implicite survient lorsque les actes ou l'inaction de la personne permettent raisonnablement de déduire qu'il y a consentement. (paragraphe 2.1)

La notion de consentement, implicite semble essentielle au fonctionnement d'une loi sur la protection des données. Il est en effet impossible d'exiger le consentement exprimé chaque fois que l'on recueille, utilise ou communique des renseignements personnels. À titre d'exemple, lorsqu'une personne réclame un service, son consentement, loin d'être exprimé, est plutôt implicite. Le consentement est souvent implicite lorsqu'un organisme agit en faveur d'une personne. Le consentement implicite revêt une importance toute particulière dans les mesures législatives fondées sur le code de la CSA. Celui-ci est en effet un des rares documents consultés dans la préparation du présent exposé qui n'accorde pas explicitement aux organismes la souplesse nécessaire pour utiliser les renseignements personnels à des fins qui sont « compatibles avec » les fins qui sont exposées à la personne. Dans le cadre contextuel du code de la CSA, la notion de consentement implicite recoupe apparemment l'autorisation législative d'agir « à des fins compatibles ».

Le commentaire de la CSA laisse entendre que « les attentes raisonnables de la personne » (paragraphe 4.3.5) sont le critère déterminant de l'existence du consentement implicite. Cette approche semble acceptable, puisqu'elle met l'accent sur ce que *la personne* s'attend à ce que l'on fasse des renseignements qu'elle fournit, plutôt que sur ce que l'organisme juge raisonnable de son propre point de vue.

Proposition 11

Une loi sur la protection des données doit inclure la notion de consentement implicite fondé sur les attentes raisonnables de la personne.

La loi doit-elle expliquer plus en profondeur le consentement implicite ou peut-elle se contenter de parler des attentes raisonnables de la personne? Il est impossible de donner une définition exhaustive du consentement implicite; cependant, la *Loi visant le secteur public* contient une disposition qui élabore ce sujet de deux façons. Elle énonce que le particulier « ne doit pas être susceptible de désapprouver » une mesure prise par l'organisme pour que

son consentement soit considéré comme tacite, et elle énumère les principaux facteurs que l'organisme public doit prendre en considération. La proposition suivante est extraite directement du paragraphe 3.2 de l'annexe B de la *Loi visant le secteur public,* et elle contient de légères modifications de formulation.

Proposition 12

Les mesures pour lesquelles un consentement peut être tacite sont celles que le particulier devrait raisonnablement s'attendre à voir prendre par l'organisme, et qu'il n'est pas susceptible de désapprouver, eu égard à

a) la nature des renseignements personnels en question, y compris la question de savoir si les renseignements ont ou non une nature sensible ou confidentielle,

b) tout avantage ou inconvénient pour le particulier,

c) toute explication que l'organisme a donnée des mesures qu'il entend prendre,

d) toute indication que le particulier a donnée de ses désirs réels, et

e) la facilité ou la difficulté avec laquelle les désirs réels du particulier peuvent être identifiés.

c) Quand l'obtention du consentement ne serait pas appropriée?

Le troisième principe de la CSA exige le consentement de la personne pour toute collecte, utilisation ou communication de renseignements personnels qui la concernent, « à moins qu'il ne soit pas approprié de le faire ». Dans sa note accompagnant le troisième principe (laquelle fait partie intégrante du principe selon le paragraphe 3.1.2), la CSA ajoute ce qui suit :

> Dans certaines circonstances, il est possible de recueillir, d'utiliser et de communiquer des renseignements personnels à l'insu de la personne concernée et sans son consentement. Par exemple, pour des raisons d'ordre juridique ou médical ou pour des raisons de sécurité, il peut être impossible ou peu réaliste d'obtenir le consentement de la personne concernée. Lorsqu'on recueille des renseignements aux fins de l'application de la loi, de la détection d'une fraude ou de sa répression, on peut aller à l'encontre du but visé si l'on cherche à obtenir le consentement de la personne concernée. 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. De plus, les organismes qui ne sont pas en relation directe avec la personne concernée ne sont pas toujours en mesure d'obtenir le consentement prévu. Par exemple, il peut être peu réaliste pour une œuvre de bienfaisance ou une entreprise de marketing direct souhaitant acquérir une liste d'envoi d'un autre organisme de chercher à obtenir le consentement des personnes concernées. On s'attendrait, dans de tels

cas, à ce que l'organisme qui fournit la liste obtienne le consentement des personnes concernées avant de communiquer des renseignements personnels. (par. 4.3)

L'exception « à moins qu'il ne soit pas approprié de le faire » est l'une des plus difficiles à intégrer dans une loi. Les lois canadiennes sur la protection des renseignements personnels témoignent éloquemment de la complexité de cette tâche. Au fil des ans, on y a en effet ajouté de longues listes de collectes, d'utilisations et de communications non consensuelles mais néanmoins autorisées. Ces exceptions regroupent les dispositions les plus substantielles et évidentes, comme la divulgation de renseignements en vue de protéger la santé ou la sécurité d'un tiers; elles comprennent d'autres dispositions qui soulèvent davantage de questions qu'elles ne règlent de problèmes, comme la divulgation à l'avocat. Il paraît surprenant qu'une autorisation explicite en vertu de la loi soit exigée pour qu'il soit permis à une personne de faire des divulgations à son avocat. Si tel est le cas, qu'en est-il de la divulgation à d'autres professionnels ou consultants que la loi ne désigne pas de façon expresse? Les listes que contiennent les lois existantes renferment aussi habituellement une disposition générale permettant la collecte, l'utilisation et la communication de renseignements personnels sans le consentement de la personne concernée lorsque l'intérêt public l'emporte clairement sur toute atteinte à la vie privée qui pourrait en résulter.

Dans la *Loi visant le secteur public,* on a fait des efforts en vue de raccourcir ces listes et d'édicter des énoncés généraux plutôt que des dispositions particulières. La loi adopte aussi une approche en deux étapes qui force l'organisme public à s'assurer non seulement d'agir à des fins déterminées, mais aussi de faire en sorte que les mesures qu'il entend prendre sont justifiées compte tenu des circonstances. La proposition suivante est fondée sur les dispositions correspondantes de la *Loi visant le secteur public* (paragraphes 3.4 à 3.7 de l'annexe B), auxquelles on a apporté quelques modifications terminologiques et dont on a omis le paragraphe 3.5 qui touche la divulgation dans l'intérêt du public de rendre le gouvernement plus transparent et qui porte spécifiquement sur le secteur public.

Proposition 13

Le consentement ne devrait pas être nécessaire lorsqu'un organisme recueille, utilise ou divulgue des renseignements personnels

a) pour protéger la santé ou la sécurité du public ou d'un particulier,

b) aux fins d'une enquête liée à l'exécution d'une mesure législative,

c) pour protéger ou affirmer ses propres droits légaux, y compris des droits légaux contre le particulier,

d) pour vérifier auprès d'un organisme gouvernemental l'admissibilité du particulier à un programme ou à une prestation pour lequel le particulier a fait une demande à l'organisme en question,

e) pour les fins de toute recherche légitime faite dans l'intérêt de la science, de l'enseignement ou de l'ordre public ou pour des travaux d'archives,

f) tel que requis ou expressément autorisé par la loi, ou

g) pour toute autre raison importante dans l'intérêt du public, qu'elle soit ou non semblable à celle des alinéas a) à f).

Avant de recueillir, d'utiliser ou de divulguer des renseignements personnels sans consentement, un organisme doit prendre en considération la nature des renseignements en question et la fin des mesures qu'il prend, et doit se convaincre que dans les circonstances cette fin justifie les mesures projetées.

Toute collecte, toute utilisation ou toute divulgation de renseignements personnels sans consentement doit se limiter aux exigences raisonnables de la situation.

À première vue, la proposition 13 ne fait aucune distinction entre la collecte, l'utilisation et la divulgation, étant donné que le troisième principe de la CSA, auquel elle se rapporte, traite les trois opérations d'un seul bloc. Dans les faits, toutefois, les divers éléments de la proposition 13 auraient une incidence différente sur différents organismes selon leurs activités et les décisions qu'ils prendraient. À titre d'exemple, on peut supposer que très peu d'organismes du secteur privé recueilleraient des renseignements dans le but d'appliquer un texte législatif, étant donné que cette fin « ne se rattache pas directement à leurs activités », comme l'énonce la proposition 7. De plus, les organismes du secteur privé pourront rarement invoquer une « raison importante dans l'intérêt du public » pour justifier la divulgation de renseignements personnels; cependant, il importe de ne pas éliminer cette possibilité, notamment pour que les organismes du secteur privé puissent à tout le moins divulguer des renseignements aux autorités publiques responsables. L'utilisation de renseignements personnels à des fins de recherche fera aussi partie des cas inusités, étant donné que les renseignements devraient normalement être utilisés sous une forme garantissant l'anonymat, de sorte qu'il ne s'agira plus de renseignements « personnels. »

Quatrième principe de la CSA – Limitation de la collecte

L'organisme ne peut recueillir que les renseignements personnels nécessaires aux fins déterminées et doit procéder de façon honnête et licite.

La *Loi visant le secteur public* énumère les sources auprès desquelles les renseignements personnels peuvent être recueillis. Il s'agit : a) de la personne elle-même; b) d'une autre personne avec le consentement de la personne concernée; c) des sources et par les moyens auxquels la population dans son ensemble peut avoir accès; et d) de toute source dans tous les cas où, en vertu de la disposition de la *Loi* qui correspond à la proposition 13, un organisme public peut recueillir des renseignements sans le consentement de la personne concernée (par. 4.1 de l'annexe B). Un tel souci de précision à ce sujet devrait aussi caractériser la loi touchant le secteur privé.

La *Loi visant le secteur public* contient en outre une disposition interdisant à un organisme de refuser de fournir un service ou une prestation à une personne parce que celle-ci ne consent pas à fournir des renseignements qui ne sont pas essentiels aux fins légitimes de l'organisme public (par. 4.2 de l'annexe B). Cette disposition correspond au paragraphe 4.3.3 du code de la CSA.

Par ailleurs, la *Loi visant le secteur public* ne contient aucun précision au sujet de « la façon honnête et licite ». Le mot « licite » est suffisamment clair, mais on s'est demandé pendant la préparation de la *Loi* si le terme « honnête » ne devait pas être clarifié. Selon le commentaire de la CSA, « l'exigence selon laquelle les organismes sont tenus de recueillir des renseignements personnels de façon honnête et licite a pour objet de les empêcher de tromper les gens et de les induire en erreur quant aux fins auxquelles les renseignements sont recueillis » (paragraphe 4.4.2). Il s'agirait là d'un exemple de méthode malhonnête de collecte, mais la loi ne devrait pas restreindre à des situations particulières comme celle-là l'application de la notion d'honnêteté. Même si l'honnêteté est une notion générale, elle est suffisamment précise pour avoir une existence autonome dans la législation sans qu'on sente le besoin de l'expliquer davantage.

Proposition 14

Une loi sur la protection des données devrait énumérer les sources auprès desquelles les renseignements personnels peuvent être recueillis, et prévoir qu'il est interdit de refuser de fournir à une personne des biens ou des services sous prétexte qu'elle n'a pas consenti à transmettre des renseignements personnels qui ne sont pas essentiels aux fins énoncées de l'organisme.

L'exigence selon laquelle les organismes sont tenus de recueillir des renseignements personnels de façon honnête et licite n'a pas à être expliquée davantage dans la loi sur la protection des renseignements.

Cinquième principe de la CSA –
Limitation de l'utilisation, de la communication et de la conservation

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

a) Formulation

L'un des détails de la formulation du cinquième principe de la CSA a besoin d'être revu. Le principe mentionne l'utilisation et la communication exigées par la loi. Si on le lit d'un point de vue strictement juridique, le terme « exige » pourrait viser les utilisations et les communications que l'organisme est tenu par la loi de faire, mais non les situations prévues par des mesures législatives expresses ou des décisions explicites des tribunaux ou d'autres organismes investis de pouvoirs légaux qui *autorisent* (mais *n'exigent* pas) une utilisation ou

une communication en particulier. Dans la *Loi visant le secteur public,* cette lacune a été comblée en modifiant légèrement la proposition « (...) ou que la loi ne l'exige » de sorte qu'elle se lise ainsi : « (...) ou que la loi ne l'exige ou ne l'autorise expressément » (cinquième principe, annexe A). Cette lacune revêt une importance toute particulière dans le secteur public, puisque de nombreuses lois accordent une certaine discrétion aux ministres et fonctionnaires. Mais cette brèche peut exister en ce qui concerne le secteur privé.

Proposition 15

Le cinquième principe de la CSA devrait permettre les utilisations et les communications qui sont autorisées expressément par la loi en plus de celles qui sont exigées par la loi.

b) Interdépendance entre les fins, le consentement et la loi

Quel est le lien entre les trois justifications possibles de l'utilisation ou de la communication que prévoit le cinquième principe de la CSA, à savoir les fins pour lesquelles les renseignements ont été recueillis, le consentement de la personne et une exigence ou une autorisation légale? Qu'en est-il, en particulier, lorsque ces facteurs donnent des indications opposées?

En principe, les trois facteurs intégrés au cinquième principe de la CSA doivent être considérés comme équivalents. La présence de l'un d'entre eux suffit. Par conséquent, on pourrait soutenir, par exemple, qu'un refus explicite de consentir à l'utilisation ou à la communication n'empêcherait pas l'organisme de prendre les mesures que la loi l'autorise à prendre.

Dans la pratique, toutefois, la relation qui existe entre les fins déterminées, le consentement et la loi peut être plus subtile dans certains cas. Supposons, par exemple, que la personne fournit volontairement des renseignements, mais en demandant explicitement qu'ils ne soient pas utilisés d'une façon particulière qui fait partie des fins déterminées de l'organisme. Si l'organisme reçoit des renseignements personnels après une telle mise en garde, il ne pourra prétendre que ses fins documentées en régissent l'utilisation. Pensons aux situations dans lesquelles les désirs réels ou probables de la personne ont un impact sur le critère de prépondérance de la proposition 13 touchant les actes non consensuels; ces désirs détermineront donc en partie ce qui est « expressément autorisé par la loi ». Dans la préparation de la *Loi visant le secteur public,* on s'est demandé s'il était possible de prévoir des repères législatifs au sujet de l'interdépendance entre les trois justifications de l'utilisation et de la communication des renseignements personnels. On a abouti à la conclusion que ce n'était pas possible. La notion de l'équivalence des trois éléments semble se dégager clairement à la lecture du cinquième principe de la CSA, et les possibles subtilités de leur interdépendance dans des situations précises ne peuvent être résumées sous une forme qui éclairerait la situation davantage qu'elle ne la rendrait confuse.

Proposition 16

Il n'est pas nécessaire que la loi sur la protection des données élabore au sujet de la relation entre les fins, le consentement et la loi comme justifications

équivalentes de l'utilisation et de la communication de renseignements personnels.

c) Conservation

Le cinquième principe de la CSA édicte qu'on ne doit conserver les renseignements personnels qu'aussi longtemps que nécessaire pour la réalisation des finalités déterminées. Dans de nombreux cas, le respect de cette disposition entraînera la destruction de renseignements personnels devenus superflus. Cependant, une autre façon de cesser de conserver des renseignements *personnels* consiste à donner à ceux-ci une forme rendant impossible l'identification des personnes auxquelles ils se rapportent. Pour des fins de précision, on aurait avantage à prévoir cette seconde possibilité dans la loi.

Proposition 17

Une loi sur la protection des données devrait spécifier clairement que l'organisme peut satisfaire à son obligation de ne pas conserver indûment des renseignements personnels s'il conserve ceux-ci sous une forme rendant impossible l'identification des personnes auxquelles ils se rapportent.

Il faudrait aussi clarifier un autre point, soit celui de la durée de la période de conservation. La question est plus simple à régler dans le cas des renseignements personnels qui font partie d'un « système d'enregistrement des renseignements personnels » que dans le cas des autres renseignements personnels. En ce qui concerne les systèmes d'enregistrement de renseignements personnels, les décisions touchant la durée de la conservation des renseignements et le sort de ceux-ci après le traitement devraient être prises dans le cadre de l'établissement du système. Il faudrait prévoir un certain délai de façon à ne pas détruire prématurément des renseignements personnels. À l'instar de l'organisme, la personne concernée pourrait avoir intérêt à ce que les renseignements soient conservés pendant un certain temps après leur utilisation.

Hormis les systèmes d'enregistrement de renseignements personnels – dans des endroits comme les fichiers d'élaboration de politiques ou de conception de produits qui peuvent contenir à titre incident des renseignements personnels, par exemple – une approche plus flexible semble s'imposer en matière de conservation et de destruction. Tenter d'extraire tous les renseignements personnels de tels fichiers serait une tâche fastidieuse, d'autant plus que les fichiers de ce genre sont destinés à devenir quasi anonymes. Une fois le dossier fermé, tout renseignement personnel qu'il est susceptible de contenir devient relativement inaccessible. Bien sûr, si on rouvrait ultérieurement le dossier contenant des renseignements de nature non personnelle, toute utilisation ou communication des renseignements personnels qui s'y trouvent encore serait toujours assujettie à la loi.

Proposition 18

On ne devrait pas exiger des organismes qu'ils éliminent de leurs fichiers de renseignements de nature non personnelle tous les renseignements personnels qui pourraient s'y trouver à titre incident.

Sixième principe de la CSA – Exactitude

Les renseignements personnels doivent être aussi exacts, complets et à jour que l'exigent les fins pour lesquelles ils sont utilisés.

Ce principe est suffisamment explicite. L'argument principal qu'ajoute le commentaire de la CSA est le suivant : « Un organisme ne devrait pas systématiquement mettre à jour les renseignements personnels à moins que cela ne soit nécessaire pour atteindre les fins auxquelles ils ont été recueillis » (paragraphe 4.6.2). On ne devrait donc pas en déduire que le principe impose l'obligation générale de tenir les renseignements personnels à jour; en effet, un degré convenable d'exactitude ne s'impose véritablement que lorsqu'on utilise les renseignements. La formulation générale du sixième principe de la CSA permet cependant d'arriver assez facilement à cette conclusion.

Proposition 19

Le sixième principe de la CSA est suffisamment explicite. Il ne sera pas nécessaire d'inclure dans une loi sur la protection des données des dispositions additionnelles relatives à son interprétation et à son application.

Septième principe de la CSA – Mesures de sécurité

Les renseignements personnels doivent être protégés au moyen de mesures de sécurité correspondant à leur degré de sensibilité.

a Formulation

Dans la *Loi visant le secteur public*, on a substitué l'expression « dispositifs de protection » à l'expression « mesures de sécurité », parce que celle-ci semblait réduire la portée du principe. Dans son commentaire, la CSA indique que les mesures de sécurité doivent protéger les renseignements personnels contre « la perte ou le vol ainsi que contre la consultation, la communication, la copie, l'utilisation ou la modification non autorisées » (paragraphe 4.7.1). Elle indique aussi que les méthodes de protection devraient comprendre des moyens matériels, des mesures administratives et des mesures techniques ainsi que le fait pour les organismes de sensibiliser leur personnel à l'importance de protéger le caractère confidentiel des renseignements personnels (paragraphes 4.7.3 et 4.7.4). L'expression « mesures de sécurité » décrit en partie le sens des dispositions à prendre, mais elle détourne l'attention du fait que l'un des meilleurs moyens d'empêcher l'utilisation ou la divulgation non autorisée consiste à bien déterminer les types d'utilisations et de divulgations qui sont autorisés. Dans ce contexte plus global, le septième principe de la CSA impose aux organismes l'obligation de prendre elles-mêmes les mesures nécessaires pour que la loi opère. La mention de « mesures de sécurité » semble donc avoir pour effet de réduire la portée du principe.

Proposition 20

Qu'on retire l'expression « mesures de sécurité » du septième principe de la CSA de sorte à éviter d'en réduire la portée.

b) Quels genres de dispositifs de protection?

Comme il a été indiqué ci-dessus, le commentaire de la CSA fait spécifiquement mention de divers genres de mesures que chapeaute la notion de « dispositifs de protection ». Pour des fins de clarté, il convient que la loi imite cet exemple. En ce qui concerne la question des genres de dispositifs de protection qui correspondent au degré de sensibilité des renseignements personnels au sens du septième principe de la CSA, on s'est demandé s'il fallait que la loi soit plus explicite au sujet des mécanismes convenables. Toutefois, il semble que ce simple énoncé est aussi satisfaisant qu'une formule plus élaborée.

Proposition 21

Une loi sur la protection des données devrait prévoir que les dispositifs de protection qui seront mis en œuvre comprennent la formation, des moyens matériels ainsi que des mesures administratives et techniques, selon ce que commandent les circonstances. La loi ne devrait pas tenter de définir de quelle façon un dispositif de protection peut correspondre à la sensibilité des renseignements.

c) Transfert vers des tiers

L'une des sous-questions les plus importantes que soulèvent les dispositifs de protection est la suivante : quels genres de dispositifs l'organisme devrait-il prévoir, le cas échéant, lorsqu'il transfère des renseignements personnels à un autre organisme?

Selon le principe directeur en la matière, un organisme est responsable des renseignements personnels dont il a la gestion (premier principe de la CSA), et il continue d'assumer cette responsabilité au moins jusqu'au moment du transfert des renseignements personnels. L'organisme doit donc s'assurer que le transfert est autorisé par la loi, par le consentement de la personne concernée ou par les fins de la collecte originale (troisième et cinquième principes de la CSA), et il doit prendre les mesures qui s'imposent, en vertu du principe relatif aux dispositifs de protection, pour s'acquitter de la responsabilité que lui confère le premier principe de la CSA de protéger les renseignements personnels.

Les dispositifs que les organismes devront mettre en œuvre dépendront des circonstances. Dans bien des cas, le respect des troisième et cinquième principes de la CSA suffiront, notamment lorsque l'organisme destinataire est lui aussi assujetti à la loi, puisque l'utilisation qu'il pourra faire des renseignements personnels sera limitée aux fins licites pour lesquelles l'organisme qui les transfère en fait la divulgation. Dans d'autres cas, l'organisme destinataire sera assujetti à des obligations contractuelles ou professionnelles de confidentialité qui permettront à l'organisme qui transfère les renseignements de se dispenser de la mise en œuvre de dispositifs de protection additionnels. Par contre, dans certaines situations, aucun cadre juridique n'assurera la protection des renseignements personnels; l'organisme qui effectuera le transfert devra prendre des mesures pour s'assurer que les conditions de celui-ci tiennent compte de ses responsabilités.

Mais la loi peut-elle aller plus loin et décrire ces mesures? Cela est discutable. Les conditions contractuelles peuvent parfois être efficaces à cet égard, en particulier dans le contexte d'une relation continue entre les organismes concernés, mais il serait très ardu de

décrire des situations particulières dans lesquelles l'organisme qui effectue le transfert *serait tenu* de prévoir des mesures de protection contractuelles. À moins qu'on soit disposé à énumérer ces situations dans la loi, on se contenterait de laisser l'organisme libre de prendre la décision et on ne dirait rien de plus que l'énoncé général selon lequel l'organisme qui effectue le transfert doit protéger les renseignements personnels au moyen de dispositifs de protection correspondant à leur degré de sensibilité.

Proposition 22

Une loi sur la protection des données devrait établir clairement que des dispositifs de protection correspondant au degré de sensibilité des renseignements personnels peuvent être nécessaires lorsqu'un organisme transfère des renseignements à un autre organisme; elle ne devrait cependant pas prescrire la forme des dispositifs de protection requis.

Huitième principe de la CSA – Transparence

Un organisme doit mettre à la disposition de toute personne des renseignements précis sur ses politiques et ses pratiques concernant la gestion des renseignements personnels.

À l'instar d'autres principes de la CSA, le huitième semble trouver plus naturellement son application dans les grands organismes qui sont plus susceptibles que les petits d'être dotés de politiques et de pratiques en bonne et due forme. Toutefois, il semble possible de donner un sens intelligible à l'expression « politiques et pratiques », même dans les plus petits organismes. Si l'on s'informe des politiques et pratiques de l'organisme, celui-ci doit exposer la situation telle qu'elle est. On présume que tous les organismes sont en mesure de satisfaire à cette exigence élémentaire.

Proposition 23

Le huitième principe de la CSA est suffisamment explicite; une loi sur la protection des données ne doit pas chercher à le clarifier davantage.

Neuvième principe de la CSA – Accès aux renseignements personnels

Un organisme doit informer toute personne qui en fait la demande de l'existence de renseignements personnels qui la concernent, de l'usage qui en est fait et du fait qu'ils ont été communiqués à des tiers, et lui permettre de les consulter. Il sera aussi possible de contester l'exactitude et l'état complet des renseignements et d'y faire apporter les corrections appropriées.

a) Formulation

Le neuvième principe est le second de la série qui est accompagné d'une note, laquelle « fait partie intégrante de ce principe » (paragraphe 3.1.2). La note explique les raisons pour lesquelles l'accès ne peut être absolu.

> Ces raisons peuvent comprendre le coût prohibitif de l'information à fournir, le fait que les renseignements personnels contiennent des détails sur d'autres personnes, l'existence de raisons d'ordre juridique, de raisons de sécurité ou de raisons d'ordre commercial exclusives et le fait que les renseignements sont protégés par le secret professionnel ou dans le cours d'une procédure de nature judiciaire. (par. 4.9)

Les lois sur la protection des données qui ont été adoptées par d'autres administrations prévoient fréquemment des exceptions de cette nature. Dans la *Loi visant le secteur public,* on a ajouté les mots « à moins qu'il ne soit pas approprié de le faire » à la fin de la première phrase du neuvième principe de la CSA afin d'indiquer que le droit de la personne d'avoir accès aux renseignements personnels qui la concernent n'est pas absolu. Le même ajout semble s'imposer dans la loi destinée au secteur privé.

Proposition 24

Les mots « à moins qu'il ne soit pas approprié de le faire » devraient être ajoutés au droit à l'information prévu dans le neuvième principe de la CSA.

b) La nature du droit

Même si le principe de la CSA est intitulé « Accès aux renseignements personnels », il semble en réalité comporter deux éléments, soit le droit d'être informé et le droit d'avoir accès. En pratique, on invoquera vraisemblablement plus souvent le droit à *l'information* que le droit *d'accès* qui équivaut au droit d'obtenir les documents. Une simple demande de la personne suffit à obliger l'organisme en vertu de ce principe. Dans la plupart des cas, la personne se contentera probablement de demander l'information; une réponse directe satisfera alors aux exigences du neuvième principe de la CSA.

Il arrivera bien sûr que la personne demande spécifiquement d'avoir accès aux documents. Dans un tel cas, si le fait d'accéder à la demande n'entraîne pas des coûts prohibitifs (voir le point *c. Exceptions au droit d'accès)* et si aucune autre exception de fond ne trouve application, les documents devraient être mis à la disposition de la personne. Il arrivera aussi parfois que des *documents* soient soustraits au droit d'accès, mais l'organisme devra tout de même fournir de *l'information* au moins partielle au sujet de leur contenu pour se décharger de l'obligation qui lui impose ce principe.

Dans la *Loi visant le secteur public*, il était superflu de clarifier ce lien entre le droit d'être informé et le droit d'avoir accès, puisque la *Loi sur le droit à l'information* règle cette question. Dans la loi qui s'appliquerait au secteur privé, cependant, ce lien devrait être établi clairement.

Proposition 25

Une loi sur la protection des données devrait établir clairement que le fait de fournir *l'information* suffit à l'organisme pour se décharger de l'obligation que lui impose le neuvième principe, à moins que la personne ne réclame spécifiquement l'accès aux documents.

c) Exceptions au droit d'accès

La *Loi visant le secteur public* renvoie à la *Loi sur le droit à l'information* en ce qui concerne les exceptions au droit qu'a la personne d'avoir accès aux renseignements. La plupart des « organismes publics » sont déjà assujettis à cette loi. Par contre, les mesures législatives destinées au secteur privé devraient contenir leur propre liste d'exceptions.

Une partie de cette liste ressemblerait à celle que contient la proposition 13 et qui énumère les circonstances dans lesquelles la collecte, l'utilisation ou la divulgation sans consentement de renseignements personnels peuvent être effectuées. Dans bon nombre des situations énumérées, il convient aussi de permettre la non-divulgation à la personne concernée. Cependant, certains motifs additionnels justifiant la non-divulgation s'appliquent aussi dans le contexte d'une demande d'accès par un particulier. On se demande en outre si la liste devrait contenir une disposition générale traitant des situations qui ne sont pas couvertes par les points spécifiques qui y sont énumérés; par ailleurs, on s'interroge à savoir s'il faudrait, dans certaines circonstances, exiger de l'organisme qui refuse de divulguer des renseignements des explications au sujet du contenu de ceux-ci.

Proposition 26

L'organisme ne devrait pas être tenu de divulguer des renseignements personnels à la personne concernée :

a) lorsque la divulgation serait préjudiciable à la santé ou à la sécurité du public ou d'un particulier, y compris de la personne qui présente la demande d'accès;

b) lorsque la divulgation entraverait le cours d'une enquête liée à l'application d'une loi;

c) lorsque la non-divulgation est exigée ou expressément autorisée par la loi ou lorsque la personne n'aurait pas le droit d'obtenir les renseignements dans le cadre d'une instance judiciaire;

d) lorsque les renseignements ont été fournis par un tiers sous le sceau de la confidence ou sont de nature confidentielle;

e) lorsque les renseignements demandés sont inextricablement liés à des renseignements personnels concernant un tiers;

f) lorsqu'il serait indûment dispendieux ou fastidieux de fournir les renseignements demandés;

On devrait envisager d'autoriser la non-divulgation lorsqu'il existe un autre motif légitime et substantiel de refuser l'accès aux renseignements demandés.

Les cas de non-divulgation devraient se limiter aux exigences raisonnables de chacune des situations. S'il peut expliquer le contenu des renseignements qu'il

refuse de divulguer sans pour autant porter atteinte aux motifs pour lesquels ils ne sont pas divulgués, l'organisme devrait le faire.

d) Modalités

Le neuvième principe de la CSA est muet en ce qui concerne les modalités qui doivent permettre aux personnes d'obtenir les renseignements, les documents ou les corrections auxquels elles ont droit. On en déduit qu'il revient à chacun des organismes d'établir ses propres modalités.

Cette façon de procéder semble acceptable. Le neuvième principe de la CSA prévoit de nombreux scénarios allant des demandes faites sans formalités auxquelles les organismes sont en mesure de répondre rapidement et facilement, aux situations qui peuvent donner lieu à une opposition. Il serait difficile d'inclure dans la loi des modalités qui couvriraient toutes ces situations; cette solution risquerait en outre de bureaucratiser indûment le mécanisme. Si les mesures législatives sur la protection des données étaient muettes au sujet des mécanismes d'accès, elles fonctionneraient conformément au principe selon lequel la personne a des droits que l'organisme doit respecter. Selon ce principe, l'organisme doit se rendre à la demande de la personne dans un délai raisonnable; s'il ne fait pas d'efforts véritables pour permettre à la personne d'exercer ses droits, il porte atteinte au principe.

Proposition 27

Une loi sur la protection des données pourrait être muette au sujet des mécanismes d'accès prévus dans le neuvième principe de la CSA.

e) Corrections

À première vue, la notion selon laquelle il est possible pour la personne « de contester l'exactitude et l'état complet des renseignements et d'y faire apporter les corrections appropriées » semble suffisamment explicite et autonome. De toute évidence, l'organisme n'a aucun intérêt à conserver des renseignements inexacts ou incomplets dans ses dossiers. Par conséquent, le problème que soulèvera fort probablement l'application de cet élément du neuvième principe de la CSA se posera lorsque la personne et l'organisme ne s'entendront pas sur l'exactitude des renseignements. Dans une telle situation, l'organisme ne devrait pas être forcé de modifier ses renseignements, mais il devrait être tenu de prendre note du fait que la personne en conteste l'exactitude. C'est probablement ce qui se produira dans le cours normal des choses, même si la loi est silencieuse à ce sujet. Mais étant donné que le neuvième principe de la CSA est muet en ce qui concerne les désaccords entre les parties, il convient probablement de clarifier cette question par voie législative.

Proposition 28

Si la personne remet en question l'exactitude ou le caractère exhaustif des renseignements sans réussir à convaincre l'organisme, celui-ci devrait prendre note du fait que la personne conteste les renseignements concernés.

Dixième principe de la CSA –
Possibilité de porter plainte contre le non-respect des principes

Toute personne doit être en mesure de se plaindre du non-respect des principes énoncés ci-dessus en communiquant avec le ou les individus responsables de les faire respecter au sein de l'organisme concerné.

Il faut remarquer que ce principe vise un processus d'examen *interne* par l'organisme lui-même; les questions relatives aux examens *externes* par d'autres organismes sont abordées ci-dessous, sous la rubrique Application de la loi.

Dans un mécanisme d'examen interne, il importe de préserver la crédibilité du processus. Dans tous les cas, l'organisme examinera sa propre conduite; parfois, surtout dans les plus petits organismes, la personne chargée de l'examen sera aussi celle dont la décision est remise en question. Ce genre de situation est inévitable. Mais la loi peut toujours contenir une disposition exigeant la tenue d'un véritable examen. On peut bien sûr déduire cette exigence du dixième principe de la CSA, mais l'inclusion dans la loi sur la protection des données de l'obligation qu'a l'organisme de faire enquête de bonne foi ainsi que de son devoir de prendre les mesures qui s'imposent s'il conclut que la plainte est fondée a un certain mérite sur le plan de la clarté.

Proposition 29

Un organisme devrait être tenu de faire enquête de bonne foi au sujet des plaintes qu'il reçoit et de prendre les mesures qui s'imposent quand il conclut qu'une plainte est fondée.

B.3 Autres enjeux

Dans la partie 2 du document de consultation rendu public par le gouvernement fédéral en 1998, on soulève deux questions dignes d'intérêt à propos desquelles le code de la CSA est muet. La première concerne les codes sectoriels, et la seconde, l'application de la loi.

a) Codes sectoriels

La question consiste à savoir si une loi sur la protection des données pourrait permettre à des secteurs de l'industrie d'élaborer leur propre code, qu'il s'agisse d'une adaptation du code de la CSA ou d'un document entièrement inédit; dans l'affirmative, on devra déterminer la portée juridique de ces codes. Cette question se pose en raison des préoccupations que soulève la formulation du code de la CSA et des mesures législatives qu'il inspire, laquelle ne serait pas tout à fait applicable à tous les organismes ou pourrait être trop vague pour vraiment définir ce qui serait permis ou non dans certaines situations. Un code sectoriel permettrait à l'industrie d'élaborer des règles qui tiennent compte des exigences de son propre fonctionnement.

La principale question que suscite cette possibilité consiste à savoir si le code sectoriel devrait avoir un effet juridique et, plus particulièrement s'il aurait préséance sur le code légiféré en cas de conflit entre les deux. Si c'était le cas, le code sectoriel devrait recevoir l'approbation d'un organisme compétent en vertu de la loi. Autrement, les industries auraient

le pouvoir de se soustraire d'elles-mêmes à la loi. Par contre, si le code légiféré a préséance sur les codes sectoriels, le mécanisme officiel d'approbation revêtirait un caractère beaucoup moins impératif. Quelles que soient les dispositions du code sectoriel, le code légiféré contiendrait toujours les principes directeurs. Les codes sectoriels auraient ainsi moins de valeur aux yeux de l'industrie, puisque même si elle s'y conformait, elle n'aurait aucune assurance qu'elle respecte ainsi la loi.

Même si les codes sectoriels présentent certains avantages (comme tout code ou toute politique interne d'un organisme), l'approche qui semble convenir au cas qui nous occupe consisterait à encadrer le fonctionnement des codes et politiques au moyen des dispositions prévues par la loi, lesquelles auraient préséance sur ceux-ci en cas de conflit. Bien sûr, ce cadre serait exprimé en termes généraux, mais la protection des données n'est pas – peu s'en faut – le seul domaine assujetti à des règles juridiques énoncées en termes généraux, et les organismes doivent élaborer des politiques et des pratiques à la lumière de leur compréhension de la portée des règles. Si un genre d'organismes ou d'activités en particulier exige l'adoption de règles juridiques plus précises que les principes généraux du code légiféré, il serait préférable d'intégrer celles-ci par voie de règlement plutôt que dans le cadre de codes sectoriels.

Proposition 30

Les codes sectoriels ne devraient pas avoir force de loi en vertu d'une loi sur la protection des données. Celle-ci devrait édicter le pouvoir de faire les règlements qui, le cas échéant, pourraient contenir des dispositions plus précises à l'égard du genre d'organismes, de renseignements ou d'activités concerné.

b. Application de la loi

Le code de la CSA n'avait pas à se pencher sur la question de l'application de la loi, puisqu'il s'agit d'une norme purement volontaire dont le respect est régi par des mécanismes d'autosurveillance. Dans un cadre législatif, cependant, on doit aborder la question de savoir ce que l'on fera si les règles ne sont pas respectées. Si la loi était muette à ce sujet, il incomberait, en dernière analyse, aux tribunaux d'interpréter les mesures législatives et de décider des recours qu'on doit en déduire.

Les trois principales approches en matière d'application de la loi sont les suivantes : a) le recours pénal; b) le recours civil; et c) le recours administratif. Le recours pénal sert à réprimer les conduites inacceptables et à punir les contrevenants; les poursuivants sont généralement des avocats de la fonction publique, et les amendes sont versées au tribunal. Le recours civil permet aux justiciables de s'adresser aux tribunaux en leur propre nom afin d'obtenir un dédommagement en raison d'un préjudice qu'on leur a fait subir ou d'empêcher un tel préjudice. Tout dédommagement ainsi adjugé est versé au justiciable. Le recours administratif comporte la mise sur pied d'un organisme parajudiciaire qui verrait à l'application des mesures législatives concernées et qui pourrait disposer d'un éventail de pouvoirs de réparation. La position du justiciable et le rôle du tribunal varieront selon la nature de ces pouvoirs.

Le recours pénal

Selon la *Loi visant le secteur public,* commet une infraction tout organisme public ou tout dirigeant, tout employé ou tout représentant d'un organisme public qui recueille, utilise ou divulgue des renseignements personnels d'une façon qui porte intentionnellement atteinte aux troisième (consentement), quatrième (limitation de la collecte) et cinquième (limitation de l'utilisation, de la communication et de la conservation) principes du Code de pratique statutaire. Selon l'interprétation que l'on en donne habituellement, l'expression « atteinte intentionnelle » désigne le fait de commettre un acte fautif en le sachant fautif ou en négligeant de tenir compte de son caractère fautif. Les mesures législatives interdisant la divulgation fautive de renseignements sont plus courantes dans le secteur public que dans le secteur privé, mais il conviendrait peut-être de prévoir une infraction de la sorte dans la loi destinée au secteur privé. Celle-ci pourrait en outre créer une infraction de refus intentionnel de fournir des renseignements ou de faire une correction d'une façon qui porte atteinte à l'un des droits que confère aux particuliers le neuvième principe du code de la CSA. Cette question ne se pose pas dans la *Loi visant le secteur public,* puisque l'application du droit à l'accès relève de la *Loi sur le droit à l'information.*

Proposition 31

Une loi sur la protection des données pourrait énoncer que toute atteinte intentionnelle aux troisième (consentement), quatrième (limitation de la collecte), cinquième (limitation de l'utilisation, de la communication et de la conservation) et neuvième (accès aux renseignements personnels) principes de la CSA constitue une infraction.

Le recours civil

Les recours civils ont-ils leur place dans une loi sur la protection des données? Les principaux recours civils sont le jugement déclaratoire, l'injonction et l'action en dommages-intérêts. Le jugement déclaratoire se contente d'énoncer le droit et la façon dont il s'applique à une série de faits donnés. L'injonction comporte aussi une déclaration de la façon dont la loi s'applique à une série de faits donnés, mais elle présente un élément obligatoire additionnel qui sert à forcer le justiciable à faire ou à ne pas faire quelque chose. L'action en dommages-intérêts, enfin, oblige une partie à dédommager l'autre partie en raison d'un dommage imputable à un acte fautif.

Quel rôle les recours civils pourraient-ils jouer dans l'application de la loi sur la protection des données? Ces recours, pris isolément, seront examinés dans les pages qui suivent. La question sera ensuite abordée de nouveau après avoir étudié le recours administratif. Si l'on mettait sur pied un important mécanisme administratif d'application de la loi, les recours civils seraient en effet appelés à jouer un rôle beaucoup plus effacé.

La principale fonction du recours civil, par opposition au recours pénal, consiste à accorder au justiciable qui est victime d'un préjudice un droit personnel de faire valoir ses propres intérêts. Mais le recours civil a aussi un effet plus général. Même s'il porte sur des cas individuels, le recours civil permet aux tribunaux de formuler des jugements qui font jurisprudence quant à la signification de dispositions particulières de la loi. Il se produit ainsi un effet d'entraînement lorsque les tribunaux établissent des normes que doivent respecter tous

les organismes assujettis à la loi. On dit fréquemment que les instances judiciaires sont coûteuses et pénibles; mais bien des gens sont parfois prêts à plaider des questions qui leur tiennent à cœur, et ces procès peuvent trancher d'importantes questions de principes. L'un des meilleurs exemples dans le domaine de la protection des renseignements est l'affaire *McInerney* c. *Macdonald* (1992) 126 NBR (2d) 271; dans cette affaire, qui a pris naissance au Nouveau-Brunswick, la Cour suprême du Canada a reconnu le droit qu'avait le patient d'un médecin de consulter un rapport à son sujet qui avait été préparé par un consultant.

En règle générale, on serait porté à croire qu'en l'absence d'un recours administratif empêchant le justiciable de s'adresser aux tribunaux, ceux-ci devraient avoir le pouvoir d'expliquer le sens de la loi une fois qu'elle a été adoptée. Le jugement déclaratoire semble donc tout indiqué en la matière. On pense aussi tout naturellement à l'injonction, puisqu'il serait illogique de permettre aux tribunaux de déterminer le sens d'une loi tout en les privant du pouvoir d'exiger d'un organisme qu'il agisse conformément à ce que la loi lui dit de faire. Il faudra se souvenir de la possibilité de forcer les organismes à se conformer à la loi si on formule des mesures législatives; en effet, la loi doit à tout prix éviter d'imposer aux organismes des obligations qu'on ne peut raisonnablement leur demander d'assumer. Si l'on impose des obligations raisonnables, toutefois, les injonctions ne devraient susciter aucun problème.

On doit être plus circonspect à l'égard des jugements octroyant des dommages-intérêts. L'examen de documents relatifs à la protection des données dans les autres ressorts donne lieu aux deux questions suivantes : a) devrait-on pouvoir invoquer le recours en dommages-intérêts en cas d'atteinte aux principes régissant la protection des données; et b) dans l'affirmative, dans quelles circonstances pourrait-on l'invoquer? La plupart des lois canadiennes en vigueur en matière de protection des renseignements personnels dans le secteur public ne permettent pas l'octroi de dommages-intérêts. Au Québec, où la loi couvre aussi le secteur privé, les mécanismes fondamentaux de protection des renseignements personnels sont énoncés dans le *Code civil* et le justiciable peut se prévaloir du recours en dommages-intérêts. Dans les lois sur la protection des données dans le secteur privé des administrations de *common law* de l'extérieur du Canada (il n'en existe aucune au Canada à l'heure actuelle), on aborde toutefois avec circonspection la question des dommages-intérêts. La *Privacy Act 1993* de la Nouvelle-Zélande énonce explicitement qu'elle ne crée aucun droit qui serait susceptible d'être déclaré exécutoire par les tribunaux. Le Complaints Review Tribunal peut ordonner le paiement d'un dédommagement, mais il s'agit là d'un pouvoir discrétionnaire et non d'un droit dont peut se prévaloir le justiciable. Au Royaume-Uni, le *Data Protection Act 1984* permet l'octroi de dommages-intérêts dans certaines situations, mais pas dans celles où l'organisme a pris des précautions raisonnables, eu égard aux circonstances, pour que l'atteinte ne se produise. Dans l'évaluation du montant des dommages, le tribunal peut tenir compte des souffrances psychologiques qu'a endurées la victime, mais celles-ci ne donnent pas, en tant que telles, droit à un dédommagement. La présence de dommages semble être l'une des conditions préalables essentielles à l'exercice du recours (voir les articles 22 et 23).

On a raison d'être prudent lorsqu'il s'agit de permettre le recours en dommages-intérêts en raison d'une atteinte à un principe en matière de protection des données. Ceux-ci établissent des normes de pratique, mais les actes qui ne s'y conforment pas et qui ne sont donc pas tout à fait bons ne revêtent pas tous une gravité telle qu'ils justifient des

réclamations en dommages-intérêts lorsqu'ils provoquent des dommages ou de la souffrance psychologique. Si l'on définit les renseignements personnels de la façon suggérée dans la proposition 5 (tout renseignement concernant un particulier identifiable enregistré sous quelque forme que ce soit), on couvrira un vaste éventail de données, certaines sensibles, la plupart non. Le traitement des renseignements personnels – et les possibilités d'erreur qui en découlent – se fait de façon routinière dans les organismes, et la mise en œuvre de la loi exigera que l'on prenne régulièrement des décisions au sujet de ce qui est « approprié » et de ce qui ne l'est pas, de ce qui est « raisonnable » et de ce qui ne l'est pas. La loi deviendrait vite encombrante si chacune des décisions pouvait être contestée devant les tribunaux et si chaque erreur de jugement, même lorsque l'organisme a déployé des efforts sincères et importants en vue de se conformer à la loi, pouvait donner lieu à des poursuites en dommages-intérêts.

C'est la raison pour laquelle il paraît sage, en ce qui concerne le recours en dommages-intérêts, de prévoir une marge d'erreur dans une loi sur la protection des données, de sorte que le simple fait pour un organisme de ne pas satisfaire aux normes établies par la loi et de causer ainsi des dommages ne suffirait pas en soi pour donner ouverture à une réclamation en dommages-intérêts. On peut définir de diverses façons cette marge d'erreur. Au Royaume-Uni, comme il en a été fait mention auparavant, le critère applicable à l'octroi de dommages-intérêts est celui de l'absence de précautions raisonnables. On pourrait aussi examiner les conséquences du non-respect de la loi et prévoir que l'octroi de dommages-intérêts n'est permis que si la violation équivaut à une atteinte au droit à la vie privée. Il conviendrait peut-être, de préférence à ces deux scénarios, d'élaborer un critère « d'incompatibilité manifeste avec la loi » comme fondement de ce que devrait prouver le plaignant qui réclame des dommages-intérêts. Face à un tel critère, si l'organisme fait un geste erroné qui n'est pas déraisonnable, il ne s'exposerait pas à être condamné à payer des dommages-intérêts.

Proposition 32

À moins qu'une loi sur la protection des données ne prévoie des recours administratifs qui rendent superflus les recours civils, les justiciables devraient pouvoir se prévaloir du jugement déclaratoire, de l'injonction et de l'action en dommages-intérêts à titre de mesures d'application de la loi. Toutefois, on ne devrait permettre l'octroi de dommages-intérêts que lorsque la violation de la loi par l'organisme entraîne une perte et satisfait un autre critère, comme celui de l'incompatibilité manifeste avec la loi.

Le recours administratif

Dans le secteur public, la question du recours administratif soulevait relativement peu de problèmes. Un organisme statutaire existait déjà (l'Ombudsman de la province), et son mandat englobait naturellement des questions relatives au traitement des renseignements du genre de celles qui sont visées par les principes de protection des données. Ce lien a été officialisé lorsque la province a adopté son *Code de protection des renseignements personnels* en 1994; l'Ombudsman a en effet été désigné comme organisme responsable d'assurer le respect du code. Le document de travail rendu public par le ministère de la Justice en 1996 proposait que l'Ombudsman joue le même rôle dans le cadre de la loi sur la protection des données dans le secteur public; cette proposition a été entérinée par le Comité de modification

des lois, et c'est ce que prévoit actuellement la *Loi visant le secteur public.* En vertu de la *Loi,* le recours administratif exercé devant l'Ombudsman est en réalité le recours prépondérant, et les recours judiciaires ont une portée beaucoup plus restreinte.

Toutefois, les choses ne sont pas aussi simples dans le secteur privé. Aucun organisme n'a actuellement un mandat qui englobe naturellement la protection des données dans la plupart, voire dans l'ensemble, des « organismes » qui seraient assujettis à la loi sur la protection données en vertu de la proposition 4. Cependant, dans de nombreux secteurs d'activité, on trouve des organismes de réglementation prévus sous le régime d'une loi dont le mandat englobe ou pourrait englober les questions relatives à la protection des données. Au rang des organismes assujettis à la réglementation, on compte les assureurs, les établissements financiers, les agences de recouvrement, les enquêteurs privés et les foyers de soins, pour n'en nommer que quelques-uns. Les occupations assujetties à l'autoréglementation, comme celles d'avocat et de médecin, font aussi l'objet de mécanismes légaux de traitement des plaintes qui pourraient servir dans les affaires relatives à la protection des données et qui servent déjà probablement dans le cadre de l'examen de questions relatives au caractère confidentiel des communications avec le client. Des organismes volontaires de normalisation, comme les associations sectorielles, ont aussi mis sur pied des mécanismes non statutaires de traitement des plaintes. Le récent document de discussion du gouvernement fédéral mentionne que tous ces organismes pourraient avoir un rôle à jouer dans l'application non judiciaire des mesures législatives sur la protection des données dans le secteur privé (p. 21).

Les discussions en ce qui concerne les recours administratifs dans le cadre d'une loi sur la protection des données ont toutefois tendance à porter sur la question de savoir s'il faut mettre sur pied un organisme désigné de protection des données qui serait chargé d'assurer le respect de la loi. On utilise souvent l'expression « commissariat à la protection de la vie privée » pour désigner cet organisme, mais cette expression est trompeuse. Elle laisse entendre que l'organisme s'occupe de la vie privée entendue dans le sens large et naturel décrit dans la partie II du présent document, et non des questions plus restreintes ayant trait à la protection des données, qui constituent le mandat premier de l'organisme. Dans le présent document, l'expression « organisme de protection des données » sera donc utilisée, plutôt que les termes « commissariat à la protection de la vie privée ». Bien sûr, la création de recours administratifs dans le cadre de la loi sur la protection des données ne doit pas nécessairement entraîner la mise sur pied d'un organisme de protection des données. Il existe d'autres possibilités.

Deux grandes raisons justifieraient la création de recours administratifs dans le cadre d'une loi sur la protection des données. La première consisterait à restreindre le rôle que les tribunaux joueraient autrement dans l'application de la loi. C'est ce qui pourrait se produire, par exemple, si les obligations établies par la loi ne se prêtaient pas aisément à l'exécution par les tribunaux ou si on craignait que la loi fasse courir aux organismes des risques exagérés de poursuites pour une foule de motifs. Deuxièmement, on pourrait soutenir que même si les recours judiciaires ont leur place dans les mesures législatives sur la protection des données, ils ne sont pas suffisamment exhaustifs en la matière. Certains les jugent trop lents ou trop coûteux pour régler les questions courantes d'observation de la loi et ils les estiment inefficaces en matière de prévention et d'éducation, un secteur que doit englober la protection des données, selon eux.

La première de ces raisons laisse essentiellement sous-entendre que les recours judiciaires n'ont pas leur place dans la loi sur la protection des données. Certains soutiennent, par exemple, que le code de la CSA doit être considéré comme un énoncé déontologique plutôt que comme une mesure législative; on ne pourrait donc pas concrètement s'attendre à ce que les organismes se conforment aux critères qu'il établit, et ils ne devraient pas être menacés de poursuites judiciaires toutes les fois qu'ils y contreviennent. Compte tenu de cet argument, un recours administratif en grande partie fondé sur la dissuasion pourrait mieux convenir que l'intervention des tribunaux.

La force de cet argument dépend du degré de précision avec lequel le code de la CSA et les mesures législatives sur la protection des données qui s'en inspirent décrivent des normes réalistes de pratiques convenables. Elle dépend aussi de la nature des recours judiciaires proposés; à la lumière des propositions 31 et 32, ceux-ci prendraient la forme a) de poursuites en cas d'atteintes intentionnelles de principes particuliers, b) de poursuites en dommages-intérêts lorsqu'un acte « manifestement incompatible avec la loi » cause une perte et c) de requêtes en jugement déclaratoire et en injonction en cas de non-respect de la loi. La question de savoir si cet équilibre entre les obligations et les recours est satisfaisant et réaliste devra alimenter le débat public.

Il convient cependant de souligner que les obligations énoncées dans le code de la CSA sont de la nature de celles que les tribunaux font respecter dans d'autres contextes. Le code contient des assouplissements (« à moins qu'il ne soit pas approprié de le faire » dans le troisième principe, « les attentes raisonnables de la personne » au paragraphe 4.3.5). Les tribunaux sont habitués de manipuler des notions souples comme celles-là. Il suffit de penser par exemple à la « prudence raisonnable » du droit de la responsabilité et aux « attentes raisonnables en matière d'intimité » de l'article 8 de la *Charte canadienne des droits et libertés*. En fait, les tribunaux sont probablement beaucoup plus à l'aise que la plupart des organismes administratifs lorsqu'il s'agit de faire respecter des normes génériques semblables, à plus forte raison s'ils sont en présence d'un vaste éventail de secteurs d'activité. Par conséquent, on voit mal comment on pourrait prétendre que les obligations que comportent les mesures législatives sur la protection des données ne se prêtent pas à l'interprétation et à l'application qu'en feraient les tribunaux. On pourrait bien sûr songer à restreindre le rôle des tribunaux sous prétexte que les organismes et les particuliers seront « plus à l'aise » de faire affaires avec un organisme administratif en cas de litige en vertu de la loi. Mais cette position est différente de celle qui soutient que les tribunaux ne sont pas l'arène convenable pour interpréter des principes comme ceux du code de la CSA.

Ce raisonnement nous amène à la deuxième raison énoncée ci-dessus qui pourrait justifier la création de recours administratifs dans le cadre d'une loi sur la protection des données (les recours judiciaires pourraient convenir en matière de protection des données, mais les recours administratifs seraient préférables). Cette position soulève deux points importants. Le premier a trait aux plaintes et à la nature du mécanisme de résolution des différends. Le second porte sur des questions comme la prévention et l'éducation qui, si elles étaient intégrées au projet législatif, ne pourraient manifestement pas relever des tribunaux.

En ce qui concerne les plaintes, l'argument en faveur de la création de recours administratifs peut être énoncé de façon très abrupte : les litiges coûtent cher et sont intimidants, et la plupart des gens dans la plupart des situations n'intenteront pas de poursuites au sujet des genres de questions que soulève la protection des données. Selon cet argument, en l'absence de recours administratif, l'application de la loi sera impossible. On serait tenté d'ajouter que l'application de la loi par voie administrative pourrait se faire en grande partie au moyen de la médiation et de la conciliation, alors que les recours judiciaires sont fondés sur le principe de l'antagonisme.

Certains répondent à cet argument que les recours administratifs sont l'exception et non la règle dans la plupart des litiges juridiques. Même s'il existe des organismes comme le médiateur des loyers, les agents des normes d'emploi et les commissions des droits de la personne, les parties à un litige juridique doivent normalement régler elles-mêmes leur différend, accepter leur sort ou intenter des poursuites. C'est cette position qu'adopte la loi en ce qui concerne les questions relatives aux « renseignements personnels » comme la diffamation et l'abus de confiance. C'est également le cas des droits fondamentaux de la personne énoncés dans la *Charte canadienne des droits et libertés,* y compris du droit à la vie privée qui en découle, de l'avis des tribunaux. C'est aussi en grande partie le cas des lois sur la protection des consommateurs (en vertu desquelles les consommateurs s'adressent généralement à la Division des petites créances s'ils doivent plaider leur cause). L'analogie avec la protection des consommateurs est pertinente, puisqu'une grande partie des discussions au sujet des mesures législatives sur la protection des données dans le secteur privé, y compris le récent document de consultation du gouvernement fédéral, situent la protection des données dans le contexte de la nécessité de protéger les droits des consommateurs, spécialement sur l'autoroute de l'information.

On ne devrait donc pas tenir pour acquise la création d'un mécanisme administratif de traitement des plaintes. Il faudra faire des choix au chapitre des coûts, des avantages et des priorités. D'une part, les ressources administratives consacrées à l'application des mesures législatives sur la protection des données feront sans doute accroître le respect des méthodes équitables de traitement de l'information. D'autre part, étant donné que les ressources administratives sont toujours très sollicitées, le fait de laisser aux justiciables l'initiative de se prévaloir de leurs recours devant les tribunaux s'ils le désirent ne diminue en rien les valeurs dont la loi sur la protection des données fait la promotion. Les organismes de réglementations existants continueraient bien sûr de recevoir les plaintes dans leur domaine de compétence.

Même si un mécanisme administratif de traitement des plaintes en matière de protection des données peut sembler *a priori* souhaitable, il faut aussi se demander ce que comporterait un tel mécanisme. L'une des possibilités serait d'en faire un processus de médiation et de conciliation auquel ne serait rattaché aucun pouvoir de contrainte légale. Cette façon de procéder améliorera sans doute les possibilités de règlements à l'amiable; cependant, sa faiblesse apparente ne manquera pas de susciter des critiques. Par contre, si on va plus loin en ajoutant des pouvoirs de contrainte à l'exercice du recours administratif, on devra s'interroger sur la portée de ces pouvoirs. S'ils comprenaient celui de délivrer des ordonnances exécutoires, il faudrait sans doute aussi prévoir le pouvoir de tenir des audiences, en plus d'y rattacher celui d'assigner des témoins et de forcer la production d'éléments de preuve. Les pouvoirs de pénétrer dans des lieux et d'inspecter des registres et des dossiers

pourraient aussi être nécessaires, sans compter l'examen que l'on devrait faire des mécanismes d'application de la loi chargés d'assurer le respect de ces ordonnances exécutoires.

Bref, tout s'enchaîne. La question qui doit être soumise au débat à l'heure actuelle est la suivante : Jusqu'où doit-on aller dans la mise sur pied d'un mécanisme administratif de traitement des plaintes. Voici les trois façons de procéder qui ressortent de l'éventail des solutions possibles : 1) s'en remettre entièrement au processus judiciaire; 2) mettre sur pied un mécanisme administratif sans pouvoir de contrainte légale; et 3) mettre en œuvre un mécanisme administratif doté de pouvoirs de contrainte qui seraient probablement assez exhaustifs. Quelle approche s'impose dans le contexte du respect des pratiques équitables en matière de renseignements personnels?

L'autre question qui a été soulevée au sujet des recours administratifs consiste à savoir si le mécanisme administratif présente certains avantages dont seraient dénués les recours judiciaires essentiellement enclenchés par des plaintes. L'un des aspects déjà mentionné est celui de la prévention; on peut aussi penser à l'éducation.

Si l'on veut prendre en considération des fonctions comme celles-là, le mécanisme de redressement administratif en vertu de la loi sur la protection des données commence à prendre des allures d'organisme permanent, pas nécessairement spécialisé uniquement dans la protection des données, mais qui aurait au moins une existence permanente et dont le mandat comprendrait la protection des données. Par contre, le mécanisme de traitement des plaintes décrit au paragraphe précédent pourrait être une entité plus éphémère mise sur pied au besoin pour traiter les plaintes au fur et à mesure qu'elles se présentent.

Quoiqu'il en soit, certaines des questions que soulèvent ces fonctions additionnelles se comparent aux interrogations que suscite le mécanisme de traitement des plaintes. La prévention semble souhaitable à première vue. Mais si la prévention signifie en pratique qu'un organisme administratif a le pouvoir de pénétrer dans les locaux de toute organisation et d'y inspecter les registres et les méthodes même en l'absence d'une plainte, convient-il de déléguer un tel pouvoir pour assurer le traitement adéquat des renseignements personnels?

Par ailleurs, la prévention pourrait signifier de donner des conseils aux organismes afin de leur permettre de rendre leurs méthodes conformes aux mesures législatives. Mais cette possibilité soulève aussi des interrogations, puisque l'organisme administratif devrait toujours se réserver le droit de faire enquête de façon impartiale au sujet des questions relativement auxquelles on solliciterait son avis si un particulier déposait subséquemment une plainte. Par conséquent, les avis de l'organisme ne pourraient pas faire autorité; dans ce cas, ils ne seraient pas très utiles aux organisations qui les demanderaient.

Les fonctions d'éducation, entendue dans le sens de fournir de l'information générale à la population au sujet des mesures législatives, et de promotion de la cause, entendue dans le sens d'inciter les gouvernements et les organisations à porter une plus grande attention aux questions relatives à la protection des données dans leurs décisions et dans leurs méthodes, présenteront probablement moins de difficultés pratiques ou techniques. Toutefois, il faut penser en termes de priorités et de ressources. Ces fonctions pourraient être souhaitables dans le cadre du mandat d'un organisme essentiellement axé sur le traitement des plaintes. Mais on

peut se demander si elles justifieraient en elles-mêmes un mandat distinct, en l'absence d'une quantité importante de plaintes.

Il est bon de noter que le nombre de plaintes reçues par le Bureau de l'Ombudsman en vertu des dispositions du *Code de protection des renseignements personnels* en vigueur dans le secteur public du Nouveau-Brunswick au cours des trois premières années suivant son entrée en vigueur a été peu élevé, soit moins de 25 plaintes chaque année. On ne peut pas tirer beaucoup de conclusions de ces quelques chiffres, mais on peut à tout le moins déduire que les politiques concernant la loi sur la protection des données ne devraient pas prendre pour acquis que la quantité de plaintes sera élevée. Il sera intéressant de vérifier si le remplacement du *Code de protection des renseignements personnels* par la *Loi sur la protection des renseignements personnels* dans le secteur public entraînera une augmentation du nombre des plaintes.

Proposition 33

La création de recours administratifs n'est pas essentielle à une loi sur la protection des données; mais elle représente un choix politique. Les grandes questions à être examinées dans le cadre des consultations publiques sont les suivantes :

a) Les recours judiciaires sont-ils suffisants et convenables?

b) La création d'un mécanisme administratif de traitement des plaintes sans pouvoir de contrainte serait-elle utile?

c) Le fait d'assortir le mécanisme administratif de traitement des plaintes de pouvoirs de contrainte serait-il improductif ou exagéré?

d) Peut-on penser à une fonction qui ne serait pas axée sur les plaintes, qui serait substantielle et viable et qui justifierait à elle seule que l'on consacre des ressources à un organisme administratif ayant un mandat précis en matière de protection des données?

II. La vie privée en général

Comme on peut le lire dans l'introduction du présent rapport, la notion de « vie privée » ne se restreint pas à la « protection des données ». Lorsque les gens parlent de leur vie privée, ils pensent normalement au confort de leur foyer, à leur capacité de communiquer sans indiscrétion de la part de tiers et à la protection des détails de leur vie contre toute publicité non désirée. L'article 17 du *Pacte international relatif aux droits civils et politiques*, qui classe la protection de la vie privée parmi les droits de la personne reconnus à l'échelle internationale et dont le Canada est signataire, résume bien cette notion :

> Nul ne sera l'objet d'immixtions arbitraires ou illégales dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes illégales à son honneur et à sa réputation. Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes.

Dans son rapport intitulé *La vie privée : Où se situe la frontière?,* publié en 1997, le Comité permanent des droits de la personne et de la condition des personnes handicapées de la Chambre des communes présente comme suit son énoncé des garanties et droits fondamentaux (p. 37) :

> Chaque citoyenne et citoyen dispose du droit fondamental de jouir des éléments suivants :
>
> - intimité physique;
> - protection des renseignements personnels;
> - protection contre la surveillance;
> - protection des communications personnelles;
> - protection de l'espace personnel.

La protection des données n'est, bien sûr, que l'un des aspects du droit à la vie privée. Elle s'inscrit dans le cadre de la « protection des renseignements personnels », quoique la protection des données, qui met l'accent sur les renseignements enregistrés et sur les « organismes » à l'exclusion des activités personnelles ou domestiques, ne cerne pas tout le sujet.

Par conséquent, la présente partie du rapport a pour objectif d'établir si le Nouveau-Brunswick doit adopter des mesures législatives en vue de protéger la « vie privée » dans son sens large. On y examine deux approches, la première consistant à élargir la portée des recours *judiciaires* existants en créant un « délit civil » de violation de la vie privée. Le délit civil est un acte fautif dont la personne lésée peut demander réparation en se prévalant

des recours civils normaux que sont les actions en jugement déclaratoire, en dommages-intérêts et en injonction. L'autre approche vise la création de recours *non judiciaires* (ou administratifs) en cas d'atteinte à la vie privée. Ces deux approches sont la suite logique de l'examen effectué dans la partie I des « recours civils » et des « recours administratifs » possibles en vertu de la loi sur la protection des données. Le Comité permanent des Communes, qui était clairement en faveur de la création de recours non judiciaires en cas d'atteinte à la vie privée, n'a pas porté une grande attention aux recours judiciaires. Voilà qui est surprenant. La principale recommandation du comité suggérait au gouvernement d'adopter, dans son champ de compétence, une « Charte canadienne des droits à la protection de la vie privée » qui aurait une portée quasi constitutionnelle (p. 49). Toutefois, comme nous le verrons, les principaux éléments des « droits fondamentaux à la vie privée » (mentionnés ci-dessus) sont déjà pris en considération par certaines provinces dans le contexte de délits civils de violation du droit à la vie privée; c'est ce que pourrait faire le Nouveau-Brunswick.

A. Recours judiciaires en cas d'atteinte au droit à la vie privée

Le chemin emprunté dans les pages qui suivent est relativement bien tracé. De nombreuses études ont été réalisées notamment en Angleterre, en Australie et au Canada au sujet des recours judiciaires semblables qui protègent le droit à la vie privée. Ces études ont été effectuées dans le contexte de l'absence de recours idoine bien établi en cas d'atteinte à la vie privée; cependant, le droit à la vie privée peut être protégé par un certain nombre d'autres recours, notamment l'action pour trouble de jouissance ou pour abus de confiance. On abordera donc la portée des recours en vigueur, des mesures supplémentaires qui pourraient ou devraient être prises pour assurer la protection de la vie privée, de la question de savoir s'il serait préférable de procéder par voie législative ou par voie jurisprudentielle et de déterminer si, dans l'une ou l'autre de ces optiques, le meilleur cadre légal consiste à peaufiner les recours existants ou à créer un délit civil « d'atteinte au droit à la vie privée ».

On doit aussi faire référence à l'expérience américaine afin d'établir des contrastes. Les tribunaux y ont en effet reconnu depuis belle lurette que le droit à la vie privée est protégé en *common law*. La jurisprudence permet de dégager quatre principales catégories d'atteintes au droit à la vie privée susceptibles de donner ouverture à un recours. Il s'agit des suivantes : 1) l'intrusion dans la solitude ou l'isolement ou dans les affaires personnelles du requérant; 2) la divulgation en public de faits embarrassants concernant le requérant; 3) la publicité présentant le requérant sous un mauvais jour au public; et 4) le fait pour l'intimé de s'approprier à son avantage du nom ou de l'image du requérant.

Au Canada, dont la position est décrite en long et en large par Ian Lawson dans son livre intitulé *Privacy and Free Enterprise* (1993, Public Interest Advocacy Centre), la discussion prend une teinte particulière. Parmi les particularités du pays, notons que cinq provinces ont déjà légiféré afin de créer un délit spécifique d'atteinte au droit à la vie privée. Quatre d'entre elles, soit la Colombie-Britannique, la Saskatchewan, le Manitoba et Terre-Neuve, sont des provinces de *common law* où le recours est nouveau. La cinquième province est le Québec, où le recours a évolué par l'entremise de l'interprétation des dispositions générales touchant la responsabilité civile de l'ancien *Code civil;* il a été intégré

en bonne et due forme au nouveau *Code civil.* La *Charte des droits et libertés de la personne* du Québec contient aussi la disposition suivante à l'article 5 : « Toute personne a droit au respect de sa vie privée ». Contrairement à la charte canadienne, cette disposition est directement exécutoire dans les litiges privés.

Le débat canadien se distingue aussi du fait que dans les provinces de *common law* qui n'ont pas adopté de mesures législatives en la matière, les tribunaux ont de plus en plus tendance à opiner qu'un délit civil général d'atteinte à la vie privée existe peut-être en *common law.* Dans certains affaires ontariennes, le tribunal a octroyé des dommages-intérêts pour ce motif. Dans une récente décision, la Cour d'appel de l'Île-du-Prince-Édouard fait remarquer que « (...) les tribunaux du Canada sont sur le point de reconnaître un droit à la vie privée en *common law*, s'ils ne l'ont pas déjà fait » (le juge en chef Carruthers de l'Île-du-Prince-Édouard, *Dyne Holdings Ltd.* c. *Royal Insurance Co. of Canada* (1996) 138 Nfld. & PEI R., 318). Ces développements obscurcissent la question de savoir si ce sont les *législateurs* qui doivent prendre les mesures nécessaires pour faire de l'atteinte à la vie privée un délit civil, ou si les tribunaux doivent élaborer, décision par décision, ce nouveau secteur du droit de la responsabilité. Si la jurisprudence permettait de conclure clairement à l'existence ou à la non-existence d'un délit civil général, nous aurions moins de difficultés à évaluer la contribution que pourraient à bon escient apporter les mesures législatives.

En ce qui concerne les recours judiciaires, on cherchera surtout à savoir, dans les pages qui suivent, si le Nouveau-Brunswick doit adopter des mesures législatives qualifiant de « délit civil » l'atteinte à la vie privée. Comme c'était le cas dans la partie du rapport qui portait sur la protection des données, la discussion sera axée sur un modèle législatif particulier. Il s'agit de la *Loi uniforme sur la protection de la vie privée* adoptée par la Conférence sur l'harmonisation des lois du Canada en 1994. Cette loi s'inspire des mesures législatives en vigueur dans certaines provinces qui sont semblables dans leurs grandes lignes, mais qui diffèrent dans leurs détails. Il n'y a aucune raison pour chercher à inventer un mécanisme tout à fait inédit. Le présent document se contentera donc de décrire la loi et d'exposer trois grands choix politiques en ce qui concerne les recours judiciaires en cas d'atteinte au droit à la vie privée. Le premier consiste à adopter des mesures législatives assez semblables à la loi uniforme. Le second équivaut à décider de ne pas créer de délit civil d'atteinte à la vie privée. Enfin, le troisième consiste à confier l'élaboration du délit civil aux tribunaux, plutôt qu'au législateur, le cas échéant.

Proposition 34

L'examen de la création d'un délit civil d'atteinte au droit à la vie privée devrait être effectué à la lumière de la *Loi uniforme sur la protection de la vie privée* préparée par la Commission sur l'harmonisation des lois au Canada, compte tenu des recours judiciaires existants qui sont susceptibles de protéger le droit à la vie privée.

A.1 Recours existants

Les recours qui existent en cas d'atteinte à la vie privée se trouvent dans la *Charte canadienne des droits et libertés,* dans diverses lois fédérales et provinciales et dans certains

délits civils. Aucun d'entre eux ne prévoit un recours établi, généralisé et autonome en cas d'atteinte à la vie privée. Comme nous l'avons mentionné auparavant, un débat théorique a actuellement lieu quant à l'existence en *common law* d'un délit civil « d'atteinte à la vie privée ». En fait, si un tel délit existe, il n'est certainement pas encore « établi ». Par contre, les autres recours dont nous parlerons sont clairement « établis » et peuvent être invoqués pour protéger *en partie* la vie privée; ils ne sont cependant pas « généralisés ».

a. La Charte canadienne des droits et libertés

On peut traiter assez succinctement la question de la vie privée dans le contexte de la *Charte des droits et libertés.* En effet, la *Charte* ne contient aucun droit explicite à la vie privée. Toutefois, les tribunaux, y compris la Cour suprême du Canada, ont conclu que le droit à la vie privé est prévu de façon implicite dans d'autres dispositions expresses de la *Charte,* notamment aux articles 7 et 8. Les tribunaux parlent assez abondamment d'un « droit constitutionnel à la vie privée », en dépit de l'absence de toute disposition explicite à cet effet dans la *Charte.*

L'article 7 de la *Charte* se lit comme suit : « Chacun a droit à la vie, à la liberté et à la sécurité de sa personne; il ne peut être porté atteinte à ce droit qu'en conformité avec les principes de justice fondamentale ». Les tribunaux ont jugé que la vie privée pouvait être un élément de la « liberté » et de la « sécurité de la personne ». Ils ont décidé qu'il existe au moins un « noyau de renseignements de nature biographique » qui ont tendance à révéler des « détails intimes au sujet de modes de vie ou de choix personnels » et qui sont protégés en vertu de cet article. Il se peut que la *Charte* aille plus loin, mais pour le moment on accepte qu'elle aille au moins jusqu'à ce point.

L'article 8 de la *Charte* édicte ce qui suit : « Chacun a droit à la protection contre les fouilles, les perquisitions ou les saisies abusives ». Les tribunaux ont jugé que le critère applicable au caractère raisonnable de la fouille, de la perquisition ou de la saisie consiste à savoir si celle-ci porte atteinte à « des expectatives raisonnables en matière de vie privée ». Les fouilles, perquisitions et saisies en question ne sont pas restreintes à celles qui ont lieu dans le contexte évident de l'application des lois pénales; elles englobent aussi d'autres formes de collecte de renseignements. Le fait d'obtenir des renseignements de tiers consentants a été qualifié de fouille ou de perquisition dans certaines affaires comme *La Reine* c. *Dyment* (1988) 89 N.R. 249, dans laquelle un médecin a volontairement fourni aux policiers un échantillon de sang provenant d'un conducteur blessé et prouvant que celui-ci avait les facultés affaiblies au moment d'un accident, et *La Reine* c. *Plant* (1993) RCS 281, dans laquelle un service public d'électricité a volontairement mis à la disposition de la police ses dossiers relatifs à la consommation d'énergie. (Dans cette dernière affaire, la « perquisition » effectuée par les policiers lors de leur vérification des dossiers a été jugée « non abusive », puisque la majorité des juges de la Cour suprême – mais pas tous – était d'avis que des dossiers portant sur la consommation d'énergie ne révélaient pas de « détails intimes au sujet de modes de vie ou de choix personnels » à l'égard desquels l'occupant pouvait avoir « des expectatives raisonnables en matière de vie privée ».)

La protection offerte par la *Charte* n'est toutefois pas absolue. Si l'on prend l'article 7, par exemple, on *peut* priver une personne de « la vie, la liberté ou la sécurité de sa

personne », si on le fait « en conformité avec les principes de justice fondamentale ». De son côté, l'article 8 protège « des expectatives *raisonnables* en matière de vie privée ». Qui plus est, en vertu de l'article 1, tous les droits prévus par la *Charte* peuvent être restreints « par une règle de droit, dans des limites qui soient raisonnables et dont la justification puisse se démontrer dans le cadre d'une société libre et démocratique ». Mais le fait que la *Charte* ne s'applique qu'aux actes des gouvernements joue encore davantage en ce qui concerne la disponibilité d'un recours *généralisé* en cas d'atteinte à la vie privée. En effet, la *Charte* ne trouve généralement pas application dans les questions de vie privée opposant des citoyens. Par conséquent, le droit à la vie privée que protège la *Charte* tient à bien peu de recours dans le contexte privé.

b. Lois fédérales et provinciales

Il faudra encore moins de temps pour traiter de la protection de la vie privée qu'offrent les lois fédérales et provinciales. Contrairement aux dispositions de la *Charte* qui ne trouvent leur application, aussi généralisée soit-elle, que dans les relations entre les citoyens et les gouvernements, les lois fédérales et provinciales sont spécifiques. Elles contiennent parfois des dispositions sur la protection de la vie privée, mais celles-ci se confinent à un domaine en particulier.

Dans le champ de compétence du fédéral, des mesures législatives comme le *Code criminel* et la *Loi sur la protection des renseignements personnels* viennent tout naturellement à l'esprit. Les dispositions relatives à la procédure du *Code criminel* régissent les pouvoirs des policiers lorsqu'ils font enquête au sujet d'infractions; de plus, les infractions substantielles prévues dans le *Code* touchent des questions comme l'interception de communications privées (art. 184) ou le fait de « cerner et surveiller » (art. 423). La *Loi sur la protection des renseignements personnels,* quant à elle, traite de la protection des données dans les institutions du gouvernement fédéral; les mesures législatives que le fédéral prépare actuellement pour le secteur privé étendront les règles relatives à la protection des données aux éléments du secteur privé qui relèvent de sa compétence législative.

Aucune loi générale sur la protection de la vie privée n'existe à l'échelon fédéral. Normalement, la vie privée serait considérée comme un domaine relevant de la compétence des législatures provinciales en vertu de l'article 92 de la *Loi constitutionnelle de 1867,* puisqu'il s'agit d'une question relative « à la propriété et aux droits civils dans la province ». Même si une loi de portée générale était en vigueur dans l'un ou l'autre des champs de compétence de notre système fédéral – on peut penser aux pouvoirs en matière de droit criminel – il est permis de se demander à bon droit, dans le cadre d'un rapport comme celui-ci, s'il serait souhaitable de mettre à la disposition des justiciables des recours civils en vertu des lois provinciales en sus de la protection que peuvent leur procurer les mesures législatives fédérales.

En ce qui concerne la protection de la vie privée dans les mesures législatives provinciales, on remarque que certaines lois particulières du Nouveau-Brunswick traitent de questions qu'on associe souvent aux préoccupations en matière de protection de la vie privée; par contre, aucune loi de portée générale n'aborde la question de la vie privée en tant que telle, que ce soit sous l'angle des recours civils ou sous celui du pouvoir de la province de

créer des infractions communément qualifiées de « quasi-criminelles » dans des domaines qui relèvent de sa compétence législative. Les mesures législatives provinciales qui portent sur des questions soulevant couramment des préoccupations en matière de vie privée comprennent la *Loi sur le démarchage,* la *Loi sur les agences de recouvrement* et la *Loi sur les détectives privés et les services de sécurité.*

c. La common law

Dans son livre intitulé *Privacy and Free Enterprise,* Ian Lawson décrit de façon détaillée un certain nombre de recours susceptibles de s'offrir, en *common law,* en cas d'atteinte à la vie privée, selon la nature de l'atteinte dont on se plaint. Il parle aussi de l'émergence possible du délit civil d'atteinte à la vie privée. Parmi les nombreux délits civils que mentionne Lawson, ceux-ci semblent les plus importants :

i) Atteinte directe à la propriété immobilière. Selon la théorie relative à ce délit civil, l'occupant de la propriété a le droit de décider de l'identité des personnes qui y sont et n'y sont pas admises. Il s'agit certes d'un instrument utile pour protéger « l'espace privé ». On parle moins souvent du délit qui consiste à « cerner et surveiller » le lieu de résidence ou de travail afin de forcer l'occupant à faire une chose; cette disposition étend la protection du droit de la responsabilité délictuelle à certains actes faits *à l'extérieur* de la propriété immobilière de l'occupant. L'application libérale des dispositions relatives au délit civil de *nuisance* a aussi permis de sanctionner certains actes faits sans effraction dans la propriété immobilière de l'occupant. Parmi les exemples, citons l'affaire *Poole and Poole* c. *Ragen and the Toronto Harbour Commissioners* [1958] O.W.N. 77, à l'issue de laquelle les demandeurs ont obtenu des dommages-intérêts ainsi qu'une injonction contre la police du port de Toronto qui suivait depuis trois mois l'embarcation des demandeurs dans ses déplacements dans le port, ainsi que l'affaire *Motherwell* c. *Motherwell* (1976) 73 D.L.R. (3rd) 62, une chicane de famille dans laquelle le demandeur harcelait les défendeurs en les appelant par téléphone à un nombre incalculable de reprises pour se plaindre d'un autre membre de la famille.

ii) Voies de fait et *atteinte à l'intégrité.* Au sens de ces délits civils, il est illicite de toucher une personne sans son consentement. Ces délits civils sanctionnent les atteintes à « l'intégrité physique de la personne ».

iii) Diffamation et *abus de confiance.* Le vieux délit civil de diffamation vise la publication de renseignements faux qui portent atteinte à la réputation du demandeur. L'abus de confiance est un délit civil qui évolue lui-même et qui comporte un recours en cas de divulgation de renseignements confidentiels que la personne obtient d'un tiers et au sujet desquels la personne concernée a des expectatives raisonnables de non-divulgation. Ces deux délits civils trouvent bien sûr leur application dans le domaine du « droit à la protection des renseignements ». Le délit civil de *mensonge préjudiciable* pourrait aussi trouver une application en la matière; il s'agit de la fabrication de fausses déclarations dans le but de causer un dommage pécuniaire. Contrairement au cas de la diffamation, il n'est pas nécessaire que la déclaration soit préjudiciable à la réputation du demandeur.

Traditionnellement dans des pays comme le Canada, l'Australie et le Royaume-Uni, la question de la nécessité de mesures législatives pour assurer la protection de la vie privée a

toujours été tributaire de l'évaluation de l'efficacité de délits civils comme ceux-là. La question a été rendue plus complexe récemment au Canada, en raison de l'émergence d'un petit courant jurisprudentiel qui porte à croire que l'atteinte à la vie privée est peut-être en voie de devenir un délit civil en bonne et due forme à cause des décisions judiciaires et sans aucune intervention de la part du législateur. Parmi ces décisions, mentionnons l'affaire *Saccone* c. *Orr* (1981) 34 OR (2d) 317, dans laquelle le défendeur avait secrètement enregistré une conversation téléphonique avec le demandeur, puis l'avait fait écouter à l'assemblée du conseil municipal, ainsi que l'affaire *Roth* c. *Roth* (1991) 4 OR (3d) 740, qui mettait en scène un litige entre des voisins au sujet de l'utilisation d'un chemin d'accès, lequel a dégénéré en une campagne de harcèlement qui a conduit notamment à une atteinte au droit à la vie privée du demandeur.

Quant à savoir si les délits civils actuels sont suffisants, on trouve deux courants d'opinions. Selon le premier, ils le sont. Ses adeptes admettent qu'il n'existe aucun droit spécifique d'action en cas d'atteinte à la vie privée, mais ils ajoutent qu'aucun recours précis ne vient non plus remédier aux atteintes à d'autres droits fondamentaux, comme « la liberté » ou « la sécurité de la personne ». Ils soutiennent que les droits comme ceux-là sont abstraits et que leur exercice, comme celui du droit à la vie privée, est généralement protégé au moyen des recours spécifiques (action pour séquestration, demande d'*habeas corpus,* etc.) qui s'offrent dans des situations données.

Selon eux, les recours actuels suffisent dans l'ensemble à la tâche de protéger la vie privée; si on peut démontrer qu'ils comportent certaines lacunes, il serait préférable de les revoir, plutôt que d'en créer de nouveaux. L'expérience semble indiquer, aux États-Unis, qu'un droit à la vie privée en apparence généreux entraîne un petit nombre de plaintes qui visent des comportements semblables à ceux qui caractérisent les délits civils. Ils craignent que le délit civil d'atteinte au droit à la vie privée, en raison de sa nouveauté, ne nuise à d'autres causes importantes comme la liberté d'expression et la liberté de la presse.

Les adversaires de cette position soutiennent, quant à eux, que la notion de vie privée est suffisamment claire pour qu'on la définisse de façon adéquate, et qu'elle revêt une telle importance qu'elle doit être protégée de façon expresse. Les adeptes de ce courant d'opinion estiment que les recours actuels en responsabilité délictuelle ne suffisent pas à la tâche, puisque chacun d'eux s'inscrit dans un contexte donné qui le rend inopérant dans certaines situations. L'un des exemples classiques de circonstances semblables est relaté dans l'affaire anglaise *Kaye* c. *Robertson* (annexe I du *Report of the Committee on Privacy and Related Matters* – le comité Calcutt – 1990, HMSO). Dans cette affaire, des reporters d'un journal sont entrés dans une chambre d'hôpital où une personne célèbre se remettait d'une intervention chirurgicale au cerveau après avoir subi un grave accident. Les reporters, faisant fi des interdictions d'entrer, ont interviewé le patient et ont pris des photos. Ils ont par la suite prétendu que celui-ci ne s'y était pas opposé; la Cour d'appel était plutôt d'avis qu'il aurait dû être évident pour les reporters que le patient n'était pas en état de consentir. Quoiqu'il en soit, les reporters ont proposé de publier les photos ainsi qu'un article basé sur l'entrevue. En l'absence d'une cause d'action fondée sur l'atteinte à la vie privée, le patient a tenté d'empêcher la publication en invoquant le libelle, le mensonge préjudiciable, l'atteinte à l'intégrité physique et la contrefaçon. Il a toutefois dû se contenter d'une injonction interdisant au

journal de publier quoi que ce soit permettant de conclure à son consentement à l'entrevue. Le juge Bingham s'est exprimé comme suit dans cette décision :

> [trad.] « La conduite des défendeurs en l'instance à l'égard du demandeur équivaut à une " monstrueuse atteinte à sa vie privée " (pour paraphraser l'expression de l'honorable juge Griffiths dans l'affaire *Bernstein* c. *Skyviews Ltd.* [1978] QB 479, p. 489G). S'il est un endroit où on a le droit de ne pas être importuné par des étrangers qui ne servent aucun intérêt public, c'est bien lorsqu'on gît dans un hôpital en train de se remettre d'une chirurgie au cerveau et jouissant d'un contrôle minimal de ses facultés. C'est cette atteinte à sa vie privée qui justifie la plainte du demandeur. Pourtant, en soi et malgré son caractère répugnant, elle ne lui donne droit à aucune mesure de redressement en droit anglais. »

Les deux courants d'opinions au sujet de la création d'un délit civil d'atteinte à la vie privée sont crédibles. Les deux sont aussi grandement tributaires des vues opposées de leurs adeptes respectifs quant à la faculté du législateur et des tribunaux de trouver une définition de « l'atteinte à la vie privée » qui est à la fois simple et manifestement utile. Ceux qui désirent continuer à faire confiance au mécanisme établi des délits civils craignent que la création d'une notion englobante d'atteinte à la vie privée ne soulève plus de questions qu'elle n'en règle. Le comité Calcutt était de cet avis; en effet, malgré des décisions comme celle rendue dans l'affaire *Kaye* c. *Robertson,* les membres du comité estimaient que l'adoption d'autres mesures, notamment la création de certains recours criminels et civils bien ciblés, était préférable à la création d'un délit civil d'atteinte à la vie privée dont la portée serait considérable. Par contre, ceux qui préfèrent un recours spécifique en cas d'atteinte à la vie privée estiment qu'on peut arriver à une définition pratique, et que sans recours spécifique on ne sera jamais en mesure de résoudre le vrai problème.

A.2 Un délit civil d'atteinte à la vie privée?

Pour obtenir la matière permettant d'arriver à une conclusion, le présent rapport adoptera une approche semblable à celle suivie en matière de protection des données et à l'égard du code de la CSA. En se fondant sur la *Loi uniforme sur la protection de la vie privée,* un certain nombre de propositions au sujet de la formulation possible de mesures législatives créant un délit civil d'atteinte au droit à la vie privée y seront formulées . Il pourra ensuite y avoir un débat public au sujet du caractère souhaitable de mesures législatives formulées de cette façon ou en des termes semblables. L'intégralité de la loi uniforme figure à l'annexe C. On pourra aussi prendre connaissance, à l'annexe D, du résumé d'une approche légèrement remaniée découlant des propositions formulées dans la présente partie du rapport.

a. Atteinte à la vie privée

Les principaux éléments de la loi uniforme sont : a) un énoncé général indiquant que l'atteinte à la vie privée d'un particulier par une autre personne est un délit civil punissable sans preuve de dommage (art. 2); b) une liste d'activités précises qui, en l'absence de preuve à l'effet contraire, sont réputées constituer des atteintes à la vie privée (art. 3); et c) une liste de moyens de défense (art. 4). La loi partage ce cadre général avec d'autres mesures législatives

canadiennes, mais celles-ci divergent entre elles en ce qui concerne la question de savoir si seulement les particuliers (par oppositions aux sociétés, par exemple) peuvent intenter des poursuites en cas d'atteinte au droit à la vie privée.

Les activités qui sont considérées par la loi uniforme comme des atteintes présumées à la vie privée sont (en résumé) : a) la surveillance auditive ou visuelle d'un particulier; b) le fait d'écouter ou d'enregistrer les conversations d'un particulier; c) la publication de lettres, du journal intime ou d'autres documents personnels; et d) la diffusion illicite de renseignements concernant le particulier. Cette liste n'est pas exhaustive; d'autres actes qui n'y figurent pas peuvent aussi constituer des atteintes à la vie privée.

Les moyens de défense (pareillement résumés) sont les suivantes : a) le demandeur a consenti à l'activité; b) le défendeur a agi de façon à défendre légalement sa personne ou ses biens; c) l'activité est autorisée ou exigée par la loi; d) le défendeur faisait légalement enquête au sujet d'une infraction; e) les actes du défendeur sont raisonnables, compte tenu de la relation domestique ou autre entre les parties; f) le défendeur ignorait ou ne pouvait raisonnablement savoir que ses actes porteraient atteinte à la vie privée de quiconque; et g) les actes dont on se plaint constituent une publication raisonnable dans l'intérêt public.

L'un des éléments que ne contient pas cette approche est une description ou une définition générale de ce qu'est une atteinte à la vie privée. Les moyens de défense représentent des activités *qui ne constituent pas* des atteintes à la vie privée et on cite en exemples certaines activités précises qui sont *susceptibles* de constituer des atteintes à la vie privée. Ces précisions mises à part, le principal énoncé de la loi est simplement la mention vague voulant que « toute atteinte à la vie privée d'une personne (...) constitue un délit civil ».

Est-ce acceptable? Les mesures législatives doivent-elles être plus explicites? La logique de la loi uniforme et d'autres mesures législatives semblables est prétendument fondée sur l'hypothèse selon laquelle si la loi tente de définir ce qu'est une atteinte à la vie privée, elle limitera la faculté des tribunaux d'élaborer ce nouveau secteur du droit de la responsabilité délictuelle dans le contexte des affaires qu'ils instruisent. En revanche, on peut soutenir qu'en l'absence d'une quelconque définition, le nouveau délit civil est exagérément vague.

On serait porté à penser qu'une description générale de ce qu'est une atteinte à la vie privée serait, en principe, un attribut utile de la loi. La proposition qui suit suggère donc une formulation. Si elle est satisfaisante, elle pourrait être intégrée à un texte de loi. Sinon, une approche qui ressemble davantage à celle de la loi uniforme serait peut-être plus indiquée.

Il est bon de noter que cette définition ne doit pas nécessairement être exhaustive (du genre « les droits fondamentaux à la vie privée » énumérés par le Comité permanent des droits de la personne et de la condition des personnes handicapées de la Chambre des communes). Elle aurait pour objet de décrire un acte passible de sanctions plutôt qu'un « droit de la personne », et elle s'inscrirait parallèlement à des recours justifiés par d'autres délits civils, de sorte que l'atteinte au droit à la vie privée par l'intrusion, les voies de fait, le libelle, l'abus de confiance et autres continuent d'être traitée à l'aide de moyens différents. La définition décrirait l'essence du nouveau délit civil que la loi ajouterait au répertoire actuel.

Proposition 35

L'atteinte au droit à la vie privée pourrait se définir comme suit :

Tout acte constitue une atteinte à la vie privée,

a) s'il s'immisce indûment dans les affaires personnelles ou les activités d'un particulier, qu'il se produise dans un endroit public ou en privé, ou

b) s'il donne une publicité indue à des renseignements concernant un particulier.

Si une définition semblable à celle-là est trop restrictive, l'approche de la loi uniforme est-elle acceptable ou fait-elle la part trop grande à l'incertitude? Il est bon de remarquer au passage que certaines lois provinciales en vigueur donnent plus de précisions au sujet du critère du caractère abusif que la loi uniforme mentionne à peine dans les moyens de défense, à l'alinéa 4(1)e). À titre d'exemple, voici ce que prévoit la loi de la Colombie-Britannique :

> [trad.]
> 1(2) La vie privée à laquelle toute personne a droit dans une situation donnée ou relativement à une affaire donnée équivaut, en nature et en intensité, à ce qu'elle peut raisonnablement attendre dans les circonstances, eu égard aux intérêts légitimes des tiers.
>
> 1(3) Lorsqu'on détermine si l'acte ou la conduite d'une personne porte atteinte au droit à la vie privée d'une autre personne, on doit prendre en considération la nature, l'incidence et le contexte de l'acte ou de la conduite ainsi que toute relation domestique ou autre existant entre les parties.

D'autres mesures législatives en vigueur dans les provinces de *common law* (mais pas au Québec) sont plus circonspectes que la loi uniforme dans leur description du genre de conduite qui équivaut à une atteinte au droit à la vie privée. En Colombie-Britannique, en Saskatchewan et à Terre-Neuve, ne commet un délit civil que la personne qui porte « intentionnellement et sans apparence de droit » atteinte au droit à la vie privée d'une autre personne. En Saskatchewan, la loi parle de « façon substantielle et déraisonnable et sans apparence de droit ».

La nécessité d'intégrer de tels critères dans une loi créant un délit civil d'atteinte à la vie privée dépend en grande partie de la présence ou de l'absence dans la loi d'une définition générale de l'atteinte au droit à la vie privée semblable à celle que contient la proposition 35. En règle générale, on serait porté à croire que le critère du « caractère raisonnable » serait l'un des éléments pertinents de la loi. Le fait d'exiger la présence d'un caractère intentionnel pourrait cependant sembler un peu excessif.

Proposition 36

Si une définition semblable à celle qu'énonce la proposition 35 se révèle trop restrictive, la loi sur la protection de la vie privée devrait au moins prévoir qu'un acte ou une conduite doit échouer le critère du « caractère déraisonnable » pour être qualifiée d'atteinte au droit à la vie privée.

L'article 3 de la loi uniforme contient un exemple d'une atteinte au droit à la vie privé :

> d) la diffusion de renseignements concernant le particulier qui ont été recueillis à des fins commerciales ou gouvernementales si
>
> (i) la diffusion est contraire à une loi ou à un règlement, ou
>
> (ii) les renseignements ont été fournis par le particulier sous le sceau du secret et leur diffusion a été faite à des fins autres que celles pour lesquelles ils ont été fournis.

Les moyens de défense généraux que prévoit la loi s'appliqueraient bien sûr, y compris les notions de « consentement » et de « caractère raisonnable » (voir ci-dessous).

À cet égard, il existe un lien important avec les questions relatives à la protection des données. On peut considérer le paragraphe 3d) comme un exemple de la façon dont des dispositions législatives sur un délit civil pourraient résumer l'essence de la législation en matière de protection des données en quelques mots simples qui pourraient rendre superflue toute mesure législative plus élaborée. On ne trouve pas de disposition comparable au paragraphe 3d) dans les lois sur la protection de la vie privée de la Colombie-Britannique, de l'Alberta, de la Saskatchewan et de Terre-Neuve. Au Québec, par contre, les principes fondamentaux en matière de protection des données sont énoncés aux articles 37 et 41 du *Code civil;* les lois particulières sur la protection des données dans les secteurs privé et public constituent le prolongement des dispositions législatives du *Code civil.*

On devra de toute évidence examiner avec soin toute disposition comme le paragraphe 3d) afin de décider de l'inclure dans des mesures législatives portant sur les atteintes à la vie privée. Si le Nouveau-Brunswick adopte une loi sur la protection des données semblable à celle qui est décrite dans la partie I du présent document, ce serait probablement l'endroit où il conviendrait d'énoncer la politique en matière de recours civils, à savoir si on a décidé de les inclure ou de les exclure délibérément. Toutefois, si on renonce à adopter une loi sur la protection des données, on aura avantage à examiner de plus près le paragraphe 3d). Sa portée semble moins grande que celle d'une loi sur la protection des données, ce qui pourrait le rendre encore plus acceptable. Par contre, si les consultations permettent de conclure que l'application d'une loi sur la protection des données dans le secteur privé n'est pas souhaitable, les motifs pourraient être tels qu'une disposition comme le paragraphe 3d) ne conviendrait pas non plus.

Proposition 37

On devrait attendre les résultats des consultations au sujet des mesures législatives sur la protection des données dans le secteur privé avant de décider que le fait de « communiquer de façon illicite des renseignements au sujet d'un particulier » constitue un délit civil d'atteinte au droit à la vie privée.

b) Moyens de défense

Passons maintenant à la question de savoir si les moyens de défense prévus à l'article 4 de la loi uniforme sont convenables et doivent être énumérés. À ce sujet aussi, les lois provinciales sont généralement cohérentes. Toutes prévoient un moyen de défense contre une action pour atteinte au droit à la vie privée si le défendeur a agi avec le consentement du plaignant, a défendu légalement sa personne ou ses biens, était autorisé par la loi, a agi dans le but d'appliquer la loi ou a publié des renseignements dans l'intérêt public. Deux caractéristiques de la loi uniforme sont moins typiques toutefois; il s'agit de l'alinéa 4(1)e), selon lequel la conduite doit être raisonnable eu égard à toute relation domestique ou autre existant entre les parties, et de l'alinéa 4(1)f), qui prévoit le cas où « le défendeur ignorait ou ne pouvait raisonnablement savoir que l'acte, la conduite ou la divulgation porterait atteinte à la vie privée d'un particulier ». Ces deux moyens de défense semblent acceptables dans leurs aspects essentiels; leur place dans la loi serait cependant tributaire de la présence d'une définition générale de l'atteinte au droit à la vie privée ainsi que du critère du caractère déraisonnable.

Soulignons enfin, en passant, que les rédacteurs de la loi uniforme ont délibérément omis un moyen de défense particulier qui ne figure que dans la loi de la Saskatchewan. Il s'agit d'alléguer que l'auteur de l'acte est une personne s'occupant de collecte des informations pour le compte de tout journal ou diffuseur, que l'acte était raisonnable dans les circonstances et qu'il était nécessaire ou accessoire aux activités ordinaires de collecte des informations. Le rapport préparé pour le compte de la Conférence sur l'harmonisation des lois du Canada soutient que la disposition spéciale à l'intention des préposés à la collecte des informations est superflue. En effet, si une telle disposition leur accordait une protection réelle, ne leur consentirait-elle pas un privilège particulier qui leur permettrait de porter atteinte à la vie privée des citoyens?

Proposition 38

Pour l'essentiel, les moyens de défense énumérés à l'article 4 de la loi uniforme sont convenables.

c. Recours

L'article 5 de la loi uniforme traite des recours. Il énonce que le tribunal peut adjuger des dommages-intérêts, émettre des injonctions, ordonner au défendeur de rendre compte de tout profit découlant de l'atteinte au droit à la vie privée et de remettre tout bien qu'il en a tiré, et accorder au demandeur toute autre mesure de redressement qu'il juge nécessaire dans les circonstances.

Ces recours se trouvent en substance dans les lois sur la protection de la vie privée de la Saskatchewan, du Manitoba et de Terre-Neuve. Par contre, la loi de la Colombie-Britannique et les dispositions sur la protection de la vie privée du *Code civil* du Québec sont muettes au sujet des recours, qu'elles renvoient implicitement au droit commun en la matière. L'approche la plus souhaitable dépend en grande partie d'un jugement technique fondé sur la meilleure évaluation possible de ce que les tribunaux feront en présence ou en l'absence de directives législatives à ce sujet. Mais dans l'ensemble, l'article 5 semble contenir un énoncé raisonnable des recours qui devraient être disponibles.

Proposition 39

On devrait pouvoir se prévaloir des recours prévus à l'article 5 de la loi uniforme en cas d'atteinte au droit à la vie privée, même s'ils ne sont pas expressément intégrés à la loi.

L'article 6 de la loi uniforme mentionne une gamme de facteurs que le tribunal peut examiner lorsqu'il adjuge des dommages-intérêts par suite d'une atteinte au droit à la vie privée. Parmi ceux-ci, mentionnons la nature de l'acte et le contexte dans lequel il a lieu ainsi que la conduite du demandeur et du défendeur avant et après l'acte, y compris toute excuse ou offre de faire amende honorable de la part du défendeur. L'article précise en outre que le tribunal peut octroyer des dommages-intérêts exemplaires dans les cas qui s'y prêtent.

Cet article semble à prime abord ne soulever aucune objection; en fait, nous sommes probablement en présence d'un cas où le moins le législateur en dit, le mieux tout le monde se porte. L'article a essentiellement pour effet de préciser que la conduite du défendeur peut être pertinente en ce qui concerne le calcul des dommages par suite d'une atteinte au droit à la vie privée; mais on se demande s'il est vraiment nécessaire de le préciser, voire de le mettre en valeur par rapport à d'autres facteurs qui pourraient être tout aussi importants. Les tribunaux du Québec ont de nombreuses années d'expérience dans l'octroi de dommages-intérêts en raison d'atteintes au droit à la vie privée; par ailleurs, dans quelques récentes affaires ontariennes, le calcul des dommages-intérêts octroyés ne tenait pas uniquement compte des pertes financières. Les octrois de dommages-intérêts finiront par se stabiliser au bout d'un certain temps, qu'on adopte ou non une disposition semblable à l'article 6. Mais même en l'absence d'une telle disposition, on pourra certes s'en remettre aux tribunaux pour élaborer les mesures qui s'imposent.

Proposition 40

On pourrait à bon escient laisser les tribunaux élaborer les règles applicables au calcul des dommages-intérêts relatifs au délit civil d'atteinte au droit à la vie privée.

d. Questions d'ordre technique

La loi uniforme se termine par quelques dispositions juridiques de nature technique, comme la relation avec les autres délits civils et le fait que la loi lie la Couronne. D'autres lois provinciales traitent de questions comme la prescription, l'ordre de préséance entre la loi

et les autres mesures législatives, l'inadmissibilité dans les instances civiles d'éléments de preuve obtenus en contravention de la loi ainsi que la question de savoir s'il est possible de porter atteinte au « droit à la vie privée » d'une personne décédée.

Il n'est pas nécessaire d'examiner de telles questions techniques dans le cadre de cette réflexion. La meilleure façon de les régler semble consister à adopter l'approche générale selon laquelle le délit civil d'atteinte au droit à la vie privée qui est créé par une loi est comparable à tout autre délit civil. On trouverait, dans cette disposition, réponse à la plupart des questions d'ordre technique. La question la plus épineuse reste celle de savoir s'il est possible de porter atteinte au « droit à la vie privée » d'une personne décédée. La réponse qui semble aller de soi est « non », en particulier à la lumière de l'article 2 qui laisse entendre que seuls les particuliers peuvent intenter des poursuites en cas d'atteinte au droit à la vie privée. La Colombie-Britannique, la Saskatchewan et Terre-Neuve semblent pousser ce raisonnement un peu plus loin en précisant que même si l'atteinte à la vie privée se produit avant le décès d'une personne, le droit d'action qui s'y rattache s'éteint, lui, au moment du décès. Quant à savoir s'il s'agit là de la meilleure approche, il faudrait examiner la question de plus près.

Proposition 41

Les questions d'ordre technique relatives à la prescription, au fait que la Couronne soit ou non liée par la loi et à l'admissibilité de la preuve devraient être réglées en traitant le délit civil d'atteinte à la vie privée de la même façon que les autres délits civils. L'atteinte à la vie privée d'une personne décédée ne devrait donner ouverture à aucun droit d'action.

A.3 Légiférer ou ne pas légiférer?

À la suite de cet examen de la loi uniforme, nous pouvons retourner à la principale question abordée dans la présente partie du rapport : Doit-il ou non exister une loi créant le délit civil d'atteinte au droit à la vie privée? On trouvera deux modèles possibles en annexe. La loi uniforme figure à l'annexe C, tandis que l'annexe D présente le résumé d'une approche légèrement différente qui se fonde sur les propositions énoncées dans le présent rapport. Les deux se ressemblent. Les principaux points qui les distinguent sont les suivants : 1) l'annexe D contient une définition générique de l'atteinte au droit à la vie privée, contrairement à l'annexe C; et 2) l'annexe D ne tient pas compte de la plus grande partie des dispositions sur les recours que contient l'annexe D. Dans leurs grandes lignes, cependant, les deux sont comparables. La décision de mettre en œuvre des dispositions sur l'atteinte au droit à la vie privée exige que l'on décide d'adopter des mesures législatives de ce genre.

Comme il a été indiqué auparavant, la présente consultation pourrait déboucher sur trois solutions. La première consisterait à adopter une loi très semblable à loi uniforme. La seconde énoncerait qu'il ne devrait pas exister de délit civil d'atteinte au droit à la vie privée. La troisième énoncerait que s'il devait exister un délit civil d'atteinte au droit à la vie privée, il appartient aux tribunaux, plutôt qu'au législateur, de l'établir. Puisqu'il n'a pas été fait mention des arguments en faveur de ces deux dernières solutions depuis un certain temps, il convient d'y revenir brièvement avant de clore la discussion à ce sujet.

« Il ne devrait pas exister de délit civil d'atteinte au droit à la vie privée »

En bref, l'argument global qui milite contre la création d'un délit civil d'atteinte au droit à la vie privée, est celui-ci : que ce délit est superflu, indéfinissable, inopportun et mal conçu. Il est superflu parce que d'autres recours établis en matière de responsabilité délictuelle suffisent dans l'ensemble à protéger la vie privée. Il est indéfinissable parce que la vie privée est une notion trop subjective pour être traduite par une définition juridique réaliste. Il est inopportun parce qu'il présente une trop grande menace pour des activités souhaitables (p. ex. : le journalisme légitime) en tentant de régler un problème beaucoup plus petit. Il est mal conçu parce qu'il ne tient pas compte des compromis que la vie quotidienne nous force à faire et qu'il présume trop témérairement que toute atteinte à la dignité d'un individu doit nécessairement donner ouverture à un recours en justice.

Les modèles législatifs examinés dans le présent rapport peuvent jeter un éclairage sur ces questions. Commençons avec celle de la définissabilité : l'examen des modèles législatifs déterminera si le délit civil peut être décrit de façon satisfaisante. La prochaine étape est celle du caractère opportun : les mesures législatives de cette nature présentent-elles, oui ou non, des risques pour des activités désirables? La mesure à laquelle le délit civil est mal conçu dépend aussi de la façon dont la loi est énoncée : décrit-elle avec assez de précision les genres d'atteintes à la dignité qui *devraient* donner ouverture à des recours en justice, ou va-t-elle trop loin? Toutefois, on ne peut vérifier si le délit civil est nécessaire en se contentant d'examiner sa formulation. Les recours établis en responsabilité délictuelle comportent certainement des failles qu'un délit civil d'atteinte au droit à la vie privée serait susceptible de combler. Aux yeux des adversaires du délit, toutefois, ces failles sont petites et tolérables.

Il faut peut-être ajouter que si l'on conclut, à la suite de ces consultations, qu'on *ne doit pas* créer de délit civil d'atteinte au droit à la vie privée, il y aurait peut-être lieu d'examiner de nouveau la jurisprudence à ce propos et de se demander si son évolution future au Nouveau-Brunswick devrait être tuée dans l'œuf. Mais cette décision peut attendre.

« S'il devait exister un délit civil d'atteinte au droit à la vie privée, il appartient aux tribunaux, plutôt qu'au législateur, de l'établir. »

Même si l'argument à ce sujet porte surtout sur la méthode, il concerne aussi certaines questions de fond.

Lorsque les tribunaux créent des délits civils, ils procèdent étape par étape, une affaire à la fois. Au fur et à mesure qu'ils rendent des décisions, ils dégagent des similitudes et des fils conducteurs. Les tribunaux déduisent parfois de nouveaux principes en examinant de vieilles décisions sous un jour nouveau. Cette façon de procéder présente l'avantage de permettre une évolution graduelle du droit, puisque chaque décision découle d'une série de faits qui illustrent ce dont est réellement constitué le délit civil. Par contre, cette méthode présente l'inconvénient de faire évoluer le droit lentement et de façon imprévisible. Tout dépend des faits que les plaideurs exposent aux tribunaux et des décisions que les juges rendent à la lumière de ces faits.

La jurisprudence semble suffisamment abondante au Canada à l'heure actuelle pour permettre aux tribunaux du Nouveau-Brunswick d'élaborer un délit civil d'atteinte au droit à la vie privée si des affaires idoines leur sont présentées. Par contre, ils peuvent décider de ne pas le faire. Il se peut qu'ils donnent crédit à l'argument selon lequel un délit civil général d'atteinte au droit à la vie privée est tout simplement trop vague pour être acceptable. Ils peuvent aussi décider que d'autres délits civils offrent un cadre juridique plus opportun pour le règlement des litiges en instance. Chaque affaire donnera lieu à l'énoncé de motifs circonstanciés justifiant la décision. Si la jurisprudence ne parvient pas à établir un délit civil d'atteinte à la vie privée, il se peut que l'expérience montre que le délit envisagé était entaché de lacunes trop importantes pour être comblées.

La décision, le cas échéant, de laisser les tribunaux élaborer le délit civil d'atteinte au droit à la vie privée dénote une préférence pour l'approche graduelle du développement du droit dans ce domaine, une attitude de temporisation et une reconnaissance du fait que les résultats de l'exercice pourraient être différents de ceux que l'on jugeait souhaitables à l'origine. Cette façon de procéder s'applique non seulement à la question de savoir s'il faut ou non reconnaître le délit civil, mais aussi à ses éléments s'il est reconnu. Par exemple, quant à savoir si une personne morale a une « vie privée » à laquelle on peut « porter atteinte », le tribunal pourrait arriver à une conclusion tout à fait différente de celle que nous avons décrite dans le présent document.

On aura peut-être intérêt à adopter une attitude de temporisation en cas d'ambivalence fondamentale quant au bien-fondé de l'existence d'un délit civil d'atteinte au droit à la vie privée ou quant à sa description. Dans le contexte actuel, il semble probable qu'un délit civil d'atteinte au droit à la vie privée se dégagera de la jurisprudence (certains diraient même qu'il est déjà établi, même s'il n'est pas encore élaboré), mais nul ne peut prédire l'avenir. La seule façon de s'assurer que le délit civil existe bel et bien consiste à adopter une loi en ce sens. Cependant, si la loi est mal formulée, on risque de freiner une évolution qui pourrait autrement se dérouler de façon plus satisfaisante par la jurisprudence. C'est la critique qui a été formulée, par exemple, à l'égard de l'expression « intentionnellement et sans apparence de droit » qui qualifie « l'atteinte au droit à la vie privée » susceptible de donner ouverture à une poursuite en vertu de certaines lois canadiennes sur la protection de la vie privée.

Proposition 42

Les grandes questions à être examinées dans le cadre des consultations publiques sont les suivantes :

a) L'atteinte à la vie privée devrait-elle constituer un délit civil?

b) Une loi fondée sur la loi uniforme décrirait-elle adéquatement l'atteinte au droit à la vie privée de façon à ne pas mettre en péril des activités désirables?

c) La prudence exige-t-elle que l'élaboration du délit civil soit confiée aux tribunaux, plutôt qu'au législateur?

B. Recours non judiciaires en cas de violation du droit à la vie privée

Dans la présente partie du document, nous examinerons si des recours non judiciaires (recours dispensés par un organisme administratif ou un agent, plutôt qu'un tribunal) devraient être prévus en cas de violation du droit à la vie privée. L'expression « vie privée » est toujours utilisée ici dans son sens large, conformément à la définition qu'en fait le Comité permanent des droits de la personne et de la condition des personnes handicapées de la Chambre de communes, qui la considère comme un droit fondamental de la personne qui englobe l'intimité physique, la protection des renseignements personnels, la protection contre la surveillance, la protection des communications personnelles et la protection de l'espace personnel. On emploie le mot « violation » pour établir une distinction par rapport à la notion d'atteinte examinée dans la partie précédente. On y décrivait l'atteinte à la vie privée comme une conduite suffisamment inacceptable pour donner droit à la partie lésée aux recours judiciaires en jugement déclaratoire, en injonction et en dommages-intérêts. Par contre, la violation de la vie privée pourrait désigner une réalité plus globale. Tout acte qui ne tient pas suffisamment compte de la vie privée d'autrui pourrait, par exemple, être qualifié de violation de la vie privée. Cependant, toutes les violations de la vie privée n'équivalent pas à une atteinte, qui est un délit civil.

L'emploi de cette terminologie permet de faire une distinction entre les deux raisons pour lesquelles on pourrait envisager de créer un recours non judiciaire en cas de violation de la vie privée. La première raison est la suivante : même dans les cas qui pourraient donner ouverture à un recours judiciaire, le recours non judiciaire pourrait être préférable pour des motifs de coûts, de commodité ou autres. Quant à l'autre, disons que dans certains cas, même si la conduite dont se plaint la personne n'équivaut pas à un délit civil, elle est suffisamment inacceptable pour qu'on puisse au moins disposer d'une façon de la dénoncer (qu'elle donne lieu ou non à une sanction) et de chercher à établir des normes pour l'avenir.

L'autre motif qui nous incite à examiner les recours non judiciaires en cas de violation de la vie privée dans le cadre du présent document est que la même question a été étudiée dans le contexte plus restreint de la protection des données. Il serait contraire à la logique de présumer, sans autre forme de discussion, que la protection des données est le seul contexte auquel pourraient convenir les recours non judiciaires. Certains pourraient même soutenir que les recours non judiciaires se prêtent mieux à la protection du droit à la vie privée en général qu'à la seule protection des données. Ils ajouteraient sans doute que les recours non judiciaires en matière de protection des renseignements pourraient facilement être inclus dans un mandat plus vaste de protection de la vie privée.

Dans la présente partie, la discussion ressemblera sous certains aspects à celle de la partie I. Des questions comparables se posent quant à ce que pourrait faire un organisme administratif et à ce que pourraient être ses pouvoirs. Mais sous d'autres aspects les questions sont différentes. Lors de l'examen des recours administratifs, on a tenu pour acquis qu'il fallait assurer le respect d'une série de règles établies – les pratiques convenables du code de la CSA – et on s'est demandé si les tribunaux, un organisme administratif ou les deux devaient faire ce travail. En matière de violation du droit à la vie privée, cependant, la discussion ne porte sur aucune série de règles établies.

B.1 Violation de la vie privée

Une question qui se pose à ce sujet consiste à déterminer l'aspect de la violation de la vie privée qui pourrait être assujetti aux recours non judiciaires. Les violations de la vie privée revêtent toutes sortes de formes selon le moment. L'une des sources de plaintes les plus classiques concerne les activités importunes des journalistes et des photographes. Plus récemment, on s'est inquiété au sujet d'un certain nombre de questions relatives au lieu de travail. Par exemple, des employeurs ont exigé que leurs employés subissent des tests de dépistage de drogues ou se prêtent au polygraphe. On s'interroge aussi pour savoir si les employeurs devraient avoir accès au courrier électronique de leurs employés, qui pourrait contenir des messages personnels, et on se demande quels genres de mécanismes de surveillance du rendement seraient acceptables. L'utilisation croissante de dispositifs secrets ou apparents de surveillance dans les lieux publics comme dans les endroits privés suscite aussi ouvertement des inquiétudes au sujet de ce que certains considèrent être la perte progressive du droit à la vie privée dans la société moderne.

De plus, les gens divergent d'opinions en ce qui concerne les questions qui revêtent ou non de l'importance en matière de vie privée. L'affichage des appels sur les appareils téléphoniques pourrait être un exemple. Certaines personnes s'opposent, d'autres pas, à ce que leur nom ou le numéro de téléphone de l'endroit d'où elles appellent soient automatiquement affichés sur l'appareil de leur interlocuteur. On peut aussi penser au démarchage téléphonique, que certains jugent être une violation de leur vie privée. D'autres le considèrent inoffensif, mais pourraient changer d'avis si les appels de cette nature se multipliaient.

Au delà d'exemples précis, on peut soutenir que la vie privée en soi est toujours l'objet de préoccupations; même si on ne peut définir précisément le genre de conduite qui l'objet des préoccupations du moment à une époque donnée, on peut avoir la certitude que le débat se poursuit. Par conséquent, l'adoption d'un recours non judiciaire en cas de violation de la vie privée pourrait à tout moment être à la disposition des justiciables pour leur permettre de régler les questions de l'heure.

Proposition 43

Un grand nombre de questions actuelles et potentielles en matière de protection de la vie privée échapperaient à la portée du recours judiciaire en cas d'atteinte à la vie privée et du recours non judiciaire créé en vertu une loi sur la protection des données.

B.2 Au-delà de la sanction sociale?

Il est possible d'être d'accord avec tout ce qui a été exposé jusqu'à maintenant dans la présente partie du document, tout en demeurant incapable de conclure à la nécessité de créer un recours non judiciaire en cas de violation de la vie privée. On peut convenir que les questions relatives à la vie privée ont toujours été, sont encore et continueront d'être d'actualité sans pour autant conclure qu'il faut adopter des lois ou mettre sur pied des bureaucraties pour les régler. La véritable sanction rattachée à la violation de la vie privée, de

ce point de vue, est la sanction sociale (les pratiques douteuses disparaîtront si suffisamment de gens les trouvent inadmissibles), et la mesure réelle de la violation de la vie privée est la vigueur ou l'absence de vigueur de la réaction sociale (si trop peu de gens s'y opposent, l'acte en question ne constitue pas une violation de la vie privée à la lumière des normes sociales de l'époque).

La vaste portée de la notion de violation de la vie privée peut être perçue par certains comme un appel à la prudence. Un nombre si effarant de paroles et de gestes à l'égard d'autrui pourraient être perçus (à notre insu, bien sûr) comme des violations de la vie privée. La création d'un recours non judiciaire pourrait être considérée comme une ouverture à une foule de plaintes, dont bon nombre porteraient sur des actes avec lesquels les gens doivent simplement apprendre à composer dans le cadre de la vie en société.

Dans un rapport intitulé *Report on the Law of Privacy,* qui a été rédigé en 1973 à l'intention du parlement de New South Wales, en Australie, W.L. Morrison a saisi l'ambiguïté qui caractérise ce débat :

> Le grand dilemme auquel doivent faire face les organismes auxquels on demande de formuler des recommandations et les législateurs qui doivent se prononcer sur des projets de loi a toujours été le fait que les propositions qui leur sont présentées accordent un niveau exceptionnel de discrétion à ces organismes auxquels on confierait la mise en œuvre et l'application de la loi. Étant donné que ces organismes sont inévitablement eux-mêmes de nature gouvernementale, de telles mesures législatives soulèvent toujours la perspective d'une nouvelle ingérence arbitraire de la part du gouvernement dans les libertés de la personne, laquelle contrebalancerait les avantages que présentent intrinsèquement lesdites mesures législatives en matière de protection de la vie privée. (...) La grande discrétion dont jouissent les responsables de la mise en œuvre des mesures législatives proposées est attribuable à l'incapacité de ceux qui les conçoivent de cerner avec suffisamment de précision les problèmes qui se manifesteront dans un domaine si vaste ainsi que les mesures précises à prendre pour y faire face. Par conséquent, on se contente de renvoyer la balle à l'organisme subalterne prévu par la loi (trad. p. 15).

Le rapport Morrison recommandait toutefois la création d'un recours non judiciaire en cas de violation de la vie privée sous la forme d'un mécanisme non intrusif qui ressemble à celui de l'Ombudsman et qui est assorti du mandat nécessaire pour conseiller, informer, faire enquête et concilier, mais qui n'exerce aucun pouvoir de coercition. Cette recommandation a donné lieu à la mise sur pied du New South Wales Privacy Committee, qui sera abordé plus amplement ci-dessous.

La question consiste donc de savoir si la protection de la vie privée dans son sens large devrait être assurée par les citoyens eux-mêmes dans le cadre de leurs interactions sociales, ou si elle suscite des préoccupations telles que l'on doive faire appel à un organisme officiel d'une forme quelconque pour influencer les pratiques des citoyens, des organisations

ou de la société dans son ensemble. Si l'ensemble de la société ou des groupes particuliers ont besoin de conseils au sujet des normes convenables en matière de respect de la vie privée ou si des particuliers ont besoin d'aide en vue de régler un différend privé, les recours non judiciaires pourraient être tout indiqués. Par contre, si on décide que les violations de la vie privée relèvent des interactions sociales, la création de recours non judiciaires serait inopportune.

Proposition 44

La principale question en vue des discussions publiques consiste à savoir si les violations de la vie privée relèvent des interactions sociales ou si l'intervention d'un organisme officiel serait de nature à assurer le respect de la vie privée de chacun.

B.3 Modèles possibles

Il y a plusieurs façons de constituer un organisme non judiciaire de protection de la vie privée. Le New South Wales Privacy Committee de l'Australie en offre un exemple. Voici ce qu'énonce la page Web du comité (http://www.agd.nsw.gov.au/privacy.html) :

> (trad.) Le comité est un organisme prévu par la loi de New South Wales qui a été créé en 1975 en vertu du Privacy Committee Act et qui a pour mandat de faire enquête au sujet des questions relatives à la vie privée qui touchent les habitants de New South Wales. Le comité a un rôle semblable à celui d'un ombudsman; il n'assure le respect d'aucune mesure législative en matière de protection de la vie privée.
>
> Le comité s'occupe de promouvoir et de protéger le droit à la vie privée grâce aux moyens suivants :
>
> Il conseille les particuliers, les organismes gouvernementaux et les organisations commerciales sur les lignes de conduite à adopter afin de protéger le droit à la vie privée;
>
> Il fait des recherches au sujet des développements importants dans les domaines des politiqes, de la loi et de la technologie qui ont une incidence sur la vie privée, et il présente des rapports et des recommandations aux autorités concernées
>
> Il fait des enquêtes et, dans les cas qui le permettent, il joue le rôle de conciliateur relativement aux plaintes portant sur des atteintes au droit à la vie privée; de plus, il répond aux demandes de renseignements de la collectivité et il éduque celle-ci relativement aux questions ayant trait à la vie privée.

Au Québec, la structure juridique est tout à fait différente, mais les résultats peuvent parfois se ressembler - à moins que l'on ne considère que la protection des données. La Commission des droits de la personne et de la jeunesse y a la responsabilité de promouvoir la *Charte des droits et libertés de la personne* du Québec, dont l'article 5 énonce que « toute personne a droit au respect de sa vie privée ». La promotion que doit faire la commission de

l'article 5 (et d'autres dispositions de la charte) donne lieu à des activités d'éducation publique et d'analyse des lois et politiques. La commission formule aussi des opinions sur les questions qui sont soumises à son attention et elle les fait parvenir aux parties concernées; elle a en outre le pouvoir d'intervenir dans des litiges entre des tiers qui mettent en cause l'interprétation de la charte. Toutefois, elle n'a aucun pouvoir d'enquête en bonne et due forme en ce qui concerne les violations de la vie privée en tant que telles. Elle peut tenter d'aider les parties sans formalités et d'agir comme organisme de conciliation quand des différends lui sont présentés, mais son mécanisme officiel de traitement des plaintes ne concerne que les cas de discrimination. Les questions relatives à la vie privée peuvent parfois s'immiscer dans des plaintes fondées sur la discrimination (par exemple, les plaintes à la suite du dépistage médical des maladies héréditaires peuvent être fondées à la fois sur la discrimination et sur une violation de la vie privée), mais lorsqu'elle est en présence d'un différend portant uniquement sur le respect de la vie privée, la commission est dépourvue de pouvoirs.

Par contre, la Commission d'accès à l'information du Québec, qui est distincte de la précédente, est dotée d'un mandat qui se limite à la protection des données, mais elle exerce un vaste pouvoir qui lui permet de recommander ou d'ordonner la mise en œuvre de mesures de réparation; ses ordonnances sont exécutoires au même titre que les ordres d'un tribunal.

Si l'on juge souhaitable de créer un recours non judiciaire en cas de violation de la vie privée au Nouveau-Brunswick, on pourrait soit mettre sur pied un tout nouveau recours, soit élargir le mandat d'un organisme existant. Parmi les organismes en place, la Commission des droits de la personne du Nouveau-Brunswick est le candidat le plus évident, étant donné que le droit à la vie privée fait partie des droits fondamentaux reconnus à l'échelle internationale. Cette décision modifierait cependant le mandat de la commission de façon considérable. À l'heure actuelle, elle ne s'occupe que des plaintes en matière de discrimination fondées sur divers motifs énumérés et dans des contextes particuliers. Néanmoins, si on doit choisir un organisme existant, le rôle que joue la commission en matière de droits de la personne semble naturellement correspondre au droit de la personne à la protection de sa vie privée.

Le fait de confier à la commission un mandat à l'égard de la protection de la vie privée est aussi de nature à réactiver les pouvoirs dont elle dispose en matière de mise en œuvre. Parmi ceux-ci, mentionnons le pouvoir d'éduquer et d'informer ainsi que ceux de faire enquête et de jouer le rôle de médiateur dans les dossiers de plaintes. Si la médiation échoue, la commission a alors le pouvoir de demander au ministre responsable de tenir une enquête officielle à l'issue de laquelle des ordonnances exécutoires pourront être prononcées. La commission peut aussi intenter des poursuites avec l'autorisation du ministre. Toutefois, si on décidait que ces pouvoirs ne conviennent pas aussi bien en matière de violations de la vie privée que dans le cadre du mandat actuel de la commission à l'égard de la discrimination, on devrait effectuer les modifications législatives nécessaires.

Par contre, si on créait un nouveau recours, on aurait le choix entre toutes les possibilités. On pourrait songer à un organisme de protection de la vie privée doté de pouvoirs obligatoires. Un organisme du genre de l'Ombudsman, à l'image du New South Wales Privacy Committee, serait une autre possibilité. On pourrait aussi choisir de ne pas établir d'organisme permanent et de mettre sur pied à la place un mécanisme en vertu duquel

une personne pourrait être désignée pour entendre les plaintes de violation de la vie privée au fur et à mesure qu'elles sont déposées.

Les possibilités ressemblent à celles que nous avons décrites dans la partie I en ce qui concerne les recours administratifs dans le cadre des mesures législatives sur la protection des données. Il est aussi important de régler la question de savoir si le mandat de l'organisme se limiterait au traitement des plaintes, et de déterminer le rôle que joueraient, le cas échéant, les pouvoirs obligatoires dans ce contexte. Certaines personnes remettront en doute la valeur d'un groupe comme le New South Wales Privacy Committee en raison du fait qu'ils sont dépourvus de pouvoir lorsqu'ils en auraient le plus besoin. Par contre, l'explication que donne W.L. Morrison de la difficulté de déléguer des pouvoirs obligatoires à un organisme doté d'un vaste mandat flou en matière de protection de la vie privée a un certain poids.

Les dispositions de la *Loi sur les droits de la personne* du Nouveau-Brunswick représentent un compromis intéressant. La responsabilité prépondérante de la commission consiste à faire enquête au sujet des plaintes formulées en vertu de l'article 17 et à s'efforcer de régler la question qui fait l'objet de la plainte [par. 18(1)]. La commission n'a pas le pouvoir autonome de pénétrer dans les lieux, d'inspecter les registres ou d'exiger la production d'éléments de preuve, mais un juge de la Cour provinciale peut l'autoriser à désigner une personne qui exercera ces pouvoirs dans le but d'obtenir le règlement d'un litige (articles 18, 19 et 19.1). La commission ne peut tenir des audiences de son propre chef. Elle doit demander au ministre concerné de décréter la tenue d'une audience. C'est la commission d'enquête (et non la commission elle-même) qui délivrera les ordonnances, lesquelles peuvent être déposées à la Cour du Banc de la Reine et être exécutées comme si elles étaient des ordres du tribunal (art. 21).

Certaines personnes peuvent conclure que cette approche assure un juste équilibre entre le rôle essentiellement conciliatoire et la *possibilité* de faire appel au besoin à des mesures coercitives. (Elles ajouteraient peut-être qu'un mécanisme semblable pourrait convenir à un organisme spécialisé dans la protection des données si, en dernière analyse, on décidait de d'y limiter les recours administratifs). Par contre, on pourrait soutenir qu'il n'existe pas de juste milieu entre la présence et l'absence de pouvoirs obligatoires et que même si des dispositions comme celles de la *Loi sur les droits de la personne* semblent adoucir l'élément obligatoire, les apparences sont trompeuses.

Proposition 45

On pourrait s'inspirer de modèles existants pour créer des recours non judiciaires en cas d'atteinte au droit à la vie privée. Comme c'était le cas pour les recours en matière de protection des renseignements, les principales questions qui devraient être soumises au débat public sont les suivantes :

a) Les recours non judiciaires devraient-ils être accompagnés de pouvoirs obligatoires?

b) Le rôle de l'organisme devrait-il se limiter au traitement des plaintes?

Conclusion

Les divers choix législatifs décrits dans le présent document sont à la fois indépendants et potentiellement interdépendants. Chacun peut être considéré isolément, et l'ensemble, l'un ou l'autre ou toute combinaison d'entre eux pourra être mis en vigueur. Il se peut aussi qu'aucune des mesures décrites dans le document ne soit adoptée et que l'on puisse tout de même soutenir que la vie privée est aussi bien protégée que nécessaire au Nouveau-Brunswick. Chacun de ces choix sera commenté brièvement en commençant par le dernier.

Le fait de n'adopter aucune nouvelle mesure législative sur la protection de la vie privée signifierait qu'on n'a pas besoin d'une loi sur la protection des données dans le secteur privé, que les protections prévues en *common law* au chapitre de la vie privée (y compris le délit civil d'atteinte à la vie privée qui est appelé à évoluer) sont adéquates et que les recours non judiciaires en cas de violation de la vie privée en général ne sont pas utiles. Le premier élément de cette proposition fait probablement ressortir que l'autoréglementation et le jeu des rapports sociaux suffisent à eux seuls en matière de protection des données - où bien qu'ils réussiront aussi bien qu'une loi. Le second élément de la proposition est probablement axé sur le champ d'application des délits civils actuels ainsi que sur les préoccupations que susciterait le caractère évolutif de tout nouveau délit civil d'atteinte à la vie privée. Le troisième élément, quant à lui, est probablement fondé sur l'argument voulant que les violations de la vie privée devraient rester en grande partie du ressort des interactions sociales et qu'un organisme de protection de la vie privée doté d'un vaste mandat serait un remède pire que le mal.

Une deuxième possibilité consisterait à opter pour l'un des choix législatifs décrits dans le présent document de préférence aux autres. La mise en œuvre de mesures législatives ne visant que la protection des données signalerait, en soi, qu'il s'agit du seul aspect que le jeu des rapports sociaux n'arrive plus à protéger adéquatement. L'adoption de mesures législatives portant uniquement sur le délit civil pourrait être perçue comme la seule véritable protection qui mérite d'être reconnue *par la loi;* on peut en effet soutenir qu'une telle loi viserait l'aspect essentiel de la protection des données et de celle de la vie privée . Enfin, le fait de créer un recours non judiciaire de vaste portée en cas de violation de la vie privée pourrait être perçu comme une réponse complète en soi; étant donné que l'organisme pourrait s'intéresser à *tous* les aspects de la protection de la vie privée, on n'aurait besoin de rien de plus, en toute logique.

On peut aussi justifier la combinaison de deux des choix, tout comme celle des trois choix. Les trois sont en effet combinés dans la loi actuelle du Québec, qui s'est doté d'une Commission d'accès à l'information traitant des questions relatives à la protection des données dans le secteur public et dans le secteur privé, d'un délit civil en cas d'atteinte à la vie privée en général en vertu du *Code civil* et de délits civils particuliers axés sur les éléments fondamentaux des principes de protection des données, ainsi que d'une Commission des droits de la personne dotée d'un vaste mandat en matière de protection de la vie privée en vertu de la *Charte des droits et libertés de la personne* du Québec.

Quelle voie le Nouveau-Brunswick doit-il emprunter? Le débat est dorénavant lancé.

ANNEXE A

RÉSUMÉ DES PROPOSITIONS

I. Protection des données dans le secteur privé

A. Doit-on légiférer dans le secteur privé?

Proposition 1

Les objectifs généraux des initiatives en matière de protection des données sont louables. Les grandes questions à être examinées dans le cadre des consultations publiques sont les suivantes:

a) L'adoption d'une loi est-elle la bonne façon de réaliser ces objectifs?

b) La loi atteindrait-elle ses objectifs?

c) Les avantages de l'adoption d'une loi justifient-ils les coûts et les restrictions qui en découleraient?

B. Quel pourrait être le contenu des mesures législatives sur la protection des données ?

Proposition 2

La possible loi sur la protection des données dans le secteur privé devrait s'inspirer du *Code type sur la protection des renseignements personnels* de l'Association canadienne de normalisation.

Proposition 3

Une loi sur la protection des données devrait adopter dans la mesure du possible les dix principes de la CSA tels que formulés dans le code. Les définitions, les notes et les commentaires du code de la CSA devraient être utilisés comme matériel de référence pour l'élaboration de la loi sur la protection des données, mais leurs éléments essentiels pourraient être adoptés en tout état de cause.

B.1 La portée d'une loi sur la protection des données

a. À qui la loi s'applique-t-elle?

Proposition 4

Une loi sur la protection des données pourrait s'appliquer à tous les organismes constitués ou non en personnes morales ainsi qu'aux particuliers lorsqu'ils recueillent et utilisent des renseignements personnels à des fins autres que leurs fins personnelles ou domestiques.

b. Qu'entend-on par renseignements personnels?

Proposition 5

Une loi sur la protection des données pourrait s'inspirer de la définition que donne le code de la CSA des renseignements personnels; elle traiterait donc des renseignements concernant un individu identifiable enregistrés sous quelque forme que ce soit.

B.2 Les principes de la CSA

Premier principe de la CSA – Responsabilité

Un organisme est responsable des renseignements personnels dont il a la gestion et doit désigner une ou des personnes qui devront s'assurer du respect des principes énoncés ci-dessous.

Proposition 6

À moins qu'une personne soit désignée conformément au premier principe de la CSA, la personne responsable d'assurer le respect de la loi au sein d'un organisme devrait être :

a) le chef de la direction, si ce poste existe au sein de l'organisme; ou

b) la ou les personne(s) qui dirigent les activités de l'organisme, si le poste de chef de la direction n'existe pas au sein de celui-ci.

Deuxième principe de la CSA – Détermination des fins de la collecte des renseignements

Les fins pour lesquelles des renseignements personnels sont recueillis doivent être déterminées par l'organisme avant ou au moment de la collecte.

Proposition 7

Les fins pour lesquelles un organisme recueille des renseignements personnels doivent être licites et se rattacher directement à une de ses activités existantes ou proposées.

Proposition 8

Le deuxième principe de la CSA pourrait être accompagné d'une obligation pour l'organisme de documenter les fins pour lesquelles il tient un système d'enregistrement des renseignements personnels; dans ce cas, cette obligation ne s'appliquerait pas lorsque le fait de documenter les fins ne serait d'aucune utilité au contrôle administratif.

Proposition 9

Si les fins documentées de l'organisme ne correspondent pas aux explications qu'il fournit à la personne, ces dernières prévaudront conformément au troisième principe de la CSA relatif au consentement.

Troisième principe de la CSA – Consentement

Toute personne doit être informée et consentir à toute collecte, utilisation ou communication de renseignements personnels qui la concernent, à moins qu'il ne soit pas approprié de le faire.

a. Formulation

Proposition 10

Le troisième principe de la CSA porte essentiellement sur le consentement. Une loi sur la protection des données ne doit pas faire de l'obligation d'informer la personne un critère distinct et indépendant auquel devraient satisfaire les organismes.

b. Consentement exprimé et consentement implicite

Proposition 11

Une loi sur la protection des données doit inclure la notion de consentement implicite fondé sur les attentes raisonnables de la personne.

Proposition 12

Les mesures pour lesquelles un consentement peut être tacite sont celles que le particulier devrait raisonnablement s'attendre à voir prendre par l'organisme, et qu'il n'est pas susceptible de désapprouver, eu égard à

a) la nature des renseignements personnels en question, y compris la question de savoir si les renseignements ont ou non une nature sensible ou confidentielle,

b) tout avantage ou inconvénient pour le particulier,

c) toute explication que l'organisme a donnée des mesures qu'il entend prendre,

d) toute indication que le particulier a donnée de ses désirs réels, et

e) la facilité ou la difficulté avec laquelle les désirs réels du particulier peuvent être identifiés.

c. Quand l'obtention du consentement ne serait pas appropriée?

Proposition 13

Le consentement ne devrait pas être nécessaire lorsqu'un organisme recueille, utilise ou divulgue des renseignements personnels

a) pour protéger la santé ou la sécurité du public ou d'un particulier,

b) aux fins d'une enquête liée à l'exécution d'une mesure législative,

c) pour protéger ou affirmer ses propres droits légaux, y compris des droits légaux contre le particulier,

d) pour vérifier auprès d'un organisme gouvernemental l'admissibilité du particulier à un programme ou à une prestation pour lequel le particulier a fait une demande à l'organisme en question,

e) pour les fins de toute recherche légitime faite dans l'intérêt de la science, de l'enseignement ou de l'ordre public ou pour des travaux d'archives,

f) tel que requis ou expressément autorisé par la loi, ou

g) pour toute autre raison importante dans l'intérêt du public, qu'elle soit ou non semblable à celle des alinéas a) à f).

Avant de recueillir, d'utiliser ou de divulguer des renseignements personnels sans consentement, un organisme doit prendre en considération la nature des renseignements en question et la fin des mesures qu'il prend, et doit se convaincre que dans les circonstances cette fin justifie les mesures projetées.

Toute collecte, toute utilisation ou toute divulgation de renseignements personnels sans consentement doit se limiter aux exigences raisonnables de la situation.

Quatrième principe de la CSA – Limitation de la collecte
L'organisme ne peut recueillir que les renseignements personnels nécessaires aux fins déterminées et doit procéder de façon honnête et licite.

Proposition 14

Une loi sur la protection des données devrait énumérer les sources auprès desquelles les renseignements personnels peuvent être recueillis, et prévoir qu'il est interdit de refuser de fournir à une personne des biens ou des services sous prétexte qu'elle n'a pas consenti à transmettre des renseignements personnels qui ne sont pas essentiels aux fins énoncées de l'organisme.

L'exigence selon laquelle les organismes sont tenus de recueillir des renseignements personnels de façon honnête et licite n'a pas à être expliquée davantage dans la loi sur la protection des renseignements.

Cinquième principe de la CSA – Limitation de l'utilisation, de la communication et de la conservation

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

a. Formulation

Proposition 15

Le cinquième principe de la CSA devrait permettre les utilisations et les communications qui sont autorisées expressément par la loi en plus de celles qui sont exigées par la loi.

b. Interdépendance entre les fins, le consentement et la loi

Proposition 16

Il n'est pas nécessaire que la loi sur la protection des données élabore au sujet de la relation entre les fins, le consentement et la loi comme justifications équivalentes de l'utilisation et de la communication de renseignements personnels.

c. Conservation

Proposition 17

Une loi sur la protection des données devrait spécifier clairement que l'organisme peut satisfaire à son obligation de ne pas conserver indûment des renseignements personnels s'il conserve ceux-ci sous une forme rendant impossible l'identification des personnes auxquelles ils se rapportent.

Proposition 18

On ne devrait pas exiger des organismes qu'ils éliminent de leurs fichiers de renseignements de nature non personnelle tous les renseignements personnels qui pourraient s'y trouver à titre incident.

Sixième principe de la CSA – Exactitude

Les renseignements personnels doivent être aussi exacts, complets et à jour que l'exigent les fins pour lesquelles ils sont utilisés.

Proposition 19

Le sixième principe de la CSA est suffisamment explicite. Il ne sera pas nécessaire d'inclure dans une loi sur la protection des données des dispositions additionnelles relatives à son interprétation et à son application.

Septième principe de la CSA – Mesures de sécurité

Les renseignements personnels doivent être protégés au moyen de mesures de sécurité correspondant à leur degré de sensibilité.

a. Formulation

Proposition 20

Qu'on retire l'expression « mesures de sécurité » du septième principe de la CSA de sorte à éviter d'en réduire la portée.

b. Quels genres de dispositifs de protection?

Proposition 21

Une loi sur la protection des données devrait prévoir que les dispositifs de protection qui seront mis en œuvre comprennent la formation, des moyens matériels ainsi que des mesures administratives et techniques, selon ce que commandent les circonstances. La loi ne devrait pas tenter de définir de quelle façon un dispositif de protection peut correspondre à la sensibilité des renseignements.

c. Transfert vers des tiers

Proposition 22

Une loi sur la protection des données devrait établir clairement que des dispositifs de protection correspondant au degré de sensibilité des renseignements personnels peuvent être nécessaires lorsqu'un organisme transfère des renseignements à un autre organisme; elle ne devrait cependant pas prescrire la forme des dispositifs de protection requis.

Huitième principe de la CSA – Transparence

Un organisme doit mettre à la disposition de toute personne des renseignements précis sur ses politiques et ses pratiques concernant la gestion des renseignements personnels.

Proposition 23

Le huitième principe de la CSA est suffisamment explicite; une loi sur la protection des données ne doit pas chercher à le clarifier davantage.

Neuvième principe de la CSA – Accès aux renseignements personnels

Un organisme doit informer toute personne qui en fait la demande de l'existence de renseignements personnels qui la concernent, de l'usage qui en est fait et du fait qu'ils ont été communiqués à des tiers, et lui permettre de les consulter. Il sera aussi possible de contester l'exactitude et l'état complet des renseignements et d'y faire apporter les corrections appropriées.

a. Formulation

Proposition 24

Les mots « à moins qu'il ne soit pas approprié de le faire » devraient être ajoutés au droit à l'information prévu dans le neuvième principe de la CSA.

b. La nature du droit

Proposition 25

Une loi sur la protection des données devrait établir clairement que le fait de fournir *l'information* suffit à l'organisme pour se décharger de l'obligation que lui impose le neuvième principe, à moins que la personne ne réclame spécifiquement l'accès aux documents.

c. Exceptions au droit d'accès

Proposition 26

L'organisme ne devrait pas être tenu de divulguer des renseignements personnels à la personne concernée :

a) lorsque la divulgation serait préjudiciable à la santé ou à la sécurité du public ou d'un particulier, y compris de la personne qui présente la demande d'accès;

b) lorsque la divulgation entraverait le cours d'une enquête liée à l'application d'une loi;

c) lorsque la non-divulgation est exigée ou expressément autorisée par la loi ou lorsque la personne n'aurait pas le droit d'obtenir les renseignements dans le cadre d'une instance judiciaire;

d) lorsque les renseignements ont été fournis par un tiers sous le sceau de la confidence ou sont de nature confidentielle;

e) lorsque les renseignements demandés sont inextricablement liés à des renseignements personnels concernant un tiers;

f) lorsqu'il serait indûment dispendieux ou fastidieux de fournir les renseignements demandés;

On devrait envisager d'autoriser la non-divulgation lorsqu'il existe un autre motif légitime et substantiel de refuser l'accès aux renseignements demandés.

Les cas de non-divulgation devraient se limiter aux exigences raisonnables de chacune des situations. S'il peut expliquer le contenu des renseignements qu'il refuse de divulguer sans pour autant porter atteinte aux motifs pour lesquels ils ne sont pas divulgués, l'organisme devrait le faire.

d. Modalités

Proposition 27

Une loi sur la protection des données pourrait être muette au sujet des mécanismes d'accès prévus dans le neuvième principe de la CSA.

e. Corrections

Proposition 28

Si la personne remet en question l'exactitude ou le caractère exhaustif des renseignements sans réussir à convaincre l'organisme, celui-ci devrait prendre note du fait que la personne conteste les renseignements concernés.

Dixième principe de la CSA –
Possibilité de porter plainte contre le non-respect des principes

Toute personne doit être en mesure de se plaindre du non-respect des principes énoncés ci-dessus en communiquant avec le ou les individus responsables de les faire respecter au sein de l'organisme concerné.

Proposition 29

Un organisme devrait être tenu de faire enquête de bonne foi au sujet des plaintes qu'il reçoit et de prendre les mesures qui s'imposent quand il conclut qu'une plainte est fondée.

B.3 Autres enjeux

a. Codes sectoriels

Proposition 30

Les codes sectoriels ne devraient pas avoir force de loi en vertu d'une loi sur la protection des données. Celle-ci devrait édicter le pouvoir de faire les règlements qui, le cas échéant, pourraient contenir des dispositions plus précises à l'égard du genre d'organismes, de renseignements ou d'activités concerné.

b. Application de la loi

Le recours pénal

Proposition 31

Une loi sur la protection des données pourrait énoncer que toute atteinte intentionnelle aux troisième (consentement), quatrième (limitation de la collecte), cinquième (limitation de l'utilisation, de la communication et de la conservation) et neuvième (accès aux renseignements personnels) principes de la CSA constitue une infraction.

Le recours civil

Proposition 32

À moins qu'une loi sur la protection des données ne prévoie des recours administratifs qui rendent superflus les recours civils, les justiciables devraient pouvoir se prévaloir du jugement déclaratoire, de l'injonction et de l'action en dommages-intérêts à titre de mesures d'application de la loi. Toutefois, on ne devrait permettre l'octroi de dommages-intérêts que lorsque la violation de la loi par l'organisme entraîne une perte et satisfait un autre critère, comme celui de l'incompatibilité manifeste avec la loi.

Le recours administratif

Proposition 33

La création de recours administratifs n'est pas essentielle à une loi sur la protection des données; mais elle représente un choix politique. Les grandes questions à être examinées dans le cadre des consultations publiques sont les suivantes :

a) Les recours judiciaires sont-ils suffisants et convenables?

b) La création d'un mécanisme administratif de traitement des plaintes sans pouvoir de contrainte serait-elle utile?

c) Le fait d'assortir le mécanisme administratif de traitement des plaintes de pouvoirs de contrainte serait-il improductif ou exagéré?

d) Peut-on penser à une fonction qui ne serait pas axée sur les plaintes, qui serait substantielle et viable et qui justifierait à elle seule que l'on consacre des ressources à un organisme administratif ayant un mandat précis en matière de protection des données?

II. La vie privée en général

A. Recours judiciaires en cas d'atteinte à la vie privée

Proposition 34

L'examen de la création d'un délit civil d'atteinte au droit à la vie privée devrait être effectué à la lumière de la *Loi uniforme sur la protection de la vie privée* préparée par la Commission sur l'harmonisation des lois au Canada, compte tenu des recours judiciaires existants qui sont susceptibles de protéger le droit à la vie privée.

A.1 Recours existants

[Aucune proposition n'est présentée en cette matière.]

A.2 Un délit civil d'atteinte à la vie privée?

a. Atteinte à la vie privée

Proposition 35

L'atteinte au droit à la vie privée pourrait se définir comme suit :

Tout acte constitue une atteinte à la vie privée,

a) s'il s'immisce indûment dans les affaires personnelles ou les activités d'un particulier, qu'il se produise dans un endroit public ou en privé, ou

b) s'il donne une publicité indue à des renseignements concernant un particulier.

Proposition 36

Si une définition semblable à celle qu'énonce la proposition 35 se révèle trop restrictive, la loi sur la protection de la vie privée devrait au moins prévoir qu'un acte ou une conduite doit échouer le critère du « caractère déraisonnable » pour être qualifiée d'atteinte au droit à la vie privée.

Proposition 37

On devrait attendre les résultats des consultations au sujet des mesures législatives sur la protection des données dans le secteur privé avant de décider que le fait de « communiquer de façon illicite des renseignements au sujet d'un particulier » constitue un délit civil d'atteinte au droit à la vie privée.

b. Moyens de défense

Proposition 38

Pour l'essentiel, les moyens de défense énumérés à l'article 4 de la loi uniforme sont convenables.

c. Recours

Proposition 39

On devrait pouvoir se prévaloir des recours prévus à l'article 5 de la loi uniforme en cas d'atteinte au droit à la vie privée, même s'ils ne sont pas expressément intégrés à la loi.

Proposition 40

On pourrait à bon escient laisser les tribunaux élaborer les règles applicables au calcul des dommages-intérêts relatifs au délit civil d'atteinte au droit à la vie privée.

d. Questions d'ordre technique

Proposition 41

Les questions d'ordre technique relatives à la prescription, au fait que la Couronne soit ou non liée par la loi et à l'admissibilité de la preuve devraient être réglées en traitant le délit civil d'atteinte à la vie privée de la même façon que les autres délits civils. L'atteinte à la vie privée d'une personne décédée ne devrait donner ouverture à aucun droit d'action.

A.3 Légiférer ou ne pas légiférer?

Proposition 42

Les grandes questions à être examinées dans le cadre des consultations publiques sont les suivantes :

a) L'atteinte à la vie privée devrait-elle constituer un délit civil?

b) Une loi fondée sur la loi uniforme décrirait-elle adéquatement l'atteinte au droit à la vie privée de façon à ne pas mettre en péril des activités désirables?

c) La prudence exige-t-elle que l'élaboration du délit civil soit confiée aux tribunaux, plutôt qu'au législateur?

B. Recours non judiciaires en cas de violation du droit à la vie privée

B.1 Violation de la vie privée

Proposition 43

Un grand nombre de questions actuelles et potentielles en matière de protection de la vie privée échapperaient à la portée du recours judiciaire en cas d'atteinte à la vie privée et du recours non judiciaire créé en vertu une loi sur la protection des données.

B.2 Au-delà de la sanction sociale?

Proposition 44

La principale question en vue des discussions publiques consiste à savoir si les violations de la vie privée relèvent des interactions sociales ou si l'intervention d'un organisme officiel serait de nature à assurer le respect de la vie privée de chacun.

B.3 Modèles possibles

Proposition 45

On pourrait s'inspirer de modèles existants pour créer des recours non judiciaires en cas d'atteinte au droit à la vie privée. Comme c'était le cas pour les recours en matière de protection des renseignements, les principales questions qui devraient être soumises au débat public sont les suivantes :

a) Les recours non judiciaires devraient-ils être accompagnés de pouvoirs obligatoires?

b) Le rôle de l'organisme devrait-il se limiter au traitement des plaintes?

ANNEXE B

LA LOI VISANT LE SECTEUR PUBLIC

CHAPTER P-19.1

Protection of Personal Information Act

Assented to February 26, 1998

Chapter Outline

CHAPITRE P-19.1

Loi sur la protection des renseignements personnels

Sanctionnée le 26 février 1998

Sommaire

Her Majesty, by and with the advice and consent of the Legislative Assembly of New Brunswick, enacts as follows:

1(1) In this Act

"agent" means

(a) a person who collects personal information for a public body, and

(b) a person to whom a public body discloses personal information so that the person may provide a service on behalf of the public body;

"personal information" means information about an identifiable individual, recorded in any form;

"public body" means

(a) a body to which the *Right to Information Act* applies, and

(b) any other body, designated by regulation, that is established by a body referred to in paragraph (a) or by a public Act of New Brunswick;

"Statutory Code of Practice" means the code of practice set out in Schedule A.

1(2) Information that relates to an identifiable individual but is collected, used or disclosed in a form in which the individual is not identifiable is not personal information when so collected, used or disclosed.

1(3) An individual is identifiable for the purposes of this Act if

(a) information includes his or her name,

(b) information makes his or her identity obvious, or

Sa Majesté, sur l'avis et du consentement de l'Assemblée législative du Nouveau-Brunswick, décrète:

1(1) Dans la présente loi

«agent» désigne

a) une personne qui recueille des renseignements personnels pour un organisme public, et

b) une personne à qui un organisme public divulgue des renseignements personnels pour qu'elle puisse rendre un service au nom de l'organisme public;

«Code de pratique statutaire» désigne le code de pratique établi à l'Annexe A;

«organisme public» désigne

a) un organisme auquel la *Loi sur le droit à l'information* s'applique, et

b) tout autre organisme, désigné par règlement, qui est établi par un organisme visé à l'alinéa a) ou par une loi d'intérêt public du Nouveau-Brunswick;

«renseignement personnel» désigne un renseignement sur un particulier identifiable, enregistré sous quelque forme que se soit.

1(2) Les renseignements qui concernent un particulier identifiable mais qui sont recueillis, utilisés ou divulgués sous une forme dans laquelle le particulier n'est pas identifiable ne constituent pas des renseignements personnels lorsqu'ils sont recueillis, utilisés ou divulgués de cette façon.

1(3) Un particulier est identifiable aux fins de la présente loi si des renseignements

a) comprennent son nom,

b) rendent évidente son identité, ou

(c) information does not itself include the name of the individual or make his or her identity obvious but is likely in the circumstances to be combined with other information that does.

c) ne comprennent pas son nom ou ne rendent pas évidente son identité mais sont susceptibles dans les circonstances d'être adjoints à d'autres renseignements qui comprennent son nom ou rendent son identité évidente.

2(1) Every public body is subject to the Statutory Code of Practice.

2(1) Tout organisme public est soumis au Code de pratique statutaire.

2(2) The Statutory Code of Practice shall be interpreted and applied in accordance with Schedule B and with any regulations made under paragraph 7(b).

2(2) Le Code de pratique statutaire doit être interprété et appliqué conformément à l'Annexe B et à tous règlements établis en vertu de l'alinéa 7b).

3(1) The *Ombudsman Act* applies to this Act and to the activities of any public body under it, whether or not that public body is otherwise subject to the *Ombudsman Act.*

3(1) La *Loi sur l'Ombudsman* s'applique à la présente loi et aux activités de tout organisme public établi sous son régime, que cet organisme soit ou non assujetti de toute autre manière à la *Loi sur l'Ombudsman.*

3(2) Subject to sections 4 and 6, any complaint of a violation of this Act shall be made to the Ombudsman.

3(2) Sous réserve des articles 4 et 6, toute plainte contre une infraction à la présente loi doit être portée devant l'Ombudsman.

4(1) In relation to a public body to which the *Right to Information Act* applies, an individual may enforce under that Act any right to information that this Act confers.

4(1) Un particulier peut, relativement à un organisme public auquel la *Loi sur le droit à l'information* s'applique, exercer en vertu de cette loi tout droit à l'information que confère la présente loi.

4(2) Subsection (1) does not confer any right to obtain under the *Right to Information Act* information to which there would not otherwise be a right under that Act.

4(2) Le paragraphe (1) ne confère aucun droit d'obtenir des renseignements en vertu de la *Loi sur le droit à l'information* qui ne pourraient de toute autre façon être obtenus en vertu de cette loi.

5(1) Nothing in this Act displaces any duty of confidentiality that exists in relation to personal information under any other Act or law.

5(1) Aucune disposition de la présente loi ne supprime l'obligation de confidentialité à l'égard des renseignements personnels imposée par toute autre loi ou droit.

5(2) Where another Act confers on a public body, or an officer or employee of a public body, a discretion that may be exercised in relation to personal information, that body or person shall have regard to this Act in the exercise of that discretion, to the extent that the other Act allows.

5(2) Lorsqu'une autre loi accorde à un organisme public, ou à un dirigeant ou à un employé d'un organisme public, un pouvoir discrétionnaire qui peut être exercé relativement à des renseignements personnels, cet organisme ou cette personne doit prendre en considération la présente loi dans l'exercice de ce pouvoir discrétionnaire, dans la mesure où l'autre loi le permet.

6(1) A public body, or an officer, employee or agent of a public body, who collects, uses or discloses personal information in wilful contravention of Principles 3, 4 or 5 of the Statutory Code of Practice commits an offence punishable under Part II of the *Provincial Offences Procedure Act* as a category F offence.

6(2) A person to whom a public body discloses personal information on terms that limit the further use or disclosure of the information, and who wilfully contravenes those terms, commits an offence punishable under Part II of the *Provincial Offences Procedure Act* as a category F offence.

7 The Lieutenant-Governor in Council may make regulations

(a) designating bodies as public bodies;

(b) making special provision respecting the interpretation and application of the Statutory Code of Practice in relation to

(i) particular public bodies,

(ii) particular kinds of personal information, or

(iii) particular activities involving the handling of personal information;

(c) respecting forms to be used under this Act;

(d) respecting procedures to be followed under this Act;

(e) respecting fees payable under this Act;

(f) respecting exemptions from this Act for personal information, or for any arrangement

6(1) Commet une infraction punissable en vertu de la Partie II de la *Loi sur la procédure relative aux infractions provinciales* à titre d'infraction de la classe F, tout organisme public, ou tout dirigeant, tout employé ou tout agent d'un organisme public qui recueille, utilise ou divulgue des renseignements personnels en contravention délibérée du Principe 3, 4 ou 5 du Code de pratique statutaire.

6(2) Commet une infraction punissable en vertu de la Partie II de la *Loi sur la procédure relative aux infractions provinciales* à titre d'infraction de la classe F, toute personne à qui un organisme public divulgue des renseignements personnels à des conditions qui limitent l'usage ou la divulgation ultérieurs des renseignements et qui délibérément contrevient à ces conditions.

7 Le lieutenant-gouverneur en conseil peut établir des règlements

a) désignant des organismes à titre d'organismes publics;

b) prenant des dispositions spéciales relativement à l'interprétation et à l'application du Code de pratique statutaire relativement

(i) à des organismes publics particuliers,

(ii) à des genres particuliers de renseignements personnels, ou

(iii) à des activités particulières comportant le traitement des renseignements personnels;

c) concernant les formules à utiliser en vertu de la présente loi;

d) concernant les procédures à suivre en vertu de la présente loi;

e) concernant les droits à payer en vertu de la présente loi;

f) concernant les exemptions à la présente loi en matière de renseignements personnels ou de

for the management of personal information, that exists on the commencement of this Act.

8(1) ***Section 1 of the Archives Act, chapter A-11.1 of the Acts of New Brunswick, 1977, is amended:***

(a) by adding after the definition "hospital corporation" the following:

"identifiable individual" means an individual who can be identified by the contents of information because the information

(a) includes the individual's name,

(b) makes the individual's identity obvious, or

(c) is likely in the circumstances to be combined with other information that includes the individual's name or makes the individual's identity obvious;

(b) by repealing the definition "personal information" and substituting the following:

"personal information" means information about an identifiable individual;

8(2) ***Subsection 10(3) of the Act is amended by adding after paragraph (b) the following:***

(b.1) would reveal personal information concerning the applicant that

(i) was provided by another person in confidence, or is confidential in nature, or

(ii) could reasonably be expected to threaten the safety or mental or physical health of the applicant or another person;

mesures relatives à la gestion des renseignements personnels, qui existent lors de l'entrée en vigueur de la présente loi.

8(1) ***L'article 1 de la Loi sur les Archives, chapitre A-11.1 des Lois du Nouveau-Brunswick de 1977, est modifié***

a) par l'adjonction après la définition «Ministre» de ce qui suit:

«particulier identifiable» désigne un particulier qui peut être identifié par le contenu de renseignements qui

a) comprennent son nom,

b) rendent son identité évidente, ou

c) sont susceptibles dans les circonstances d'être adjoints à d'autres renseignements qui comprennent son nom ou rendent son identité évidente;

b) par l'abrogation de la définition «renseignement personnel» et son remplacement par ce qui suit:

«renseignement personnel» désigne un renseignement sur un particulier identifiable;

8(2) ***Le paragraphe 10(3) de la Loi est modifié par l'adjonction après l'alinéa b) de ce qui suit:***

b.1) pourrait dévoiler des renseignements personnels sur le demandeur qui

(i) ont été fournis par une autre personne à titre confidentiel, ou qui sont de nature confidentielle, ou

(ii) pourraient raisonnablement menacer la sécurité ou la santé mentale ou physique du demandeur ou d'une autre personne;

9(1) ***Section 1 of the Right to Information Act, chapter R-10.3 of the Acts of New Brunswick, 1978, is amended***

(a) by adding after the definition "hospital corporation" the following:

"identifiable individual" means an individual who can be identified by the contents of information because the information

(a) includes the individual's name,

(b) makes the individual's identity obvious, or

(c) is likely in the circumstances to be combined with other information that includes the individual's name or makes the individual's identity obvious;

(b) by repealing the definition "personal information" and substituting the following:

"personal information" means information about an identifiable individual;

9(2) ***The Act is amended by adding after section 2 the following:***

2.1 Without limiting section 2, subject to this Act, every individual is entitled to request and receive information about himself or herself.

9(3) ***Section 6 of the Act is amended by adding after paragraph (b) the following:***

(b.1) would reveal personal information concerning the applicant that

(i) was provided by another person in confidence, or is confidential in nature, or

(ii) could reasonably be expected to threaten the safety or mental or physical health of the applicant or another person;

9(1) ***L'article 1 de la Loi sur le droit à l'information, chapitre R-10.3 des Lois du Nouveau-Brunswick de 1978, est modifié***

a) par l'adjonction après la définition «ministre compétent» de ce qui suit:

«particulier identifiable» désigne un particulier qui peut être identifié par le contenu de renseignements qui

a) comprennent son nom,

b) rendent son identité évidente, ou

c) sont susceptibles dans les circonstances d'être adjoints à d'autres renseignements qui comprennent sont nom ou rendent son identité évidente;

b) par l'abrogation de la définition «renseignement personnel» et son remplacement par ce qui suit:

«renseignement personnel» désigne un renseignement sur un particulier identifiable.

9(2) ***La Loi est modifiée par l'adjonction après l'article 2 de ce qui suit:***

2.1 Sans restreindre la portée de l'article 2 et sous réserve de la présente loi, tout particulier a le droit de demander et de recevoir toute information sur lui-même.

9(3) ***L'article 6 de la Loi est modifié par l'adjonction après l'alinéa b) de ce qui suit:***

b.1) pourrait dévoiler des renseignements personnels concernant le demandeur qui

(i) ont été fournis par une autre personne à titre confidentiel, ou qui sont de nature confidentielle, ou

(ii) pourraient raisonnablement menacer la sécurité ou la santé mentale ou physique du demandeur ou d'une autre personne;

10 ***This Act or any provision of it comes into force on a day or days to be fixed by proclamation.***

10 ***La présente loi ou l'une quelconque de ses dispositions entre en vigueur à la date ou aux dates fixées par proclamation.***

Schedule A

The Statutory Code of Practice

Principle 1: Accountability

A public body is responsible for personal information under its control. The chief executive officer of a public body, and his or her designates, are accountable for the public body's compliance with the following principles.

Principle 2: Identifying Purposes

The purposes for which personal information is collected shall be identified by the public body at or before the time the information is collected.

Principle 3: Consent

The consent of the individual is required for the collection, use, or disclosure of personal information, except where inappropriate.

Principle 4: Limiting Collection

The collection of personal information shall be limited to that which is necessary for the purposes identified by the public body. Information shall be collected by fair and lawful means.

Principle 5: Limiting Use, Disclosure and Retention

Personal information shall not be used or disclosed for purposes other than those for which it was collected, except with the consent of the individual or as required or expressly authorized by law. Personal information shall be retained only as long as necessary for the fulfilment of those purposes.

Principle 6: Accuracy

Personal information shall be as accurate, complete and up-to-date as is necessary for the purposes for which it is to be used.

Annexe A

Code de pratique statutaire

Principe 1: Responsabilité

Un organisme public est responsable des renseignements personnels dont il a la gestion. Le directeur exécutif d'un organisme public et ses représentants doivent s'assurer du respect par l'organisme public des principes suivants.

Principe 2: Détermination des fins de la collecte

Les fins pour lesquelles les renseignements personnels sont recueillis doivent être déterminées par l'organisme public avant ou au moment de la collecte.

Principe 3: Consentement

Tout particulier doit consentir à toute collecte, utilisation ou divulgation de renseignements personnels, à moins qu'il ne soit pas approprié de le faire.

Principe 4: Limitation de la collecte

L'organisme public ne peut recueillir que les renseignements personnels nécessaires aux fins déterminées et doit procéder de façon honnête et licite.

Principe 5: Limitation de l'utilisation, de la divulgation et de la conservation

Les renseignements personnels ne doivent pas être utilisés ou divulgués à des fins autres que celles auxquelles ils ont été recueillis, à moins que le particulier n'y consente ou que la loi ne l'exige ou ne l'autorise expressément. On ne doit conserver les renseignements personnels qu'aussi longtemps que nécessaire pour la réalisation des fins déterminées.

Principe 6: Exactitude

Les renseignements personnels doivent être aussi exacts, complets et à jour que l'exigent les fins pour lesquelles ils doivent être utilisés.

Principle 7: Safeguards

Personal information shall be protected by safeguards appropriate to the sensitivity of the information.

Principle 8: Openness

A public body shall make readily available to individuals specific information about its policies and practices relating to the management of personal information.

Principle 9: Individual Access

Upon request, an individual shall be informed of the existence, use and disclosure of his or her personal information and shall be given access to that information, except where inappropriate. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.

Principle 10: Challenging Compliance

An individual shall be able to address a challenge concerning compliance with the above principles to the individual or individuals accountable for the public body's compliance.

Principe 7: Dispositifs de protection

Les renseignements personnels doivent être protégés par des dispositifs de protection correspondant à leur degré de sensibilité.

Principe 8: Transparence

Un organisme public doit mettre à la disposition des particuliers des renseignements précis sur ses politiques et ses pratiques concernant la gestion des renseignements personnels.

Principe 9: Accès individuel

Un organisme public doit informer tout particulier qui en fait la demande de l'existence de renseignements personnels qui le concernent, de l'usage qui en est fait et du fait qu'ils ont été divulgués à des tiers et lui permettre de les consulter, à moins qu'il ne soit pas approprié de le faire. Il sera aussi possible de contester l'exactitude et l'état complet des renseignements et d'y faire apporter les corrections appropriées.

Principe 10: Possibilité de porter plainte contre le non-respect des principes

Tout particulier doit être en mesure de se plaindre du non-respect des principes indiqués plus haut en communiquant avec le ou les particuliers responsables de les faire respecter au sein de l'organisme public.

Schedule B

Interpretation and Application of the Statutory Code of Practice

The provisions of the Statutory Code of Practice that are referred to in this Schedule shall be interpreted and applied in accordance with this Schedule.

Principle 2: Identifying Purposes

2.1 The purposes identified by the public body must directly relate to an existing or proposed activity of the public body.

2.2 The public body must document, in relation to any personal records system, the purpose or purposes for which the personal information in the system is held.

2.3 A "personal records system" is a computerized or manual records system which contains information about individuals and which is structured in such a way that information about specified individuals can be easily recovered.

Principle 3: Consent

3.1 Consent may be express or implied.

3.2 The actions for which consent can be implied are those that an individual should reasonably expect the public body to take, and would be unlikely to disapprove of, having regard to

(a) the nature of the personal information in question, including whether it is or is not sensitive or confidential,

(b) any benefit or detriment to the individual,

Annexe B

Interprétation et application du Code de pratique statutaire

Les dispositions du Code de pratique statutaire qui sont visées dans la présente annexe doivent être interprétées et appliquées conformément à la présente annexe.

Principe 2: Détermination des fins de la collecte

2.1 Les fins déterminées par l'organisme public doivent se rattacher directement à une de ses activités existantes ou proposées.

2.2 L'organisme public doit documenter, relativement à tout système d'enregistrement des renseignements personnels, la ou les fins pour lesquelles les renseignements personnels sont conservés dans le système.

2.3 Un «système d'enregistrement des renseignements personnels» est un système d'enregistrement informatisé ou manuel qui contient des renseignements sur des particuliers et qui est organisé de manière à donner facilement accès à des renseignements sur des particuliers spécifiques.

Principe 3: Consentement

3.1 Un consentement peut être expresse ou tacite.

3.2. Les mesures pour lesquelles un consentement peut être tacite sont celles que le particulier devrait raisonnablement s'attendre à voir prendre par l'organisme public, et qu'il n'est pas susceptible de désapprouver, eu égard à

a) la nature des renseignements personnels en question, y compris la question de savoir si les renseignements ont ou non une nature sensible ou confidentielle,

b) tout avantage ou inconvénient pour le particulier,

(c) any explanation that the public body has given of its intended actions,

(d) any indication that the individual has given of his or her actual wishes, and

(e) the ease or difficulty with which the actual wishes of the individual might be discovered.

3.3 Consent can be given by a parent, guardian or other representative of the individual in appropriate circumstances.

3.4 Consent is not required when a public body collects, uses or discloses personal information

(a) to protect the health, safety or security of the public or of an individual,

(b) for purposes of an investigation related to the enforcement of an enactment,

(c) to protect or assert its own lawful rights or those of another public body, including lawful rights against the individual,

(d) to verify the individual's eligibility for a government program or benefit for which the individual has applied,

(e) for purposes of legitimate research in the interest of science, of learning or of public policy, or for archival purposes,

(f) as required or expressly authorized by law, or

(g) for some other substantial reason in the public interest, whether or not it is similar in nature to paragraphs (a) to (f).

c) toute explication que l'organisme public a donné des mesures qu'il entend prendre,

d) toute indication que le particulier a donné de ses désirs réels, et

e) la facilité ou la difficulté avec laquelle les désirs réels du particulier peuvent être identifiés.

3.3 Un consentement peut être donné par un parent, un tuteur ou un autre représentant du particulier selon les circonstances.

3.4 Un consentement n'est pas requis lorsqu'un organisme public recueille, utilise ou divulgue des renseignements personnels

a) pour protéger la santé ou la sécurité du public ou d'un particulier,

b) aux fins d'une enquête liée à l'exécution d'une mesure législative,

c) pour protéger ou affirmer ses propres droits légaux ou ceux d'un autre organisme public, y compris des droits légaux contre le particulier,

d) pour vérifier l'admissibilité du particulier à un programme ou à une prestation gouvernemental pour lequel le particulier a fait une demande,

e) pour les fins de toute recherche légitime faite dans l'intérêt de la science, de l'enseignement ou de l'ordre public ou pour des travaux d'archives,

f) tel que requis ou expressément autorisé par la loi, ou

g) pour toute autre raison importante dans l'intérêt du public, qu'elle soit ou non semblable à celle des alinéas a) à f).

3.5 A public body may disclose personal information under paragraph 3.4(g) in furtherance of the public interest in open government.

3.6 Before collecting, using or disclosing personal information without consent under paragraph 3.4 or 3.5, a public body shall consider the nature of the information in question and the purpose for which it is acting, and shall satisfy itself that in the circumstances that purpose justifies the action proposed.

3.7 Any collection, use or disclosure of personal information without consent shall be limited to the reasonable requirements of the situation.

Principle 4: Limiting Collection

4.1 A public body may collect personal information

(a) from the individual,

(b) from another person with the individual's consent,

(c) from a source and by means available to the public at large,

(d) from any source if the public body is acting under paragraphs 3.4 to 3.7.

4.2 An individual shall not be refused a service or benefit because he or she declines to provide personal information which is not necessary for a legitimate purpose of the public body.

Principle 5: Limiting Use, Disclosure and Retention

5.1 A public body may discharge its obligation not to retain personal information by converting that information into non-identifying form.

3.5 Un organisme public peut divulguer des renseignements personnels en vertu de l'alinéa 3.4g) dans l'intérêt du public de rendre le gouvernement plus transparent.

3.6 Avant de recueillir, d'utiliser ou de divulguer des renseignements personnels sans consentement en vertu du paragraphe 3.4 ou 3.5, un organisme public doit prendre en considération la nature des renseignements en question et la fin des mesures qu'il prend, et doit se convaincre que dans les circonstances cette fin justifie les mesures projetées.

3.7 Toute collecte, toute utilisation ou toute divulgation de renseignements personnels sans consentement doit se limiter aux exigences raisonnables de la situation.

Principe 4: Limitation de la collecte

4.1 Un organisme public peut recueillir des renseignements personnels auprès

a) du particulier,

b) d'une autre personne avec le consentement du particulier,

c) d'une source et par des moyens qui sont à la disposition du grand public,

d) de toute source si l'organisme public agit en vertu des alinéas 3.4 à 3.7.

4.2 Il est interdit de refuser tout service ou toute prestation à un particulier qui refuse de fournir des renseignements personnels qui ne sont pas nécessaires pour une fin légitime de l'organisme public.

Principe 5: Limitation de l'utilisation, de la divulgation et de la conservation

5.1 Un organisme public peut satisfaire à l'obligation de ne pas conserver des renseignements personnels en convertissant ces renseignements sous une forme non identifiable.

5.2 Personal information that is maintained outside a personal records system and is not readily accessible to a person who has no prior knowledge of the information shall be deemed to be converted into non-identifying form when the use of the information ceases.

Principle 7: Safeguards

7.1 The safeguards to be adopted include training and administrative, technical, physical and other measures, as appropriate in the circumstances, and include safeguards that are to be adopted when a public body discloses personal information to a third party or makes arrangements for a third party to collect personal information on its behalf.

Principle 9: Individual Access

9.1 A public body to which the *Right to Information Act* applies may only refuse to provide an individual with personal information relating to himself or herself if the individual would have no right to that information under the *Right to Information Act.*

9.2 A public body to which the *Right to Information Act* does not apply shall establish a procedure comparable to the procedure in that Act for the purpose of ensuring that the individual can obtain access to information about himself or herself.

9.3 The procedure established under paragraph 9.2 may include exceptions to access comparable to those in the *Right to Information Act.*

9.4 When an individual has made a challenge to the accuracy or completeness of personal information relating to himself or herself but has not satisfied the public body that an amendment is appropriate, the public body shall note that the individual disputes the information in its possession.

5.2 Les renseignements personnels qui sont conservés en dehors d'un système d'enregistrement des renseignements personnels et qui ne sont pas facilement accessibles à une personne qui n'a pas de connaissance préalable de ces renseignements sont réputés être convertis sous une forme non identifiable lorsque l'usage des renseignements cesse.

Principe 7: Dispositifs de protection

7.1 Les dispositifs de protection qui doivent être adoptés comprennent des mesures de formation et des mesures administratives, techniques, physiques et autres, comme il convient dans les circonstances, et comprennent les dispositifs de protection qui doivent être adoptés quand un organisme public divulgue des renseignements personnels à un tiers ou prend des mesures pour qu'un tiers recueille des renseignements personnels en son nom.

Principe 9: Accès individuel

9.1 Un organisme public auquel la *Loi sur le droit à l'information* s'applique ne peut refuser de fournir à un particulier des renseignements personnels qui le concernent que si le particulier n'a aucun droit de les avoir en vertu de la *Loi sur le droit à l'information.*

9.2 Un organisme public auquel la *Loi sur le droit à l'information* ne s'applique pas doit établir une procédure comparable à celle de cette loi pour s'assurer que les particuliers peuvent avoir accès aux renseignements qui les concernent.

9.3 La procédure établie au paragraphe 9.2 peut comprendre des exceptions à l'accès aux renseignements personnels comparables à celles de la *Loi sur le droit à l'information.*

9.4 Lorsqu'un particulier a contesté l'exactitude ou l'état complet de renseignements personnels qui le concernent mais qu'il n'a pas convaincu l'organisme public qu'une modification s'imposait, l'organisme public doit noter que le particulier conteste les renseignements en sa possession.

Principle 10: Challenging Compliance

10.1 A public body shall investigate in good faith the complaints it receives about its management of personal information and shall take appropriate measures if a complaint is found to be justified.

Principe 10: Possibilité de porter plainte contre le non-respect des principes

10.1 Un organisme public doit faire une enquête de bonne foi sur les plaintes qu'il reçoit sur sa gestion des renseignements personnels et doit prendre les mesures appropriées s'il s'avère qu'une plainte est justifiée.

ANNEXE C

LA LOI UNIFORME SUR LA PROTECTION DE LA VIE PRIVÉÉ

Définition
1. Dans la présente loi, « tribunal » désigne la [Cour du Banc de la Reine du Nouveau-Brunswick].

Délit civil
2. Toute personne qui porte atteinte à la vie privée d'un particulier commet un délit civil qui donne un droit d'action sans qu'il soit nécessaire de prouver un dommage.

Preuve en l'absence de preuve contraire
3. Sans restreindre la généralité de l'article 2, la preuve de l'un ou l'autre des actes suivants constitue la preuve d'une atteinte à la vie privée d'un particulier en l'absence de preuve à l'effet contraire:

a) la surveillance auditive ou visuelle du particulier, de sa résidence ou de son véhicule par quelque moyen que ce soit, y compris l'écoute, le guet, l'espionnage et la filature, que la surveillance donne ou non lieu à une intrusion;

b) l'écoute ou l'enregistrement par une personne qui n'est pas partie à la conversation ni destinataire du message d'une conversation à laquelle participe un particulier ou d'un message destiné à un particulier ou transmis par lui par télécommunications;

c) le fait de rendre publics des lettres, des agendas ou d'autres documents personnels appartenant au particulier;

d) la diffusion de renseignements concernant le particulier qui ont été recueillis à des fins commerciales ou gouvernementales si,

i) la diffusion est contraire à une loi ou à un règlement, ou

ii) les renseignements ont été fournis par le particulier sous le sceau du secret et leur diffusion a été faite à des fins autres que celles pour lesquelles ils ont été fournis.

Moyens de défense
4(1) Nul acte, comportement ou divulgation ne constitue une atteinte à la vie privée d'un particulier si,

a) le particulier y a expressément consenti de façon explicite ou implicite, elle avait le droit de donner son consentement et le tribunal est convaincu que celui-ci a été donné librement;

b) l'acte, le comportement ou la divulgation découle logiquement de l'exercice d'un droit prévu par la loi qui permet de défendre sa personne ou ses biens;

c) sous réserve du paragraphe 2), il est autorisé ou exigé

i) par une loi ou un règlement,

ii) par un tribunal judiciaire ou par une personne, un tribunal ou un organisme, autre qu'un commissaire à la prestation des serments ou un notaire public, que la loi autorise à faire prêter serment aux fins pour lesquelles la personne, le tribunal ou l'organisme est autorisé à entendre la preuve,

iii) par tout acte judiciaire d'un tribunal judiciaire, d'une personne, d'un tribunal ou d'un organisme mentionné à l'alinéa ii);

d) l'acte, le comportement ou la divulgation est attribuable à un agent de la paix ou à un organisme public qui agit dans le cadre d'une enquête et de ses tâches normales, il n'est pas disproportionné par rapport à la gravité de l'affaire qui fait l'objet de l'enquête et il n'est pas commis par intrusion ni autre moyen illégal;

e) il est raisonnable, compte tenu des relations domestiques ou autres qui existent entre les parties; ou

f) le défendeur ignorait ou ne pouvait raisonnablement savoir que l'acte, le comportement ou la divulgation porterait atteinte à la vie privée d'un particulier.

2) Nulle autorisation ni exigence d'une loi ou d'un règlement ne peut servir de moyen de défense à une action pour atteinte à la vie privée, à moins que la loi ou le règlement n'autorise ou n'exige expressément l'acte, le comportement ou la divulgation aux fins pour lesquelles elle ou il a été édicté.

3) La divulgation d'une affaire ne constitue pas une atteinte à la vie privée d'un particulier si,

a) il existe des motifs raisonnables de croire que la divulgation est faite dans l'intérêt public;

b) la divulgation est privilégiée en vertu des dispositions législatives en matière de diffamation.

4) Le paragraphe 3) ne s'applique pas à tout acte ou comportement grâce auquel l'affaire est divulguée, si l'acte ou le comportement constitue une atteinte à la vie privée.

Recours

5. Dans une action pour atteinte au droit à la vie privée, le tribunal peut rendre l'une ou l'autre des ordonnances suivantes :

a) il peut octroyer des dommages-intérêts;

b) il peut émettre une injonction;

c) il peut ordonner au défendeur de rendre compte au demandeur de tout profit qu'il a réalisé ou qu'il réalisera par suite de l'atteinte à la vie privée du demandeur;

d) il peut ordonner au défendeur de remettre au demandeur tous les articles ou documents qui se trouvent en sa possession par suite de l'atteinte à la vie privée du demandeur;

e) il peut accorder au demandeur toute autre mesure de redressement que le tribunal estime nécessaire dans les circonstances.

Dommages-intérêts
6(1) Lorsqu'il octroie des dommages-intérêts par suite d'une action pour atteinte à la vie privée, le tribunal doit prendre en considération toutes les circonstances de l'affaire, y compris :

a) la nature de l'acte, du comportement ou de la divulgation et le contexte dans lequel il s'est produit;

b) l'effet de l'acte, du comportement ou de la publication sur la santé et le bien-être du demandeur ou de ses proches ainsi que sur la situation sociale, commerciale ou financière de ceux-ci;

c) le comportement du demandeur et du défendeur avant et après l'acte, le comportement ou la divulgation, y compris toute excuse ou offre de compensation de la part du défendeur.

2) Dans une action pour atteinte à la vie privée, le tribunal peut octroyer des dommages-intérêts punitifs, compte tenu du caractère flagrant de l'atteinte à la vie privée et du comportement du défendeur.

Droit d'action en sus des autres droits
7(1) Le droit d'action que confère la présente loi en cas d'atteinte à la vie privée ainsi que les recours prévus par la présente loi s'ajoutent à tout autre droit et recours dont peut se prévaloir le demandeur en vertu de toute autre loi, et ils n'y dérogent pas.

2) Le paragraphe 1) n'exige pas que l'on fasse abstraction des dommages-intérêts octroyés par suite d'une action pour atteinte à la vie privée dans l'évaluation des dommages-intérêts qui pourraient être octroyés dans le cadre de toute autre instance découlant de l'acte, du comportement ou de la divulgation constituant une atteinte à la vie privée.

La loi oblige la Couronne
8. La Couronne est liée par la présente loi.

ANNEXE D

SOLUTION DE RECHANGE (RÉSUMÉ)

1. L'atteinte au droit à la vie privée est un délit civil pouvant donner lieu à des poursuites sans qu'il soit nécessaire d'établir la preuve des dommages.

2. Un acte constitue une atteinte au droit à la vie privée :

a) s'il s'immisce indûment dans les affaires personnelles ou les activités d'un particulier, qu'il se produise dans un endroit public ou en privé; ou

b) s'il donne une publicité indue à des renseignements concernant un particulier.

3. Sans restreindre la généralité des articles 1 et 2, les activités suivantes sont susceptibles de porter atteinte au droit à la vie privée :

a) la surveillance d'un particulier;

b) le fait d'écouter ou d'intercepter les communications d'un particulier; ou

c) la publication de documents intimes d'un particulier.

4. Les moyens de défense à une poursuite fondée sur une atteinte au droit à la vie privée sont les suivants :

a) le particulier a consenti à l'acte dont elle se plaint;

b) l'acte dont on se plaint a eu lieu dans le cadre de l'exercice légal du droit de défendre sa personne ou ses biens;

c) l'acte dont on se plaint est autorisé ou exigé par la loi;

d) l'acte dont on se plaint est celui d'un agent de la paix agissant de bonne foi dans l'exercice de ses fonctions;

e) l'acte dont on se plaint est raisonnable compte tenu de l'ensemble des circonstances et eu égard à la relation domestique ou autre qui existe entre les parties;

f) le défendeur ignorait ou ne pouvait raisonnablement savoir que l'acte, la conduite ou la publication porterait atteinte au droit à la vie privée de quiconque; et

g) l'acte dont on se plaint est une publication

i) que le défendeur croit, pour des motifs raisonnables, être dans l'intérêt public; ou

ii) qui est privilégiée en vertu du droit de la diffamation.

[Aucune disposition en matière de recours n'est incluse.]