

**LA PROTECTION DE LA VIE PRIVÉE ET L'AUTOROUTE  
CANADIENNE DE L'INFORMATION**

---

*EXAMEN DES COMMENTAIRES FORMULÉS À L'ÉGARD DU DOCUMENT DE TRAVAIL  
D'INDUSTRIE CANADA*

**AKAY INFORMATION CONSULTING INC.**  
B.P. 1268, CARLETON PLACE  
ONTARIO, K7C 4L4  
(613) 257-1072

Mars 1995

# TABLE DES MATIÈRES

<b>RÉSUMÉ</b> .....	2
<b>INTRODUCTION</b> .....	13
<i>Origine du Document de travail</i> .....	13
<i>Réponses reçues</i> .....	13
<i>Base de l'examen</i> .....	14
<b>QU'EST-CE QUE LA PROTECTION DE LA VIE PRIVÉE?</b> .....	15
<i>Définition</i> .....	15
<i>Qui détient des renseignements personnels?</i> .....	15
<i>Protection de la vie privée - Un droit à intégrer à la Charte?</i> .....	16
<b>QUELLES SONT LES PRÉOCCUPATIONS AU SUJET DE LA PROTECTION DE LA VIE PRIVÉE?</b> .....	17
<i>Existe-t-il de véritables préoccupations au sujet de la protection de la vie privée</i> .....	17
<i>Préoccupations concernant la liberté contre l'intrusion</i> .....	18
<i>Préoccupations concernant la protection des renseignements personnels</i> .....	20
<i>Préoccupations concernant la technologie</i> .....	22
<i>Préoccupations découlant du manque de connaissances et de pouvoirs</i> .....	22
<i>Recherches médicale et sociale</i> .....	23
<b>COMMENT ASSURER LA PROTECTION DE LA VIE PRIVÉE?</b> .....	25
<i>L'expérience canadienne</i> .....	25
<i>Les expériences internationales</i> .....	26
<i>Les principes de protection de la vie privée</i> .....	28
<i>Les secteurs public et privé</i> .....	29
<i>Des chances égales pour tous</i> .....	30
<i>La législation et la réglementation</i> .....	31
<i>Les codes et les normes volontaires</i> .....	34
<i>Les solutions technologiques</i> .....	36
<i>L'éducation des consommateurs</i> .....	38
<b>CONCLUSIONS</b> .....	40
<i>Préoccupations</i> .....	40
<i>Comment assurer la protection de la vie privée?</i> .....	40
<i>Le fait de ne pas affronter les problèmes</i> .....	41
<b>ANNEXES</b> .....	
<i>Annexe A Résumé des mémoires reçus</i> .....	42
<i>Table des matières</i> .....	43
<i>Annexe B CSA Projet de «Code modèle sur la protection des renseignements personnels»</i> .....	169

## **RÉSUMÉ**

---

### **INTRODUCTION**

Les soixante-seize réponses reçues englobent une vaste gamme d'intérêts et de domaines. Afin de simplifier les comparaisons entre elles, les réponses ont été réparties en huit catégories. Voici ces catégories et le nombre pertinent de réponses dans chacune : recherche médicale et sociale (21); télécommunications et technologie (12); particuliers (11); défenseurs des consommateurs et de la vie privée (11); groupes de services financiers, de crédit et de marketing (5); commissaires à la protection de la vie privée (4); gouvernement (4); divers (8).

Le résumé de chaque mémoire est structuré en fonction des commentaires généraux sur la protection de la vie privée, des préoccupations à l'égard de la protection de la vie privée et les diverses méthodes visant à assurer celle-ci. Les propositions et recommandations particulières, découlant des quatre démarches possibles proposées dans le Document de travail, figurent dans chaque résumé, le cas échéant. Ces divers éléments sont réunis et résumés dans l'examen lui-même, qui renferme aussi les conclusions connexes.

### **QU'EST-CE QUE LA PROTECTION DE LA VIE PRIVÉE?**

La définition de la vie privée proposée dans le Document de travail est généralement acceptée par la grande majorité des répondants.

Une des questions qui sont fréquemment posées est la suivante : «Qui détient des renseignements personnels?». La majorité des défenseurs des consommateurs et de la vie privée et les commissaires à la protection de la vie privée estiment que les renseignements personnels sont détenus par les particuliers. Toutefois, la plupart des organismes du secteur privé tendent à considérer ceux-ci comme un produit sur lequel les consommateurs exercent divers degrés de contrôle.

Un certain nombre de répondants soutiennent que le droit à la protection de la vie privée devrait être intégré à la Charte des droits et libertés. Cependant, comme ils savent qu'il est difficile de modifier la Charte, ils proposent que toute modification de la *Loi sur la protection des renseignements personnels* ou que toute nouvelle loi fédérale sur le sujet comporte un préambule dans lequel serait reconnu le principe de la protection de la vie privée.

## **QUELLES SONT LES PRÉOCCUPATIONS AU SUJET DE LA PROTECTION DE LA VIE PRIVÉE?**

La grande majorité des répondants, y compris ceux du secteur privé, reconnaissent que le grand public se préoccupe de plus en plus de la protection de la vie privée sur l'autoroute de l'information. Cet avis est d'ailleurs corroboré par les résultats de plusieurs enquêtes menées par des organismes privés ces dernières années. Les enquêtes les plus souvent citées sont celles d'Ekos et Equifax réalisées en 1992 et celle de Gallup effectuée en 1994.

La liberté contre l'intrusion suscite nombre de préoccupations. Le contrôle et la surveillance sont vus comme les formes d'intrusion les plus susceptibles d'être préjudiciables. Au nombre des exemples les plus souvent cités figurent la surveillance des déplacements d'un particulier au moyen des systèmes de communications personnelles, sans fil ou par satellite, l'établissement du profil de marché d'un particulier grâce aux «traces» laissées par les données issues d'une série de transactions et la surveillance des employés. La surveillance du courrier électronique, y compris la question connexe de la propriété du message envoyé électroniquement, est aussi considérée comme un problème. Plusieurs répondants s'inquiètent également fort de la surveillance des conversations sur téléphone cellulaire au moyen d'appareils de balayage électronique, ainsi que de la surveillance électronique à la maison. Néanmoins, la surveillance et le contrôle sont vus comme procurant certains avantages, particulièrement dans les domaines de la recherche et du sauvetage, de la sécurité à la maison et de la gestion du parc automobile. En fin de compte, tout dépend de l'utilisation qui est faite de la surveillance et du contrôle. D'autres types d'intrusion, de moindre importance, sont plutôt considérés comme un ennui, c'est le cas notamment du télémarketing auquel le particulier peut toutefois mettre fin quand il le désire.

La protection des renseignements personnels est la principale préoccupation du grand public. Ce qui inquiète surtout, c'est le fait que les particuliers exercent peu de contrôle sur leurs renseignements personnels. L'utilisation de ces derniers pour créer des profils personnels de particulier et la perception selon laquelle les fonds de renseignements personnels ne sont pas suffisamment protégés sont aussi considérées comme des questions importantes. Certains répondants se préoccupent également beaucoup de l'usage non autorisé du numéro d'assurance-sociale (NAS), de la protection des renseignements médicaux et en matière de santé et des transferts transfrontières d'information. De même, le monde des affaires s'inquiète, car il souhaite que les avantages sociaux et économiques de la collecte et de l'utilisation des renseignements personnels soient reconnus. Certains journalistes et écrivains craignent que les dispositions de la Charte relatives à la liberté d'expression ne soient bouleversées par l'imposition de règles injustifiées sur la protection de la vie privée. Il a aussi été fait

mention de l'étrange ambivalence du grand public. Très souvent des membres de celui-ci estiment qu'ils ont le droit de connaître tous les détails sordides de la vie privée des célébrités, mais ils seraient horrifiés si on divulguait des renseignements similaires les concernant.

L'évolution continue et rapide de la technologie est aussi une source de préoccupation : des répondants se demandent si cela n'entraînera pas l'effritement de la protection de la vie privée. La sécurité des données stockées est également une source d'inquiétude importante. Néanmoins, on reconnaît de plus en plus que la technologie peut être utile et que son utilisation peut procurer des avantages. Par contre, le monde des affaires s'inquiète du fait que l'imposition de règles visant à assurer la protection de la vie privée pourrait empêcher le lancement de nouvelles technologies. On estime qu'il faut établir un juste équilibre entre les demandes des tenants du développement de la technologie et celles des partisans de la protection de la vie privée.

Certaines des préoccupations susmentionnées peuvent s'expliquer par le sentiment d'ignorance et d'impuissance qu'éprouvent des particuliers. Souvent, ces derniers ne savent pas qui détient des renseignements sur eux, et ils se sentent vulnérables, en raison des violations du droit à la protection de la vie privée dont on parle beaucoup.

La recherche médicale et sociale, plus particulièrement le volet lié à la protection des renseignements personnels, est une question importante. Ce sont d'ailleurs de chercheurs oeuvrant dans ces domaines qu'est provenu le plus grand nombre de réponses, et de loin. Ils se préoccupent du fait que l'imposition de règles strictes en matière de protection de la vie privée pourrait empêcher le stockage à long terme de données médicales et de santé personnelles et rendre obligatoire l'obtention du consentement des intéressés avant l'utilisation de telles données, et ce, malgré les mesures de sécurité rigoureuses qui sont prises. Selon eux, une telle situation pourrait nuire à la réalisation de précieux travaux de recherche visant le bien public. Sont cités à titre d'exemple les activités de suivi de l'incidence de maladies mortelles comme le cancer et certaines maladies du coeur et les études sur lesquelles se basent les autorités publiques pour prendre d'importantes décisions dans le domaine de la politique sociale.

Somme toute, bon nombre de répondants de tous les secteurs croient fermement que si on ne parvient pas à apaiser les diverses craintes du grand public, il ne sera possible d'exploiter pleinement l'autoroute de l'information.

### **COMMENT ASSURER LA PROTECTION DE LA VIE PRIVÉE?**

Comme toile de fond aux changements qu'est susceptible de subir la protection de la vie privée, certains répondants ont tracé plus ou moins en

détail l'évolution historique des pratiques et des lois en la matière, et ce, aussi bien au Canada qu'à l'étranger. Il est noté qu'au Canada, seuls le gouvernement fédéral et cinq provinces ont adopté des lois permettant de protéger les renseignements personnels détenus par les autorités publiques. Seul le Québec s'est doté d'une loi régissant la protection des renseignements personnels dans le secteur privé. Au niveau fédéral, certaines lois s'appliquant à des secteurs particuliers, comme les télécommunications et les institutions financières, renferment des dispositions prévoyant la prise de règlements pour la gestion des renseignements personnels. Jusqu'à présent, toutefois, de tels règlements n'ont été mis en application que dans le secteur des télécommunications. Des répondants ont aussi brossé un tableau de l'évolution de la situation dans le secteur privé, où on a assisté à l'élaboration de codes volontaires. Dans l'ensemble, ces interventions éparses sont vues comme une manière disparate et insatisfaisante de procéder. Elles sèment la confusion parmi les particuliers moyens, et elles ne permettront pas de composer avec la situation issue des nouvelles normes internationales et des dangers de l'évolution rapide des technologies, ni de répondre aux attentes du grand public.

Des développements internationaux sont également passer en revus. L'Europe est considérée comme celle qui ouvre la voie à l'échelle mondiale, particulièrement depuis les dix ou quinze dernières années. En 1982, l'Organisation de coopération et de développement économiques (OCDE) a publié un ensemble de lignes directrices sur la protection de la vie privée. Ces lignes directrices comportaient des principes d'une grande portée visant à assurer la protection des renseignements personnels, conjuguée à des dispositions ayant pour objet de limiter les flux transfrontières de données personnelles à destination des pays dépourvus de normes de protection similaires. Il est à noter que la presque totalité de la législation canadienne en matière de protection de la vie privée est fondée sur les principes figurant dans les lignes directrices de l'OCDE. La Communauté européenne (CE) s'emploie actuellement à moderniser ces dernières et à les transformer en directives qui, une fois qu'elles auront été adoptées par le Parlement européen, devront être respectées par tous les membres de la CE. Le plus important facteur lié aux directives proposées, de l'avis du Canada, est le fait que celles-ci sont susceptibles d'entraver le commerce en empêchant la circulation de renseignements personnels, sous forme automatisée ou manuelle, vers les pays qui n'ont pas adopté de normes acceptables en la matière. À l'heure actuelle, il est peu probable que le Canada serait reconnu, puisqu'il ne s'est pas doté de normes nationales régissant le secteur privé. On a aussi résumé l'évolution de la situation de la protection de la vie privée aux États-Unis. Ce pays n'a pas adopté de normes nationales s'appliquant à l'ensemble du secteur privé, ni de lois régissant le secteur public qui ait une portée aussi grande que la *Loi sur la protection des renseignements personnels* du gouvernement fédéral.

La demande de commentaires présentée dans le Document de travail et portant sur les principes qui devraient former la base d'une protection efficace de la vie privée a suscité une grande variété de réponses, dont la plupart sont fondées sur les lignes directrices de l'OCDE. Certains défenseurs des consommateurs et de la vie privée et commissaires à la protection de la vie privée font reposer leur argumentation sur la prémisse selon laquelle le droit à la vie privée est un droit de la personne fondamentale. En se basant sur cette prémisse, ils soutiennent que ce qui importe le plus est le droit de contrôler ses propres renseignements personnels et que ce droit est indissociable du principe du consentement. Les opinions divergent toutefois sur la question du consentement. Selon bon nombre de défenseurs des consommateurs et de la vie privée et de commissaires à la protection de la vie privée, consentement veut dire «consentement éclairé». Dans le secteur privé, cependant, on tend à considérer le consentement comme un «consentement», peu importe la manière dont il est obtenu. De plus, les premiers estiment que le consentement est une forme «d'acceptation», alors que le second croit qu'il s'agit d'une «renonciation». Outre les principes figurant dans les lignes directrices de l'OCDE, il a été question du principe selon lequel les particuliers ne devraient pas avoir à payer pour maintenir la protection fondamentale dont ils bénéficient actuellement. Les opinions divergent aussi dans ce cas. Certains répondants estiment qu'il conviendrait de payer pour profiter d'une protection allant au-delà de la protection de base, tandis que d'autres soutiennent que la protection de la vie privée ne devrait pas être limitée par la capacité de payer. Un autre des principes soulevés a trait à la liberté des particuliers de décider s'ils veulent ou non être branchés à l'infrastructure d'information, d'accepter ou de rejeter les services qui peuvent influencer sur leur niveau de protection et de s'abonner aux services qu'ils désirent recevoir et de payer pour l'obtention de ceux-ci. Il est toutefois précisé que ces choix ne devraient pas avoir d'incidence sur le niveau de service offert. En fin de compte, dans l'ensemble, les opinions divergent peu. La plupart des répondants sont favorables aux principes que renferme le projet de «code modèle de la protection des renseignements personnels» de l'Association canadienne de normalisation (CSA). Les auteurs d'autres mémoires ont proposé l'adoption de principes visant à régir l'autoroute de l'information elle-même.

On considère que le fait que s'estompe la distinction entre l'information que détient le secteur public et celle que possède le secteur privé pourrait poser un problème. En Europe, les directives proposées par la CE ont notamment eu pour effet que cette distinction ne soulève plus de questions. Dans le secteur privé, il existe une autre situation floue. En raison de l'intégration croissante des divers médias sur l'autoroute de l'information, la distinction initiale entre les différents intervenants (compagnies de téléphone, sociétés de câblodiffusion, presse, radiodiffuseurs, etc.) s'estompe aussi, ce qui fait qu'il est de plus en plus difficile de délimiter clairement les «frontières» entre les

secteurs. Il en résulte que l'établissement efficace de codes sectoriels volontaires pourrait poser plusieurs problèmes.

L'ensemble disparate de lois adoptées par les gouvernements fédéral et provinciaux et de codes volontaires créés par le secteur privé à travers le Canada incitent les intéressés à demander que «tout le monde soit traité sur le même pied». Des lois différentes dans des territoires différents créent des «riches et des pauvres» en matière de protection de la vie privée. Certaines provinces n'ont adopté aucune loi dans ce domaine, alors que le Québec s'est doté de lois régissant à la fois le secteur public et le secteur privé. Une telle situation pourrait mener à la création de «paradis des données», où les entreprises pourraient s'établir pour éviter d'avoir à satisfaire aux exigences imposées en matière de protection de la vie privée, ce qui aboutirait à une concurrence déloyale. Tous les intervenants sont donc intéressés par l'établissement d'une norme nationale encadrant la protection de la vie privée, mais les avis divergent sur la façon d'établir une telle norme.

Le Document de travail portait surtout sur les manières possibles de procéder pour favoriser la protection de la vie privée dans le secteur privé. Les auteurs ont retenu quatre démarches : les lois et la réglementation; les codes et normes volontaires; les solutions technologiques; et l'éducation des consommateurs. Si les avis ne divergent guère quant à la contribution des deux dernières démarches, il en va tout autrement en ce qui concerne la façon d'utiliser les lois et les codes volontaires.

La majorité des répondants estiment que le gouvernement doit intervenir de manière plus énergique et adopter de nouvelles lois. Comme il n'y a que deux répondants du secteur privé qui sont en faveur d'un tel mode d'intervention, il est clair que ceux qui sont favorables à l'adoption de lois sont des défenseurs des consommateurs et de la vie privée et des commissaires à la protection de la vie privée. Les intéressés estiment que les lois et règlements permettent d'assurer à tous les Canadiens un niveau égal de protection et d'établir les mécanismes nécessaires pour obtenir des moyens de redressement, imposer des sanctions, déposer des plaintes et faire appel de décisions jugées insatisfaisantes. De plus, l'instauration d'un tel régime satisferait aux normes de la CE, ce qui permettrait d'éviter les problèmes commerciaux possibles. Les répondants ont suggéré plusieurs façons de procéder pour établir un tel régime. Il ressort toutefois une méthode de leurs propos : l'adoption d'une loi visant à encadrer l'élaboration d'un ensemble de normes nationales en matière de protection de la vie privée, normes auxquelles les codes du secteur privé devraient se conformer. Pour compléter ce cadre, il a été suggéré de créer un corps administratif indépendant et impartial dont le mandat consisterait à assurer l'observation des normes, à entendre les plaintes, à accorder un recours à ceux qui auraient été lésés et à imposer des sanctions. Il a aussi été proposé de fonder un tel régime sur la pertinente du Québec, *Loi sur la*

*protection des renseignements personnels dans le secteur privé* et d'attacher une importance particulière à l'efficacité de l'appareil administratif, à la minimisation des frais et à la rentabilité. Il est de plus recommandé de prévoir une période de mise en application progressive et de mener rapidement des consultations auprès des provinces en vue d'harmoniser dans l'ensemble du pays à la fois les lois s'appliquant au secteur public et celles régissant le secteur privé. Parmi les autres suggestions citons la modification et la modernisation de la *Loi sur la protection des renseignements personnels*, adoptée par le gouvernement fédéral, pour la rendre conforme à la loi proposée et le déploiement d'un effort d'harmonisation par le secteur privé. En fait, il est soutenu que le gouvernement fédéral doit jouer un important rôle de chef de file dans ce dossier. Par contre, ceux qui s'opposent au recours à la voie législative font reposer leur argumentation sur le fait que celle-ci pose plusieurs problèmes. Ils estiment que ce mode d'action est rigide et ne se prête pas à une adaptation rapide, considérée nécessaire pour tenir compte de la prompt évolution de la technologie et du marché, et pourrait entraver le lancement de nouvelles initiatives et l'investissement. Ils soulignent que le temps requis pour parvenir à un consensus fédéral-provincial représente une autre difficulté, et que la tendance actuelle est la déréglementation du marché mondial, et non le contraire. Ils ajoutent que, dans une période de restrictions financières, cela coûterait plus cher. En résumé, donc, le secteur privé en général s'oppose au recours à la voie législative. L'industrie des télécommunications, en particulier, est contre l'adoption d'une autre loi pour assurer la protection des renseignements personnels, car elle est d'avis que les directives en matière de protection de la vie privée émises par le Conseil de la radiodiffusion et des télécommunications canadiennes (CRTC) sont suffisantes pour répondre aux préoccupations des intéressés. D'autre part, elle est très favorable à l'adoption d'une mesure législative visant des technologies particulières, laquelle ferait en sorte que serait considéré comme une infraction le fait d'intercepter les radiocommunications et interdirait généralement la fabrication, l'importation, la vente et la distribution d'appareils de balayage électronique permettant de surveiller les radiocommunications par téléphone, y compris par téléphone cellulaire. Malgré tout, le secteur privé ne s'oppose de façon absolue à une loi générale en matière de protection de la vie privée en autant qu'une telle loi ne soit mise en application qu'une fois qu'on aura essayé les codes volontaires et qu'on aura constaté qu'ils ne sont pas efficaces. L'adoption d'autres lois provinciales, en l'absence d'une loi fédérale, n'est pas considérée comme une solution viable, puisque cela irait à l'encontre de l'uniformisation des normes au Canada.

Le secteur privé préfère les codes et normes volontaires, en raison de leur flexibilité et de la possibilité de les adapter pour répondre aux besoins particuliers des différentes technologies et des divers segments du marché. Il estime que ce mode d'intervention coûte moins cher que les autres,

permet de mettre la protection de la vie privée plus en évidence au sein d'une organisation et peut contribuer à l'éducation des consommateurs. Il souligne que les codes et les normes volontaires peuvent avoir une portée nationale et servir à mettre tous les membres d'un secteur sur un pied d'égalité. Il souligne aussi qu'ils peuvent être imposés à tous les membres d'une organisation sectorielle ou renforcer par suite de l'exercice de pressions par des pairs, de la manifestation claire d'intérêts liés à la compétitivité ou d'une demande des consommateurs. Le principal argument invoqué par ceux qui s'opposent aux codes et aux normes volontaires est que ceux-ci ne sont que cela, «volontaires». De l'avis des opposants, bon nombre de ces codes et normes ne permettent pas de répondre à toutes les préoccupations des consommateurs, notamment en ce qui concerne l'équité des pratiques en matière de protection des renseignements et l'efficacité des mécanismes établis pour porter plainte ou obtenir réparation. Les opposants estiment aussi qu'il arrive que ces codes et normes favorisent davantage la défense des intérêts des entreprises que la protection du droit à la vie privée des consommateurs. Ils croient enfin qu'ils ne permettraient peut-être pas de satisfaire aux exigences formulées dans les directives proposées par la CE et portant sur l'adoption de normes «suffisantes» pour assurer la protection de la vie privée. Cela étant dit, il convient de préciser que les défenseurs des consommateurs et de la vie privée et les commissaires à la protection de la vie privée ne sont pas entièrement contre les codes volontaires. Ils considèrent que ceux-ci ont un rôle important à jouer, en raison de leur flexibilité et de leurs possibilités d'adaptation, mais qu'il faut les encadrer au moyen d'une loi. Soulignons à cet égard que tous les intéressés (le secteur privé, les défenseurs des consommateurs et de la vie privée et les commissaires à la protection de la vie privée) sont très favorables aux initiatives lancées récemment par la CSA en vue d'élaborer un code volontaire et de faire de celui-ci une norme nationale. Le projet de code de la CSA est mis au point par un groupe de travail composé de représentants de tous les intéressés. Le code, une fois en vigueur, pourrait servir à évaluer les codes volontaires du secteur privé et satisfaire aux exigences des directives de la CE en matière d'adoption de normes suffisantes pour assurer la protection de la vie privée.

Les répondants sont d'avis que les solutions technologiques ont aussi un rôle à jouer. Même si la technologie peut menacer la protection de la vie privée, ils savent qu'il est maintenant possible de prévoir dès le début de la conception d'un système les mécanismes nécessaires pour assurer le respect de la vie privée. Un certain nombre de répondants ont d'ailleurs souligné qu'il faudrait intégrer au processus de développement des systèmes un stade d'évaluation des incidences sur la protection de la vie privée. Le degré de protection assuré par l'autoroute de l'information et la mesure dans laquelle cette dernière va ralentir le rythme et faire augmenter le coût de l'innovation sont d'autres questions abordées par un bon nombre de répondants. L'intégration de mesures de sécurité est considérée comme

un élément clé à cet égard. Au nombre des nouvelles innovations envisagées figurent le chiffrage avancé, l'utilisation de cartes intelligentes et la mise en oeuvre de la technologie numérique. Sont considérées comme essentielles des mesures de protection de base, qui pourraient être conjuguées à d'autres mécanismes de sécurité moyennant des frais supplémentaires. Il est aussi suggéré que l'État encourage le développement de nouvelles technologies de protection et soutienne la recherche et le développement afin d'offrir de nouvelles possibilités à l'industrie canadienne. En général, les répondants ne pensent pas que les mesures de protection de la vie privée vont augmenter le coût de l'innovation, dans la mesure où celles-ci ne sont pas excessives. Les avis sont nombreux et partagés quant aux façons dont les Canadiens peuvent participer davantage à la conception des technologies susceptibles de menacer la vie privée. Il est bien sûr possible de prendre part aux audiences du CRTC et à l'élaboration des normes techniques de la CSA . Toutefois, selon un grand nombre de répondants dans tous les secteurs, il est nécessaire de participer plus directement aux activités au stade de la conception, pourvu que cette participation se limite à des consultations officieuses et à la prestation de conseils par des groupes comme les défenseurs des consommateurs et les commissaires à la protection de la vie privée.

Le manque de sensibilisation du grand public et la confusion qui semble régner parmi celui-ci sont considérés comme des problèmes importants. Les répondants s'accordent donc généralement pour reconnaître qu'il est essentiel d'assurer l'éducation des consommateurs. La sensibilisation des employés et des dirigeants d'entreprise aux responsabilités qui leur incombent en matière de protection de la vie privée est aussi considérée comme nécessaire. De l'avis général, il appartient et aux pouvoirs publics et aux entreprises de faire progresser cet aspect du dossier. La plupart des entreprises se sont dites disposées à agir, et un bon nombre d'entre elles ont déjà mis en oeuvre des programmes d'éducation. Les défenseurs des consommateurs et de la vie privée et les commissaires à la protection de la vie privée ont aussi indiqué qu'ils étaient prêts à faire leur part, à condition qu'ils disposent des ressources requises. Dans la même foulée, il est reconnu que les consommateurs ont également des responsabilités à assumer et doivent lancer des initiatives dans ce domaine. De l'avis des répondants, les outils pédagogiques sont nombreux et variés. Mentionnons notamment les campagnes de publicité visant à faire connaître les codes sur la protection des renseignements personnels du secteur privé et le code de la CSA, les campagnes de sensibilisation périodiques du grand public et la production de matériel et de brochures s'adressant à divers groupes et destinés à être distribués dans les centres d'information, les bibliothèques, etc.

## **CONCLUSIONS**

Les questions liées à la protection de la vie privée suscitent nombre de préoccupations réelles dans le grand public. Si on ne s'occupe pas rapidement de ces préoccupations, elles pourraient s'intensifier au point de mettre en danger le fonctionnement efficace de l'autoroute de l'information.

La majorité des membres du secteur privé et les défenseurs des consommateurs et de la vie privée et les commissaires à la protection de la vie sont en désaccord quant aux avantages relatifs du recours à la voie législative et de l'utilisation des codes volontaires. Il est toutefois possible d'aborder de façon pragmatique et conciliante ces divergences d'opinions et de parvenir ainsi à un compromis.

Il n'existe pas de méthode unique permettant de régler les problèmes qui se posent. Il semble donc tout à fait légitime de penser qu'une combinaison des démarches proposées dans le Document de travail puisse donner les résultats escomptés, vu que celles-ci sont interreliées et se complètent mutuellement.

Afin de trouver des solutions satisfaisantes aux divers problèmes relevés par les répondants, et ce, dans le délai le plus court possible, il conviendrait d'élaborer un plan bien coordonné.

Voici les éléments susceptibles d'être intégrés à un tel plan, que le Comité consultatif pourrait examiner :

- Établissement par voie législative d'un cadre national visant à permettre l'élaboration de normes en matière de protection de la vie privée, qui serait probablement fondé sur le code modèle de la CSA et auquel devraient se conformer les codes du secteur privé.
- Apport de changements à la *Loi sur la protection des renseignements personnels* en vue de combler ses lacunes actuelles, y compris une révision du préambule et l'ajout de dispositions ayant pour objet d'assurer la protection et la sécurité des renseignements personnels et de permettre l'instauration au sein du secteur public d'un cadre d'évaluation des incidences de divers projets sur la protection de la vie privée.
- Élaboration d'un programme visant à renforcer et à mettre à jour l'application des pratiques en matière de protection de la vie privée dans le secteur public.
- Dans les plus brefs délais, tenue de discussions avec les provinces en vue de mettre en application des normes nationales.

- Adoption d'une loi qui ferait en sorte que serait considérée comme une infraction l'interception des radiocommunications privées et qui interdirait généralement la fabrication, l'importation, la vente et la distribution d'appareils de balayage électronique permettant de surveiller les radiocommunications par téléphone, y compris par téléphone cellulaire.
- Mise sur pied d'un programme visant à promouvoir systématiquement la création de codes du secteur privé fondés sur le code modèle de la protection des renseignements personnels de la CSA.
- Création d'un programme conjoint, gouvernement/industrie, ayant pour objet de promouvoir et de soutenir le développement de technologies de protection de la vie privée.
- Promotion de consultations entre l'industrie, le gouvernement, les groupes de défense des consommateurs et les commissaires à la protection de la vie privée en ce qui concerne le développement de technologies et de systèmes importants susceptibles de menacer la protection de la vie privée.
- Mise sur pied d'un programme conjoint, gouvernement/industrie, de sensibilisation à la protection de la vie privée, de concert avec les groupes de consommateurs et les commissaires à la protection de la vie privée.
- Tenue de consultations entre le gouvernement et les groupes de recherche médicale et sociale afin de clarifier l'apparente dichotomie entre la protection des renseignements personnels et la nécessité d'effectuer les recherches médicales et sociales nécessaires pour favoriser le bien public.
- Élaboration par le gouvernement d'une clause type en matière de protection de la vie privée, qui serait ajoutée à tous les contrats ou accords prévoyant le transfert ou l'échange de renseignements personnels avec tous les établissements non publics.
- Annonce publique après l'adoption du plan et son approbation par les ministres compétents.

Si des mesures ne sont pas prises pour régler les principaux problèmes cernés par les répondants, les préoccupations du grand public à l'égard de la protection de la vie privée pourraient s'intensifier et les intéressés pourraient éviter d'utiliser l'autoroute de l'information. Dans un tel cas, il est aussi possible que les normes du Canada en matière de protection de la vie privée soient considérées comme ne satisfaisant pas aux exigences formulées dans les directives de la CE.

## **INTRODUCTION**

---

### **Origine du Document de travail**

En octobre 1994, Industrie Canada, en collaboration avec le Comité consultatif de l'autoroute de l'information, a publié le Document de travail *La protection de la vie privée et l'autoroute canadienne de l'information*. Ce document a été le premier d'une série de documents de travail publiés par Industrie Canada et portant sur des questions sociales, économiques et technologiques. Il avait pour objet de mieux connaître les opinions du grand public et d'alimenter le débat sur les questions liées à la protection de la vie privée touchant la construction et l'exploitation de l'autoroute de l'information. Les personnes et les groupes intéressés ont été invités à faire connaître par écrit leurs avis (mémoires, commentaires, etc.) sur les diverses options et démarches proposées dans le Document de travail ou sur tout autre aspect de celui-ci. Ils avaient jusqu'au 23 décembre 1994 pour faire parvenir leurs observations. Il est à noter que, pendant une période d'un an, les intéressés peuvent consulter les documents reçus, dont on trouve copie à la bibliothèque d'Industrie Canada située au 2<sup>e</sup> étage de la Tour Journal Sud, 365, avenue Laurier Ouest, Ottawa, Ontario, et dans les bureaux régionaux d'Industrie, à Halifax, à Montréal, à Toronto, à Edmonton et à Vancouver.

### **Réponses reçues**

Les soixante-seize réponses reçues englobent une vaste gamme d'intérêts et de domaines et vont d'une page à soixante pages. Afin de simplifier les comparaisons entre elles, les réponses ont été réparties en huit catégories donnant une idée de la principale affiliation des répondants. Voici ces catégories et le nombre pertinent de réponses dans chacune : recherche médicale et sociale (21); télécommunications et technologie (12); particuliers (11); défenseurs des consommateurs et de la vie privée (11); groupes de services financiers, de crédit et de marketing (5); commissaires à la protection de la vie privée (4); gouvernement (4); divers (8). La catégorie «divers» comprend une organisation syndicale, un organisme de normalisation, une entreprise de sécurité des télécommunications, un journaliste, un écrivain/producteur d'émissions télévisées, un expert en apprentissage et en formation et deux répondants étrangers. L'annexe A renferme des résumés des mémoires, répartis par catégorie.

## ***Base de l'examen***

Le résumé de chaque mémoire est structuré en fonction des commentaires généraux sur la protection de la vie privée, des préoccupations à l'égard de la protection de la vie privée et les diverses méthodes visant à assurer celle-ci. Les propositions et recommandations particulières, découlant des quatre démarches possibles proposées dans le Document de travail, figurent dans chaque résumé, le cas échéant. Ces divers éléments sont réunis et résumés dans l'examen lui-même, qui renferme aussi les conclusions connexes.

## **QU'EST-CE QUE LA PROTECTION DE LA VIE PRIVÉE?**

### **Définition**

Dans le Document de travail, la définition du droit à la vie privée comprend deux éléments :

- le droit de vivre en paix, sans intrusion ni interruption;
- le droit de contrôler les renseignements qui touchent sa personne.

Aussi bien explicitement qu'agrémentée d'exemples, la définition est acceptée par la plupart des répondants. Deux d'entre eux toutefois proposent de la modifier.

Une des associations technologiques est d'avis que le mot «interruption» n'ajoute rien au concept de la protection de la vie privée et que son emploi laisse supposer que toutes les interruptions, bienvenues ou non, sont des invasions de la vie privée. Elle suggère donc d'utiliser le terme «non invité» qu'elle considère comme étant la clé de toute notion d'intrusion dans la vie privée dans la société d'aujourd'hui.

La seconde proposition a été faite par un des défenseurs des consommateurs et de la vie privée. De l'avis de celui-ci, le concept de protection de la vie privée devrait être élargi pour englober celui de «réputation» (reconnu par la Charte du Québec), vu que les renseignements personnels peuvent influencer sur ce que l'on pense de quelqu'un. Il devrait aussi être élargi pour comprendre le concept de «dignité» (aussi reconnu par la Charte du Québec), qui a trait à «l'identité informationnelle» de chacun.

### ***Qui détient des renseignements personnels?***

La question «qui détient des renseignements personnels» est considérée comme un élément essentiel du droit à la vie privée par certains défenseurs des consommateurs et de la vie privée ainsi que par un commissaire à la protection de la vie privée. Ces derniers estiment que les renseignements personnels sont détenus par les particuliers et qu'il s'agit là d'une prémisses fondamentale sous-tendant toute la question du contrôle de ces renseignements (collecte, utilisation, divulgation, rétention et élimination).

Par contre, la plupart des organismes du secteur privé semblent croire que les renseignements personnels sont un produit sur lequel les consommateurs devraient être en mesure d'exercer divers degrés de contrôle. Cependant, une association technologique assimile la discussion sur la propriété de l'information issue des transactions à celle sur la propriété intellectuelle.

## **Protection de la vie privée - Un droit à intégrer à la Charte?**

Un certain nombre de répondants, particulièrement les défenseurs des consommateurs et de la vie privée, estiment que le droit à la protection de la vie privée devrait être intégré à la Charte des droits et libertés. À leur avis, la protection de la vie privée est un droit de la personne fondamental qui doit être reconnu.

Cependant, comme il est difficile de modifier la Charte, les intéressés proposent que toute modification de la *Loi sur la protection des renseignements personnels* ou que toute nouvelle loi fédérale sur le sujet comporte un préambule dans lequel serait reconnu le principe de la protection de la vie privée. Cette proposition est comparable à la disposition qui figure dans le projet de loi sur la protection de la vie privée de la Communauté européenne.

## **QUELLES SONT LES PRÉOCCUPATIONS AU SUJET DE LA PROTECTION DE LA VIE PRIVÉE?**

---

### **Existe-t-il de véritables préoccupations au sujet de la protection de la vie privée?**

Confirmant l'opinion généralement acceptée, la très grande majorité des répondants estiment que les consommateurs se préoccupent beaucoup et de plus en plus des questions liées à la protection de la vie privée, particulièrement en rapport avec l'autoroute de l'information. Les opinions ne divergentes guère à cet égard, qu'elles soient exprimées par des représentants du secteur privé, des défenseurs des consommateurs et de la vie privée, des commissaires à la protection de la vie privée ou des particuliers. Les sondages sur la protection de la vie privée menés ces dernières années confirment d'ailleurs l'existence de ces préoccupations, et plusieurs répondants ont fait expressément mention des résultats de certains de ces sondages pour étayer leurs opinions.

Effectué en 1992 au nom d'un certain nombre d'organismes des secteurs public et privé, le sondage d'Ekos "La vie privée exposée - Le sondage canadien sur le respect de la vie privée" est celui qui est le plus souvent cité dans les réponses. Il a révélé que 52 p. 100 des Canadiens se préoccupent au plus haut point de la protection de la vie privée mais que 92 p. 100 s'inquiètent à tout le moins modérément de cette question. De plus, 83 p. 100 croient fermement que toute organisation devrait leur demander leur permission avant de transmettre des renseignements à leur sujet à une autre organisation, et 71 p. 100 conviennent qu'il faudrait que les règlements en matière de protection de la vie privée s'appliquent et aux administrations publiques et aux entreprises. De même, «de plus en plus de gens ont le sentiment que diverses menaces technologiques, commerciales et sociales pèsent sur leur vie privée». Il convient de souligner que l'on se préoccupe davantage des organisations du secteur privé que de celles du secteur public. Toutefois, comme l'ont précisé certains membres du secteur privé, le sondage a aussi révélé que la protection de la vie privée est une question qui suscite plus de préoccupations dans l'abstrait. En d'autres termes, les Canadiens se préoccupent du contrôle des renseignements les concernant, mais ils sont plus disposés à accepter qu'on utilise ceux-ci dans des situations particulières lorsqu'on leur explique clairement les raisons et les avantages connexes.

Les auteurs de l'*Equifax Canada Report on Consumers and Privacy in the Information Age*, publié en 1992, ont aussi constaté que la très grande majorité des consommateurs s'inquiètent des menaces pesant sur leur vie privée. Toutefois, un nombre tout aussi important de répondants conviennent que les ordinateurs permettent aux gens d'avoir plus facilement accès à des renseignements et à des services utiles et contribuent à

l'amélioration de leur qualité de vie. En outre, les mêmes gens ont répondu qu'ils étaient en faveur de l'utilisation de renseignements personnels pour la fixation des taux automobiles, l'approbation des prêts, l'émission d'une carte de crédit ou l'établissement de limites de crédit. Les auteurs du rapport ont conclu que 62 p. 100 des «Canadiens envisagent de façon pragmatique l'équilibre entre la protection de leur vie privée et l'accès à des avantages précieux pour eux, décidant domaine par domaine les pratiques, les règles et la protection équitables nécessaires et ceux qui devraient les appliquer».

En 1994, un sondage réalisé par Gallup Canada pour Andersen Consulting et portant sur ce que les Canadiens pensent de l'autoroute de l'information a notamment révélé que 67 p. 100 croient que l'autoroute de l'information est une bonne idée mais que 83 p. 100 se préoccupent fort ou quelque peu de la mesure dans laquelle celle-ci est susceptible d'influer sur leur vie privée. Toutefois, une enquête menée par Decima Research en 1993, qui diffère du sondage de Gallup sur ces points, a montré que 70 p. 100 des répondants pensent que la société compte trop sur la technologie et que 61 p. 100 estiment que la technologie complique les choses au lieu de les simplifier. Un sondage mené par TELUS Longwoods en 1994 a révélé que 39 p. 100 des répondants se préoccupent tellement de l'invasion de leur vie privée qu'ils n'utiliseront probablement pas l'autoroute de l'information.

Ces résultats sont renforcés et corroborés par le fait que presque tous les commentaires formulés par des particuliers ont trait aux préoccupations à l'égard de la protection des renseignements personnels et de la liberté contre l'intrusion.

Les préoccupations varient beaucoup, allant de la liberté contre l'intrusion, de la protection des renseignements personnels, du manque de connaissances et de puissance à la technologie.

### ***Préoccupations concernant la liberté contre l'intrusion***

Ces préoccupations sont liées au droit de vivre en paix. Les auteurs du Document de travail ont traité plus particulièrement des quatre démarches qui pourraient permettre d'atténuer les préoccupations relatives à la protection des renseignements personnels, mais des répondants se sont dits fort préoccupés par la question de l'intrusion non invitée. Les préoccupations à cet égard ont été exprimées tout autant par les représentants du monde des affaires que par des consommateurs et peuvent être réparties en deux grandes catégories. La première a trait au contrôle et à la surveillance, la deuxième, aux intrusions non voulues ou ennuyeuses dans la vie d'une personne.

Le contrôle et la surveillance sont considérés comme l'intrusion la plus ennuyeuse et la plus susceptible de causer des préjudices, et bon nombre

d'exemples sont donnés. Un exemple typique est la «laisse électronique» créée par les capacités améliorées de poursuite inhérentes aux systèmes de communications personnelles sans fil ou par satellite qui, en l'absence de mécanismes de contrôle efficaces, permettent de suivre les déplacements d'un particulier, et ce, sans son autorisation. De même, les «traces» laissées par les données issues d'une série de transactions effectuées par un particulier peuvent être réunies pour dresser le profil de celui-ci, son style de vie, ses habitudes ainsi que son pouvoir et des préférences d'achat. La surveillance des employés, au moyen de systèmes vidéo ou de mécanismes électroniques de contrôle de la productivité, est aussi considérée comme une question importante. La surveillance du courrier électronique, par un employeur ou quelqu'un de l'extérieur, est également une source de préoccupation. En rapport avec la surveillance des employés, elle donne d'ailleurs lieu à un débat énergique, les intéressés se demandant si l'employeur a le droit de surveiller les messages personnels envoyés par courrier électronique. Des répondants se préoccupent aussi beaucoup de l'utilisation d'appareils de balayage électronique pour intercepter les communications téléphone cellulaire ou d'autres types de radiocommunications privées. Cette préoccupation est exprimée et par des consommateurs et par des représentants du secteur des télécommunications, à l'instar de celle sur le blocage de l'affichage du nom que permet un service téléphonique. Enfin, la surveillance de l'activité à la maison est vue comme un problème possible, vu que les systèmes proposés permettront la prestation de services de sécurité par voie électronique, le contrôle électronique de la consommation et du service par les entreprises de services publics et la fourniture de services multimédias interactifs au moyen de la télévision et des ordinateurs. Les répondants estiment néanmoins que la surveillance et le contrôle procurent des avantages, particulièrement dans les domaines de la sécurité à domicile, de la recherche et du sauvetage et de la gestion des parcs de véhicules commerciaux. En fin de compte, toute cette question tient à l'utilisation que l'on fait du contrôle et de la surveillance.

Les intrusions non voulues ou non invitées dans la vie d'une personne sont aussi considérées comme une préoccupation, comme en témoignent les réponses aux sondages et celles des répondants, mais de moindre importance que celle suscitée par le contrôle et la surveillance. Alors que le premier type d'intrusion est vu comme un ennui, le second est considéré comme susceptible de représenter une menace. Les répondants estiment toutefois que le télémarketing est une forme d'intrusion plus importante que la publicité envoyée par la poste, bien que la décision récente du CRTC interdisant l'utilisation des dispositifs de composition automatique et de communication des messages pour la sollicitation commerciale et restreignant les heures durant lesquelles le télémarketing «en direct» est

possible devrait contribuer grandement à remédier au problème. De toute façon, le consommateur est habituellement en mesure de mettre fin quand bon lui semble à cette forme d'intrusion.

### ***Préoccupations concernant la protection des renseignements personnels***

La perception selon laquelle on n'est pas en mesure de contrôler l'accès aux renseignements personnels et l'utilisation par d'autres de ces derniers sont la principale source de préoccupations touchant la protection de la vie privée. S'ajoute à cela la commercialisation non autorisée des renseignements personnels. Ces préoccupations sont reconnues tout autant par les organisations d'entreprises, les défenseurs des consommateurs et de la vie privée et les commissaires à la protection de la vie privée. Ce sont aussi les préoccupations les plus fréquemment exprimées par les particuliers.

L'utilisation non autorisée des données transactionnelles et l'établissement de profils personnels par le jumelage et la collecte de renseignements personnels sont des questions importantes. En fait, ils suscitent de grandes préoccupations, qu'ils soient le résultat de l'emploi de cartes de crédit, du marketing direct, de transactions bancaires, etc.

Le manque de mesures de sécurité et de protection adéquates inquiète également. Ces lacunes sont attribuées soit au manque de connaissances ou au laxisme des employés des organisations détenant des renseignements personnels, soit au manque de mesures de sécurité et de protection intégrées ou établies.

Un certain nombre de questions précises liées à des types particuliers de renseignements personnels sont aussi une source d'inquiétude pour des répondants. Sont considérés comme les plus importantes l'utilisation du numéro d'assurance-sociale (NAS) et la protection des renseignements médicaux et de l'information sur la santé. Des particuliers se préoccupent notamment des lacunes dans le contrôle de l'emploi du NAS et par le secteur privé et les éléments du secteur public qui ne sont pas expressément autorisés à s'en servir. Nombre de répondants s'inquiètent également de la protection des renseignements médicaux en matière de santé et des transferts transfrontières d'information. Ces inquiétudes n'ont pas été exprimées seulement par des particuliers, des défenseurs des consommateurs et de la vie privée et des commissaires à la protection de la vie privée, mais aussi par le secteur privé et le milieu de la recherche médicale.

Un autre sujet de préoccupation générale est la question des transferts transfrontières de renseignements personnels. Dans ce cas-ci, les

intéressés s'inquiètent du fait que les renseignements personnels ne seront alors plus visés par des lois nationales ou provinciales et qu'on ne pourra donc plus les protéger.

Une autre préoccupation, qui semble aller à l'encontre des préoccupations précitées, est celle selon laquelle il importe de reconnaître les avantages commerciaux, économiques et sociaux de la collecte et de l'utilisation des renseignements personnels. Par avantages commerciaux, on entend l'étendue des marchés et la capacité d'offrir de nouveaux services améliorés. Par avantages économiques, on entend la capacité de créer davantage d'emplois dans des domaines comme le marketing direct, pendant que par avantages sociaux, on fait référence à la mise en application des lois, à la recherche médicale et sociale et à la capacité d'effectuer les transactions de consommation d'une manière plus efficace, plus efficiente et moins coûteuse. Non seulement cette préoccupation a été formulée par des personnes autres que des représentants du monde des affaires et des chercheurs oeuvrant dans les domaines de la médecine et des sciences sociales, mais les avantages susmentionnés ont été reconnus par des défenseurs des consommateurs et de la vie privée et des commissaires à la protection de la vie privée.

Deux journalistes/écrivains craignent que la prise de mesures visant à assurer la protection de la vie privée ne restreigne l'accès à un nombre considérable de dossiers, même protégés par l'anonymat, ce qui pourrait porter atteinte aux dispositions sur la liberté d'expression figurant dans la Charte des droits et libertés. Certaines organisations du secteur privé s'inquiètent du fait que les fournisseurs de réseaux pourraient être considérés comme la force de police chargée de faire respecter la vie privée sur l'autoroute de l'information. À cet égard, un certain nombre de répondants conviennent que cela serait une tâche impossible et que les mesures ayant pour objet de protéger la vie privée devraient viser les fournisseurs d'information qui interagissent sur l'information. Une autre des préoccupations exprimées a trait à l'importance de reconnaître qu'il incombe aussi aux consommateurs d'assurer la protection de leur propre vie privée.

En ce qui concerne la protection de la vie privée en général, quelques répondants ont relevé l'étrange ambivalence du grand public. Nombre de membres de celui-ci sont en effet favorables à l'adoption de principes stricts dans ce domaine, particulièrement lorsqu'ils sont touchés directement, mais ils ne se montrent pas aussi préoccupés lorsqu'il s'agit de certains de leurs concitoyens. Ce degré moindre de préoccupation est d'ailleurs exprimé éloquemment par le désir de savoir où se trouvent les personnes qui ont fini de purger leurs sentences (les violeurs, les batteurs d'enfants, etc.), la soif de détails sur la vie privée des personnes publiques et l'appui apporté à l'utilisation de nouvelles technologies en vue de mettre un terme aux fraudes et aux abus, d'éliminer le gaspillage et le double emploi et d'augmenter l'efficacité de l'appareil bureaucratique.

## ***Préoccupations concernant la technologie***

L'évolution continue et rapide de la technologie, conjuguée aux avantages que celle-ci peut procurer, est une source de préoccupation : des répondants se demandent si cela n'entraînera pas l'effritement de la protection de la vie privée. Ce n'est pas tant les applications de la technologie qui inquiètent le plus mais le fait que l'on pourrait négliger de s'occuper de la protection de la vie privée devant «l'assaut technologique». Ce qui préoccupe également les intéressés, c'est qu'il arrive trop souvent que les mesures de protection nécessaires ne sont pas «intégrées» au développement de la technologie mais «rajoutées» ultérieurement sous forme de dispositif inefficace.

Malgré ces préoccupations, il est reconnu que le grand public accepte de plus en plus l'utilisation de la technologie. Le recours aux guichets automatiques des banques, au service de paiement direct Interac, aux ordinateurs personnels, aux modems, à Internet, à la production électronique des déclarations de revenus, etc. l'illustre d'ailleurs bien.

Par contre, certains, particulièrement des représentants du monde des affaires, s'inquiètent du fait que les préoccupations ou les exigences en matière de respect de la vie privée pourraient empêcher le lancement de nouvelles technologies. Ils estiment donc qu'il faut établir un juste équilibre entre les demandes des tenants du développement de la technologie et celles des tenants de la protection de la vie privée.

## ***Préoccupations découlant du manque de connaissances et de pouvoirs***

Certaines des préoccupations susmentionnées peuvent s'expliquer en partie par le sentiment d'ignorance et d'impuissance qu'éprouvent des consommateurs. D'une part, ces derniers se sentent frustrés parce qu'ils ne savent pas exactement ce que permet de faire la technologie; ils ne saisissent donc pas bien les incidences possibles sur le respect de la vie privée. D'autre part, ils se sentent impuissants dans bien des circonstances, particulièrement parce qu'ils ne disposent d'aucun moyen efficace de donner suite aux plaintes liées à la vie privée portées contre le secteur privé.

Des préoccupations particulières dans ce domaine sont attribuables au fait qu'il arrive très souvent que des consommateurs n'aient absolument aucune idée de ceux qui pourraient détenir des renseignements les concernant. De plus, ces mêmes personnes se sentent vulnérables en raison des cas bien connus où des violations ou des problèmes liés au respect de la vie privée n'ont été dévoilés qu'après coup.

## **Recherche médicale et sociale**

Ce sont de chercheurs oeuvrant dans les domaines de la médecine et des sciences sociales qu'est provenu le plus grand nombre de réponses, et de loin. Ils conviennent qu'il faut assurer la protection des renseignements personnels, mais ils se préoccupent presque tous de l'incidence négative possible des mesures de protection proposées sur la recherche médicale et sociale.

Les types de recherche dont il est question comprennent diverses études, notamment : le maintien et l'efficacité des services de santé, l'utilisation de nombreux médicaments sur ordonnance par les aînés, l'incidence de maladies graves et mortelles, comme le cancer et les maladies du coeur, les résultats de l'action thérapeutique et des médicaments, les effets de l'environnement sur la santé, la façon dont les familles et les particuliers réagissent à l'évolution de la situation sociale et économique. Elles procurent des avantages publics importants liés à l'amélioration de la santé dans la collectivité et à la capacité de prendre des décisions efficaces touchant les politiques de la santé et sociale.

Les intéressés craignent que l'adoption par le Canada de principes identiques à ceux qui figurent dans les projets de directives sur la vie privée de la CE n'entrave la réalisation de travaux de recherche essentiels pour assurer le bien public. Ils fondent leurs craintes sur le fait que les directives de la CE ne prévoient pas d'exemptions touchant l'obtention du consentement pour la collecte et l'utilisation de renseignements personnels, ni pour la conservation de tels renseignements après leur emploi initial. Selon eux, interdire le stockage à long terme de renseignements personnels rendrait impossible l'étude de l'évolution de cas durant toute une vie, et la nécessité d'obtenir le consentement causerait des problèmes de logistique et de coût.

Les mémoires présentés par les membres du milieu de la recherche médicale renferment beaucoup de détails sur les mesures de sécurité qui sont prises pour protéger les renseignements personnels. Mentionnons notamment la préservation de l'anonymat des données personnelles au moyen de techniques de codage; le blocage de l'accès aux laboratoires de recherche; l'utilisation de systèmes de sécurité informatiques; les serments de respect du secret; l'approbation et l'application des protocoles de projet par des corps universitaires ou provinciaux; et la séparation structurelle entre les fonctions de recherche et les fonctions administratives. De plus, il n'a jamais été porté à la connaissance des répondants des cas de non-respect de la confidentialité. Ces derniers soulignent également que les recherches ne portent pas sur des patients en particulier mais plutôt sur des groupes ou des populations de patients. Ils estiment donc que rien ne justifie l'imposition au domaine de la recherche des mêmes restrictions (obtention du consentement, utilisation et conservation des données) que

celles qui sont proposées pour les données détenues pour d'autres fins dans les secteurs public et privé. Comme l'a affirmé un chercheur : «Sommes-nous en train de chercher un remède pour une maladie imaginaire?».

Somme toute, bon nombre de répondants de tous les secteurs croient fermement que si on ne parvient pas à apaiser les diverses craintes du grand public, il ne sera pas possible d'exploiter pleinement l'autoroute de l'information.

## **COMMENT ASSURER LA PROTECTION DE LA VIE PRIVÉE?**

### ***L'expérience canadienne***

Certains des documents présentés font état de l'expérience acquise par le Canada en matière de législation, de réglementation et de codes volontaires dans le domaine de la protection de la vie privée, pour mieux faire comprendre la situation actuelle.

Il est indiqué que seulement six gouvernements ont, pour le secteur public, une législation efficace sur la protection de la vie privée, c'est-à-dire le gouvernement fédéral, le Québec, l'Ontario, l'Alberta, la Saskatchewan et la Colombie-Britannique. Seul le Québec a une législation régissant le secteur privé. D'autres lois fédérales ont également des dispositions relatives à cette protection. La *Loi sur les télécommunications* possède des dispositions visant à protéger la vie privée des personnes, qui réglementent notamment les communications non sollicitées. En outre, des modifications apportées au *Code criminel* et à la *Loi sur la radiocommunication* interdisent maintenant la divulgation des communications radiotéléphoniques interceptées, sans compter que les nouvelles *Loi sur les banques*, *Loi sur les compagnies d'assurance* et *Loi sur les compagnies fiduciaires et les compagnies de prêt* permettent de prendre des règlements régissant l'utilisation des renseignements fournis par les clients. Enfin, toutes les provinces anglophones, à l'exception du Nouveau-Brunswick et de l'Alberta, ont une législation quelconque protégeant l'information sur le crédit à la consommation.

Sur le plan fédéral, les règlements officiels protègent très peu la vie privée. De récentes décisions du CRTC ont restreint l'utilisation des CMA, de la publicité importune par télécopieur et des communications téléphoniques aux fins de la sollicitation. De plus, elles ont interdit le recours aux appels préenregistrés ou informatisés pour les mêmes fins et indiqué clairement que les compagnies de téléphone peuvent, moyennant préavis de deux jours, annuler le service dont bénéficient les utilisateurs de CMA qui sont en infraction. En approuvant le «service d'affichage du nom», le CRTC a également enjoint aux compagnies de téléphone de fournir gratuitement la possibilité d'empêcher cet affichage, pour tous les appels. Il a indiqué enfin qu'il ne permettra rapidement aucun dépôt concurrentiel des compagnies de téléphone si ce dépôt soulève des préoccupations en matière de protection de la vie privée. En vertu de la *Loi sur les banques*, de la *Loi sur les compagnies d'assurances* ainsi que de la *Loi sur les compagnies fiduciaires et les compagnies de prêt*, aucun règlement n'a encore été établi en matière d'utilisation des renseignements sur la clientèle.

Dans le secteur privé, un certain nombre d'associations industrielles d'entreprises ont institué des codes volontaires de protection de la vie

privée. Dans l'industrie des télécommunications, le ministre des Communications de l'époque a énoncé en 1992 une série de six «Principes de protection de la vie privée lors des télécommunications». Ces principes ont été mis en oeuvre par un organisme de protection de la vie privée lors des télécommunications, composé d'un représentant de l'industrie et des groupements de consommateurs. Toutefois, celui-ci n'a jamais exercé vraiment son activité, pour un certain nombre de raisons politiques, économiques et pratiques. L'Association canadienne du marketing direct (ACMD), l'Association des banquiers canadiens et la société Stentor ont toutes délivré à leurs membres un code de protection de la vie privée. L'industrie de la télédistribution a pour sa part enchâssé des principes de protection dans une série de normes industrielles appliquées par un organisme indépendant, le Conseil canadien des normes de télédistribution. En outre, un certain nombre de sociétés ont élaboré leur propre code volontaire de protection de la vie privée.

Mais en résumé, malgré les efforts considérables déployés pour ces initiatives, bon nombre de répondants voient la situation comme confuse et difficile à comprendre pour l'individu moyen. Elle ne tient pas compte non plus des nouvelles normes internationales, des dangers que représentent les technologies en évolution rapide, ni des attentes du public.

### ***Les expériences internationales***

De nombreux répondants considèrent les expériences internationales comme étant à l'origine des initiatives canadiennes en matière de protection de la vie privée, et comme un modèle pouvant inspirer les initiatives futures.

Au cours des années 70, de nombreux pays européens avaient adopté une législation dans ce domaine, qui était souvent incompatible d'un pays à un autre. C'est pourquoi l'OCDE a délivré en 1982 une série de *Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données à caractère personnel*, pour qu'elles soient adoptées par ses membres. Ces lignes directrices, qui établissaient des principes de base dans ce domaine, prévoyaient également des restrictions en matière de transmission de renseignements personnels vers des pays qui ne se conformaient pas à des principes équivalents de protection de la vie privée. Une grande partie de la législation canadienne visant le secteur public et portant sur la protection en question est fondée sur les principes de ces lignes directrices. Toutefois, bien que le Canada soit devenu assujéti à celles-ci en 1984, l'incidence des dispositions restreignant les flux transfrontières de données a été négligeable à cause de leur nature facultative. Par la suite, c'est-à-dire en 1990, la CE a rédigé des directives sur la protection des personnes en matière de traitement des renseignements personnels, qui visaient à harmoniser toutes les législations européennes sur la protection de ces données pour qu'elles offrent des

niveaux de protection communs et élevés et facilitent ainsi le commerce. Si le Parlement européen les adopte, les directives en question auront force de loi. Leur version la plus récente, qui ajoute aux lignes directrices et aux principes de l'OCDE, tient compte des difficultés concrètes posées par ces dernières et réduit un peu la rigidité des dispositions antérieures. Les flux transfrontières de données sont donc permis aux pays qui ont pris des mesures de protection suffisantes plutôt qu'équivalentes. Et surtout, ils font de la protection de la vie privée un droit humain fondamental, portent sur le secteur public et sur le secteur privé, et s'appliquent aux relevés automatisés aussi bien que manuels.

Depuis les années 70, les États-Unis ont, au palier fédéral, adopté diverses lois relatives à la protection de la vie privée, depuis une *Privacy Act* générale jusqu'à des lois sectorielles portant sur des questions comme les rapports de crédit, la fraude informatique et la protection de la vie privée dans les télécommunications. Toutefois, aucune de ces lois ne vise la protection des renseignements personnels dans l'ensemble du secteur privé. Car en 1977, la Privacy Protection Study Commission a rejeté explicitement l'idée d'une loi générale de protection des données dans le secteur privé, inspirée du modèle européen. Elle a favorisé une combinaison de lois et de codes non réglementaires qui serait sectorielle et par conséquent plus sensible aux diverses pratiques de traitement de l'information ainsi qu'aux besoins d'industries différentes. En outre, la législation américaine n'a aucune disposition en cas d'oubli ou de négligence, ni aucun conseil de protection des données, ni aucune commission de protection de la vie privée. Mais récemment, de nouvelles études ont été amorcées aux États-Unis en matière de protection de la vie privée sur l'autoroute de l'information. Comme dans le cas de l'étude actuelle du Comité consultatif, elles sont effectuées par le Privacy Working Group (Groupe de travail sur la protection de la vie privée) de la National Information Infrastructure (NII) et par la National Telecommunications and Information Administration (NTIA). La NII a élaboré de nouveaux principes généraux et provisoires touchant la protection de la vie privée, et la NTIA a rendu public un document de travail pour obtenir des commentaires à son sujet. De plus, de nouveaux projets de loi sur les télécommunications, dont le Congrès a été saisi, portent eux-aussi sur les préoccupations soulevées par la protection de la vie privée dans le domaine des télécommunications.

Un certain nombre de répondants voient également d'un oeil favorable ce qui s'est fait dans d'autres pays comme la Hollande, la Grande-Bretagne, la Nouvelle-Zélande, Hong Kong, etc. en matière de protection de la vie privée.

## **Les principes de protection de la vie privée**

Un large éventail de réactions a été suscité par la demande formulée dans le Document de travail, laquelle visait à obtenir des observations sur les principes qui devraient être le fondement d'une bonne protection de la vie privée. Ces réactions figurent donc s'il y a lieu dans chacun des résumés des commentaires reçus (voir l'annexe A). Toutefois, on peut discerner certaines constantes.

À la base des arguments invoqués par certains défenseurs de la vie privée et des consommateurs, de même que par certains commissaires à la protection de la vie privée, il y a la prémisse selon laquelle le droit à la vie privée est un droit humain fondamental. Il en découle que la protection de la vie privée est considérée comme trop importante pour être laissée au bon plaisir du marché, et qu'il faut l'envisager comme indispensable pour faire des affaires.

C'est peut-être l'aptitude des personnes à exercer un contrôle sur leurs renseignements personnels qui passe pour être la principale question touchant la protection de la vie privée. Ce contrôle s'étend à la collecte de ces derniers, sous réserve de prescriptions légales ou réglementaires, ainsi qu'à leur utilisation et à leur divulgation conformément aux pratiques d'information loyales ou équitables.

Un élément de contrôle essentiel est le consentement. Toutefois, il est interprété différemment d'un secteur à l'autre. En général, les défenseurs des consommateurs et de la vie privée, ainsi que les commissaires à la protection de la vie privée, le considèrent comme un «consentement informé», ce qui passe pour être une bonne compréhension des raisons de la collecte de renseignements et des utilisations qu'on fera de ces derniers, ainsi que l'absence de toute forme de «coercition». Dans le secteur des entreprises, bon nombre de gens semblent également souscrire à la notion de «consentement informé», bien qu'ils la définissent autrement. D'autres ont tendance à penser que le consentement est réputé avoir été donné lorsqu'il y a transaction. En outre, alors que les défenseurs de la vie privée et des consommateurs, ainsi que les commissaires à la protection de la vie privée, jugent que le consentement est donné lorsqu'il y a «participation», les milieux d'affaires préfèrent la notion de «non-participation».

D'autres principes, fondés dans une large mesure sur les lignes directrices de l'OCDE et sur les dispositions de la *Loi sur la protection de la vie privée*, sont notamment : la détermination des buts de la collecte de données; la limitation de cette dernière aux renseignements nécessaires; la garantie que les renseignements personnels sont aussi exacts et à jour que possible; l'accès des personnes à leurs renseignements personnels, notamment la possibilité de faire corriger ces derniers s'il y a lieu; la mise en place de mécanismes de règlement des plaintes et de recours.

Certains principes supplémentaires sont apparus ces dernières années, à cause des progrès technologiques et de l'évolution du marché. Ce sont notamment la nécessité de protéger les renseignements personnels grâce à des sauvegardes convenant à leur caractère délicat, et le principe selon lequel les personnes ne devraient pas être forcées d'engager des frais pour maintenir les niveaux fondamentaux et existants de protection de leur vie privée. En ce qui a trait à ce principe, les points de vue diffèrent à certains égards. Certains répondants soutiennent que les consommateurs devraient payer pour que leur vie privée soit protégée au-delà du niveau fondamental, tandis que d'autres affirment que l'incapacité de payer ne devrait pas nuire au respect de la vie privée. Un autre principe comporte la liberté des personnes de choisir de se rattacher ou non à l'infrastructure d'information, d'accepter ou de rejeter des services qui peuvent nuire à la protection de leur vie privée, ainsi que de ne souscrire qu'aux services qu'elles désirent recevoir, et de n'assumer les frais que pour ces derniers. Toutefois, elles ne devraient pas voir les niveaux des services dont elles bénéficient diminuer à cause de leur choix.

Dans l'ensemble, il n'y a, à l'égard des principes de protection de la vie privée, aucune différence d'opinion importante entre, d'une part, les défenseurs des consommateurs et de la vie privée, et, d'autre part, les milieux d'affaires. Car les deux parties appuient fermement les principes de protection de la vie privée contenus dans le projet de code modèle de la CSA, qui équivalent dans l'ensemble à ceux qui précèdent.

Certains des documents présentés font également état de principes qui devraient régir la mise au point de l'autoroute de l'information, en particulier dans ses rapports avec les questions de protection de la vie privée. Ils comprennent notamment le principe selon lequel les mesures de protection doivent être compatibles avec l'évolution dynamique et souvent imprévisible de l'autoroute en question, et cette protection doit tenir compte du droit des créateurs de savoir qui se sert de leurs oeuvres (propriété intellectuelle).

### ***Les secteurs public et privé***

Certains des défenseurs des consommateurs et de la vie privée, de même que certains commissaires à la protection de la vie privée, se rendent compte d'un problème relativement nouveau touchant cette protection sur l'autoroute de l'information. Ils estiment qu'on ne perçoit plus très bien la distinction entre l'information qui appartient au secteur public et celle qu'on trouve dans le secteur privé. C'est pourquoi la sous-traitance d'un nombre de plus en plus grand de fonctions publiques au secteur privé aura probablement une incidence croissante sur ses pratiques en matière de protection de la vie privée. Au fur et à mesure que le secteur privé se verra céder des renseignements personnels par le secteur public pour l'exécution de ces marchés, ce dernier s'assurera sans doute que les marchés en

question feront état de ses obligations touchant la protection de la vie privée. En outre, le souci croissant de faire concorder les renseignements du secteur public avec ceux du secteur privé, c'est-à-dire de confronter par exemple les données sur les bénéficiaires de l'aide sociale avec les renseignements bancaires ou financiers pour assurer l'admissibilité, est perçu comme rétrécissant l'écart entre les deux secteurs sur ce chapitre. De la même façon, compte tenu de l'évolution, les efforts continus des commissaires à la protection de la vie privée, ainsi que de la presse, pour mieux faire connaître les questions relatives à cette protection, auront des retombées. En fait, un répondant international est d'avis que l'abandon de la distinction entre le secteur public et le secteur privé, dans la version la plus récente des directives proposées par la CE en matière de protection de la vie privée, montre bien que la circulation croissante des renseignements personnels entre les deux secteurs rend caduque cette distinction.

Dans le secteur privé seulement, les observateurs constatent également que la distinction s'estompe entre les industries ayant recours à l'autoroute de l'information. Comme les technologies et les médias divers sont fusionnés en un «réseau sans couture», l'ancienne distinction claire entre les compagnies de téléphone, les compagnies de télédistribution, les radiodiffuseurs, la presse, les organismes de commercialisation, etc., disparaît de plus en plus. Il s'ensuit qu'il est difficile de déterminer où un secteur prend fin et où un autre commence, de sorte que le fait d'assurer la protection de la vie privée sur une base purement sectorielle risque de poser un problème.

### ***Des chances égales pour tous***

Nous avons précédemment fait référence à l'amalgame de lois et de règlements fédéraux ou provinciaux, de même qu'à la multitude de codes privés différents qui existent dans l'ensemble du Canada et dans tous les secteurs du marché. Cette situation suscite des préoccupations tant au sein des groupes du secteur privé qu'au sein des groupes de défense des consommateurs et de la vie privée, et chez les commissaires à la protection de la vie privée. Le problème que voient certains membres de tous ces groupes, c'est que si une norme nationale de protection de la vie privée n'est pas établie ni appliquée d'un bout à l'autre du pays, il continuera d'y avoir à cet égard des inégalités entre diverses personnes, à cause des lieux géographiques où elles se trouveront respectivement, et à cause des organismes commerciaux avec lesquels elles feront des affaires. De plus, certains organismes commerciaux s'assureront peut-être des avantages discriminatoires et injustes. Le fait de ne pas voir à ce que tous soient sur un pied d'égalité risque de mener à la création de «refuges informatiques», où les gouvernements les moins exigeants pourront attirer les entreprises cherchant à se soustraire aux mesures de protection de la vie privée. Enfin,

il faudra établir des distinctions juridiques difficiles en matière d'emplacement des données lorsqu'elles circuleront sur l'autoroute électronique.

### ***La législation et la réglementation***

Le débat le plus vif et les différences d'opinion les plus nombreuses sont de loin ceux qui portent sur la question de savoir si ce sont les lois et les règlements qui sont la meilleure façon de protéger la vie privée, ou bien les codes et les normes volontaires. Chacune de ces possibilités a ses promoteurs et ses opposants, pour un large éventail de raisons qui paraissent fondées.

La plupart des répondants qui ont étudié la question estiment que le gouvernement doit prendre des mesures plus fermes pour protéger le caractère confidentiel des renseignements. Tout en reconnaissant les différences entre le gouvernement fédéral et les provinces, ainsi que la difficulté d'harmoniser les méthodes respectives de ces pouvoirs publics, la plupart de ceux qui préconisent des mesures plus rigoureuses estiment qu'une législation et une réglementation supplémentaires, portant aussi bien sur le secteur public que sur le secteur privé, s'imposent. En outre, l'enquête sur la protection de la vie privée, que l'Ekos a menée en 1992, a révélé qu'«à un modèle d'autoréglementation purement volontaire de chaque entreprise, les Canadiens préfèrent de beaucoup des mesures législatives prises par le gouvernement».

Les raisons pour lesquelles cette législation et cette réglementation sont jugées nécessaires impressionnent par leur diversité. Celles-ci sont perçues comme la seule façon de donner des chances égales à tous dans l'ensemble du Canada, et de garantir au public un niveau de protection de la vie privée suffisant, sans confusion et sans inégalités régionales et sectorielles. De plus, il se pourrait que les flux transfrontières de données subissent un préjudice si l'on jugeait que les mesures de protection de la vie privée ne sont pas conformes aux directives proposées par la CE sur le sujet. Une législation et des normes nationales donneraient de bons résultats. Enfin, des normes nationales équitables et prescrites par une loi, tant pour le secteur public que pour le secteur privé, feraient beaucoup pour éliminer la préoccupation soulevée par la distinction floue entre les renseignements appartenant au secteur public et ceux qu'on trouve dans le secteur privé. Comme l'a indiqué un défenseur des consommateurs, la discussion a assez duré et il y a eu assez de preuves de l'insuffisance des codes volontaires au cours des dix dernières années : le gouvernement doit agir dès maintenant et être perçu comme assumant un rôle de leadership. Vient étayer cette opinion l'observation selon laquelle le Canada est l'une des rares démocraties occidentales qui n'ont adopté aucune législation visant à la fois le secteur public et le secteur privé.

La façon dont la législation et la réglementation peuvent être mises en oeuvre est elle aussi très diverse. En commençant par le secteur public, soulignons qu'on laisse entendre que le gouvernement devrait «nettoyer sa propre boutique». Il devrait tout d'abord apporter des modifications à la *Loi sur la protection de la vie privée*. Un préambule à cette loi établirait clairement le principe selon lequel cette protection est un droit fondamental (ce principe est également considéré comme une exigence qui figurerait dans toute législation supplémentaire régissant le secteur privé). Il devrait y avoir une disposition visant à la protection et à la sécurité des renseignements personnels. L'évaluation des répercussions sur la vie privée deviendrait obligatoire dans le cadre du processus de conception de toutes les révisions nouvelles ou importantes apportées aux systèmes et aux programmes gouvernementaux. Enfin, un processus serait instauré, en vertu duquel un comité parlementaire permanent tiendrait des audiences sur le rapport annuel du Commissaire à la protection de la vie privée et sur les rapports annuels respectifs des ministères, processus semblable à celui qui permet au Comité des comptes publics d'examiner le rapport du Vérificateur général et les comptes publics de chaque ministère. Ajoutons qu'un certain nombre de répondants demandent que le gouvernement fédéral, en assumant son rôle de leadership, oblige par une loi les organismes privés qui lui sont assujettis à satisfaire aux exigences de protection de la vie privée et prenne tous les autres moyens possibles de promouvoir l'adoption de mesures appropriées par le secteur privé.

Pour ce qui est de légiférer au sujet de la vie privée dans ce secteur, les promoteurs de la proposition ont tendance à favoriser l'instauration par une loi d'un cadre national de normalisation en vertu duquel des codes de protection seraient en vigueur. Viendrait s'ajouter un organisme administratif indépendant et impartial qui imposerait la conformité, entendrait les plaintes, assurerait des correctifs et des sanctions. Un certain nombre de personnes proposent qu'un tel système soit fondé sur la loi québécoise relative à la protection des renseignements personnels dans le secteur privé, qui est la seule à y régir cette protection au Canada. Toutefois, cette opinion n'est pas unanime. Une institution privée estime que la loi en question n'atteint pas au juste équilibre entre la protection de la vie privée et la libre circulation des renseignements, si nécessaire dans une économie de marché. De plus, une autre a indiqué que cette loi n'avait pas beaucoup influé sur ses politiques et ses procédures, bien qu'elle ait été considérée comme excessive à certains égards. On reconnaît également qu'une telle loi devrait être rédigée et mise en oeuvre de la façon la moins bureaucratique et la plus rentable possible. Un répondant britannique vient renforcer cette opinion en déclarant que les dispositions sur l'enregistrement des données de la *Data Protection Act* du Royaume-Uni sont souvent ignorées parce qu'elles sont trop bureaucratiques et qu'elles n'ont pour ainsi dire aucun sens. En outre, on suggère que toute législation soit instaurée graduellement pour éviter les perturbations économiques dans des

domaines comme l'industrie de la commercialisation directe, qui emploie des milliers de Canadiens. D'autres propositions en vue d'une telle législation contiennent une disposition permettant de «sonner l'alarme» lorsque des organismes s'adonnent à des activités illégales, et prévoyant la reconnaissance de la culpabilité commune. Enfin, on presse le gouvernement d'entamer sans délai des discussions avec les provinces pour harmoniser au Canada la législation qui porte sur le secteur public et celle qui vise le secteur privé.

Les opposants à la législation et à la réglementation voient un certain nombre de problèmes dans le fait de suivre la voie législative. Ils jugent que la législation n'est pas assez pointue, qu'elle serait rigide et incapable de réagir aux changements de plus en plus rapides et aux impératifs tant de la technologie que du marché. De plus, ils estiment qu'elle risque d'entraver les nouvelles initiatives et de nuire à l'investissement nécessaire. À cet égard, le fait que les exigences des entreprises et les technologies diffèrent d'un secteur à l'autre ne ferait qu'aggraver le problème. Le temps qu'il faudrait pour en arriver à un accord entre le gouvernement fédéral et les provinces passe aussi pour être un facteur important qui milite contre la législation. Enfin, certains estiment que les codes et les normes volontaires n'en sont qu'à leurs balbutiements, et qu'ils n'ont pas encore eu la chance de faire leurs preuves, de sorte que la législation ne devrait être utilisée qu'en dernier ressort. Ajoutons que la législation et la réglementation sont considérées comme allant à l'encontre de la tendance actuelle à la déréglementation des marchés mondiaux, comme exigeant des fonds publics supplémentaires à une époque de restrictions financières, et peut-être aussi comme débouchant sur la «microgestion» du marché.

En général, les défenseurs des consommateurs et de la vie privée ainsi que les commissaires à la protection de cette dernière sont en faveur de la législation, tandis que le secteur privé s'y oppose. Toutefois, la situation n'est pas tout à fait en noir et blanc. Une association technologique appuie la législation afin de garantir des niveaux uniformes et appropriés de protection de la vie privée, alors qu'une société de télécommunications estime qu'une industrie des télécommunications réglementée devrait échapper à toute législation future parce qu'elle est déjà régie par les dispositions sur la protection de la vie privée contenues dans la *Loi sur les télécommunications*. D'autres organismes privés ne seraient pas contre la législation si on leur faisait valoir, au bout d'une période raisonnable, que les codes et les normes volontaires ne donnent pas les résultats escomptés, à condition qu'elle tienne compte des réalités du marché.

Toutefois, l'industrie des radiotélécommunications est tout à fait en faveur d'une législation exclusivement technologique. Elle estime que le gouvernement devrait agir rapidement et légiférer de façon que ce soit une infraction d'intercepter des radiotélécommunications, et qu'il soit en général

interdit de fabriquer, d'importer, de vendre et de distribuer des analyseurs capables de surveiller les radiotéléphones, notamment les téléphones cellulaires.

En ce qui a trait à la question de savoir si l'on peut protéger suffisamment la vie privée au moyen d'une législation provinciale ou sectorielle, les opinions sont quelque peu contradictoires. Mais en général, on semble convenir qu'une telle méthode ne suffirait pas à elle seule. Les répondants qui s'opposent vivement à la législation ne changent pas d'avis, que cette dernière soit fédérale, provinciale ou sectorielle, alors que d'autres pensent que pour être adoptée, la législation doit être fondée sur des normes nationales, afin que tous soient sur un pied d'égalité. On s'inquiète tout autant de la «balkanisation» qui risque d'avoir lieu et qui irait de pair avec la création de «refuges informatiques». En résumé, on estime que toute décision d'opter pour la législation doit absolument faire suite à des échanges de vues et à des activités de coordination avec les provinces.

### ***Les codes et les normes volontaires***

On estime que les principaux avantages des codes et des normes volontaires sont leur souplesse et leur adaptabilité. On signale que des secteurs différents ont recours à diverses pratiques commerciales et à diverses technologies. Par conséquent, cette polyvalence leur permet d'aligner leurs pratiques en matière de protection de la vie privée sur la nature spécifique de l'entreprise et sur les besoins de sa clientèle. En outre, ils peuvent s'adapter plus rapidement et être plus sensibles aux changements dans les méthodes d'affaires, ainsi qu'à la technologie en évolution et aux préoccupations des consommateurs au chapitre de la protection de leur vie privée. Sans compter que des examens peuvent être effectués à intervalles réguliers pour permettre d'évaluer les effets des situations évolutives. Les codes volontaires peuvent en fait avoir une envergure nationale, donner des chances égales à tous les intervenants de chaque secteur, et éviter ainsi les problèmes posés par les différences entre les paliers fédéral et provincial. En guise d'avantages supplémentaires, citons également le fait que les frais d'exploitation peuvent être moindres, et que ces frais et les responsabilités peuvent être ciblés au sein de l'organisme. Enfin, la protection de la vie privée peut être plus en évidence à l'intérieur de ce dernier, ce qui contribue à sensibiliser le public et accroît ainsi la confiance des consommateurs tout en leur permettant de profiter de tous les avantages de l'autoroute de l'information.

Les codes et les normes volontaires peuvent être mis en oeuvre de bien des façons, chacune étant adaptée aux besoins particuliers d'un secteur. Ils peuvent être rendus obligatoires pour les membres d'une association sectorielle donnée, comme dans le cas du code de l'Association canadienne du marketing direct, ou incorporés dans les Conditions du service

confidentielles approuvées par le CRTC, comme dans celui des transporteurs réglementés régis par la *Loi sur les télécommunications*. En outre, l'adoption et la mise en oeuvre de codes volontaires peuvent être rendues nécessaires par les pressions exercées par les pairs, par la nécessité de soutenir la concurrence et par les exigences des consommateurs, ce qui signifie que ceux-ci exprimeront leur mécontentement en exerçant leur droit de vote s'ils ne sont pas convaincus qu'on tient compte de leurs préoccupations au sujet de la protection de leur vie privée.

À l'heure actuelle, l'une des principales innovations en matière de codes volontaires passe pour être le projet de code modèle de protection de la vie privée, appuyé fortement non seulement par le secteur privé, mais aussi par les groupes de défense des consommateurs et les commissaires à la vie privée. Il contient dix principes de protection des renseignements personnels (voir l'annexe B), fondés sur les lignes directrices de l'OCDE. Son principal avantage est qu'il est mis au point grâce aux opinions convergentes des membres du Comité technique de la CSA sur la protection de la vie privée, composé de représentants des gouvernements, des commissaires à la vie privée, des défenseurs de cette dernière et des consommateurs, des syndicats et du secteur privé. En outre, il pourrait être le fondement d'une norme nationale qui permettrait d'évaluer d'autres codes volontaires. Et il pourrait tout aussi bien fournir une norme grâce à laquelle la communauté internationale pourrait juger de l'utilité des méthodes canadiennes de protection des renseignements personnels. Toutefois, la manière dont il pourrait être mis en oeuvre est toujours à l'étude.

La principale objection à l'utilisation de codes volontaires, c'est justement qu'ils sont volontaires et que, comme les chaînes, ils ne sont pas plus efficaces que leurs maillons les plus faibles. De plus, ils ne sont parfois que des demi-mesures qui ne répondent pas vraiment aux préoccupations des consommateurs en matière de protection de la vie privée, c'est-à-dire qu'ils ne tiennent pas toujours compte du plein éventail de pratiques équitables dans le domaine de l'information. Ils ne sont souvent accompagnés d'aucune disposition prévoyant l'arbitrage indépendant, d'aucune disposition pour la surveillance et la mesure du rendement, d'aucune disposition stipulant des sanctions et des amendes, ni d'aucune disposition en ce qui a trait au règlement des plaintes et aux mécanismes de recours. En outre, ils sont parfois mal administrés sur les plans ministériel et sectoriel et peuvent être axés davantage sur les pratiques commerciales que sur la protection de la vie privée, sans compter que leur rôle au sein d'un secteur donné risque souvent d'être insatisfaisant et inconsistant. Les consommateurs sont susceptibles de ne pas connaître l'existence de ces codes volontaires, et ils n'ont souvent pas grand chose à voir avec leur élaboration. Enfin, les codes en question ne répondent peut-être pas aux normes «suffisantes» de protection de la vie privée qu'exigent les directives provisoires de la CE.

Ce sont les milieux d'affaires qui sont les plus en faveur de codes et de normes volontaires; mais les défenseurs des consommateurs et de la vie privée, ainsi que les commissaires à la vie privée, estiment eux aussi que ces codes et ces normes ont un rôle important à jouer, à condition d'être régis par une législation efficace. Ils connaissent toutefois aussi bien les lacunes de cette dernière, p. ex. sa rigidité, le temps qu'il faut pour la mettre en oeuvre, etc., que les avantages des codes volontaires, p. ex. leur souplesse, leur capacité de répondre aux besoins particuliers, etc. En ce sens, ils considèrent ces codes comme un premier pas vers la protection des données, comme méritant d'être appuyés par une législation pour être vraiment efficaces, et comme un élément acceptable de la solution si la démonstration est faite de leur utilité. Ils reconnaissent également que les codes en question peuvent aider à sensibiliser davantage les employés à la protection de la vie privée. En outre, certains membres des groupes de défense des consommateurs et de la vie privée, ainsi que des groupes de commissaires à la vie privée, sont d'avis que les codes volontaires pourraient aider l'industrie à «prendre son essor» avant le dépôt de la législation, et, ce faisant, éclairer les législateurs sur les questions sectorielles et les modes de mise en oeuvre.

### ***Les solutions technologiques***

On s'entend généralement pour déclarer que les solutions technologiques ont aussi leur place. Même si bon nombre de répondants soutiennent que l'évolution technologique accélérée menace la vie privée, ils reconnaissent que les progrès de la technologie peuvent maintenant permettre d'instaurer dès le début de meilleurs mécanismes de protection dans ce domaine. Ils jugent que cette dernière possibilité est très importante, et ils sont d'avis qu'avant de mettre au point de nouvelles technologies et de nouveaux systèmes, il faut voir à ce que l'évaluation de leur incidence sur la vie privée soit partie intégrante du processus. En réalité, un répondant a élaboré un processus raisonné pour arriver à ce but, et un autre a proposé des règles en matière d'évaluation des répercussions des nouvelles technologies sur la vie privée. Nombreux sont les répondants qui estiment que cette évaluation des conséquences augmente le coût des nouveaux systèmes et risque d'en retarder la mise au point, mais d'autres sont d'avis qu'elle peut permettre d'éviter des frais futurs en éliminant la nécessité d'apporter plus tard des modifications coûteuses pour tenir compte des impératifs de la protection de la vie privée. Signalons à cet égard que le fait de forcer les compagnies de téléphone d'assurer le blocage gratuit des appels avant de leur permettre d'afficher les noms est un bon exemple, tout comme l'abandon du système «Lotus Marketplace : Households».

En outre, de nombreux répondants soulèvent la question de savoir si l'autoroute de l'information devrait être conçue pour assurer de hauts niveaux de protection de la vie privée, et si elle ralentira le rythme de

l'innovation et en augmentera le coût. Des mesures de sécurité intégrées sont considérées comme primordiales à cet égard. De façon générale, on reconnaît qu'il existe une responsabilité évidente en matière de mesures protectrices de base. Toutefois, ces dernières devraient être proportionnées aux questions de protection de la vie privée relatives à chaque demande donnée. Par exemple, l'Internet n'exige pas beaucoup de mesures de protection intégrées, tandis que les transactions bancaires et l'accès aux dossiers médicaux nécessitent un haut degré de protection. Entre ces deux extrêmes, diverses mesures de protection pourraient être instituées, et les consommateurs auraient la liberté de choisir celles qu'ils préfèrent, moyennant parfois des frais supplémentaires. Au-delà des mesures de protection normales, comme l'utilisation de codes d'accès, les nouveaux progrès du chiffrement, comme le chiffrement «public-key», et l'utilisation de cartes à mémoire sont considérés comme des innovations supplémentaires. De plus, la mise en oeuvre de la technologie numérique passe pour être une contribution importante. Et l'on suggère que le gouvernement cherche à promouvoir la nouvelle technologie dans ce domaine, et encourage la recherche et le développement afin d'offrir de nouvelles possibilités à l'industrie canadienne. Sur la question de savoir si ces mesures seront plus coûteuses ou si elles entraveront l'innovation, l'opinion la plus courante est que ce ne sera pas le cas à condition qu'elles ne soient pas franchement excessives. Toutefois, comme le suggère un commissaire à la vie privée, les coûts y afférents, soit une perte de dignité humaine et d'autonomie, sont trop considérables pour ne pas exiger l'intégration de hauts niveaux de protection. En dernière analyse, le secteur privé reconnaît que si les consommateurs ne sont pas convaincus que l'autoroute de l'information protégera leur vie privée, ils n'utiliseront pas pleinement cet outil.

Sur la question de la façon dont les Canadiens peuvent participer davantage à la conception de technologies et de services susceptibles de menacer la vie privée, il y a un large éventail d'opinions. On souligne qu'à l'heure actuelle, les consommateurs ont déjà l'occasion de jouer un rôle. On cite comme exemple les audiences du CRTC sur l'instauration de nouveaux services de télécommunications réglementés. On invoque également la participation et les conseils en matière d'élaboration de nouvelles normes techniques de la CSA. N'empêche que les défenseurs des consommateurs et de la vie privée, ainsi que les commissaires à la vie privée, appuient fermement la participation du public à la mise au point de tous les nouveaux systèmes importants qui risquent de constituer une menace. Deux organismes privés appuient également la participation du public en alléguant que la consultation peut prévenir les retards et d'éventuels litiges. Ils donnent un exemple relatif au débat actuel sur la question de savoir si les services de liaison par fibres optiques devraient être directs à domicile, ou s'ils devraient se terminer à une distance de cent mètres, les radiocommunications prenant ensuite la relève. Cette dernière possibilité est moins coûteuse mais lourde de conséquences en matière de protection de

la vie privée. De toute façon, on est d'avis que des consultations préalables avec les consommateurs et/ou les commissaires à la protection de la vie privée peuvent être avantageuses pour l'entreprise privée, à condition qu'elles soient relativement informelles et qu'elles ne fassent pas l'objet d'audiences publiques traînant en longueur.

### ***L'éducation des consommateurs***

On reconnaît largement, au sein du public, un manque de sensibilisation aux avantages et aux services que fournit actuellement et que continuera d'assurer l'autoroute de l'information, et de la confusion à cet égard. Cela va de pair avec un manque tout aussi important de connaissance du droit à la protection de la vie privée, de la façon d'obtenir ce droit, des conséquences de la communication de renseignements personnels, ainsi que des mesures de protection disponibles. Résultat : des préoccupations vagues mais réelles qui pourraient nuire au succès de l'autoroute en question. On convient donc un peu partout que l'information du public sur ces questions est aussi essentielle qu'urgente pour atténuer les préoccupations, surtout à cause de la croissance rapide de ladite autoroute. En outre, on reconnaît que tant les employés que les entreprises ont besoin d'être informés sur leurs responsabilités à l'égard de la protection de la vie privée.

Il y a en général unanimité sur le fait que les gouvernements comme les entreprises ont de lourdes responsabilités dans ce domaine. La plupart des organismes privés indiquent leur détermination. Bon nombre d'entre eux exécutent déjà des programmes d'information, à l'intention non seulement de leurs clients mais aussi de leurs employés. De plus, les défenseurs des consommateurs et de la vie privée, de même que les commissaires à la vie privée, indiquent qu'ils désirent participer davantage, à condition que les fonds et les ressources nécessaires soient disponibles. Et l'on estime que les médias ont eu aussi un rôle important à jouer. Toutefois, on reconnaît également que les consommateurs eux-mêmes doivent prendre l'initiative d'étudier le contenu des documents d'information qui leur sont fournis ainsi que de marchander autour d'eux pour obtenir le meilleur dosage de services et de protection de leur vie privée, et comprendre leurs propres responsabilités quant aux questions relatives à cette protection. De la même façon, les entreprises doivent prendre l'initiative d'informer leurs clients sur les éventuels problèmes de protection de la vie privée posés par leurs produits et leurs services, et ne rien dissimuler jusqu'à ce qu'une crise ait lieu.

On juge que les outils disponibles sont nombreux et variés. Les pratiques commerciales journalières, jointes aux renseignements sur les codes de l'industrie, seront des mécanismes très efficaces, tout comme le fait de rendre public le modèle de code de protection de la vie privée de la CSA. On ne recommande pas les campagnes de publicité de grande envergure,

mais plutôt des campagnes périodiques de sensibilisation du public, qui pourraient prendre bien des formes. On est également d'avis que pour la distribution de documents comme des brochures, le recours aux centres d'information, notamment aux bibliothèques publiques et universitaires, est un autre possibilité. Les publications (p. ex. les brochures) peuvent s'adresser à divers publics, notamment à la population en général, aux écoles et aux universités, ainsi qu'aux clients des entreprises. D'autres suggestions sont l'instauration pour les consommateurs d'une ligne ouverte 24 heures sur 24, nationale, sans frais d'interurbain et financée par le secteur privé, et l'insertion d'une clause de confidentialité dans tous les marchés.

## **CONCLUSIONS**

---

### **Préoccupations**

Il va sans dire que la population exprime un large éventail de préoccupations réelles en matière de protection de la vie privée qui, si l'on n'en tient pas compte rapidement, risquent tôt ou tard de compromettre le bon fonctionnement de l'autoroute de l'information.

### **Comment assurer la protection de la vie privée?**

Il y a une divergence de vues importante entre la plupart des membres du secteur privé et les groupes de défense des consommateurs et de la vie privée, ainsi que les groupes de commissaires à la protection de la vie privée, en ce qui concerne les avantages relatifs de la législation et des codes volontaires. Toutefois, une façon pragmatique et conciliante d'aborder ces différences permet d'envisager un compromis.

Aucune méthode unique pour résoudre les problèmes n'est vraiment efficace, de sorte que c'est une combinaison des lignes de conduite indiquées dans le Document de travail qui a le plus de chances de réussir, parce que celles-ci sont interreliées et s'étayent les unes les autres.

Afin de résoudre globalement les divers problèmes déterminés par les répondants, et ce, dans les meilleurs délais possibles, un plan concerté devrait être élaboré.

On trouvera ci-après les éléments éventuels d'un plan que le Comité consultatif désirera peut-être prendre en considération :

- L'instauration par législation de normes nationales de protection de la vie privée, fondées probablement sur le modèle de code de protection de la CSA, en vertu desquelles les codes applicables au secteur privé seraient en vigueur et exécutoires.
- Les révisions à apporter à la *Loi sur la protection des renseignements personnels* fédérale, pour en éliminer les lacunes actuelles, notamment un préambule remanié, une disposition prévoyant la protection et la sécurité des renseignements en question, ainsi qu'une disposition visant à l'évaluation des incidences sur la vie privée au sein du secteur public.
- La mise sur pied d'un programme pour renforcer, étayer et mettre à jour les moyens de tenir compte des exigences de protection de la vie privée au sein du secteur public.

- L'amorce rapide de pourparlers avec les provinces pour mettre en oeuvre des normes nationales dans l'ensemble du pays.
- L'élaboration d'une législation qui ferait une infraction de l'interception des radiotélécommunications privées, et l'interdiction générale de fabriquer, d'importer, de vendre et de distribuer des analyseurs en mesure d'assurer le monitoring des radiotéléphones, notamment des téléphones cellulaires.
- L'élaboration d'un programme visant à promouvoir systématiquement l'élaboration de codes du secteur privé fondés sur le modèle de code de protection de la vie privée de la CSA.
- La création d'un programme conjoint (gouvernement-industrie) pour promouvoir et appuyer la mise au point de technologies de protection de la vie privée.
- Les consultations entre l'industrie/le gouvernement, les groupes de consommateurs et les commissaires à la protection de la vie privée au sujet de la mise au point de technologies et de systèmes importants et nouveaux qui risquent de constituer une menace pour la vie privée.
- L'élaboration d'un programme d'information conjoint (industrie-gouvernement) avec le concours des groupes de consommateurs et des commissaires à la protection de la vie privée.
- La tenue de consultations entre le gouvernement et les groupes de chercheurs médicaux et sociaux, pour résoudre la dichotomie apparente entre la protection des renseignements personnels et la nécessité de mener les recherches médicales et sociales nécessaires à la promotion du bien public.
- L'élaboration par le gouvernement d'une clause normalisée de protection de la vie privée, pour tous les marchés ou les accords de transfert ou d'échange de renseignements personnels avec les institutions ou établissements privés.
- Une annonce publique après l'adoption du plan et l'approbation du Ministre.

### ***Le fait de ne pas affronter les problèmes***

Le fait de ne pas tenter de régler les principaux problèmes indiqués par les répondants pourrait donner lieu à des préoccupations croissantes du public au sujet de la protection de la vie privée, doublées d'une répugnance à utiliser l'autoroute de l'information. Les normes canadiennes de protection de la vie privée risqueraient alors d'être jugées insatisfaisantes à la lumière des directives de la Communauté européenne.

**LA PROTECTION DE LA VIE PRIVÉE ET L'AUTOROUTE  
CANADIENNE DE L'INFORMATION**

---

***RÉSUMÉ DES MÉMOIRES REÇUS***

## TABLE DES MATIÈRES

<b>INTRODUCTION</b> .....	46
<b>RECHERCHE MÉDICALE ET SOCIALE</b> .....	48
<i>Patricia Baird, M.D., CM, FRCPC, FCCMG</i> .....	48
<i>Université Dalhousie</i> .....	48
<i>Allan S. Detsky, M.D., Ph.D, FRCPC</i> .....	49
<i>L'Institut canadien des recherches avancées, Le programme pour la santé des populations</i> .....	49
<i>Institute for Clinical Evaluative Sciences (ICES) de l'Ontario</i> .....	50
<i>Robert C. James, M.A., M.Sc.</i> .....	52
<i>Manitoba Cancer Treatment and Research Foundation</i> .....	52
<i>Judith Maxwell</i> .....	55
<i>McGill Health Services and Outcomes Research Group</i> .....	56
<i>Medical Society of Nova Scotia</i> .....	57
<i>Cam Mustard, Sc.D.</i> .....	58
<i>Howard B. Newcombe</i> .....	60
<i>Noralou P. Roos, Ph.D.</i> .....	61
<i>Leslie L. Roos, Ph.D.</i> .....	62
<i>Jorge Segovia, M.D., M.Sc. (santé communautaire)</i> .....	62
<i>Evelyn Shapiro, M.A.</i> .....	63
<i>Colin L. Soskolne, Ph.D., FACE</i> .....	64
<i>R. A. Spasoff, M.D.</i> .....	64
<i>University of Manitoba, Programmes de recherche et programmes externes</i> .....	65
<i>Université d'Ottawa, Centre de recherche et d'enseignement sur les droits de la personne</i> .....	65
<i>University of Waterloo, Bureau de la recherche</i> .....	68
<b>PARTICULIERS</b> .....	69
<i>Norah Duck</i> .....	69
<i>Brian Fitzgibbon</i> .....	69
<i>Harold Genz</i> .....	70
<i>Khalid Saeed, Holaser</i> .....	70
<i>J.C. Holst</i> .....	71
<i>Jorg P. Kranz</i> .....	71
<i>Steven Lotz</i> .....	72
<i>D.B. Morrow</i> .....	72
<i>R.B. Oulton</i> .....	73
<i>Richard D. Speers, D.D.S.</i> .....	73
<i>J.S. Tate</i> .....	75

<b>TÉLÉCOMMUNICATIONS ET TECHNOLOGIE</b> .....	<b>77</b>
<i>Association canadienne de télévision par câble (ACTC)</i> .....	77
<i>Association canadienne des utilisateurs de satellites (ACUS)</i> .....	79
<i>Consortium UBI</i> .....	81
<i>Association canadienne de la technologie de l'information (ACTI)</i> .....	82
<i>Mobility Canada</i> .....	86
<i>Conseil consultatif canadien de la radio</i> .....	87
<i>Association RadioComm du Canada (ARC)</i> .....	87
<i>Rogers Cantel Inc.</i> .....	89
<i>Rogers Communications Inc.</i> .....	91
<i>Stentor Telecom Policy Inc.</i> .....	93
<i>TELUS</i> .....	100
<i>Unitel Communications Inc.</i> .....	104
<b>DÉFENSEURS DES CONSOMMATEURS ET DE LA VIE PRIVÉE</b> .....	<b>107</b>
<i>Association des Consommateurs du Québec Inc.</i> .....	107
<i>Colin J. Bennett</i> .....	108
<i>The British Columbia Public Interest Advocacy Centre</i> .....	111
<i>Association des consommateurs du Canada (ACC)</i> .....	112
<i>Conseil canadien des consommateurs</i> .....	115
<i>Fédération Nationale des Associations de Consommateurs du Québec (FNACQ), L'Association</i> <i>Coopérative d'Économie Familiale du Centre de Montréal (ACEF-Centre) (Présentation conjointe)</i> .....	118
<i>La Ligue des droits et libertés</i> .....	122
<i>Le centre pour la défense de l'intérêt public</i> .....	125
<i>Charles D. Raab</i> .....	127
<i>Riley Information Services Inc.</i> .....	128
<i>Leslie Regan Shade</i> .....	132
<b>GROUPES DE SERVICES FINANCIERS, DE CRÉDIT ET DE MARKETING</b> .....	<b>134</b>
<i>Canada Trust</i> .....	134
<i>Association des banquiers canadiens</i> .....	134
<i>Association canadienne du marketing direct (ACMD)</i> .....	136
<i>Association Interac</i> .....	138
<i>Equifax Canada Inc.</i> .....	139
<b>COMMISSAIRES À LA PROTECTION DE LA VIE PRIVÉE</b> .....	<b>142</b>
<i>Commission d'accès à l'information du Québec</i> .....	142
<i>Commissariat à l'information et à la protection de la vie privée de la Colombie-Britannique</i> .....	144
<i>Commissaire à l'information et à la protection de la vie privée de l'Ontario</i> .....	146
<i>Commissariat à la protection de la vie privée du Canada</i> .....	151

<b>GOUVERNEMENTS</b> .....	155
<i>Gouvernement de la Colombie-Britannique</i> .....	155
<i>Santé et Bien-être social Canada</i> .....	157
<i>Ministère de la Santé et des Services sociaux de l'Île-du-Prince-Édouard</i> .....	158
<i>Secrétariat provincial de la Saskatchewan</i> .....	158
 <b>DIVERS</b> .....	 160
<i>Congrès du travail du Canada</i> .....	160
<i>Association canadienne de normalisation (CSA)</i> .....	161
<i>COMSEC Services Inc.</i> .....	162
<i>Bill Doskoch</i> .....	162
<i>Eridani Productions Ltd.</i> .....	163
<i>Curtis E.A. Karnow</i> .....	163
<i>Veronica Lacey</i> .....	164
<i>Detective Superintendent Ken Grange</i> .....	165

## **RÉSUMÉ DES MÉMOIRES REÇUS**

### **INTRODUCTION**

---

Les 76 mémoires reçus ont été classés dans huit catégories dont voici la répartition selon le nombre de répondants : Recherche médicale et sociale (21); Particuliers (11); Télécommunications et technologie (12); Défenseurs des consommateurs et de la vie privée (11); Finances, crédit et vente directe (5); Commissaires à la protection de la vie privée (4); Gouvernement (4); Autres (8).

On présente ci-après le résumé de chacun des mémoires selon les catégories et l'ordre susmentionnés. Puisque la longueur des mémoires (y compris les pièces jointes) variait entre une et soixante pages, il a fallu apporter un bon nombre de remaniements afin d'obtenir des proportions traitables. En général, les remaniements consistaient à supprimer les répétitions et les exemples fournis à l'appui. Toutefois, on a gardé les principaux éléments des questions soulevées et la justification de celles-ci. Ainsi, on estime avoir retenu les aspects importants de chaque mémoire.

Pour faciliter la comparaison, chaque mémoire a été résumé et remanié conformément à la structure générale du rapport principal. La présentation comprend donc un aperçu général et, s'il y a lieu, des commentaires sur la vie privée, les préoccupations et les moyens d'assurer la protection de la vie privée. Les commentaires sur les moyens d'assurer la protection de la vie privée sont ceux qui ont été fournis par les répondants au sujet des démarches exposées dans le Document de travail et correspondent aux chiffres romains ci-dessous. De la même façon, les réponses fournies à des questions particulières correspondent aux chiffres arabes ci-dessous. En outre, on présente les propositions et les recommandations formulées à l'égard des quatre démarches principales abordées dans le Document de travail.

#### **Démarches**

- I. La législation et la réglementation
- II. Les codes et les normes volontaires
- III. Les solutions technologiques
- IV. L'éducation des consommateurs

## **Réponses aux questions**

1. **Quels principes devraient être à la base d'une protection efficace de la vie privée?**
2. **Le gouvernement doit-il introduire des mesures plus fermes pour protéger la vie privée et la sécurité de l'information? Comment peut-on utiliser efficacement chacune des quatre démarches décrites ci-dessus?**
3. **Faut-il instaurer une protection à l'échelle nationale ou au contraire faire confiance à une réglementation provinciale ou sectorielle?**
4. **Dans quelles circonstances conviendrait-il de recourir à des lignes directrices volontaires sur la vie privée préparées par le monde des affaires?**
5. **L'autoroute de l'information devrait-elle être conçue pour assurer un niveau élevé de protection ou, au contraire, une telle structure ralentirait-elle le rythme et ferait-elle augmenter le coût de l'innovation?**
6. **Comment les Canadiens peuvent-ils participer davantage au processus de conception de techniques et de services susceptibles de menacer la vie privée?**
7. **Comment les Canadiens peuvent-ils se renseigner davantage sur la valeur de leurs renseignements personnels et sur la nécessité d'en contrôler l'utilisation? Quel rôle le monde des affaires et les pouvoirs publics doivent-ils jouer dans l'éducation du public?**

## **RECHERCHE MÉDICALE ET SOCIALE**

---

### **Patricia Baird, M.D., CM, FRCPC, FCCMG**

Patricia Baird est professeure à l'Université de la Colombie-Britannique.

Elle estime que le droit de chaque personne de contrôler l'information qui la concerne est une valeur fondamentale dans la société canadienne et que ce droit doit être respecté. Par ailleurs, la société a aussi intérêt à utiliser l'information des dossiers médicaux pour étudier les tendances des maladies ou des incapacités, pour examiner l'utilisation de procédures nuisibles et de drogues et pour évaluer les résultats des traitements. Les citoyens canadiens comptent sur les gouvernements pour protéger leur sécurité à cet égard. L'accès à cette information, le couplage des dossiers et d'autres techniques de recherche sont donc essentiels. Elle croit fermement qu'il est possible de protéger la vie privée des personnes tout en retirant les avantages de ces types de recherches dont a besoin la société.

#### **Propositions et recommandations**

La législation et la réglementation sur la protection de la vie privée devraient permettre le couplage, l'agrégation et l'analyse de l'information sur les personnes à des fins de recherches sur la santé.

### **Université Dalhousie**

Le mémoire est présenté par le Dr John Ruedy, doyen de la Faculté de médecine et président du Comité consultatif, de la Section de recherches sur la santé de la population.

La Section de recherches administre une base de données sur les contacts avec le système de santé. Cette base de données est utilisée dans les recherches destinées à améliorer l'efficacité et l'efficacé du système de santé canadien. Les recherches nécessitent l'utilisation de données longitudinales sur les personnes et le couplage de ces données avec celles qui proviennent de sources et de programmes différents. Puisque les chercheurs accordent une grande importance à la protection de la vie privée, ils assurent l'anonymat des personnes en procédant au chiffrement des données à différents niveaux de programme et de source. De plus, des principes et des procédures ont été établis afin de prévenir la divulgation de renseignements par inadvertance, et tous les travaux de recherches sont filtrés par un comité de recherche et renvoyés à un comité d'éthique de l'université, s'il y a lieu. Ainsi, la confidentialité des dossiers personnels est protégée, et l'information peut servir à des recherches légitimes et importantes.

L'auteur dit craindre que les futures normes, exigeant le consentement pour l'utilisation de renseignements personnels ou limitant la collecte et la conservation des données, empêchent la réalisation de recherches et privent ainsi le public des avantages de celles-ci. Il faut un juste équilibre entre la nécessité de protéger la vie privée et la nécessité de maximiser l'utilisation des ressources limitées du système de santé.

#### **Propositions et recommandations**

Dans les futures lois sur la protection de la vie privée, les renseignements sur les personnes, dépouillés d'identificateurs et utilisés pour l'analyse systématique approuvée, ne devraient pas être assimilés aux renseignements personnels.

Les nouvelles politiques doivent reconnaître les avantages pour le public d'avoir accès aux données sur les personnes à des fins de recherches sur la santé.

### ***Allan S. Detsky, M.D., Ph.D., FRCPC***

Allan Detsky est chercheur national et professeur en administration de la santé et en médecine à l'Université de Toronto.

Le professeur Detsky craint que les éventuelles lois sur la protection de la vie privée ne permettent pas aux chercheurs d'utiliser les fichiers administratifs dans des recherches ultérieures. De telles recherches aideront les décideurs à déterminer la répartition des ressources qui est essentielle au dénouement de la crise dans les coûts des soins de santé au Canada. L'utilisation de données administratives est cruciale pour la recherche et nécessite un couplage des fichiers en l'absence d'un consentement explicite. Dans tous les cas dont le professeur Detsky a eu connaissance, les identificateurs des patients ont été supprimés, et l'identité de ces personnes ne pourrait nullement être compromise.

### ***L'Institut canadien des recherches avancées, Le programme pour la santé des populations***

«La santé des populations» est un réseau de chercheurs principaux du Canada et de l'étranger qui sont rattachés à des universités et à d'autres organismes tels que Statistique Canada. Ces chercheurs font avancer la connaissance des facteurs fondamentaux qui expliquent les écarts marqués entre les différentes tranches de la population canadienne sur le plan de la santé. Ils effectuent également des recherches sur le fonctionnement du système de soins de santé.

Dans leurs travaux de recherche, les membres du réseau et de nombreux autres épidémiologistes et spécialistes en sciences sociales dépendent

énormément de l'accès aux bases de données provinciales sur la santé et du couplage des données sur les soins de santé et des données socio-économiques pour répondre à des questions clés sur la santé des Canadiens et sur le recours au système de santé. Il leur faut donc rassembler des données tirées de nombreuses sources sur une longue période, car l'évolution de l'état de santé d'un patient et son recours au système de santé ne sont pas un événement unique dans le temps. Des recherches de ce genre permettront de répondre à une question bien typique, à savoir est-ce que la réduction du nombre et de l'utilisation de lits pour malades hospitalisés a pour effet d'abaisser la qualité des soins? Les chercheurs effectuent leurs travaux sans compromettre la vie privée des personnes en faisant un couplage anonyme des données sur les patients. De la même façon, les membres du réseau ont travaillé étroitement avec les commissaires fédéral et provinciaux à la protection de la vie privée afin d'obtenir la permission de faire ces couplages. De plus, tous les travaux de recherches sont examinés par le comité d'éthique universitaire compétent.

Certaines démarches proposées dans le Document de travail soulèvent des préoccupations. Bien qu'elles satisfassent à des exigences importantes en matière de protection de la vie privée, elles pourraient avoir des effets dévastateurs et mettre fin à certaines des recherches les plus prometteuses actuellement réalisées dans le domaine de la santé au Canada. «Au médecin dont les recommandations ne tiendraient pas compte des effets secondaires, on reprocherait à juste titre de s'attaquer à la maladie, mais d'exposer le patient à des risques inutiles». Des inquiétudes sont également exprimées au sujet de l'adoption des directives provisoires de la Communauté européenne sur la confidentialité des données (particulièrement celles qui se rapportent au consentement, aux utilisations et aux délais proposés pour la conservation) qui risquent de mettre un terme aux recherches et d'avoir de lourdes conséquences sur la santé publique. Dans les cas où les recherches sont justifiées et la protection des données est adéquate, des restrictions générales concernant la conservation, le couplage et l'utilisation de données personnelles dépasseraient nettement les normes minimales de protection de la vie privée et iraient à l'encontre de l'intérêt public.

#### **Propositions et recommandations**

Il ne faudrait pas que des restrictions excessives puissent mettre en péril le milieu fructueux de la recherche.

### ***Institute for Clinical Evaluative Sciences (ICES) de l'Ontario***

L'ICES est un organisme de recherche sans but lucratif financé par le ministère de la Santé de l'Ontario. Il a pour mandat d'effectuer des recherches qui amélioreront la qualité, l'efficacité et l'efficience des services fournis par les médecins et les autres professionnels de la santé en

Ontario. Le mémoire est présenté par C. David Naylor, M.D., D.Phil., FRCP, en sa qualité de directeur de l'épidémiologie clinique au Sunnybrook Health Science Centre de l'Université de Toronto et à titre de président-directeur général de l'ICES.

L'utilisation d'une vaste gamme de données sur la santé et leur couplage à l'aide d'identificateurs uniques constituent la pierre angulaire de la recherche sur la santé et procurent des avantages réels aux Canadiens. Il existe une nette différence entre l'utilisation qu'en font les entreprises à but lucratif engagées dans le groupement et la revente des données, les compagnies d'assurances voulant déterminer l'assurabilité d'une personne et le gouvernement lui-même. Les chercheurs dans le secteur de la santé travaillent dans des centres d'enseignement supérieur, font revoir leurs travaux par un comité d'éthique et se soucient grandement de la protection de la vie privée. Bien que les recherches sur la santé suivent chaque patient sur une période déterminée, elles ne portent pas sur un patient en particulier, mais sur des groupes ou des populations de patients. Même si les personnes craignent une mauvaise utilisation des renseignements par les fournisseurs de services et les employeurs, l'Institut estime que les Canadiens sont disposés à accepter que les chercheurs aient un accès limité aux données sur la santé, à condition que la confidentialité soit assurée.

Pour assurer la confidentialité des données, l'Institut a recours notamment au brouillage des identificateurs des patients, au déchiquetage et à l'élimination des papiers rebuts confidentiels. De même, le personnel signe une entente stricte de non-divulgateion. L'Institut a publié, en annexe à un document de travail, une analyse bibliographique sur l'éthique et les recherches sur les services de santé, ce qui témoigne de l'importance qu'il accorde à la protection de la vie privée.

Des préoccupations sont exprimées au sujet de certains aspects du Document de travail, particulièrement les restrictions possibles de l'utilisation d'identificateurs numériques uniques. Sans ces identificateurs, les chercheurs ne peuvent pas comprendre le mouvement des patients dans le système de santé. Par exemple, les recherches concernant un risque particulier pour la santé pourraient comporter l'étude de données sur des dizaines de milliers de patients afin de déterminer s'il y a lieu de s'inquiéter de ce risque. On dit également craindre que l'adoption des directives provisoires de la Communauté européenne, particulièrement en ce qui concerne le consentement, pourrait nuire à la validité des résultats des recherches. La possibilité de généralisation du reste des données pourrait être mise en doute si un grand nombre de patients refusaient de donner leur consentement parce qu'ils comprennent mal les mesures de protection de la vie privée utilisées par les chercheurs.

### **Propositions et recommandations**

L'ICES propose d'approfondir les consultations entre les chercheurs de la santé et d'autres citoyens et parties intéressées afin d'assurer l'établissement de principes de fonctionnement normalisés qui satisfassent aux exigences en matière de protection de la vie privée.

### ***Robert C. James, M.A., M.Sc.***

Robert C. James est étudiant de doctorat en sciences de la santé communautaire à l'Université du Manitoba.

Reconnaissant l'importance de protéger les données, il dit craindre que l'application aveugle de règles de protection des données et de la vie privée, qui visent généralement à restreindre le gouvernement et les entreprises, peut gêner ou faire échouer d'importants travaux de recherches ou d'élaboration de politiques. Il redoute plus particulièrement qu'une interprétation stricte du Document de travail mène à une situation semblable à celle qui existe en Europe. À cet égard, on avait prédit que les directives provisoires de la Communauté européenne auraient un effet dissuasif dans le secteur de la santé publique, vu la nécessité du consentement et les limites concernant l'utilisation secondaire des données. Au Canada, un tel effet occasionnerait des coûts sociaux importants et peut être évité si l'on reconnaît le rôle important de la recherche médicale et sociale. En effet, la réalisation de ces recherches repose sur l'utilisation de données pouvant être couplées au niveau des personnes, et la nécessité du consentement ouvre la voie à un faux biais susceptible d'invalider les recherches.

### **Propositions et recommandations**

Bien qu'il ne demande pas une exemption générale pour les chercheurs, il presse le Comité consultatif de travailler avec ces derniers afin de définir des normes appropriées pour l'élaboration, la mise à jour, l'utilisation et l'élimination des données sur les personnes. Il faut se pencher sur la question du consentement et de l'utilisation secondaire des données.

### ***Manitoba Cancer Treatment and Research Foundation***

La Manitoba Cancer Treatment and Research Foundation, qui administre le registre provincial du cancer du Manitoba (RPCM), exerce un mandat qui lui a été conféré par une loi provinciale (dont un exemplaire est joint à la présente). Cette fondation existe depuis plus de soixante-dix ans et vise principalement à soutenir la recherche sur le cancer.

La Fondation a énoncé huit principes sur lesquels est fondée la protection de la vie privée. Elle soutient aussi la législation qui reconnaît les avantages publics et privés de recueillir et d'enregistrer des renseignements

personnels et appuie l'application de normes volontaires assorties aux lois. Elle estime que la technologie peut constituer une partie de la solution et qu'il faut manifestement sensibiliser les consommateurs.

Selon la Fondation, il faudrait reconnaître que la recherche épidémiologique a contribué à réduire l'incidence de la maladie ou à l'enrayer. De plus, grâce à la collecte, à la conservation et au couplage des données sur les personnes, le public reçoit de nombreux avantages, notamment dans les secteurs de l'éducation, des services sociaux et des soins de santé. Un autre point soulevé est le fait que les registres provinciaux du cancer continuent d'être accessibles pour les travaux permanents de recherche épidémiologique et d'évaluation des soins de santé.

Le RPCM applique des lignes directrices strictes en ce qui concerne la diffusion des données. Lorsqu'il s'agit de données qui permettraient d'identifier une personne, leur diffusion doit être approuvée par le comité d'accès du RPCM. De la même façon, s'il est nécessaire de communiquer avec les personnes inscrites au registre, il faut l'approbation du comité d'accès et un examen approfondi par le comité d'éthique de la Faculté de médecine de l'Université du Manitoba. La Fondation prend très au sérieux sa responsabilité de garantir la protection de la vie privée et la confidentialité de l'information stockée dans le RPCM.

#### **Démarches**

- I. Les lois doivent faire la distinction entre l'information recueillie pour le bien privé et celle qui est recueillie pour le bien public.
- II. L'application et la mise en oeuvre de normes volontaires permettent d'améliorer la réaction générale face à l'évolution de l'opinion publique, d'exercer un contrôle permanent et d'améliorer la qualité des décisions.
- III. Les mécanismes de verrouillage électroniques (accès, chiffrement, mots de passe) figurent parmi les outils de base destinés à assurer la sécurité des données.
- IV. Il faut renseigner le consommateur afin qu'il comprenne les capacités de la technologie, les lois et lignes directrices permettant l'utilisation des renseignements personnels, ainsi que les mesures actuelles de protection.

#### **Réponses aux questions**

1. Les huit principes suivants sont présentés.
  - Les renseignements concernant une personne lui appartiennent.
  - Les personnes ont le droit de conclure des ententes commerciales en ce qui concerne leur information.

- Les transactions commerciales fondées sur les caractéristiques d'une personne (âge, santé, etc.) doivent se limiter à l'information recueillie avec son consentement.
  - La société doit veiller à ce que soient exécutées des transactions justes et libres de contrainte.
  - La société, par l'entremise de ses gouvernements et organismes, a l'obligation de procurer des avantages publics réels.
  - La société a des droits d'accès limités à l'information décrivant la société dans son ensemble et des membres en particulier.
  - Les personnes ont droit à une juste compensation pour l'utilisation des renseignements qui les concernent.
  - La société a l'obligation de protéger la vie privée et l'anonymat d'une personne lorsque des données sont recueillies en vue de procurer un bien public.
2. Les lois doivent protéger les personnes contre les pertes financières ou les dommages personnels qui découlent de l'utilisation de renseignements personnels sans autorisation et restreindre l'information pouvant être utilisée dans des transactions privées. Elles doivent fournir un cadre garantissant que l'information demandée est juste et raisonnable, qu'elle ne porte pas atteinte à la vie privée d'une personne et qu'elle servira uniquement aux fins pour lesquelles elle a été recueillie. Toute nouvelle réglementation en la matière doit reconnaître et refléter les mesures de protection en vigueur, l'existence de corps professionnels dûment constitués qui sont dotés de codes d'éthique, et les politiques institutionnalisées de longue date qui régissent la confidentialité des renseignements sur la santé et l'examen par un comité d'éthique ou par les pairs.
3. Bien que des normes nationales soient nécessaires, elles doivent admettre des libertés locales appropriées. Il faut également prévoir une protection nationale de façon à permettre le partage des données entre les provinces tout en protégeant la vie privée. Pour obtenir des résultats fiables, il faut souvent effectuer des recherches épidémiologiques et des études d'évaluation de la santé sur un grand nombre de personnes, et la seule solution consiste à mener ces travaux à l'échelle nationale.
4. Des lignes directrices volontaires ont précédé certaines lois dans bien des domaines, et un grand nombre d'organisations et de professionnels ont un code d'éthique que le public peut examiner. De même, l'utilisation de normes volontaires permet une éducation et une évaluation permanentes. De plus, pour être efficaces, ces normes doivent être revues par une tierce partie ou par des organismes externes. On ne pourrait imaginer que les lois et les

politiques à elles seules puissent atteindre le niveau de protection de la vie privée et de confidentialité qui serait obtenu si elles étaient assorties de normes volontaires.

5. De toute évidence, le coût de la sécurité influe toujours sur le coût et l'utilité de l'innovation.
6. Les Canadiens peuvent participer davantage au processus en élaborant des principes et des lignes directrices qui dictent les principes et les droits en matière de protection de la vie privée.
7. Il incombe aux gouvernements et aux organismes de faire connaître les avantages éventuels, les avantages passés et les travaux actuels, tout en s'assurant que le public comprend le rôle du chien de garde, du protecteur du citoyen et de la sécurité. Il faut aussi renseigner le public sur les lois destinées à protéger les consommateurs et à les aider à prendre des décisions éclairées. Le plus grand risque auquel s'expose le public c'est de n'avoir aucun recours adéquat simplement parce qu'il n'a pas les connaissances à cet égard ou que les processus ne sont pas offerts.

#### **Propositions et recommandations**

Il faudrait autoriser clairement, sinon encourager, l'utilisation d'information lorsqu'il y va de l'intérêt public et qu'il n'en découle pas de coûts excessifs pour la personne.

Il faut un chien de garde ou un protecteur du citoyen pour répondre aux préoccupations du public et offrir un recours non judiciaire.

### ***Judith Maxwell***

M<sup>me</sup> Maxwell présente ses commentaires en tant que chercheuse en sciences sociales. Sa principale préoccupation est de veiller à ce que le Canada puisse continuer d'utiliser les fichiers administratifs afin d'observer les réactions des familles et des personnes face aux changements sociaux et économiques. L'utilisation de ces fichiers joue un rôle essentiel dans la prise de décisions judicieuses d'ordre public et dans l'évaluation des programmes et politiques du gouvernement et influe grandement sur les réformes des politiques sociales et économiques. En bref, c'est une façon de responsabiliser les gouvernements et de les aider à être réceptifs. De plus, si les gens comprennent leurs concitoyens, le processus démocratique s'en trouve amélioré.

L'information nécessaire est obtenue par deux moyens : le couplage des fichiers administratifs et statistiques à un moment précis dans le temps et le suivi chronologique des faits nouveaux dans un fichier administratif. Ces deux moyens réunis permettent une base d'analyse encore plus solide. Ce

genre de recherche est abordable comparativement aux délais et aux coûts astronomiques que comportent les enquêtes.

Il faut un juste équilibre entre les nombreux intérêts de la société. Il est donc essentiel de tenir compte des intérêts des chercheurs et des décideurs. Ainsi, l'accès aux fichiers administratifs ne devrait jamais être autorisé sans une évaluation minutieuse du bien-fondé de la recherche, et le couplage de ces fichiers doit se révéler très avantageux pour le public.

En matière de protection de la vie privée, on devrait pouvoir élaborer des règles qui répondent aux normes énoncées dans le Document de travail. Toutefois, des mesures comme celles qui sont mentionnées dans le document poseraient des difficultés insurmontables pour la recherche sociale, p. ex. la suppression de tous les identificateurs empêcherait le couplage des données, l'interdiction du stockage à long terme ne permettrait pas de suivre un dossier durant toute une vie, et la nécessité d'un consentement explicite présenterait des obstacles sur les plans logistique et financier.

#### **Propositions et recommandations**

La responsabilité du couplage des fichiers et de la mise à jour des données pourrait être confiée à un organisme indépendant ayant la capacité technique et la crédibilité politique, p. ex. Statistique Canada.

Le Comité consultatif devrait chercher à établir des règlements qui permettraient aux nouvelles technologies de procurer un bien public grâce au couplage des fichiers.

### ***McGill Health Services and Outcomes Research Group***

Le Groupe est formé de professeurs et de chercheurs du Département de médecine, du Département d'épidémiologie et de biostatistique, de l'École de physiothérapie et d'ergothérapie et de l'École de santé au travail de l'Université McGill.

En résumé, le Groupe se préoccupe beaucoup du fait que des règles d'accès de plus en plus restrictives limiteront de précieuses recherches sur la santé et iront à l'encontre de l'intérêt public. De nos jours, les conseils d'éthique et les organismes provinciaux examinent régulièrement l'utilisation des données et la sécurité des programmes de recherches sur la santé. On estime que ces procédures protègent adéquatement la vie privée, tout en permettant de produire des renseignements importants qui protègent la santé publique.

Le Groupe ne traite que d'un aspect du Document de travail, soit l'accès aux données sur les services de santé par les chercheurs. Il craint que les problèmes de protection de la vie privée découlant de l'accès aux données

recueillies à des fins commerciales soient assimilés aux problèmes découlant de l'accès aux données sur la santé. Le commerce et la santé sont des domaines complètement différents : les intervenants sont différents, de même que les codes de déontologie qui les régissent. Avoir un ensemble de règles pour deux fichiers tout à fait différents risque de mener à des compromis, ce qui pourrait imposer trop de restrictions à un groupe, et pas suffisamment à l'autre. Dans le secteur de la santé, les chercheurs analysent l'information concernant l'état de santé et non la personne. C'est la principale différence entre les activités des deux domaines.

Le Groupe cite en exemple différents avantages importants des recherches sur la santé, tels que la continuité et l'efficacité des services de santé, l'étendue de la consommation de plusieurs drogues chez les personnes âgées, etc. De même, il s'interroge sur la nécessité de prévoir diverses formes de protection de la vie privée dans les recherches sur la santé. Il estime que la nécessité d'un consentement préalable fait augmenter les coûts administratifs à une période où les services aux patients diminuent. L'utilisation d'identificateurs personnels et le couplage entre les bases de données sont nécessaires aux recherches sur des maladies graves et mortelles comme le cancer et les maladies du coeur. La conservation des données pendant de longues périodes est rentable, car ces données peuvent servir à répondre à bien des questions sur la santé longtemps après avoir été recueillies.

Il semble beaucoup plus important d'assurer de hauts niveaux de sécurité que de restreindre l'accès et le couplage des données. D'importantes mesures de sécurité sont le brouillage des identificateurs personnels, le verrouillage des locaux de recherches, les systèmes de sécurité informatique, l'adhésion à un code d'éthique, et l'élaboration et la mise en application par les tierces parties d'un protocole pour les projets de recherche. De même, les chercheurs sont indépendants des corps administratifs à qui la collecte et l'analyse des données pourraient profiter. Ils ne font qu'analyser les données afin de répondre aux questions importantes sur la santé publique et ont la formation nécessaire pour bien cerner la question et rejeter les données invalides. Par conséquent, cet examen indépendant et professionnel protège le public et le met à l'abri des mauvaises décisions de principe qui pourraient être à la fois coûteuses et dangereuses pour les personnes qui ont besoin de services de santé.

### ***Medical Society of Nova Scotia***

La Medical Society of Nova Scotia est une section de l'Association médicale canadienne.

Cette société appuie fermement la réalisation d'études sur les soins de santé et estime que ce serait une perte inestimable si la capacité de mener

ces études était compromise. Elle soutiendrait toute politique qui permettrait l'utilisation de données anonymes sur les personnes dans le cadre de recherches systématiques.

### **Propositions et recommandations**

Toute définition de «renseignements personnels» prévue par les futures lois sur la protection de la vie privée devrait exclure expressément les renseignements traités de manière anonyme dans le cadre de recherches systématiques.

### ***Cam Mustard, Sc.D.***

Cam Mustard est membre du corps professoral du Manitoba Centre for Health Policy and Evaluation et professeur adjoint des sciences de la santé communautaire à la Faculté de médecine de l'Université du Manitoba.

Comme remarque générale, le Dr Mustard dit que le Document de travail ne traite pas de façon adéquate des questions concernant l'information sur la santé. Il soulève quatre points particuliers à cet égard.

Le document ne tient pas compte des conséquences d'une obligation légale d'obtenir au préalable le consentement d'une personne, obligation susceptible de détériorer, sinon de détruire, la fonction de recherche qui présente de précieux avantages à la société et aux personnes.

Puisque l'information sur la santé des personnes est utilisée depuis fort longtemps à des fins de statistique et de recherche, la surveillance de la maladie ainsi que le contrôle de l'efficacité et de l'efficience du système de santé sont des fonctions fondamentales de la société canadienne et ne sont pas moins importantes que la protection de la vie privée.

Le document ne fait nullement état de l'importance des précédents qui ont été créés en matière de protection volontaire de la vie privée au pays en ce qui concerne l'utilisation de renseignements sur la santé des personnes pour la recherche; c'est là une omission inacceptable qui déforme la réalité. Ces précédents s'expliquent par la croyance selon laquelle la protection de la vie privée d'une personne est aussi importante que la poursuite de tout projet de recherche, comme en témoigne la vaste gamme de mesures de protection qui ont été prises. Les mesures consistent notamment à rendre anonymes les données sur les personnes, à interdire la présentation des résultats de recherches au niveau des personnes, à séparer du point de vue structurel la recherche et les fonctions administratives, à utiliser d'importants systèmes de sécurité informatique, à faire revoir systématiquement toutes les activités de recherche par des organismes gouvernementaux et scientifiques de surveillance, et à conclure avec tous les employés des ententes de non divulgation qui prévoient des mesures disciplinaires.

Le document ne fait pas la distinction entre l'appréhension générale du public à l'égard de la protection de la vie privée et son appui énergique et soutenu à la recherche sur la santé. Le taux de consentement dans le cadre de l'Enquête nationale sur la santé de la population dépasse actuellement 90 %.

Afin d'approfondir ces questions, le Dr Mustard joint à son mémoire un rapport de 1990 destiné au Groupe de travail national sur l'information en matière de santé et intitulé «Les conséquences de la protection des renseignements personnels et de leur confidentialité pour l'utilisation des données sur la santé dans le domaine de la recherche et de la statistique». Le rapport, préparé par une équipe de projet dirigée par Louise Desramaux de Statistique Canada, a été rédigé par le professeur David H. Flaherty. L'auteur traite en détail de l'historique et du contexte de quatorze problèmes et préoccupations touchant à la protection de la vie privée, cherche à les expliquer et, si possible, présente des moyens de les résoudre. Les préoccupations, particulièrement celles des défenseurs de la vie privée, portent sur les questions suivantes : l'éventail des bases de données administratives et statistiques et l'étendue des couplages des enregistrements; l'appariement des données statistiques et administratives; la gamme des identificateurs uniques; la nécessité d'un consentement éclairé pour l'utilisation secondaire des données personnelles sur la santé; l'utilisation de données statistiques permettant l'identification des personnes à des fins administratives; les risques de divulgation involontaire de renseignements permettant l'identification des personnes; et le fait que les données statistiques sont souvent centralisées et conservées pendant de longues périodes et qu'elles ne sont pas toujours rendues anonymes. De plus, le rapport fait ressortir les points suivants : il est essentiel que les défenseurs de la vie privée et le grand public reconnaissent qu'il existe une distinction fonctionnelle nécessaire entre l'utilisation des données personnelles à des fins de recherche et de statistique et leur utilisation à des fins administratives; ces défenseurs appuient l'application de lois provinciales générales en matière de protection des données partout au pays et de lois sectorielles particulières pour l'information sur la santé dans les secteurs public et privé; le grand public et ces défenseurs ne comprennent pas très bien que les renseignements personnels fournis à Statistique Canada sont strictement confidentiels; ces défenseurs restent prudents lorsqu'il s'agit de reconnaître l'intérêt de disposer de renseignements améliorés et essentiels sur la santé qui doivent être fondés sur des couplages d'enregistrements statistiques; ces défenseurs reconnaissent que les solutions techniques peuvent et doivent garantir la confidentialité; et les taux de réponse aux enquêtes sur la santé sont très élevés, ce qui suppose que le public comprend l'importance capitale des connaissances sur la santé. Face à ces préoccupations et à ces questions, le professeur Flaherty voit différentes solutions possibles, notamment : tenir des consultations entre la communauté de chercheurs et de statisticiens et les groupes mandataires, par exemple les commissaires à la protection de

la vie privée, les associations de consommateurs, etc; faire en sorte que les chercheurs et les statisticiens sensibilisent de façon continue le public au travail sérieux dans lequel ils sont engagés, aux mesures de protection des données qu'ils appliquent minutieusement, aux problèmes que peuvent poser les taux de réponse et les relations avec le public, et au fait que les couplages à des fins de statistique et de recherche peuvent s'effectuer dans un cadre contrôlé qui présente peu de menace réelle pour la vie privée; appliquer des lois provinciales visant à restreindre l'utilisation d'identificateurs sur la santé à des fins de recherche dans les secteurs public et privé; appliquer des lois, des politiques et des méthodes qui établissent une nette distinction fonctionnelle entre l'utilisation des données personnelles à des fins de recherche et de statistique et leur utilisation à des fins administratives; s'assurer que l'on reconnaisse que le consentement éclairé de l'utilisation secondaire de données personnelles risque de bloquer l'amélioration du système d'information sur la santé; promouvoir activement l'application de lois générales de protection des données dans le secteur public de toutes les provinces; et appuyer le renforcement de lois particulières sur la protection des données sur la santé dans les secteurs public et privé.

#### **Propositions et recommandations**

Il doit y avoir un équilibre entre les intérêts publics et les intérêts privés en ce qui concerne la protection de renseignements personnels dans les recherches sur la santé. Cet équilibre peut être atteint en partie par les moyens suivants : reconnaître l'appui et l'engagement sérieux du public à l'égard des recherches sur la santé et, par le fait même, son consentement à l'utilisation de renseignements personnels dans les recherches sur la santé; mettre en application des lois prévoyant des poursuites criminelles dans les cas de divulgation de renseignements personnels sur la santé par les chercheurs ou les organismes de recherche; et rendre obligatoires les fonctions actuelles de surveillance par les organismes publics et scientifiques dans toute nouvelle initiative de protection de la vie privée.

#### ***Howard B. Newcombe***

Selon M. Newcombe, notre «droit de vivre en paix» et de nous opposer à l'utilisation de renseignements personnels nous concernant est une idée fort intéressante, mais elle ne reflète pas ce que les gens veulent vraiment. Bien qu'ils veuillent que la confidentialité soit rigoureusement respectée, ils s'attendent aussi à une protection, à des services et à des avantages de toutes sortes qui dépendent de renseignements personnels. Il dit que les registres du cancer sont actuellement menacés en Europe par les lois sur la «protection de la vie privée» qui entreront prochainement en vigueur et que les mêmes dangers ont été maintes fois invoqués publiquement en Ontario.

Personne ne conteste la nécessité de la confidentialité, mais ne soyons pas bernés par l'attrait politique d'une vision irréaliste et néfaste de ce qu'est la protection de la vie privée.

### ***Noralou P. Roos, Ph.D.***

Noralou Roos est directrice du Manitoba Centre for Health Policy and Evaluation, professeure des sciences de la santé communautaire à la Faculté de médecine de l'Université du Manitoba; chercheuse nationale et collaboratrice de l'Institut canadien des recherches avancées. Elle travaille avec des banques de données sur les contacts avec le système de santé depuis les vingt dernières années.

De façon générale, Dr Roos redoute que le Canada suive l'exemple de la Communauté européenne (CE) et tente d'adopter des normes si restrictives qu'elles mettent en péril d'importants travaux de recherche dont pourrait profiter le public.

Elle joint à son mémoire des copies d'articles de diverses revues médicales dans lesquels on dit craindre que les normes proposées par la CE, ainsi que les opinions de nombreux défenseurs canadiens de la vie privée, menacent la tenue d'études valides sur l'épidémiologie et les soins de santé (par exemple pour le cancer et les maladies du coeur) et la prestation efficace des services de santé.

Elle s'inquiète plus particulièrement du fait que les normes proposées par la CE prévoient les dispositions suivantes : la conservation des données personnelles sous forme identifiable seulement aussi longtemps que nécessaire aux fins pour lesquelles elles ont été enregistrées; l'interdiction de traiter les données sur la santé, sauf si les personnes en cause y consentent par écrit; et l'interdiction de coupler les dossiers entre les bases de données à moins du consentement explicite des patients.

Elle affirme que les données administratives, notamment celles qui sont utilisées pour la rémunération des médecins et l'enregistrement des patients traités à l'hôpital, constituent une source précieuse pour étudier les questions de la santé publique, etc. De telles recherches nécessitent le couplage des dossiers de milliers de personnes, mais aucun fichier de recherche ne contient de noms ou d'adresses, et aucun patient ou médecin n'a été identifié dans le cadre des recherches. Dr Roos joint à son mémoire une copie des règles du Manitoba Centre for Health Policy and Evaluation concernant la protection de la confidentialité afin de montrer les précautions extraordinaires prises à cet égard. Elle estime aussi qu'il est rarement possible de connaître d'avance les nombreuses possibilités de recherche que présenteront les données dix ou quinze ans plus tard. De même, le Conseil de recherches médicales, dans ses lignes directrices de 1987 en matière de recherches sur les sujets humains, reconnaît l'importance des

recherches épidémiologiques et insiste sur la nécessité d'autoriser la recherche dans les dossiers sans consentement préalable.

Elle est convaincue que des lignes directrices protégeant l'identité des personnes devraient être adoptées au Canada, mais qu'elles devraient être axées sur la protection de la confidentialité des dossiers et ne pas empêcher les chercheurs d'y accéder pour des raisons valables. Il faudrait alors que les dossiers soient conservés pendant de longues périodes et que le couplage entre les fichiers soit autorisé. Il faut veiller à ne pas priver la société des avantages pouvant découler de l'utilisation consciencieuse des données recueillies aux frais du contribuable dans l'intérêt public.

#### **Propositions et recommandations**

Le Comité consultatif devrait adopter une approche différente des normes dites européennes et proposer des lignes directrices qui reconnaissent et assurent les possibilités de recherches à des fins légitimes.

#### ***Leslie L. Roos, Ph.D.***

Leslie Roos est directeur de la base de données de recherches sur la santé pour le Manitoba Centre for Health Policy and Evaluation, professeur des sciences de la santé communautaire à la Faculté de médecine de l'Université du Manitoba, chercheur national et collaborateur de l'Institut canadien des recherches avancées.

À titre de chercheur actif participant à l'analyse de grosses bases de données administratives depuis dix-neuf ans, Dr Roos n'a eu connaissance d'aucun problème concernant leurs données. Grâce à un examen adéquat des activités par des comités universitaires et gouvernementaux, les données sur les soins de santé au Manitoba ont servi à un certain nombre d'études longitudinales sur les personnes, et les mesures de protection de la vie privée ont donné les résultats escomptés. Dr Roos serait heureux de fournir le détail de ces mesures au Comité. Il joint également à son mémoire une copie du rapport annuel de 1993-1994 du Manitoba Centre for Health Policy and Evaluation, qui renferme des détails sur les projets de recherche du Centre.

#### ***Jorge Segovia, M.D., M.Sc. (santé communautaire)***

Jorge Segovia est professeur de médecine sociale et vice-doyen de médecine communautaire à la faculté de médecine du Health Sciences Centre de la Memorial University of Newfoundland.

La création de grandes bases de données a permis aux chercheurs médicaux de concevoir et d'entreprendre d'importantes études visant à surveiller et à évaluer la prestation de services de santé et d'étudier les

effets des interventions thérapeutiques et des techniques de diagnostic ainsi que des médicaments. Pendant de nombreuses années, la recherche faisant appel à la participation d'êtres humains a été approuvée par les comités de déontologie d'université ou de faculté afin de s'assurer du consentement informé des participants et de la préservation de la confidentialité et de l'anonymat. Toutefois, les nouveaux progrès technologiques permettent maintenant de relier plusieurs sources de données au profit de la recherche.

Il est extrêmement important d'avoir un bon équilibre entre la stricte protection des droits des individus et les avantages de la recherche sur les soins de santé. Il faut donc établir une distinction claire entre les données obtenues à des fins commerciales et les données servant à la recherche scientifique. Il faut également examiner de façon continue les questions liées à l'éthique dans le domaine de la recherche.

### ***Evelyn Shapiro, M.A.***

Evelyn Shapiro est professeure de sciences de la santé communautaire à la faculté de médecine de la University of Manitoba, membre du corps professoral du Manitoba Centre for Health Policy Evaluation et ancienne présidente de la Manitoba Health Services Commission.

En sa qualité de chercheuse en services de santé depuis plus de 20 ans, la professeure Shapiro a de sérieuses réserves quant à l'importance du Document de travail. Elle croit que le système, qui consiste à obtenir l'approbation préalable du comité sur l'accès et la confidentialité et du comité de déontologie de la faculté de médecine et à utiliser de faux identificateurs, a permis de protéger les renseignements personnels et, enfin, que les gouvernements fédéral et provinciaux ont pu tirer profit des études effectuées. Elle assure le Conseil consultatif qu'il n'y a jamais eu de divulgation de renseignements personnels lors de l'utilisation de données sur les services de santé, et elle croit également que cette situation ne se produira pas.

Pour effectuer des études transversales et longitudinales, le couplage de dossiers revêt une importance capitale. De plus, les études longitudinales, qui sont nécessaires pour prédire des tendances et des événements sérieux au regard de l'utilisation du service ou l'incidence de maladies particulières, ne peuvent être effectuées si des limites de temps s'appliquent au stockage des données. De plus, le consentement préalable ne permettrait pas d'effectuer les études dans les délais prescrits par les décideurs et entraînerait des coûts exorbitants. L'adoption du modèle européen est particulièrement inquiétante parce que de nombreux chercheurs en Europe ont jugé qu'il était impossible de poursuivre la recherche longitudinale.

Elle croit que la recherche sur les soins de santé axés sur la population est essentielle pour la prise de décision et qu'il faut protéger l'accès aux données tout en assurant la protection des renseignements personnels.

**Colin L. Soskolne, Ph.D., FACE**

Colin Soskolne est professeur de santé publique à la faculté de médecine de la University of Alberta. Il présente un exposé en qualité de président du comité directeur sur la déontologie et la philosophie de l'International Society for Environmental Epidemiology et de membre du comité sur la déontologie et les normes de pratique de l'American College of Epidemiology.

Il souhaite que le Canada n'adopte pas la position très négative de la Communauté européenne qui semble affaiblir la capacité de l'épidémiologie à entreprendre des recherches sur les risques pour la santé. Pour appuyer cette affirmation, il joint copie de deux lettres adressées à la Communauté européenne, la première de l'International Society for Pharmacology and Epidemiology et la deuxième de l'International Society for Environmental Epidemiology. Ces deux lettres mettent en lumière l'éternelle tension au regard de l'éthique entre le bien public, qui découle de l'établissement par l'épidémiologie de liens concernant les renseignements personnels, et la possibilité d'effets négatifs sur le particulier en raison de l'accès aux renseignements personnels. Il croit que cette dernière inquiétude n'est que théorique puisqu'on ne connaît pas de cas au Canada où des chercheurs auraient compromis le caractère confidentiel de dossiers ayant servi à leur travail. Pour protéger le public, l'épidémiologie a élaboré des lignes directrices en matière de déontologie, y compris la nécessité de préserver le caractère confidentiel des données. En outre, le serment de discrétion est obligatoire pour les personnes qui utilisent des données et font des liens aux niveaux national et provincial.

Il croit que le Document de travail comporte un parti pris commercial (sauf à la page 8, première colonne); c'est pourquoi il voulait que l'on tienne compte des discussions concernant la santé publique. Il faut faire une distinction entre les intérêts de ceux qui fournissent de l'information et les intérêts du public qui préoccupent, entre autres, les épidémiologistes.

**R. A. Spasoff, M.D.**

M. Spasoff est professeur d'épidémiologie et de médecine communautaire à la faculté de médecine de l'Université d'Ottawa.

Il est d'avis que lorsque nous nous inquiétons d'abus possibles au regard de l'utilisation de données électroniques, nous ne devons pas oublier les avantages que présente l'utilisation de ces mêmes données pour la recherche en matière de santé. Les propositions relatives à la protection de

données au Canada, de même que celles qui sont contenues dans l'ébauche de directive de la Communauté européenne, peuvent ralentir la recherche épidémiologique et donc nuire à la santé de la population. Les questions qui inquiètent particulièrement les épidémiologistes sont les suivantes : données suffisantes pour permettre le couplage de dossiers; données conservées pendant une période plus longue que le temps que prennent les maladies chroniques à se développer; possibilité que les dossiers soient utilisés à des fins autres que celles pour lesquelles ils avaient été obtenus. Il cite par exemple une étude de 40 000 \$ portant sur des anciens combattants canadiens déjà exposés à des radiations. Une étude similaire aux États-Unis, pour laquelle un couplage de dossiers n'est pas possible, coûte 7 000 000 \$ US.

Il ne connaît pas un seul cas où des renseignements personnels ont été pris en compte dans des études épidémiologiques ayant recours au couplage de dossiers. Il demande : «Sommes-nous en train d'inventer un remède pour lequel il n'y a pas de maladie?».

### ***University of Manitoba, Programmes de recherche et programmes externes***

Mémoire présenté par Terrence P. Hogan, vice-président, Programmes de recherche et programmes externes.

Même si le droit qu'ont les personnes de préserver le caractère confidentiel des données qui les concernent est un principe très valorisé et légitime au Canada, le Conseil consultatif devrait savoir que l'information électronique joue un rôle de plus en plus important dans la recherche. Cette recherche est fondée sur des protocoles ayant pour objet de préserver la confidentialité et de prévenir tout manquement à l'éthique. On ne connaît aucun cas où la confidentialité des renseignements connus sur le médecin ou sur le patient a été compromise, ce qui signifie que les renseignements personnels peuvent être protégés et qu'il est possible en même temps d'effectuer d'importantes recherches et d'en tirer parti.

#### **Propositions et recommandations particulières**

Il est fortement recommandé que le Conseil veille à ce que les bases de données et le couplage de dossiers servant à la recherche universitaire soient utilisés de façon équilibrée et réfléchie.

### ***Université d'Ottawa, Centre de recherche et d'enseignement sur les droits de la personne***

Mémoire présenté par Valerie Steeves, professeure associée de recherche principale, Projets de technologie et humains.

**En règle générale, le Centre favorise l'application de lois et de règlements en même temps que l'utilisation volontaire de codes et le recours aux solutions techniques et à l'éducation.**

**L'autoroute de l'information est plus qu'une autoroute sur laquelle on échange des renseignements commerciaux. Elle constitue un échange interactif d'idées par des millions de personnes. Il est essentiel que son développement soit conforme aux valeurs culturelles. En raison de l'évolution rapide des progrès technologiques, il est difficile pour le gouvernement de régulariser le développement et la gestion du réseau. Par conséquent, il doit établir une série de principes pour que le développement de l'autoroute reflète les valeurs humaines nécessaires pour assurer la qualité de la vie. Il doit donc élaborer une définition de la confidentialité qui va plus loin que la simple protection des renseignements personnels et qui comprend les notions de dignité humaine et d'autonomie.**

**Le gouvernement doit élaborer une politique nationale qui favorise activement la transparence et l'accès et qui soit détaillée. De la même manière, une politique nationale établissant des lignes directrices en matière de déontologie permettra d'établir un équilibre entre les intérêts privés et la valeur publique des communications ouvertes et complètes. En outre, la promotion de l'accès universel doit être un élément clé afin d'éviter que des secteurs marginaux de la communauté soient privés de leurs droits.**

### **Approches**

- I. Des mécanismes de réglementation découlant de la loi doivent être créés, au besoin, pour traiter les nombreux genres de relations qui seront formés sur l'autoroute.**

**Ces mécanismes de réglementation devraient faire en sorte que : les renseignements personnels détenus par les gouvernements et le secteur privé soient assujettis à des lignes directrices strictes comprenant des mécanismes d'application administratifs et judiciaires; les communications personnelles entre les personnes soient privées, y compris les communications en milieu de travail, et qu'elles comportent des recours judiciaires; les discussions publiques concernant l'autoroute soient ouvertes et complètes et qu'elles soient assujetties à un minimum de règles. En outre, une norme nationale doit comprendre les dispositions suivantes : pertinence et consentement en ce qui a trait à la collecte de renseignements personnels, y compris les renseignements partagés par les ministères gouvernementaux; les codes volontaires doivent reconnaître l'importance du consentement éclairé, sous réserve de l'égalité des dispositions relatives au pouvoir de négociation et aux**

recours; existence d'un organisme indépendant de défense des intérêts pouvant appliquer ses décisions, mais soumis à un examen judiciaire.

- II. La conformité volontaire, fondée sur des mécanismes efficaces de mise en application, comporte certains avantages par rapport à l'application des règlements par le gouvernement, notamment une participation des secteurs et le partage des frais d'administration. Toutefois, l'application volontaire de règlements a donné des résultats inégaux dans le passé. Le succès de la conformité volontaire, y compris de codes pour l'ensemble de l'industrie, dépendra de la puissance du mécanisme d'application.
- III. L'élaboration de mécanismes de chiffrement universels devrait être encouragée.
- IV. L'éducation du public de même que les discussions et les débats publics sont nécessaires. Le gouvernement devrait tenter d'établir des alliances stratégiques avec les intéressés des secteurs public et privé de sorte que l'éducation relative aux questions pertinentes soit à la portée du public. Le Centre est en train d'élaborer un certain nombre d'initiatives en matière d'éducation, y compris : un cours interdisciplinaire annuel s'adressant à l'ensemble du milieu universitaire et qui porte sur les droits de la personne découlant de la technologie des communications; une série de séminaires à l'intention des sociétés portant sur les questions liées au marché; l'élaboration d'une bibliothèque en direct fournissant des données sur la protection des renseignements personnels, les droits de la personne et l'autoroute de l'information. Le Centre a aussi mis sur pied la plus grande base de données provenant de documents canadiens sur les droits constitutionnels et humains. L'accès direct à cette base devrait être possible en 1995.

### **Réponses aux questions**

1. Le gouvernement doit élaborer une politique nationale qui reconnaît les principes et les droits suivants en matière de renseignements personnels :
  - être libre de toute surveillance inutile;
  - contrôler la divulgation et l'utilisation des renseignements personnels;
  - être libre d'intrusions d'information inutiles ou non désirées ou de sollicitation;
  - participer librement au débat social, économique et politique et avoir un accès raisonnable, à un coût abordable, aux moyens de participation.

## **University of Waterloo, Bureau de la recherche**

Comme le Document de travail ne traite pas précisément des chercheurs universitaires, on s'inquiète du fait qu'ils pourraient être regroupés avec les entreprises et les télé-vendeurs, lesquels utilisent l'information dans un but lucratif.

Statistique Canada fournit des bases de données contenant une foule de précieux renseignements, et les chercheurs risquent de ne pas pouvoir y avoir accès. Cela s'est produit en Europe où les instituts de recherche sur la santé de la Suède et du Danemark ne peuvent plus fonctionner parce que les règlements européens ne font pas de distinction entre les différentes utilisations de renseignements personnels.

### **Propositions et recommandations particulières**

On recommande fortement au Conseil consultatif de tenir des réunions publiques et de faire la promotion du Document de travail, lequel a été diffusé de façon indirecte et trop tard pour recueillir les commentaires de la communauté universitaire.

## **PARTICULIERS**

---

### **Norah Duck**

Le mémoire de M<sup>me</sup> Duck fait suite à un article paru dans le *Toronto Star* le 15 octobre 1994. Même si elle ne possède pas d'ordinateur et n'a aucune intention d'en posséder un, elle éprouve certaines inquiétudes concernant la protection des renseignements personnels, à cause de sa propre expérience. Elle s'oppose aux demandes non restreintes ayant trait à son âge et à son NAS au cours des transactions commerciales courantes, p. ex. dans les supermarchés, les hôtels et les banques. Elle s'interroge aussi en ce qui concerne l'élaboration sans consentement de profils de consommateurs qui peuvent être vendus à des tiers et l'échange avec des gouvernements étrangers de renseignements personnels détenus par le gouvernement, par exemple l'accord entre le Canada et les États-Unis pour échanger des renseignements fiscaux.

Elle se fie peu aux nouvelles lois sur la protection des renseignements personnels parce que des personnes et des établissements peu respectueux de l'éthique trouveront toujours une façon de les contourner. Par conséquent, elle croit qu'un programme d'envergure est nécessaire pour éduquer les gens sur la façon de protéger leur vie privée, par exemple quand fournir des renseignements personnels et quand remettre en question la nécessité de les fournir.

### **Brian Fitzgibbon**

Le mémoire de M. Fitzgibbon fait suite à un article paru dans le *Toronto Star* le 15 octobre 1994. Après 30 ans au service de l'industrie des logiciels, il doute que les ordinateurs et l'autoroute de l'information soient un jour utilisés par les personnes à faible revenu en raison de leur situation financière et du manque d'intérêt.

Il répond aussi à quatre questions posées dans l'article du *Toronto Star*.

- *Pourrait-on en arriver à avoir un système qui offre une meilleure protection aux riches qu'aux pauvres?*

Il est impossible que tous soient traités sur un pied d'égalité parce que le pauvre ne voudra probablement pas posséder un ordinateur ni avoir accès à l'autoroute de l'information.

- *Le courrier électronique devrait-il être traité comme une lettre personnelle ou comme appartenant à la société?*

Le courrier électronique devrait être traité comme n'importe quelle autre pièce de correspondance parce qu'il n'y a pas de différence entre le courrier électronique et une lettre d'affaires quelconque.

- *Le télétravail est un phénomène qui se répand très rapidement - les sociétés permettent aux travailleurs de rester à la maison pour y travailler. Cette situation permet-elle aux employeurs d'espionner les employés chez eux au moyen de l'électronique?*

Le fait de permettre à un employé de travailler chez lui ne sera efficace qu'exceptionnellement. En règle générale, il y aura baisse de productivité. Le comptage des frappes aux fins de comparaison pour mesurer la productivité n'est possible que pour les commis à l'entrée des données.

- *Les personnes devraient-elles avoir un contrôle total sur l'information concernant leur vie privée et leurs transactions?*

Le contrôle total n'est pas une option pour l'utilisateur, à moins que la passerelle ne fournisse un moyen d'effectuer le chiffrement.

### **Harold Genz**

Les renseignements personnels doivent être protégés sur l'autoroute de l'information. Par conséquent, cette protection doit être un préalable à la conception du système. Lorsque des renseignements sur les habitudes d'achat sont demandés au téléphone ou sur ordinateur, un message automatique devrait apparaître indiquant qu'il n'est pas possible de fournir de renseignements personnels.

### **Khalid Saeed, Holaser**

Même s'il admet qu'il est difficile de protéger les données sur support électronique et magnétique, M. Saeed suggère cinq principes :

- toute l'information électronique, tout comme l'information écrite, ne devrait être commercialisée qu'avec l'autorisation écrite de la personne ou de la partie visée;
- une personne peut autoriser la divulgation de renseignements personnels, mais seulement à l'intention de la partie avec laquelle elle traite;
- les données contenues dans un ordinateur relié ou non relié appartiennent à la partie qui les possède, qu'elles soient ou non transmises par courrier électronique;
- une personne devrait avoir le plein contrôle sur les renseignements ayant trait à sa vie personnelle ou à ses transactions, sous réserve des prescriptions de la loi;

- l'espionnage électronique d'un employé chez lui est un geste des plus repoussants; par conséquent, les mesures d'évaluation devraient être basées sur le matériel et les services fournis au bureau.

### **J.C. Holst**

Le mémoire de J.C. Holst fait suite à un article paru dans le *Toronto Star* le 15 octobre 1994. Le gouvernement du Canada devrait promulguer une loi énonçant ce qu'il faut faire et ne pas faire au regard de l'incursion dans la vie privée.

### **Jorg P. Kranz**

M. Kranz, qui a 31 ans d'expérience dans le domaine du traitement des données, aborde des questions liées à la protection des renseignements personnels.

Il s'inquiète du fait qu'il y a prolifération de banques de données, tant au gouvernement que dans le secteur privé, et que les gens ne sont peut-être pas au courant de la chose. Ces banques sont parfois accessibles aux deux secteurs, p. ex. les compagnies d'assurance peuvent avoir accès aux dossiers provinciaux de conduite automobile.

La meilleure façon d'assurer l'accès autorisé seulement serait d'établir un service d'archives central contrôlé par le gouvernement. Toute l'information sur les particuliers y serait stockée. Seule la personne visée aurait accès à l'information à son sujet. Elle pourrait corriger les erreurs et contrôler la diffusion de l'information aux tierces parties. Même si cette solution a l'inconvénient d'ajouter aux tracasseries administratives, elle serait gérable. Il faudrait au moins recenser toutes les banques de données et fournir des copies des renseignements personnels qu'elles contiennent aux personnes visées, aux fins de vérification, de correction et de mise à jour sur une base permanente.

Le courrier électronique et la messagerie vocale devraient être traités comme on traite une lettre personnelle, et l'employeur devrait s'en voir refuser l'accès, à moins que l'employé ne l'y autorise.

Le comptage des frappes, le minutage des appels téléphoniques ou le branchement de caméras vidéo sur le réseau devraient être considérés comme une incursion dans la vie privée.

Sauf dans le cas des enquêtes criminelles, les particuliers doivent pouvoir protéger les renseignements ayant trait à leur vie personnelle et à leurs transactions.

## **Steven Lotz**

M. Lotz propose des solutions qui selon lui sont peu coûteuses pour le gouvernement et protègent la vie privée des particuliers. Il croit que les particuliers ont le droit et la responsabilité de faire leurs propres choix, qu'il s'agisse de la libre association, de la propriété ou de la vie privée, et que le gouvernement ne devrait pas intervenir. La fonction du gouvernement devrait être limitée à la défense du pays, au maintien de forces policières pour assurer la protection des individus et d'un système judiciaire pour régler les différends. Cette liberté de choix et d'association s'applique lorsqu'il s'agit de décider si l'on doit acheter ou non, si le courrier électronique est privé ou non, si un vendeur peut vendre un profil personnel ou non, et si la surveillance par les employeurs doit être permise ou non. Le gouvernement doit se rendre compte que les gens sont capables de prendre des responsabilités en ce qui a trait à leur vie personnelle. Par conséquent, selon la common law, seuls les tribunaux devraient juger les réclamations pour manquement à un accord conclu librement. L'application de ces principes à l'autoroute de l'information n'est pas nouvelle, seule la technologie est nouvelle. Si le gouvernement intervient, les particuliers perdront leurs droits en matière de choix et de libre association. Ainsi, on ne devrait pas renforcer la loi ni les règlements, parce que cela n'est pas nécessaire.

## **D.B. Morrow**

Le mémoire de D.B. Morrow fait suite à un article paru dans le *Toronto Star* le 15 octobre 1994.

M. Morrow manifeste certaines inquiétudes, en particulier pour ce qui est des renseignements recueillis, détenus et utilisés par les banques. Les vues exprimées ont trait aux banques qui ont signé avec tous les détenteurs de carte et les emprunteurs des contrats contenant des «clauses d'information» qui autorisent, entre autres, l'utilisation du NAS, les vérifications de crédit, la publicité, l'échange de listes. Et, ce qui est encore plus important, toutefois, dans le cas de la Banque Royale, sa «clause d'information» a maintenant été étendue unilatéralement à certains déposants, c.-à-d. les détenteurs de REER (une copie de l'accord révisé sur le plan d'épargne-retraite de la Banque Royale est jointe au mémoire). L'accord révisé indique qu'il n'est pas nécessaire d'informer la banque de l'acceptation des changements et que le document peut simplement être conservé pour référence. La «clause d'information» comprise dans l'accord indique que les renseignements personnels, y compris le NAS, détenus ou obtenus par la banque peuvent être utilisés à de nombreuses fins non directement liées à l'investissement dans un REER. En outre, l'information peut continuer d'être détenue et utilisée lorsque le déposant n'est plus un client de la banque ou lorsque l'accord a pris fin. Il prétend donc que les banques ont enlevé à la plupart des Canadiens leurs droits en matière de confidentialité et d'utilisation du

NAS, et aussi qu'ils n'ont pas d'autre choix que de se conformer à ces accords s'ils veulent obtenir divers services.

De plus, lorsqu'une plainte a été adressée (copie jointe au mémoire) au Surintendant des institutions financières du Canada, ce dernier a déclaré ne pas avoir de pouvoirs concernant les contrats personnels. Il a de plus transmis sans autorisation copie de la plainte à la Banque Royale. La Banque a par la suite indiqué qu'en raison de plaintes, elle prévoit effectuer certains changements.

Enfin, si les banques devaient commencer à vendre de l'assurance, elles détiendraient déjà des renseignements, tirés des contrats bancaires, qu'elles pourraient utiliser à leur guise.

### ***R.B. Oulton***

R.B. Oulton soulève deux points en ce qui concerne la protection des renseignements personnels.

Tout d'abord, c'est la personne ou la société qui pourrait vendre de l'information qui est responsable de la protection des renseignements personnels. Par exemple, les compagnies de téléphone et de câblodistribution, les distributeurs de magazines et les institutions charitables devraient obtenir la permission de publier ou de vendre l'information qu'ils ont obtenue.

Ensuite, les organismes qui doivent faire enquête sur les personnes (banques, sociétés de fiducie, services d'informations financières) devraient être tenus : a) d'aviser les personnes au sujet d'une demande d'information qui les concerne; b) d'envoyer copie de cette information à la personne visée.

### ***Richard D. Speers, D.D.S.***

M. Speers déclare que la phrase souvent citée «savoir égale pouvoir» devrait être interprétée plus justement comme le besoin insatiable de tirer profit de renseignements recueillis sur des groupes et des personnes. Il précise certaines de ses inquiétudes concernant l'incursion dans la vie privée dans quatre domaines.

À l'origine, le NAS attribué par le gouvernement du Canada visait à identifier les participants aux plans parrainés par ce même gouvernement. Il cite de nombreux exemples d'une utilisation beaucoup plus étendue de l'information que celle qui avait alors été envisagée parce qu'à ce moment-là, malgré les avertissements, le gouvernement ne croyait pas nécessaire de contrôler cette utilisation. Même dans les cas où l'on a demandé de restreindre l'utilisation de l'information, des formulaires d'autorisation ont été

utilisés pour contourner la question. Son utilisation a permis le simple regroupement de quantités considérables de données, ce qui suggère que l'extraction et la comparaison sont non seulement possibles, mais aussi probables. En utilisant des systèmes de numération de rechange, la comparaison et le cumul automatiques seront plus difficiles.

La divulgation non autorisée d'un renseignement donné sur un patient peut entraîner la perte de l'accréditation médicale par un médecin. Dans leurs relations avec des professionnels de la santé, les patients s'attendent à un respect intégral de leur vie privée et de la confidentialité, comme dans le cas de la relation avocat-client. L'accès non autorisé aux dossiers médicaux et aux fiches médicales peut avoir des effets dévastateurs. Les poursuites récentes d'Evelyn Gigantes et de David Nantes constituent de bons exemples. Des tiers ne devraient en aucun cas avoir accès aux fiches médicales ou aux dossiers de patients, à moins que ces derniers ne demandent précisément la divulgation et ce, uniquement dans le cas de plainte, de litige ou de transfert du dossier à un autre professionnel de la santé. Cependant, à l'heure actuelle, aucune loi n'empêche une tierce partie d'exiger le dossier médical d'un employé éventuel ou d'un demandeur d'assurance. En outre, maintenant que les banques ont le droit de vendre de l'assurance-vie, M. Speers ne connaît pas de loi qui interdirait d'utiliser des renseignements médicaux fournis aux fins d'assurance pour prendre une décision sur l'octroi d'un prêt. Le gouvernement fédéral n'est pas lui non plus à l'abri des critiques. En effet, Revenu Canada et Affaires des anciens combattants Canada demandent maintenant l'accès aux fiches médicales et dentaires, aux fins de vérification. En ce qui concerne les renseignements médicaux, des restrictions doivent d'abord s'appliquer aux données auxquelles ont accès les organismes gouvernementaux, les employeurs, les banquiers et les assureurs. Les dossiers médicaux identifiables doivent également être protégés. Le stockage et la transmission des renseignements médicaux posent aussi des problèmes. Le stockage de renseignements par les compagnies d'assurances canadiennes à Boston, au Massachusetts, peut entraîner une incapacité de traiter une utilisation inappropriée devant les tribunaux canadiens.

Les sociétés de fiducie et les banques ont accumulé de vastes quantités de renseignements qui montrent les tendances en matière de dépenses. Cette situation permet de définir des marchés cibles, ce qui signifie que de nombreuses personnes, en particulier les personnes âgées et les infirmes, peuvent être l'objet de sollicitations abusives ou agressives. Les renseignements sur le crédit sont aussi regroupés dans des organismes centraux. Le nom de la personne qui a accès à ces dossiers et la date de l'accès de même que le nom de la personne qui a autorisé l'accès doivent être indiqués au dossier. La personne dont il est question dans le dossier devrait aussi avoir accès à cette information. De la même manière, si des agences financières vendent des données et des renseignements, elles devraient pour ce faire obtenir l'autorisation du particulier. Le refus de

divulguer l'information ne devrait pas être puni. En ce qui concerne les données financières, les personnes visées doivent connaître les renseignements conservés, la façon dont ils sont utilisés et à qui ils sont divulgués. De plus, ces personnes doivent avoir pleinement accès aux renseignements qui les concernent et contrôler leur utilisation.

Les organismes gouvernementaux ont de plus recueilli d'énormes quantités de données personnelles. Dans le passé, les hôpitaux et les organismes gouvernementaux ont vendu des listes d'envoi aux organismes privés. À titre d'exemple, on peut mentionner la vente de renseignements concernant les plaques d'immatriculation. Revenu Canada a aussi promis que personne n'aurait accès aux données et à l'information relatives à l'impôt. Toutefois, les ministères des finances provinciaux ont maintenant accès à cette information, et les forces policières demandent elles aussi l'accès aux renseignements pour leurs enquêtes criminelles.

Les lois et les règlements doivent définir avec précision la portée de l'utilisation, de la conservation et de la gestion de l'information. Les lois et les règlements qui seront éventuellement adoptés devront aussi traiter les problèmes liés aux services d'informations financières.

La transmission électronique de renseignements médicaux et dentaires doit faire l'objet d'un examen. La transmission de toutes les données délicates doit se faire en toute sécurité. Cela signifie que les données devraient être codées ou transmises sur des lignes de transmission tout à fait sûres.

#### **Propositions et recommandations particulières**

Il faudrait faire cesser l'utilisation du NAS par d'autres organismes que les organismes fédéraux pour lesquels ce système a été conçu.

### ***J.S. Tate***

J.S. Tate s'inquiète fortement de l'abus qu'a depuis longtemps entraîné l'utilisation du NAS. La loi promulguée en 1964 sur l'utilisation du NAS ne prévoit pas de mesures pour empêcher d'autres utilisations que celles qui sont prescrites ni aucune mesure punitive pour ceux qui abusent du système. Cette situation s'est maintenue en dépit des craintes sérieuses exprimées par le Commissaire à la protection de la vie privée et par divers comités parlementaires, et malgré les interventions auprès de députés et de procureurs généraux.

Si l'on examine la situation depuis 30 ans, il est évident que les méthodes privilégiées par les divers gouvernements, à savoir les codes sans caractère obligatoire pour le secteur privé et la persuasion, n'ont pas donné les résultats escomptés. Cette expérience devrait montrer clairement au Conseil consultatif qu'il doit avoir comme objectif principal et ultime la protection de la vie privée.

Les particuliers devraient exercer un contrôle total sur les renseignements ayant trait à leur vie personnelle et à leurs transactions.

Les particuliers et les organismes qui enfreignent les règlements devraient encourir des sanctions sévères au criminel.

### ***Association canadienne de télévision par câble (ACTC)***

L'Association canadienne de télévision par câble est une organisation nationale représentant 816 membres, dont la majorité fournissent des services de télévision par câble à plus de sept millions de foyers canadiens.

Globalement, l'ACTC ne recommande pas la législation et la réglementation. Elle fait plutôt valoir que les codes et les normes volontaires, les solutions technologiques et l'éducation du consommateur peuvent être utilisés conjointement pour protéger efficacement la vie privée. Tout devrait être mis en oeuvre pour ce faire. Les mesures prises par l'ACTC depuis 1991 pour mettre en oeuvre dans toute l'industrie de la câblodistribution un code visant la protection de la vie privée code, sont également décrites dans le document.

Consciente des préoccupations relatives à la protection de la vie privée, notamment en ce qui a trait aux habitudes d'écoute des téléspectateurs, l'industrie de la câblodistribution a adopté un modèle d'autoréglementation fondamentalement différent de ceux des secteurs bancaire, du marketing direct, de l'assurance et des télécommunications. En 1988, l'industrie mettait sur pied la Fondation des normes de télévision par câble (FNTC), un organisme indépendant dont les membres sont 90 entreprises de câblodistribution détenant une licence accordée par le Conseil de la radiodiffusion et des télécommunications canadiennes (CRTC). L'adhésion à cet organisme est volontaire et n'est pas restreinte qu'aux membres de l'ACTC. La FNTC administre les Normes de service aux abonnés de la télédistribution, adoptées par l'ACTC et approuvées par le CRTC en 1991, ainsi que d'autres codes et engagements adoptés par l'ACTC. Elle se prononce sur les plaintes concernant les présumées infractions aux normes, aux codes, aux engagements et à d'autres aspects du service de télédistribution offert par ses membres. Aucune de ses constatations ne sont approuvées par l'industrie et elles sont accessibles au public. Les dispositions concernant la confidentialité et la sécurité prévues dans les Normes se fondent sur les principes de la Loi sur la protection des renseignements personnels et engagent les membres à garder confidentiels les renseignements sur leurs clients de manière conforme à l'objectif d'offrir à tous ses clients une protection contre l'atteinte à leur vie privée. Les entreprises membres doivent notamment conserver tous les renseignements personnels en vertu de la Loi sur la protection des renseignements personnels; permettre aux clients d'inspecter leurs dossiers, à la demande des clients, rayer leur nom des listes d'envoi et des listes de sollicitation téléphonique, et s'assurer que tous les employés montrent une carte d'identité avec leur photo lorsqu'ils entrent chez des clients.

## **Approches**

I. L'ACTC ne favorise pas une approche législative parce qu'elle va à l'encontre de la tendance vers un environnement commercial déréglementé qui caractérise le nouveau marché international concurrentiel. En outre, la législation tend à être inflexible et est insensible aux diverses méthodes et à la sophistication technologique des différentes industries et des différents secteurs. La législation peut également entraîner un sentiment de suffisance selon lequel «le problème s'est réglé de lui-même» et, si elle est trop généralisée, elle pourrait donner un pouvoir de réglementation trop grand aux cours. Enfin, toute loi fédérale ne viserait que les secteurs qui relèvent de la compétence fédérale et, par conséquent, ne pourrait pas offrir une protection et des droits uniformes à l'échelle du Canada.

II. L'ACTC est en faveur des codes et des normes volontaires parce qu'ils visent davantage des secteurs précis. Ils permettent d'examiner les méthodes de manutention de l'information du point de vue de l'entreprise et permettent une meilleure intégration au sein d'un secteur donné ainsi qu'une sensibilisation accrue aux questions de protection de la vie privée. En outre, ils sont plus souples et plus adaptables à l'évolution technologique, ce qui donne lieu à un examen plus régulier. De plus, on peut les utiliser comme outils éducatifs pour informer les consommateurs de leurs droits, et ils peuvent permettre de répondre aux plaintes de façon plus efficace, plus accessible et moins coûteuse.

L'ACTC appuie fermement les efforts de longue date de l'Association canadienne de normalisation (CSA) pour mettre au point un modèle de code sur la protection des renseignements personnels. L'ACTC a été représentée auprès du Comité technique de la protection des renseignements privés de la CSA par la FNTC dans l'élaboration de l'ébauche de code. Le comité de la CSA a pour objectif d'élaborer un code volontaire convivial qui équilibrerait les intérêts commerciaux et les besoins des entreprises avec le droit inhérent à la vie privée. Par conséquent, l'ACTC espère que les nouvelles initiatives du gouvernement fédéral ne constitueront pas un facteur de dissuasion pour appliquer le code de la CSA selon les spécifications de l'industrie.

III. L'ACTC est convaincue que la technologie peut grandement améliorer la protection de la vie privée des particuliers. L'industrie de la câblodistribution s'emploie à développer ce potentiel. À preuve: l'initiative du consortium UBI où on combine les concepts technologiques et les systèmes pour protéger les données personnelles et transactionnelles.

- IV. L'ACTC convient que les consommateurs doivent être informés et éduqués relativement à leur droit à la vie privée, aux risques que pose la technologie, et à ce qu'ils peuvent faire pour conserver et protéger leur vie privée. L'industrie de la câblodistribution est engagée à utiliser son réseau étendu pour sensibiliser les consommateurs, les informer et les éduquer.

#### **Propositions et recommandations précises**

L'ACTC recommande de donner une chance de fonctionner au projet de code de la CSA sur la protection de la vie privée avant que les lois et les règlements gouvernementaux soient adoptés ou préconisés.

### ***Association canadienne des utilisateurs de satellites (ACUS)***

L'Association canadienne des utilisateurs de satellites (ACUS) représente les radiodiffuseurs qui utilisent les installations spatiales de Télésat Canada.

En résumé, la position de l'ACUS est que les règlements législatifs ne sont nécessaires que pour les données les plus névralgiques et pour les données recueillies par mandat. Pour la protection à l'échelle nationale d'autres données personnelles, l'application de codes de déontologie à l'échelle de l'industrie convient le mieux. Grâce à l'éducation des consommateurs et à l'utilisation répandue d'outils technologiques, les particuliers pourront exercer le contrôle approprié sur l'utilisation des données personnelles les concernant. Il est également question de la définition de la vie privée, des techniques de collecte de données, du contrôle et de la sécurité des données, et de la pertinence du code type de la CSA sur la protection des renseignements personnels.

L'ACUS discute plus en détail de la définition de la protection de la vie privée. L'utilisation du mot «interruption» est remise en question dans la première partie de la définition de la protection de la vie privée donnée dans le Document de travail : «le droit de vivre en paix sans intrusion ni interruption». Il n'ajoute rien au concept de protection de la vie privée parce que son utilisation laisse entendre que toutes les interruptions - qu'elles soient bienvenues ou non, constituent une atteinte à la vie privée. On suggère plutôt que le concept d'interruption «non sollicitée» soit la clé de toute notion d'intrusion de la vie privée dans la société actuelle.

Les membres de l'ACUS sont de plus en plus impliqués dans le divertissement transactionnel, l'enseignement et d'autres services commerciaux offerts au public. Cela nécessite des techniques de mesure perfectionnées, qui nécessitent la collecte de données personnelles, pour leur permettre de s'adapter à leurs publics à mesure que les choix des auditeurs augmentent rapidement. Il en résultera de nouvelles occasions

d'affaires et un meilleur service au public. Ainsi, les membres se soucient de la préoccupation du public à l'égard de la protection de la vie privée.

Les techniques actuelles de collecte des données, dans quatre grands secteurs, sont décrites en détail. Premièrement, la mesure de l'auditoire est habituellement recueillie pour les diffuseurs par des tiers sans problèmes connus en matière de protection des renseignements personnels et le diffuseur reçoit des données anonymes. Dans l'avenir, les mesures seront recueillies au moyen d'appareils de mesure de l'auditoire qui permettront au diffuseur de recueillir des données directement auprès de l'auditeur. Deuxièmement, le secteur de l'achat à domicile donne lieu à la collecte directe de données transactionnelles à partir desquelles il est possible d'établir des niveaux de demande totale. Troisièmement, on commence à offrir des services de divertissement transactionnels avec l'introduction de la tarification par écran qui donne lieu également à la collecte directe de renseignements personnels. À l'avenir, les services de radiodiffusion en direct nécessiteront un centre d'autorisation pour effectuer la transaction et cela pourra se faire par l'utilisation de cartes intelligentes qui contiendront les coordonnées de l'auditeur et des renseignements sur son crédit. Quatrièmement, les diffuseurs d'émissions éducatives s'occupent de services d'apprentissage à distance. Il est important d'avoir des données personnelles pour mettre au point les programmes, commander du matériel de cours, permettre à l'étudiant d'effectuer le transfert de cours applicable et le transfert entre établissements, et pour commercialiser les cours. Sous peu, des services interactifs, comme les sondages d'opinion, les votes aux référendums et les réponses à la publicité, permettront aussi de recueillir des renseignements personnels.

Les renseignements personnels comme les données transactionnelles, les numéros de téléphone, les adresses, les choix des auditeurs, les résultats des étudiants, les coordonnées sur les auditeurs et les renseignements sur leur crédit, recueillis par ces divers services seront utiles aux publicitaires et aux diffuseurs, ainsi qu'aux tiers. Et, ce qui est encore plus important, ces renseignements permettront aux diffuseurs d'élaborer des services qui répondent le mieux possible aux exigences des auditeurs.

Pour ce qui est de l'atteinte à la vie privée, les citoyens l'acceptent dans de nombreuses circonstances. La collecte obligatoire de renseignements personnels par les gouvernements, p. ex. l'imposition et les dossiers criminels, illustre bien la situation. Cette collecte des données et leur dissémination est habituellement visée par des lois et des règlements. Toutefois, les citoyens acceptent également de fournir des données personnelles dans bon nombre d'autres types de transactions. Cette situation est différente de la collecte obligatoire, car elle s'inscrit dans une transaction librement consentie. Par conséquent, l'ACUS est d'avis que dans ces situations, la clé est le contrôle et la sécurité des données après la transaction.

Les principes touchant la protection des renseignements personnels sont également traités, et vont des lignes directrices de l'OCDE au modèle de code de la CSA. Selon l'ACUS, le code de la CSA constituera une excellente source de principes nationaux parce qu'ils sont neutres à l'égard du secteur de la technologie et de secteurs précis de la collectivité. Ainsi, ils pourront servir pour toute loi ou tout code utilisé à l'échelle de l'industrie dans l'élaboration de codes de déontologie précis.

### **Approches**

- I. Des lois et des règlements gouvernementaux ont été demandés dans le cas de renseignements personnels extrêmement délicats. L'ACUS est d'avis qu'il est approprié qu'il y ait des lois dans le domaine des renseignements recueillis par le gouvernement.
- II. Les codes s'appliquant à l'ensemble de l'industrie présentent de nombreux avantages par rapport aux lois. Ils ne nécessitent pas de fonds publics, ils peuvent viser des applications à l'échelle du pays et éviter un assortiment de lois provinciales et il est mieux de les traiter par secteurs, ce qui permet plus de souplesse pour apporter des changements à mesure que l'industrie change.
- III. Les progrès technologiques permettent une sécurité accrue pour les transactions et le stockage des données par l'encodage et l'accès contrôlé. Si on leur donne des lignes directrices claires quant à la protection nationale des renseignements personnels, les organisations seront en mesure d'évaluer les changements technologiques à la lumière des exigences en matière de protection des renseignements personnels.
- IV. On se préoccupe moins de la protection de la vie privée lorsque les particuliers comprennent ce qui se passe ainsi que les avantages associés à la collecte de renseignements personnels. Les lignes directrices proposées par la CSA fourniront l'occasion de faire connaître les droits personnels et peuvent être utilisées pour éduquer le consommateur par les commissaires à la protection de la vie privée au niveau fédéral et provincial.

### **Consortium UBI**

Le Consortium UBI a été créé en janvier 1994 et regroupait les membres suivants : Postes Canada, la Banque nationale du Canada, Hydro-Québec, Loto-Québec, Hearst Corporation, Le Groupe Vidéotron Ltée et Videoway Communications Inc. Il a pour mission d'implanter le premier outil de communication interactif, multimédia et bidirectionnel dans au moins 80 % des foyers câblables au Québec.

Depuis sa mise sur pied, le Consortium a pris un certain nombre de décisions de nature technologique et organisationnelle pour faire en sorte que les droits à la vie privée soient respectés. Sur le plan technologique, mentionnons l'introduction d'une carte intelligente permettant d'identifier et d'assurer l'authenticité des utilisateurs, l'encodage de toutes les données confidentielles sur le réseau, et le fait qu'il n'y aura pas de «dossiers clients» pour les utilisateurs.

Sur le plan organisationnel, le Consortium a retenu les services du Centre de recherche en droit public (professeur Pierre Trudel) de l'Université de Montréal pour élaborer un code de conduite, notamment en matière de protection de la vie privée. Le code tiendra compte des caractéristiques et de la fonctionnalité du système ainsi que des préoccupations des particuliers et des fournisseurs de services. La méthodologie comporte trois étapes : la première a consisté à dresser une liste de questions morales afin d'analyser les zones de conflit qui pourraient surgir dans le contexte d'une autoroute de l'information rejoignant les foyers. La deuxième étape a consisté à cerner les groupes, les associations ou les représentants du public qui se préoccupent des questions morales qui ont été identifiées. On a tenu des entrevues avec plus de 50 groupes et on met la dernière main à un rapport contenant un résumé de leurs préoccupations. La troisième étape consistera à produire un code de conduite qui tiendra compte de tous ces points, y compris des méthodes pour prévenir et régler les différends. Parce que l'étude n'est pas encore terminée, le Consortium est d'avis qu'il est trop tôt pour réagir officiellement au Document de travail.

#### **Propositions précises et recommandations**

De l'avis du Consortium, les résultats de sa recherche qui, à sa connaissance, est la seule étude professionnelle effectuée par les parties intéressées à offrir l'accès à l'autoroute de l'information, seraient utiles au Conseil consultatif de l'autoroute de l'information. Le Consortium demande qu'on l'autorise à présenter les résultats de son étude au Conseil, à la mi-février 1995.

### ***Association canadienne de la technologie de l'information (ACTI)***

L'Association canadienne de la technologie de l'information représente des membres appartenant à tous les segments des secteurs du matériel, du logiciel, des services et du contenu électronique dans les secteurs de l'informatique et des télécommunications. Ils représentent 70 pour cent des revenus de l'industrie.

En résumé, l'ACTI est en faveur de la promulgation de lois garantissant à tous un niveau raisonnable et approprié de protection de la vie privée et de sécurité des renseignements, ainsi que des recours juridiques précis. Au-

delà de ce niveau, l'ACTI est d'avis que l'industrie et les consommateurs devraient être réglementés par le marché où on trouve des services de renseignements qui sont en concurrence, offrant divers niveaux de sécurité de l'information à des prix différents. Les solutions technologiques et l'éducation des consommateurs et du secteur commercial ont également un rôle important à jouer. Une définition de la protection de la vie privée est fournie, diverses préoccupations relatives à la protection de la vie privée sont exposées et un principe important relativement à la protection de la vie privée est défini.

L'ACTI énumère cinq principes pour orienter son approche à l'intérêt public en ce qui a trait à l'infrastructure de l'information qui émerge. Sa présentation met l'accent sur le cinquième principe «Attention rigoureuse aux questions relatives à la protection de la vie privée et à la sécurité des renseignements par l'entremise de codes du secteur privé et d'organismes en assurant l'application».

La protection de la vie privée est définie comme étant le contrôle qu'exerce un particulier sur l'accès à sa personne et aux renseignements personnels le concernant. Les discussions touchant la propriété des renseignements transactionnels est comparée aux discussions sur la propriété intellectuelle.

La protection de la vie privée est devenue une question importante dans l'élaboration de politiques visant l'infrastructure de l'information. Selon une enquête effectuée en 1992 par Ekos Research Associates, 92 pour cent des Canadiens sont au moins modérément préoccupés par la protection de leur vie privée, et 81 pour cent sont d'avis que les ordinateurs entraînent une baisse de la protection de la vie privée. En outre, on a constaté que la préoccupation la plus importante était la possibilité de relier des bases de données à de nouvelles fins.

Le contrôle de l'accès à l'information transactionnelle et à son utilisation constitue une préoccupation majeure. À cet égard, bon nombre de transactions utilisant l'infrastructure de l'information laissent une «ombre de données». À mesure que des nouveaux services d'information sont introduits, des formes plus perfectionnées d'information transactionnelle apparaîtront. Par conséquent, les particuliers peuvent ne pas savoir comment les renseignements qui les concernent sont utilisés. Une autre préoccupation, concernant l'intrusion, mène à parler du recours à la surveillance électronique pour surveiller le comportement.

On note également que bien que les particuliers aient toujours partagé des renseignements personnels avec d'autres, ils ont eu tendance à considérer le partage plus poussé des mêmes renseignements comme une atteinte à la vie privée. Néanmoins, en définitive, le contrôle de ce partage dépend du degré de sécurité de l'information. Toutefois, la capacité d'ajouter de la valeur aux renseignements en les compilant, en les regroupant et en les analysant, avantage non seulement les compagnies d'information, mais

également les particuliers qui utilisent les nouveaux services d'information et qui occupent des emplois dans le secteur de la technologie de l'information.

Un des grands principes auxquels souscrit l'ACTI est que les particuliers devraient être libres de déterminer le niveau de protection de la vie privée qui leur convient. Cela signifie qu'ils peuvent choisir d'être branchés ou non à l'infrastructure de l'information, d'accepter ou de refuser les services susceptibles d'affecter le niveau de protection de leur vie privée, et de s'inscrire seulement aux services qu'ils souhaitent recevoir et n'être facturés que pour ces services. Cependant, ils ne devraient pas recevoir un moins bon service en raison de leur choix.

### **Approches**

- I. L'ACTI est en faveur de la promulgation de lois garantissant à tous les Canadiens des droits uniformes à des niveaux raisonnables et appropriés de protection de la vie privée et de sécurité de l'information, ainsi qu'à des recours juridiques. Plus précisément, elle est en faveur de lois bannissant les produits ou les services visant à compromettre la protection de la vie privée ou la sécurité de l'information, tels que l'utilisation d'appareils de balayage électronique pour intercepter les communications sans fil privées. En outre, elle appuie les lois limitant l'utilisation de renseignements personnels par les organismes et les établissements dans le secteur public. Cela comprend l'utilisation de renseignements personnels par le gouvernement et par des établissements comme les hôpitaux, les écoles et les forces policières. De même, on devrait limiter la divulgation de renseignements personnels par les entreprises privées aux organismes gouvernementaux, sans autorisation légale précise, ainsi que la communication d'information par les secteurs médical, juridique et bancaire. De plus, les gouvernements voudraient peut-être prévoir dans les lois, des dispositions permettant de communiquer des renseignements personnels aux organismes chargés de l'application de la loi lorsque les fournisseurs de services pensent que des activités frauduleuses ou criminelles ont lieu. Enfin, l'ACTI est d'avis qu'il est nécessaire d'avoir des lois qui définissent quelle partie est responsable dans le cas de communication illégale d'information. Elle recommande d'établir le principe de culpabilité conjointe selon lequel la partie «expéditrice» et la partie «réceptrice» aient clairement intérêt à respecter leurs obligations.
- II. Au-delà des niveaux établis en vertu des lois, l'ACTI est d'avis que l'industrie et les consommateurs devraient s'autoréglementer par l'entremise du marché des services d'information offerts. Les codes sectoriels devraient précisément traiter de la question de la sécurité des renseignements personnels : dans quels cas ils peuvent être recueillis, sauvegardés et compilés; dans quel cas, avec qui et à

quelles fins ils peuvent être partagés; de quelle façon est déterminée la propriété des renseignements; et de qui faut-il obtenir la permission au préalable. À cet égard, l'ACTI appuie fortement les efforts de la CSA pour élaborer un modèle de code de protection de la vie privée par l'entremise d'un comité technique sur la protection de la vie privée au sein duquel les consommateurs et l'industrie sont bien représentés. En se fondant sur les lignes directrices de l'OCDE, le modèle de code contient dix principes en matière de protection de la vie privée (voir l'Annexe B), et pourrait être utilisé comme norme par rapport à laquelle les codes volontaires pourraient être examinés. En outre, le code devrait aider à protéger la compétitivité internationale du Canada à la lumière des directives proposées de la CE qui restreindraient le transfert de renseignements aux pays qui n'ont pas une forte protection de la vie privée. Enfin, l'ACTI appuiera l'application rigoureuse du code de la CSA et des codes sectoriels, soit par des organismes sectoriels soit par un organisme indépendant du secteur privé.

- III. Les solutions technologiques ont également un rôle à jouer, notamment les normes de chiffrement. De l'avis de l'ACTI, on devrait encourager la participation du public à la planification et à la mise en oeuvre des systèmes d'information. Également, bien qu'un examen prolongé des répercussions sur la vie privée ne soit pas souhaitable dans la plupart des cas, l'introduction de nouveaux systèmes de renseignements personnels devrait s'accompagner de la soumission à une autorité indépendante d'une évaluation de l'incidence de ces systèmes sur la vie privée, pour commentaires et présentation publique.
- IV. On devrait éduquer le public pour le sensibiliser à la valeur des renseignements personnels et aux droits et concepts fondamentaux liés à sa protection. En outre, les Canadiens devraient connaître les lois gouvernementales et les codes qui existent dans l'industrie, ainsi que les mesures additionnelles de protection de la vie privée qu'offrent les fournisseurs de services d'information. De plus, le partage de certains types de renseignements personnels tend à devenir plus acceptable lorsque la raison sous-jacente et les avantages attendus sont compris. Également, des programmes éducatifs devraient être élaborés pour le secteur commercial, parce qu'on doit rappeler à bon nombre d'entreprises que la sécurité de l'information devrait faire partie intégrante de toute décision d'affaires. Par exemple, tous les contrats devraient contenir des clauses de confidentialité et les employés devraient recevoir une formation quant à l'importance de protéger les renseignements personnels.

## **Propositions précises et recommandations**

L'ACTI offre ses services pour aider à l'élaboration d'évaluations des répercussions sur la protection de la vie privée, de codes et de politiques visant la sécurité des entreprises, et d'une campagne dynamique d'éducation du public.

### ***Mobility Canada***

Mobility Canada représente les entreprises qui fournissent à un million de Canadiens des services téléphoniques sans fil.

La présentation de Mobility Canada traite principalement de la protection de la vie privée en ce qu'elle touche aux communications téléphoniques radio. Elle s'engage à fournir à ses clients la protection de la vie privée qu'ils exigent pour les communications sans fil et à protéger les renseignements confidentiels sur les clients.

Sa position a toujours été que les Canadiens qui utilisent la téléphonie sans fil devraient avoir droit au même degré de protection de la vie privée que ceux qui utilisent les services avec fil. Par le passé, elle a présenté ses vues au comité législatif pendant les audiences sur le projet de loi C-109, un projet de loi pour modifier le code criminel, la Loi sur la responsabilité civile de l'État et le contentieux administratif et la Loi sur les radiocommunications. En outre, elle a fait des démarches auprès d'Industrie Canada pour que l'importation, la fabrication et la vente d'appareils de balayage électronique analogues et numériques, ainsi que l'écoute non autorisée des conversations sur téléphone cellulaire, soient rendues illégales. Elle appuie la recommandation récente du Conseil consultatif selon laquelle les appareils de balayage électronique et l'interception non autorisée de communications téléphoniques radio doivent être déclarées illégales.

Pour ce qui est de la protection des renseignements confidentiels sur la clientèle détenus par ses compagnies membres, elle a déjà commencé à adopter un code de pratiques équitables en matière d'information qui va au-delà des règlements qu'impose présentement le CRTC.

En outre, les compagnies membres de Mobility Canada éduquent activement leurs clients sur les mesures de protection de la vie privée s'appliquant aux téléphones cellulaires. Elles sont également engagées à fournir un service numérique qui est plus difficile à intercepter et qui permet d'offrir un service de chiffrement de qualité supérieure à des prix raisonnables.

## **Conseil consultatif canadien de la radio**

De l'avis du Conseil, la protection de la vie privée est primordiale pour les Canadiens et appuie les initiatives du gouvernement et de l'industrie pour renforcer les mesures de protection de la vie privée.

Sa présentation traite fondamentalement de la protection de la vie privée dans les communications radio. Dans sa réponse au document de 1993 intitulé «Public Discussion Paper on Radio Based Telephone Communications and Privacy», le Conseil recommandait qu'on accorde à toutes les communications téléphoniques radio le même niveau de protection que les services avec fil non encodés. Il recommandait plus précisément de bannir les appareils de balayage électronique analogues et numériques et que cela viserait non seulement les fréquences pour téléphones cellulaires, mais également les autres fréquences utilisées pour les communications radio privées. Ces recommandations ont été acceptées dans l'ensemble par le Conseil consultatif et le Conseil recommande de les adopter sans tarder.

## **Association RadioComm du Canada (ARC)**

L'Association de radiocommunicateurs du Canada représente l'industrie des télécommunications sans fil au Canada, y compris les compagnies de téléphones cellulaires, les détenteurs de licences publiques pour téléphones sans fil, la recherche de personnes par radio et les opérations radio mobiles.

Dans l'ensemble, l'ARC est d'avis que toutes les approches exposées dans le Document de travail faisant appel à des partenariats industrie/gouvernement font partie de la solution. Elle est en faveur de renforcer les mesures de protection de la vie privée dans les secteurs public et privé. L'association traite plus précisément des questions liées à la protection de la vie privée par rapport aux communications radio.

Pour ce qui est des questions touchant la protection de la vie privée, l'Association est d'avis que les préoccupations liées à l'autoroute de l'information sont fondées, particulièrement en raison de l'accroissement des bases de données de renseignements personnels, y compris des bases de données transactionnelles et de profils personnels.

L'Association aborde également des questions concernant spécifiquement la protection de la vie privée relativement aux communications radio. L'ARC a émis des commentaires sur ces questions dans le passé et appuie pleinement les principes de protection de la vie privée par rapport aux télécommunications émis par le ministère des Communications en 1992, parce qu'à son avis, les Canadiens ont le droit au même niveau de protection de la vie privée pour les communications radio que pour les

communications avec fil. Par conséquent, elle appuie les recommandations récentes du Conseil consultatif voulant que les lois en vigueur soient modifiées pour que désormais, ce soit une offense d'intercepter toute communication téléphonique radio et que, dans l'ensemble, la fabrication, l'importation, la vente et la distribution d'appareils de balayage électronique permettant de surveiller les radiotéléphones soient interdites. Elle s'inquiète du fait que si cela n'est pas fait, cela nuira au déploiement et à l'évolution de la téléphonie radio et le rôle du Canada en tant que chef de file dans ce domaine pour rapidement s'éroder.

### **Approches**

- I. A part l'introduction de lois pour freiner l'interception des communications, l'Association est d'avis que, bien qu'elle soit souhaitable, l'adoption d'un cadre de normes nationales sur la protection de la vie privée dans toutes les sphères d'activité serait difficile en raison des différences dans les juridictions fédérales et provinciales.
- II. L'ARC est fortement en faveur de l'élaboration de codes dans l'industrie pour traiter les questions touchant la protection de la vie privée. Ils peuvent être appliqués par la pression des pairs et, dans certains cas, par la menace de sanctions de la part d'organismes de réglementation. A cet égard, l'ARC est en voie d'élaborer un code sur la protection de la vie privée dans l'industrie pour ses membres, qu'ils soient ou non réglementés par le CRTC, et qui traiterait de la confidentialité des renseignements sur les consommateurs.
- III. À mesure que la technologie progresse, il devient de plus en plus possible de protéger la vie privée par des moyens technologiques. Par exemple, l'industrie des communications sans fil se convertit rapidement à un système de transmission numérique qui est en soi une forme plus sécuritaire de transmission et permet l'utilisation d'encodage numérique. Toutefois, l'ARC mentionne que les lois actuelles restreignent l'importation et l'exportation d'appareils hautement encodables et qu'il pourrait être extrêmement difficile d'arriver à obtenir une norme d'encodage commune aux É.-U. et au Canada. En outre, l'ARC met en garde que, bien que le progrès technologique puisse assurer un environnement plus sécuritaire, il peut aussi ouvrir la voie aux abus.
- IV. L'ARC convient qu'il est fondamental et nécessaire de continuer d'éduquer le consommateur relativement aux questions de protection de la vie privée et affirme que l'industrie des communications sans fil s'engage à fournir à ses clients des renseignements reliés à la protection de la vie privée sur une base régulière.

## **Propositions précises et recommandations**

**Des mesures réglementaires et législatives devraient être mises en oeuvre sans tarder, pour tenir compte de l'interception des communications radio privées et pour bannir les appareils de balayage électronique.**

### ***Rogers Cantel Inc.***

**Cantel exploite à l'échelle nationale un certain nombre de services de radiocommunications, notamment des services de téléphone cellulaire, des services de recherche de personnes et de données mobiles. La société détient également une licence l'autorisant à fournir des services téléphoniques air-sol et des services téléphoniques sans fil.**

**Cantel traite principalement de questions relatives à son exploitation et, ainsi, soutient les présentations faites par Rogers Communications Inc., l'Association canadienne de la technologie de l'information, l'Association des radiocommunicateurs du Canada et le Conseil consultatif canadien de la radio.**

**Dans l'ensemble, Cantel est d'avis que le secteur privé devrait s'autoréglementer et est en faveur de l'adoption de codes de déontologie volontaires pour le secteur des télécommunications, de solutions technologiques et de l'éducation du consommateur. Si, toutefois, en raison de la nature volontaire des codes, certains participants cherchent à se soustraire à leurs modalités, le gouvernement fédéral devrait prendre toutes les mesures nécessaires pour faire en sorte que tous les participants soient soumis au même engagement concernant la protection des renseignements personnels. La présentation traite également des principes généraux de protection de la vie privée et de la protection des services radio.**

**La protection des renseignements sur les clients et des communications avec la clientèle est une question importante pour Cantel.**

**Pour ce qui des principes généraux de protection de la vie privée, Cantel est d'avis que, pour assurer une vaste utilisation des nouveaux services innovateurs que promet l'autoroute de l'information, on devra assurer aux utilisateurs le niveau souhaité de protection de l'information et des communications.**

**Pour ce qui est de la protection des messages véhiculés par les appareils de télécommunications sans fil, Cantel est d'avis que les Canadiens devraient pouvoir bénéficier du même niveau de protection de la vie privée pour les communications sans fil et pour les services de l'autoroute de l'information comme le garantit la Loi sur les télécommunications avec fil. Elle souligne également le nombre de cas dont on a parlé dans les médias qui ont mis en lumière la facilité avec laquelle on peut intercepter les transmissions cellulaires. Par conséquent, elle appuie les recommandations**

récentes du Conseil consultatif voulant que la loi actuelle soit modifiée pour que soit considéré comme un délit d'intercepter des communications téléphoniques et que, dans l'ensemble, la fabrication, l'importation, la vente et la distribution de détecteurs permettant de surveiller les radiotéléphones soient défendues.

Selon Cantel, pour assurer la protection de la vie privée des Canadiens, jusqu'à l'an 2000 et au-delà, on devrait respecter les principes suivants en matière de protection de la vie privée.

Les particuliers devraient avoir le contrôle sur l'utilisation des renseignements personnels les concernant et avoir le choix quant au niveau de protection qu'ils désirent.

Toutes les données et les messages téléphoniques provenant d'un appareil de communication personnel, qu'il soit à fil ou sans fil, devraient être considérés comme privés, et l'interception intentionnelle et/ou la divulgation de ladite information devraient être considérées comme un délit criminel.

Au-delà de la protection de base décrite ci-dessus, le gouvernement et l'industrie devraient faire en sorte que les Canadiens soient pleinement au courant de leurs choix et soient libres de choisir le niveau de protection qu'ils désirent.

#### **Approches**

- II. Cantel appuie un code de déontologie universel pour l'industrie des télécommunications, code qui pourrait s'inspirer du projet de la CSA. Des codes similaires sont déjà utilisés dans divers secteurs de l'industrie, dont certains ont résulté des décisions du CRTC. Par conséquent, Cantel est d'avis que tous les participants devraient être tenus de se conformer au même code, indépendamment du fait qu'ils soient ou non réglementés par le CRTC, ce qui assurerait une concurrence équitable. En outre, si le Ministre n'utilise pas tous les moyens à sa disposition pour faire en sorte que la disposition sur la protection des renseignements personnels contenue dans la Politique sur les télécommunications canadiennes, figure dans la Loi sur les télécommunications, cela créera des distorsions sur le plan de la concurrence et réduira à rien la protection recherchée par les Canadiens. Enfin, il explique la portion de ses Modalités de service qui traite de la confidentialité des renseignements sur la clientèle relatifs au consentement de divulgation et à l'inspection des dossiers.
- III. Deux aspects de la technologie des communications sans fil peuvent alléger les problèmes de l'interception non autorisée. Soixante-quinze pour cent des Canadiens ont maintenant accès au service numérique qui n'est pas déchiffrable par les appareils de balayage

analogues. Les appareils de balayage numériques ne sont pas encore disponibles sur le marché canadien. En outre, des services d'encodage devraient être offerts sur les services numériques au début de 1996. Par conséquent, bien que la technologie numérique soit fondamentalement plus privée, Cantel est d'avis que le gouvernement fédéral devrait prendre des mesures immédiates pour protéger la vie privée jusqu'à ce que des services d'encodage deviennent disponibles.

- IV. La responsabilité de l'éducation des utilisateurs incombe tant au gouvernement qu'à l'industrie parce qu'il est extrêmement important de sensibiliser les utilisateurs aux choix qui leur sont offerts pour assurer le degré de protection qu'ils désirent. Pour sa part, Cantel a distribué une circulaire sur l'utilisation sécuritaire des téléphones cellulaires, qu'elle a joint aux comptes envoyés, et fournit à ses clients les sections pertinentes de ses modalités de service quant à la confidentialité des renseignements sur la clientèle.

#### **Propositions précises et recommandations**

L'adoption dans l'ensemble de l'industrie d'un code visant la protection de la vie privée devrait devenir une condition pour l'octroi d'une licence de fournisseur d'un service de télécommunications sans fil.

### ***Rogers Communications Inc.***

Rogers Communications est une société de communications canadienne diversifiée, qui a des intérêts dans le domaine de la cablôdiffusion, de la radiodiffusion et des télécommunications.

Les observations de Rogers valent également pour les sociétés qui y sont affiliées ou associées, notamment Rogers Cablesystems et Canadian Home Shopping Network. En outre, l'entreprise est entièrement d'accord avec les présentations de Rogers Cantel et d'Unitel.

En bref, Rogers estime que les codes d'autoréglementation constituent la meilleure approche avec, comme source d'appui, des mesures de protection technologiques et l'éducation des consommateurs. Selon cette société, il ne convient pas d'adopter des lois ou règlements additionnels. A son avis, le problème crucial que doit résoudre le Conseil consultatif est de protéger les renseignements personnels sans restreindre les avantages de l'autoroute de l'information. Rogers expose un certain nombre de sujets de préoccupation dont il faudrait tenir compte lorsqu'on aborde cette question cruciale.

Rogers convient de l'anxiété que manifeste la population relativement à la sécurité et à la protection des renseignements personnels à caractère

délicat dans le contexte de l'autoroute de l'information. À l'égard de cette question cruciale, Rogers a toutefois d'autres appréhensions dont il faudrait tenir compte lorsqu'on élabore des mesures visant à protéger les renseignements personnels.

L'autoroute de l'information est un mode de communication changeant et dynamique, qui évolue rapidement. Par conséquent, les mesures visant à protéger les renseignements personnels doivent être compatibles avec cette progression dynamique, et souvent imprévisible.

Les mesures destinées à protéger les renseignements personnels doivent viser, de façon générale, tous les réseaux et à tous les fournisseurs de services qui se font concurrence. Par conséquent, dans une optique concurrentielle, Rogers allègue que les firmes qui fournissent des services par l'entremise de sociétés affiliées ne doivent pas être soumises à des restrictions relativement à l'utilisation des renseignements personnels, dont n'ont pas à se soucier les entreprises qui regroupent un certain nombre de divisions. Ces deux types d'organisme doivent être soumis aux mêmes règles en matière de protection des renseignements personnels pour ce qui est du transfert des renseignements personnels aux fins de la mise en marché de services et de l'évaluation du risque de crédit.

Dans un environnement complexe et en constante évolution, les prestataires de réseaux ne peuvent contrôler de façon efficace la protection des renseignements personnels. Les difficultés qu'éprouvent les compagnies de téléphone qui tentent de contrôler les télévendeurs illustrent ce problème. Les mesures de protection des renseignements personnels doivent donc viser essentiellement les fournisseurs d'information. Quant aux prestataires de réseaux, ils doivent se concentrer sur les mesures de protection techniques et l'éducation des consommateurs.

Compte tenu du fait qu'on peut désormais combiner, transformer et transmettre, sous la forme de signaux numériques, des paroles, des textes, des sons ou des images en mouvement, la possibilité de perdre les droits de propriété intellectuelle est un problème qui devient beaucoup plus important. Lorsqu'on élabore des mesures de protection des renseignements personnels, il faut donc tenir compte des droits des créateurs de savoir qui utilise leur propriété intellectuelle.

### **Approches**

- I. Rogers estime que l'adoption de lois ou de règlements additionnels créerait trop de difficultés. Les lois sont un instrument peu maniable, qui ne peut s'ajuster efficacement à l'évolution rapide de l'autoroute de l'information. En outre, l'approche législative nécessiterait l'adoption de lois

complémentaires aux niveaux fédéral et provincial, pour garantir que les sociétés qui se font concurrence et les consommateurs sont traités sur un pied d'égalité. Outre des ressources additionnelles du secteur public, cette façon de procéder nécessiterait trop de temps et d'efforts.

- II. Les codes d'autoréglementation sont préférables à la législation, en particulier parce qu'ils sont mieux adaptés aux exigences des consommateurs, du marché et de la réglementation de la branche d'activité en question. Afin de promouvoir la crédibilité et la pertinence des codes d'autoréglementation auprès de tous les intervenants de l'autoroute de l'information, Rogers approuve vivement l'initiative de l'Association canadienne des normes (ACN), qui tente d'élaborer un modèle de code normatif en matière de renseignements personnels. Un comité formé d'un large éventail de groupes qui défendent les intérêts des consommateurs, des entreprises, des travailleurs et des administrations s'occupe en ce moment d'élaborer ce code, conformément aux lignes directrices de l'OCDE. Ce comité établira en outre une norme qui permettra à la communauté internationale d'évaluer l'efficacité des mesures de protection des renseignements personnels adoptées par le Canada.
- III. Rogers sanctionne l'utilisation de la technologie, y compris du codage, pour protéger les renseignements personnels dans le contexte de l'autoroute de l'information. Cette entreprise croit également que les consommateurs peuvent participer au processus de conception de la technologie en collaborant à l'élaboration des normes techniques de l'ACN, financée par cet organisme.
- IV. L'entreprise convient également de la nécessité d'éduquer les consommateurs en ce qui a trait à la protection des renseignements personnels. Il doit s'agir d'une responsabilité que se partagent les particuliers, les administrations et les entreprises. En outre, la diffusion de normes de l'ACN devrait être utile à cet égard.

### ***Stentor Telecom Policy Inc.***

Dans l'ensemble, la firme Stentor ne favorise pas l'adoption de lois additionnelles pour garantir la protection des renseignements personnels. Elle fait valoir que la meilleure façon de procéder est de combiner un code national d'autoréglementation, des solutions technologiques et l'éducation de la population. Si, après un laps de temps raisonnable, cette approche ne fonctionnait pas, il faudrait envisager d'harmoniser les lois nationales et provinciales, en se fondant

sur les principes de la protection des renseignements personnels, les solutions technologiques et l'expérience pratique acquise à l'étape de l'autoréglementation. Des renseignements généraux sont fournis sur la façon dont les sociétés du groupe Stentor ont abordé, et traite encore, les questions relatives à la protection des renseignements personnels. Les préoccupations relatives à la protection de la vie privée des consommateurs font l'objet d'un examen en profondeur. L'entreprise décrit en détail les innovations et les services actuels et futurs dans le contexte de l'autoroute de l'information. Elle fournit également des observations exhaustives sur des aspects spécifiques de la protection des renseignements personnels ayant trait aux données transactionnelles, au profil personnel, à la sécurité des transactions et à l'identification individuelle, au contrôle et à la surveillance, et à l'intrusion.

Depuis le début du service téléphonique, la protection des renseignements personnels est un principe sous-jacent du système de télécommunications canadien. Les entreprises des groupes Stentor ont également reconnu la responsabilité qui leur incombait de protéger les consommateurs des intrusions, par exemple des appels indécents ou importuns, et elles offrent constamment de nouveaux services qui permettent à leurs clients de déterminer leur propre degré de protection des renseignements personnels. En outre, Stentor souscrit aux objectifs du gouvernement canadien en matière de création d'emplois grâce à l'innovation et à l'investissement, renforçant la souveraineté et l'identité culturelle du Canada et garantissant l'accès universel à l'autoroute de l'information sans qu'il en coûte trop cher. L'entreprise a également à coeur le principe voulant que l'autoroute de l'information devrait offrir un degré de protection des renseignements personnels et de sécurité du réseau qui satisfasse les Canadiens sans restreindre les autres avantages de ce mode de communication.

L'autoroute de l'information est perçue comme un système de transmission à large bande qui permet à presque tous les Canadiens d'échanger des messages, des textes, des données, des graphiques et des services vidéos, grâce un ensemble de réseaux appartenant à divers fournisseurs et exploités par ces derniers. Voici des exemples détaillés d'innovations en voie d'être appliquées : l'initiative «Beacon» des entreprises Stentor en vue d'élargir, d'ici 10 ans, l'accès à large bande interactif à un nombre de ménages et d'entreprises variant entre 80 % et 90 %, les couplages médicaux et éducationnels auxquels de nombreuses provinces ont procédé, etc. Plutôt que d'aboutir au soi-disant univers de 500 canaux, l'autoroute de l'information favorisera la création d'un «canal personnel» qui témoignera des intérêts et des besoins particuliers de chaque utilisateur.

Les études les plus pertinentes révèlent que l'utilisation des renseignements personnels et le droit de vivre en paix sont les

principales questions relatives à la protection de la vie privée que soulève la nouvelle autoroute de l'information. Les modifications apportées à ce niveau expliquent également qu'on accorde plus que jamais de l'importance aux questions relatives à la protection des renseignements personnels et, à mesure qu'évolue la technologie, aux nouvelles mesures de protection. Les retombées des investissements futurs au titre de l'infrastructure et des services de l'autoroute de l'information seront considérablement réduits si les Canadiens sont insatisfaits du degré de protection des renseignements personnels qu'offrent les réseaux.

Plusieurs enquêtes menées ces dernières années, en particulier celle effectuée en 1992 par Ekos Research Associates, font état des préoccupations des Canadiens eu égard à la protection des renseignements personnels. L'étude Ekos en vient à la conclusion que même si les Canadiens se soucient du contrôle des renseignements personnels, ils acceptent mieux qu'on utilise ces derniers dans certains cas où l'objet et les avantages sont clairement définis. En outre, l'utilisation subséquente, à l'intérieur, des renseignements ayant trait à la clientèle pose moins de difficultés une fois que des relations d'affaires ont été établies. Pour ce qui est du droit de vivre en paix, l'étude Ekos révèle que le télémarketing dérange plus que la publicité postale ou le porte-à-porte. En outre, cette étude signale que les Canadiens ont pris des mesures en vue de protéger leur vie privée. Bien que fort préoccupés par la protection de la vie privée, les Canadiens ne sont pas prêts, croit-on, à renoncer aux avantages découlant de la technologie informatique et des communications. Il semble qu'il faudrait en arriver à un équilibre entre les utilisations raisonnables et autres des renseignements personnels et les mesures adéquates visant à permettre aux particuliers de restreindre le mode d'utilisation des renseignements qui les concernent.

Quant au droit de vivre sans intrusion, on donne plusieurs exemples de contrôle ou de surveillance et d'intrusion. L'exemple typique de contrôle ou de surveillance est celui de la «laisse électronique», fruit des capacités accrues de repérage des systèmes de communications personnels sans fil et par satellite, qui permet, en l'absence de mesures de contrôle efficaces, de repérer une personne et de suivre ses déplacements sans y être autorisé. La surveillance des employés, qu'il s'agisse de surveillance vidéo ou de surveillance électronique de la productivité, suscite également un vif intérêt. On se préoccupe en outre de la surveillance du courrier électronique, par des employeurs ou des sources externes, et de l'utilisation des appareils de balayage électronique en vue d'intercepter des communications cellulaires ou d'autres communications radio à caractère privé. Enfin, la surveillance au foyer posera éventuellement un problème, compte tenu des systèmes proposés qui permettront de fournir des services de sécurité

par des moyens électroniques, du contrôle électronique de la consommation et des services auquel se livrent les entreprises de services publics et des services multimédias interactifs offerts par la voie de la télévision et des ordinateurs personnels. Néanmoins, la surveillance et le contrôle ne sont pas perçus comme des facteurs totalement négatifs. On admet qu'ils comportent des avantages significatifs dans le domaine de la sécurité au foyer, de la recherche et du sauvetage, de la gestion d'un parc à des fins commerciales, etc.. Le problème se résume aux utilisations du contrôle et de la surveillance. L'intrusion est également perçue comme un problème. Elle peut prendre diverses formes, mais celle dont on se préoccupe surtout est le télémarketing. Toutefois, l'incidence du télémarketing a été atténuée, dans une certaine mesure, par les récentes décisions du CRTC qui ont restreint l'utilisation des dispositifs de composition et d'annonce automatique (DCAA).

Des observations détaillées sont également soumises eu égard aux préoccupations relatives à la protection des renseignements personnels.

Il est notamment question des données transactionnelles et du profil personnel, de la sécurité des transactions et de l'identification individuelle. On donne des exemples qui font valoir qu'outre leurs aspects négatifs importants, ces questions comportent également des avantages significatifs, à condition que des mesures pertinentes de protection des renseignements enrayent l'utilisation non autorisée des renseignements personnels et que les consommateurs puissent restreindre rapidement et facilement l'utilisation de ces derniers. Le consentement relatif à l'utilisation ou au transfert des renseignements personnels est également envisagé comme un aspect clé. Toutefois, Stentor est d'avis que l'imposition d'une telle exigence sans période d'instauration progressive entraînerait un bouleversement économique important dans le secteur du marketing direct au Canada.

#### **Réponses aux questions**

1. La protection des renseignements personnels tourne autour de trois questions : la nécessité d'adopter des pratiques équitables en matière d'information pour définir les règles fondamentales de l'utilisation des renseignements personnels, le droit de vivre en paix et la nécessité de sensibiliser les fournisseurs de services d'information, les responsables du perfectionnement technologique et les utilisateurs aux préoccupations générales des consommateurs relativement à la protection de la vie privée. En ce qui a trait au premier point, Stentor estime que les dix principes du code modèle de l'ACN, qui interprète dans le contexte canadien les lignes directrices de l'OCDE, sont des critères judicieux et exhaustifs de protection des renseignements personnels dans le cadre de l'autoroute de l'information. La firme

s'est inspirée des lignes directrices de l'OCDE pour élaborer son propre code modèle de pratiques équitables en matière d'information, qui régit ses activités en matière de collecte, d'entreposage, de protection, d'utilisation, de divulgation, de vérification individuelle et de correction des renseignements personnels. Eu égard au deuxième point, le droit de vivre en paix, (l'un des six principes de la protection de la vie privée dans le domaine des télécommunications énoncés par l'ancien ministre des Communications, M. Perrin Beatty) doit être l'une des pierres d'assise de l'élaboration d'une autoroute de l'information. Pour ce qui est du troisième point, Stentor est d'avis qu'il faut offrir aux consommateurs le plus de choix possibles dans le domaine des télécommunications et de la protection des renseignements personnels dans le contexte de l'autoroute de l'information, et que le choix du degré de protection de la vie privée ne devrait pas limiter l'accès aux services et aux renseignements du réseau.

2. Les entreprises du groupe Stentor croient qu'il est trop tôt pour adopter des lois ou des règlements généraux détaillés. Dans ce domaine, l'un des principes fondamentaux devrait être de ne légiférer qu'en cas d'échec des autres mesures. De cette façon, le gouvernement pourra, plus tard, adopter des lois pour protéger les renseignements personnels si les codes d'autoréglementation, combinés aux solutions technologiques et à l'éducation des consommateurs, ne réussissent pas à protéger la vie privée des particuliers. En outre, l'adoption hâtive de lois ou de règlements qui ne tiennent pas compte des réalités du marché pourrait entraver ou décourager les investissements au titre de l'autoroute de l'information. Qui plus est, toute loi éventuelle devrait être structurée de manière à tenir compte des principes des codes déontologiques adoptés par les industries et à les respecter.
3. Stentor envisage l'autoroute de l'information comme un réseau national inter-exploitable qui offre des services multimédias interactif aux niveaux local, régional, provincial, national et international. Par conséquent, il est nécessaire d'élaborer une approche nationale en matière de protection de la vie privée pour tenir compte des services outre-frontières et éviter de semer la confusion parmi les consommateurs relativement à la divergence des niveaux de protection dans diverses régions du pays. L'adoption de lois au niveau provincial ou sectoriel n'aboutirait qu'à la «balkanisation», de la protection des renseignements personnels et inciterait les entreprises à s'établir dans les régions

où les exigences sont moins sévères. Bien que la société Stentor ne s'oppose pas, en principe, à l'adoption de lois à l'échelle nationale à des fins d'uniformisation, elle se préoccupe des interminables efforts requis pour harmoniser la législation fédérale et provinciale. Il est donc préférable d'adopter une approche nationale d'autoréglementation qui vise à garantir dès le début une protection dans tout le pays. Elle s'oppose à l'élargissement de la Loi sur la protection des renseignements personnels de façon à englober les établissements régis par l'administration fédérale, parce que les mécanismes administratifs constituent un fardeau, que le CRTC a des responsabilités clairement définies en matière de protection des renseignements personnels et que nombre de fournisseurs de services de l'autoroute de l'information ne sont pas visés par la réglementation fédérale, ce qui rend impossible l'uniformisation.

4. Selon Stentor, le rôle le plus utile que les administrations fédérale et provinciales peuvent jouer en ce moment est de surveiller l'élaboration et la mise en oeuvre des principes facultatifs dans le secteur privé, tout en supervisant la protection des renseignements personnels dans le contexte des nouveaux services interactifs élaborés conjointement par l'administration et le secteur privé. L'entreprise souscrit à l'élaboration d'un code d'autoréglementation national en vue d'assurer la protection des renseignements personnels. Ce code fournirait à tous les utilisateurs de l'autoroute de l'information une série de principes liés à la protection de la vie privée, à partir desquels il serait possible de définir des règles fondamentales communes dans ce domaine. Au nombre des facteurs qui incitent fortement les sociétés à élaborer et à maintenir des normes de protection de la vie privée, mentionnons la réputation des entreprises qui lancent de nouveaux services d'autoroute de l'information, l'influence du choix des consommateurs, les solides contrôles internes et le risque de marché lié à l'incapacité de dissiper le doute quant à la protection des renseignements personnels. Stentor sanctionne l'introduction d'un code national d'autoréglementation pour protéger les renseignements personnels et prête main-forte aux efforts de l'ACN en vue d'élaborer et de mettre en oeuvre ce type de code.
5. Les renseignements personnels seront d'autant mieux protégés par les innovations logicielles et matérielles que les utilisateurs pourront choisir, de façon rationnelle et rentable, le degré de protection de leurs renseignements personnels. Toutefois, la protection des renseignements personnels n'est pas l'unique critère de conception des futurs services interactifs. Le fait que

les normes relatives à l'autoroute de l'information, en particulier celles qui se rapportent à la sécurité des données, sont excessivement sévères ou ne tiennent pas compte des diverses applications de l'autoroute de l'information pourrait constituer un obstacle au plan de l'innovation et du coût des services. Les futurs services d'autoroute de l'information doivent être conçus de façon à permettre aux particuliers de choisir et d'obtenir le niveau de protection des renseignements personnels dont ils ont besoin, ce qui serait peut-être possible en établissant des «niveaux» d'utilisation de l'autoroute de l'information. Par exemple, il faudrait élaborer des mesures sophistiquées pour bloquer l'accès en direct aux dossiers médicaux et aux applications bancaires. Par ailleurs, le réseau Internet offrira tout au plus la possibilité d'avoir recours au codage, au besoin.

6. Les Canadiens peuvent jouer un rôle déterminant au plan de la conception des nouvelles technologies, notamment en formant des groupes de défense des consommateurs et des intérêts publics, en participant aux audiences publiques des fournisseurs de services réglementés, en se servant des médias, en établissant des contacts directs avec les fournisseurs de services et, lorsque de nouveaux services font leur apparition sur le marché, en «votant avec leurs pieds». L'exercice du choix du consommateur est devenu un rouage puissant du marché. Sans la confiance des consommateurs, l'élaboration d'applications dans le contexte de l'autoroute de l'information deviendra une aventure extrêmement hasardeuse. Par conséquent, les fournisseurs d'information seront extraordinairement préoccupés par la protection des renseignements personnels.
7. L'éducation des consommateurs est un élément essentiel du succès de l'autoroute de l'information. Les entreprises Stentor sont d'avis que les secteurs privé et public ont tous deux l'obligation de renseigner et d'éduquer les Canadiens en matière de protection des renseignements personnels. Toutes les entreprises du groupe Stentor s'occupent activement de renseigner leurs clients au sujet des options en matière de protection de la vie privée et collaboreront avec d'autres organismes à la mise en oeuvre du code de l'ACN, de même qu'aux efforts significatifs qu'il faudra déployer en matière d'éducation de la population pour promouvoir l'utilisation et la pertinence de ce dernier.

## **TELUS**

TELUS est une société de portefeuille de gestion d'AGT Limited et d'AGT Mobility Incorporated, qui fournit des services de télécommunications et des services sans fil partout en Alberta.

En résumé, TELUS ne croit pas qu'il faille adopter d'autres lois ou règlements. À son avis, l'autoréglementation, renforcée par l'éducation préconisée par l'industrie et les solutions technologiques, est la façon la plus efficace de calmer les inquiétudes de la population au sujet de la protection des renseignements personnels. L'entreprise passe également en revue les préoccupations de la population, l'historique de ses propres efforts en matière d'autoréglementation et le rôle du CRTC eu égard à la protection adéquate des renseignements personnels.

TELUS est d'avis que les Canadiens sont conscients des possibilités de l'autoroute de l'information en matière de choix des services et des fournisseurs de ces derniers, comme le démontre le pourcentage élevé de réponses favorable à l'enquête TELUS Longwoods de 1994 et au sondage Gallup de 1994. Toutefois, en ce qui a trait à la protection des renseignements personnels dans le contexte de l'autoroute de l'information, ces deux enquêtes ont révélé qu'un pourcentage tout aussi grand de répondants avaient des opinions qui variaient, certains étant très inquiets et d'autres l'étant quelque peu, ou se préoccupaient de la possibilité que leurs noms figurent sur des listes d'adresses ou que des gens peu scrupuleux se procurent des renseignements financiers ou personnels les concernant. Trente-neuf pour cent des répondants à l'enquête Longwoods se souciaient tellement de la protection de la vie privée qu'ils n'utiliseraient vraisemblablement pas l'autoroute de l'information. TELUS est d'avis que nombre de ces préoccupations sont liées à des problèmes futurs qui pourraient surgir à mesure qu'évoluent les services multimédias et la technologie complexe de l'autoroute de l'information. Toutefois, l'entreprise en vient à la conclusion que nous ne pourrions jouir de tous les avantages de l'autoroute de l'information que si nous en arrivons à un équilibre entre les nouveaux services et les préoccupations de la population en matière de protection des renseignements personnels.

L'efficacité des mesures de protection de la vie privée de l'industrie des télécommunications, en particulier celles de TELUS, font l'objet d'un examen détaillé. AGT a été la première société de télécommunications canadienne à mettre sur le marché «l'afficheur» et le service de gestion des appels. Au préalable, l'entreprise avait consulté des maisons d'hébergement pour femmes battues, des services sociaux, des organismes chargés d'appliquer la loi, des professionnels de la santé et d'autres groupes. Par conséquent, divers dispositifs de protection de la vie privée ont été adoptés, se rapportant au blocage des appels, au dépistage de ces derniers ou à la mémorisation désactivée. En outre,

AGT a adopté un code de pratiques équitables d'information, qui s'inspire du code modèle de Stentor. Ce code traite de la collecte, du stockage, de l'accessibilité, de l'utilisation et de la gestion des renseignements personnels, de même que des mesures de sécurité et d'imputabilité et de la transparence. Le code vise autant les clients que les employés. Toutes ces initiatives ont été favorablement accueillies par la population et sont perçues comme des preuves de l'efficacité de l'autoréglementation. À cet égard, AGT participe activement à l'élaboration du code modèle de protection des renseignements personnels de l'ACN.

La société passe également en détail les pouvoirs dont dispose le CRTC, en vertu de la Loi sur les télécommunications, pour mettre en application les dispositions relatives à la protection de la vie privée dans l'industrie des télécommunications. Le CRTC a invoqué ces dispositions pour imposer des normes d'autoréglementation en matière de protection des renseignements personnels à l'industrie des télécommunications, et également pour régler les télécommunications importunes.

TELUS expose un certain nombre de principes dont AGT s'inspire pour élaborer et offrir de nouveaux services. Ces principes sont les suivants :

- Il faut offrir aux clients qui se préoccupent de la protection des renseignements personnels des options qui leur permettent de mieux gérer leurs propres besoins en cette matière.
- L'appelé a le droit de savoir qui l'appelle, sans même avoir à répondre au téléphone.
- L'appelant a le droit de conserver l'anonymat, en particulier s'il existe un risque ou un danger éventuel.
- Tous les appelés ont le droit de se prémunir contre les appels anonymes, en particulier les appels importuns.
- Tous les clients ont le droit d'être avisés à l'avance, en langage clair, de l'incidence sur la vie privée de tout nouveau service, y compris les mesures de protection.
- Lorsque l'introduction de nouveaux services influe sur les intérêts des clients en matière de protection des renseignements personnels, il faut donner la chance à ces derniers d'atténuer, dans la mesure du possible, les conséquences défavorables de ces services et ce, sans coût supplémentaire.

Bien que TELUS soit consciente que l'option législative est fort populaire, elle est d'avis que la nécessité de cette option n'a pas été démontrée et que, par conséquent, il n'est pas utile de légiférer. Elle fait valoir que l'autoréglementation continuera d'être la meilleure façon de calmer les inquiétudes actuelles et futures quant à la protection des

renseignements personnels. La législation priverait les fournisseurs de services de l'essentiel contact direct avec les clients et imposerait d'autres organismes gouvernementaux ou processus d'examen fastidieux.

TELUS estime que l'autoréglementation et le recours à ce type de code permettrait de calmer, de la façon la plus pertinente et la plus efficace qui soit, les préoccupations en matière de protection des renseignements personnels et ce, d'une manière qui soit rentable et axée sur le consommateur. Le CRTC, qui est en faveur des codes d'autoréglementation, a suffisamment d'autorité pour régler les questions relevant de la protection de la vie privée dans le domaine des télécommunications. En outre, la prise en compte des préoccupations au plan de la protection des renseignements personnels est devenue partie intégrante des services offerts. Par conséquent, les clients auront le choix entre divers services et fournisseurs de services, et la concurrence permettra d'éliminer les entreprises réfractaires. Qui plus est, l'autoréglementation permet de régler rapidement les problèmes qui surgissent.

TELUS est un fervent adepte de l'éducation interne. Ses employés ont reçu des exemplaires du code de l'entreprise et d'une brochure d'information. La société a organisé des séances d'information et élaboré une vidéo pour sensibiliser les employés à leurs droits en matière de protection de la vie privée et à ceux des clients.

#### **Réponses aux questions**

1. **TELUS est en faveur d'un plan de protection des renseignements personnels doté des caractéristiques suivantes :**
  - **Recours de la part des fournisseurs de services à des codes d'autoréglementation, par exemple ceux de Stentor et de l'ACN.**
  - **Examen approfondi du CRTC et empressement de cet organisme à exercer ses pouvoirs pour garantir que les fournisseurs de services assument leurs responsabilités en matière de protection des renseignements personnels.**
  - **Sensibilisation accrue de la population par l'administration fédérale, le CRTC et l'industrie.**
  - **Engagement accru de l'industrie pour garantir qu'en matière de protection des renseignements personnels, les solutions technologiques et axées sur le client sont à la hauteur des nouveaux services et tiennent compte des principales préoccupations à cet égard.**

2. Il n'a pas été démontré qu'il était nécessaire d'adopter des lois additionnelles. L'administration fédérale et le CRTC devraient sanctionner les codes d'autoréglementation qui seraient soutenus par l'éducation et les innovations technologiques.
3. Tous les modes d'accès nationaux à l'autoroute de l'information relèvent, à l'heure actuelle, de la compétence de l'administration fédérale. Cela suffit donc pour garantir aux utilisateurs de l'autoroute de l'information un degré uniforme de protection de la vie privée à l'échelle nationale.
4. Les codes d'autoréglementation, soutenus par les mécanismes de réglementation existants, continueront d'être la meilleure façon de calmer, de façon responsable, les préoccupations en matière de protection des renseignements personnels. Il ne faut cependant pas négliger l'importance des éléments dissuasifs du Code criminel, en ce qui a trait à la protection de la vie privée, et de la législation visant à protéger les consommateurs.
5. Les fournisseurs de services de l'autoroute de l'information qui connaîtront du succès auront des motifs très puissants de faire en sorte que leurs services répondent aux exigences des clients en matière de protection des renseignements personnels.
6. Dans le contexte concurrentiel de l'autoroute de l'information, les fournisseurs de services pourront déterminer s'ils répondent aux exigences de leurs clients en matière de protection des renseignements personnels en se fondant sur le comportement de ces derniers en matière d'achats et sur leurs préférences. Qui plus est, avant de lancer un produit ou un service sur le marché, il sera possible de tenir compte des exigences des consommateurs relativement à la protection des renseignements personnels en procédant à des études de marché, en organisant des groupes de discussion et en effectuant des essais de mise en service.
7. Les entreprises responsables peuvent faire en sorte que les clients soient conscients de leurs droits en matière de protection des renseignements personnels et des obligations de l'entreprise relativement à l'utilisation et à la protection de ces renseignements. Les gouvernements peuvent également jouer un rôle complémentaire à cet égard, grâce aux activités déjà mises sur pied par Industrie Canada et certains ministères provinciaux des affaires des consommateurs en vue de sensibiliser les consommateurs.

## **Unitel Communications Inc.**

Unitel est d'accord avec les présentations de Rogers Cantel Inc. et de Rogers Communications Inc.

En résumé, l'entreprise est d'avis qu'il n'est pas nécessaire d'adopter des lois ou des règlements additionnels, car ceux qui existent déjà sont suffisants. Elle croit plutôt que la meilleure façon de protéger les consommateurs et la vie privée des employés est d'adopter des codes d'autoréglementation, soutenus par des solutions techniques et l'éducation des consommateurs. Unitel estime également que les Canadiens se préoccupent vraiment de l'éventuelle érosion de leur vie privée à l'ère de l'information. En réponse aux questions posées dans le Document de travail, la société fait état des diverses mesures qu'elle adopte pour calmer les préoccupations de ses clients et de ses employés relativement à la protection des renseignements personnels.

### **Réponses aux questions**

1. De l'avis d'Unitel, les six principes de protection de la vie privée en matière de télécommunications, adoptés par l'ancien ministre des Communications en novembre 1992, devraient servir d'assise à la politique relative à la protection des renseignements personnels des consommateurs des services de télécommunications. En outre, ces principes permettront aux fournisseurs de services d'élaborer leurs propres politiques et procédures. Unitel modifie en ce moment son propre code en fonction de ces principes et de ceux qui ont été élaborés dans le contexte du projet de code modèle de l'ACN.
2. Unitel allègue qu'en ce qui a trait aux transporteurs réglementés des télécommunications, il n'est pas nécessaire, à l'heure actuelle, d'adopter des mesures de protection plus sévères. Ces mesures pourraient miner les efforts que déploie l'ACN en vue d'élaborer un code modèle, avec l'appui général des groupes de consommateurs, des gouvernements et de l'industrie. La concurrence a forcé les entreprises à être plus attentives aux préoccupations de leurs clients en matière de protection des renseignements personnels, ce facteur ayant de l'importance aux fins de la fidélisation de la clientèle. En outre, les transporteurs réglementés sont tenus de respecter les dispositions relatives à la confidentialité de leur mandat (un exemplaire de l'article 11 du mandat d'Unitel qui traite des dispositions relatives à l'utilisation, à la divulgation et à l'inspection est inclus dans la présentation). En outre, les transporteurs réglementés doivent respecter les dispositions relatives à la protection des renseignements personnels de l'alinéa 7(i) de la Loi sur les télécommunications et de l'article 41 de cette loi, qui permettent au CRTC de

16 régler les télécommunications importunes. À cet égard, le  
20 Conseil a déjà pris des mesures pour restreindre l'utilisation des  
dispositifs de composition et d'annonce automatique (DCAA), la  
publicité importune par télécopieur et les appels téléphoniques  
en direct à des fins de sollicitation, et pour offrir à tous les clients  
la possibilité de bloquer l'affichage de noms et ce, sans frais.  
Finalement, en 1994, le Conseil a décidé de ne pas traiter  
rapidement les demandes d'approbation de tarifs en régime de  
concurrence des entreprises de téléphone, si ces demandes  
soulèvent des préoccupations en matière de protection des  
renseignements personnels.

3. Pour les raisons énoncées dans les réponses à la question 2,  
Unitel est d'avis qu'il n'est pas nécessaire d'adopter d'autres lois  
aux niveaux fédéral, provincial ou sectoriel, en ce qui a trait aux  
transporteurs réglementés des télécommunications. En outre, la  
grande majorité des transporteurs réglementés participent  
activement à l'élaboration du code modèle de protection des  
renseignements personnels de l'ACN et y souscrivent  
pleinement.

4. L'entreprise parle bien haut en faveur des codes  
d'autoréglementation qui permettront aux sociétés de  
personnaliser leurs politiques et procédures en matière de  
protection de la vie privée en fonction de la nature de leurs  
activités et de leur clientèle. Par conséquent, elle collabore à  
l'élaboration du code modèle de l'ACN, fondé sur les lignes  
directrices de l'OCDE. Les entreprises s'en inspireront pour  
élaborer leurs propres codes qui seront ensuite soumis à  
l'approbation de l'ACN. Unitel fait remarquer que le Commissaire  
à la protection de la vie privée s'est montré particulièrement  
favorable à l'initiative de l'ACN. En outre, les codes  
d'autoréglementation sont plus souples que la législation et  
peuvent facilement s'adapter à l'évolution, au fil des ans, des  
attentes des consommateurs relativement à la protection des  
renseignements personnels, possibilité dont il est fait état dans  
les principes énoncés par le gouvernement en matière de la vie  
privée dans le domaine des télécommunications.

5. Unitel est d'accord sur le fait que ce n'est pas la technologie en  
soi qui pourrait constituer un danger pour la vie privée, mais bien  
les utilisations de cette technologie. Elle croit que la technologie  
devrait servir à accroître au maximum la protection de la vie  
privée, notamment à bloquer, sans frais, l'affichage de certains  
appels.

En outre, en raison de l'exigence statutaire voulant que les  
transporteurs ne se préoccupent pas du contenu des messages

des clients, ces derniers ne doivent pas jouer le rôle d'agent de la voirie sur l'autoroute de l'information et on ne peut s'attendre qu'ils agissent en ce sens. Ce sont les fournisseurs d'information et non pas les transporteurs qui devraient être tenus responsables des infractions en matière de protection de la vie privée, dans les cas où leur responsabilité est clairement établie.

6. Unitel fait remarquer qu'en ce qui a trait aux services de télécommunications réglementés, il existe déjà une tribune où les consommateurs peuvent faire connaître leur opinion au sujet des nouvelles technologies et des nouveaux services et de leur incidence sur la protection des renseignements personnels. Il s'agit des audiences publiques devant le CRTC. En outre, les consommateurs pourront soumettre leurs observations à l'ACN relativement à son code modèle de protection des renseignements personnels. Une fois que ce code aura été officiellement adopté, Unitel s'attend que l'ACN continuera de servir de tribune pour discuter des questions relatives à la protection des renseignements personnels.
7. L'éducation des consommateurs en matière de protection des renseignements personnels est manifestement une question d'intérêt public. Tant l'administration que les entreprises ont un rôle à jouer à cet égard. En outre, en faisant connaître leurs préoccupations, les consommateurs peuvent également assumer une part de cette responsabilité.

#### **Propositions et recommandations spécifiques**

Unitel allègue que si des mesures de protection de la vie privée additionnelles sont adoptées à l'issue des audiences du Conseil consultatif, il existe des raisons valables, énoncées dans sa présentation, pour lesquelles le secteur des télécommunications réglementées devrait être exempté de l'application de ces nouvelles mesures.

## **DÉFENSEURS DES CONSOMMATEURS ET DE LA VIE PRIVÉE**

### ***Association des consommateurs du Québec Inc.***

En résumé, l'Association en arrive à la conclusion que les divers ordres de gouvernement doivent légiférer pour garantir qu'on respecte la vie privée et la confidentialité des renseignements personnels et qu'on recueille uniquement le minimum de renseignements nécessaires pour identifier un particulier.

L'Association souligne que l'informatique a connu une éclosion formidable et que les médias ont fait état ad nauseam de l'autoroute de l'information. Or, les gouvernements ont attendu jusqu'à tout récemment pour mettre sur pied des comités et des commissions chargés d'étudier les effets et les retombées de l'autoroute de l'information, notamment en ce qui touche le respect de la vie privée. L'Association a signalé trois éléments qui contribuent à créer un besoin pressant de légiférer en la matière : des initiatives du secteur privé (p. ex., la création du Consortium UBI et le projet Sirius de Bell Canada) montrent que les consommateurs auront avant longtemps accès à l'autoroute de l'information; le nombre de services d'information affiche une croissance quasi exponentielle et ces services sont de plus en plus diversifiés; et les systèmes législatifs et judiciaires sont différents dans les divers secteurs de compétence au Canada et on reconnaît la léthargie proverbiale des corps législatifs lorsqu'il s'agit d'examiner et d'adopter de nouvelles lois. Compte tenu de l'incidence de ces trois éléments, l'Association recommande fortement que les divers ordres de gouvernement accordent une véritable priorité à la question de la vie privée sur l'autoroute de l'information.

En réponse à la question posée à la page 18 du Document de travail, « Incombe-t-il au gouvernement ou au marché de déterminer les niveaux de protection à offrir? », l'Association indique clairement qu'elle ne peut imaginer que l'industrie en arrive un jour à se limiter volontairement dans sa quête de renseignements touchant les consommateurs. Elle croit en outre que les élus se doivent de faire valoir en tout premier lieu les attentes de leurs commettants compte tenu des ressources gigantesques dont dispose l'industrie. C'est pourquoi les gouvernements doivent assumer un vigoureux leadership pour freiner l'intrusion dans la vie privée.

L'Association répond ensuite à la question suivante de la page 18, « La vie privée devrait-elle être une option, que seuls certains Canadiens pourraient se permettre, ou n'entraîner aucun coût et être considérée comme inhérente aux services offerts? » Il faut assurer à tous les Canadiens une protection minimale de leur vie privée, quel que soit leur revenu ou leur statut social. Il est à prévoir que certains services qui permettront d'assurer une protection

de la vie privée supérieure au minimum prévu entraîneront des coûts, mais l'industrie doit absorber les coûts inhérents à la protection minimale de la vie privée.

Enfin, l'Association examine la question de la confidentialité. En cette matière, l'enjeu consiste à déterminer le point à partir duquel l'utilisation de renseignements portant sur un consommateur donné devient abusive. Les institutions qui traitent régulièrement avec le public peuvent avoir besoin de renseignements personnels autres que le nom, l'adresse et le numéro d'assurance sociale d'un particulier. Les questions suivantes doivent servir de guide lorsqu'on détermine s'il y a ou s'il pourrait y avoir abus :

L'institution a-t-elle recueilli beaucoup plus de renseignements que ceux dont elle avait besoin pour accomplir une tâche donnée? A-t-elle recueilli des renseignements sans l'autorisation de la personne visée ou des Canadiens dans l'ensemble? Le mode d'accès à l'information permet-il à un particulier de recueillir des renseignements personnels sur un autre? Les institutions ou les spécialistes du marketing peuvent-ils avoir accès aux renseignements pour mieux cibler ou influencer des clients éventuels?

### **Colin J. Bennett**

M. Colin J. Bennett, professeur associé au département des sciences politiques de l'université de Victoria, est un ardent défenseur de la vie privée. Cet intervenant bien connu a à son actif un grand nombre de publications dans ce domaine.

En résumé, M. Bennett croit qu'à peu près tout le monde s'accorde sur les principes d'une pratique équitable en matière d'information; personne ne souhaite être considéré comme étant opposé à la vie privée des particuliers, ni comme sous-estimant les craintes bien réelles du public canadien. C'est pourquoi on ne peut envisager le statu quo en matière de réglementation et nous avons besoin d'appliquer toute la gamme de solutions à ce problème, en l'occurrence les codes d'autoréglementation, une intervention législative, les technologies qui protègent la vie privée (chiffrement) et la sensibilisation des consommateurs. Aucune de ces options ne suffit en soi. M. Bennett a aussi présenté brièvement l'évolution de la législation concernant la vie privée un peu partout dans le monde et fait notamment état des plus récentes dispositions législatives et non législatives en vigueur au Canada à l'heure actuelle qui visent à protéger les données. Dans le même ordre d'idée, il donne un aperçu du manque d'uniformité et des lacunes de la situation présente. Il étudie actuellement pour le compte de la CSA diverses options de mise en oeuvre pour la validation de son code type. Il espère être en mesure de faire valoir son point de vue au cours des travaux du Comité consultatif.

M. Bennett résume les résultats d'une enquête récente intitulée « La vie privée exposée ». Cette enquête a révélé que 52 p. 100 des Canadiens se

préoccupent au plus haut point de la vie privée, tandis que 92 p. 100 s'en préoccupent dans une certaine mesure. De plus, 83 p. 100 des répondants se sont dits convaincus qu'une organisation doit leur demander la permission avant de transmettre à une autre des renseignements les concernant, et 71 p. 100 estiment que les règles en la matière doivent absolument s'appliquer à la fois au gouvernement et aux entreprises. En outre, « ils croient que la vie privée est menacée de toute part, que ce soit par la technologie ou par les impératifs commerciaux et sociaux ». Enfin, les organisations des milieux d'affaires suscitent une plus grande préoccupation que celles du secteur public.

Il signale que l'examen dont font actuellement l'objet les dispositions en vigueur au Canada concernant la protection des données a permis de constater que le Québec est le seul secteur de compétence à avoir adopté une loi de nature générale s'appliquant au secteur privé. Les dispositions de la loi québécoise s'appliquent à tous les renseignements personnels recueillis, stockés, utilisés ou diffusés par une autre personne et elles visent principalement les entreprises qui exercent des « activités économiques organisées ». Les dispositions relatives au consentement s'appliquent à la collecte et à l'utilisation de renseignements personnels et les bureaux de crédit sont considérés comme un type particulier d'entreprise. Cependant, ce sont les dispositions concernant les flux transfrontières de données qui sont considérées comme étant susceptibles d'avoir la plus grande incidence à l'extérieur du Québec, car elles laissent sans réponse de nombreuses questions touchant le commerce interprovincial, l'ALENA, les entreprises du secteur privé assujetties à une réglementation fédérale, etc. M. Bennett examine aussi brièvement la législation qui régit le crédit à la consommation dans l'ensemble du Canada. À son avis, le seul autre segment du secteur privé qui est doté d'une réglementation d'une certaine portée dans ce domaine est celui des télécommunications. En 1992, le ministre des Communications a énoncé six *Principes de protection de la vie privée dans les télécommunications*, dont la mise en application a été confiée à une agence de protection de la vie privée dans les télécommunications, formée de représentants de l'industrie et de groupes de consommateurs. Cependant, cette agence n'a jamais vraiment pris son essor pour diverses raisons politiques, financières et pratiques et la nouvelle *Loi sur les communications*, qui confère au CRTC le pouvoir de réglementer pour protéger la vie privée des particuliers, a pris le relais.

M. Bennett fait aussi le point sur les efforts déployés par le secteur privé en matière d'autoréglementation. Il décrit les codes établis par l'Association canadienne du marketing direct, l'Association des banquiers canadiens, l'Association canadienne des assurances de personnes, le Bureau d'assurance du Canada et la Fondation des normes de télévision par câble. De plus, les efforts déployés par la CSA pour élaborer un code type sur la protection des renseignements personnels sont considérés comme une amélioration très encourageante.

En faisant une rétrospective des codes volontaires, il en arrive à la conclusion que ceux-ci peuvent contribuer à sensibiliser les employés et les consommateurs à la question de la vie privée, qu'on peut les adapter en fonction des différents besoins des entreprises et qu'ils peuvent offrir certains recours au citoyen moyen. Toutefois, ils ne sont pas exécutoires et la plupart ne prévoient aucun mécanisme d'arbitrage par un tiers pour traiter les plaintes. Il signale que nous avons réglementé les pratiques en matière d'information de la vaste majorité des institutions du secteur public, mais que certaines organisations qui recueillent et utilisent un volume élevé de renseignements personnels ne sont soumises à pratiquement aucune réglementation. Par ailleurs, les dossiers détenus dans le secteur public ou privé qui renferment des renseignements erronés peuvent aussi porter atteinte aux droits et aux intérêts des particuliers. C'est pourquoi M. Bennett ne voit aucune raison qui empêcherait d'appliquer au secteur privé les principes qui régissent le secteur public. Il voit même trois raisons impérieuses de le faire : la modification des fonctions organisationnelles pour tenir compte des pratiques liées aux nouvelles technologies; les fortes appréhensions du public sur la protection de la vie privée (comme il en a déjà été fait mention); et les nouvelles normes internationales concernant les flux transfrontières de données.

Il signale que la démarcation entre les secteurs public et privé se modifie et devient imprécise. Il est de plus en plus difficile de savoir où commence chacun. C'est pourquoi M. Bennett prévoit que l'incidence qu'auront sur les pratiques du secteur privé les questions soulevées concernant l'application de la législation fédérale et provinciale variera au fil du temps. Le fait que les commissaires à la protection de la vie privée et les médias parleront davantage des questions relatives à la vie privée aura aussi des retombées. De même, la privatisation de certaines fonctions exercées auparavant par le gouvernement entraînera un accroissement des échanges de données entre les deux secteurs, tandis que l'appariement des données (par exemple, les données du gouvernement sur les assistés sociaux et les renseignements figurant dans les dossiers bancaires ou financiers en vue de vérifier leur admissibilité) contribuera aussi à estomper la délimitation entre les deux secteurs. Enfin, en raison de l'omniprésence et de la souplesse des nouvelles technologies, il sera difficile de déterminer si des données appartiennent au secteur public ou au secteur privé.

Les nouvelles règles qui voient le jour en Europe pour protéger les données constituent peut-être l'élément le plus important. Les directives proposées par la Communauté européenne visent à harmoniser à l'échelle de l'Europe la législation portant sur la protection des données à un haut niveau de manière à favoriser le commerce. Les anciennes lignes directrices adoptées par l'OCDE pour protéger les données ont eu une faible incidence au Canada, mais les nouvelles directives proposées pourraient offrir aux entreprises canadiennes une perspective tout à fait différente. Les restrictions portant sur le transfert de renseignements personnels à

l'extérieur de la Communauté européenne suscitent une préoccupation particulière. En principe, ce genre de transfert est permis uniquement si le pays qui reçoit les données offre un niveau de protection « adéquat ». Or, il s'agit là d'un recul par rapport à la première version, qui exigeait un niveau « équivalent ». Il y a cependant lieu de croire que seule la loi québécoise satisferait aux nouvelles normes; toutefois, le méli-mélo de codes volontaires et de principes adoptés par les autres provinces ne serait pas à la hauteur. Ces restrictions pourraient ouvrir la voie à des batailles de haute technologie portant sur l'obtention du droit de traiter des renseignements personnels. Certains pays, dont Hong Kong et la Nouvelle-Zélande, ont de toute évidence pris la situation assez au sérieux pour adopter des lois s'inspirant du modèle européen afin de protéger les données.

### ***The British Columbia Public Interest Advocacy Centre***

Le Centre est d'avis que le droit à la vie privée doit être protégé et qu'il ne faut pas laisser les forces du marché le déterminer. C'est pourquoi une loi nationale, l'intégration aux nouvelles technologies de mesures visant à protéger la vie privée et la sensibilisation des consommateurs sont trois moyens auxquels doit avoir recours le gouvernement. Les codes et normes volontaires ne sont pas assez sévères pour protéger la vie privée. Le Centre espère qu'il y aura une tribune sur laquelle on pourra formuler des recommandations plus précises à mesure que le gouvernement élaborera des options pour la protection de la vie privée.

Il s'inquiète de la suggestion voulant que les consommateurs puissent décider dans quelle mesure ils souhaitent renoncer à leur vie privée en contrepartie de leur pouvoir d'achat. Cette façon de faire pourrait nous amener à traiter la protection de la vie privée comme un élément qui fait grimper le prix et dont seules les personnes biens nanties et celles qui sont sensibilisées à cette question peuvent bénéficier. De plus, les consommateurs ne doivent pas avoir à choisir entre l'aspect pratique et la vie privée. La revente de renseignements ne devrait par être permise sans le consentement explicite du particulier visé.

#### **Approches**

- I. Parmi les approches possibles dont fait état le Document de travail, l'adoption de lois et de règlements est considérée comme la plus importante. Bien qu'il ne s'agisse pas d'une priorité absolue pour le gouvernement, la Charte, lorsqu'on la modifiera, devra faire de la vie privée un droit constitutionnel. Toutefois, il faut prévoir d'autres mesures, car la Charte ne s'applique pas au secteur privé. On a besoin d'une loi nationale, puisque les lois provinciales ou sectorielles entraîneront un manque d'uniformité dans la protection de la vie privée et des disparités entre les industries réglementées et les autres. C'est pourquoi les provinces et le gouvernement fédéral

doivent unir leurs efforts pour que les mesures de protection de la vie privée s'appliquent à tous les Canadiens. Le gouvernement fédéral devrait à tout le moins faire en sorte que la *Loi sur la protection des renseignements personnels* s'applique aux industries relevant de sa compétence. De surcroît, en vertu de la *Loi sur les télécommunications*, le CRTC pourrait obliger tous les titulaires et les demandeurs de licences à respecter les lignes directrices sur la protection de la vie privée lorsqu'ils offrent de nouveaux services. Il faudrait pour ce faire que tous les fournisseurs du service de réseau non assujettis à une réglementation à l'heure actuelle relèvent désormais de la compétence du CRTC.

- II. Malgré les efforts déployés par l'Association canadienne du marketing direct et l'Association canadienne de normalisation pour élaborer des codes volontaires, il est difficile d'appliquer ces derniers de manière efficace. L'agence de protection de la vie privée en matière de télécommunications n'est jamais arrivée à jouer un rôle efficace et c'est pourquoi on considère que les codes et les normes volontaires ne sont pas assez sévères pour protéger la vie privée.
- III. Le Centre propose un certain nombre de solutions technologiques. Le matériel et les logiciels destinés à l'autoroute de l'information doivent être conçus de manière à protéger la vie privée dès le début (les coûts sont alors moins élevés), ce qui n'entraverait pas l'innovation technologique. Le gouvernement pourrait travailler de concert avec le secteur privé pour élaborer des mesures de sécurité protégeant la vie privée, adopter des normes en la matière et accorder des subventions aux auteurs de logiciels pour qu'ils protègent la vie privée. Il pourrait aussi évaluer les nouvelles technologies afin de déterminer si elles protègent la vie privée. Il faut offrir au public la possibilité de participer au processus de conception de technologies susceptibles de menacer la vie privée.
- IV. Il faut sensibiliser les Canadiens pour qu'ils puissent bien comprendre leurs droits et les conséquences de la communication de renseignements personnels.

### ***Association des consommateurs du Canada (ACC)***

En résumé, l'ACC souhaite que le gouvernement légifère et considère les codes volontaires comme une étape de l'intervention législative. De plus, elle est d'avis que les solutions technologiques et la sensibilisation des consommateurs ont un rôle important à jouer. Enfin, l'ACC expose plusieurs principes qui permettraient selon elle de protéger efficacement la vie privée.

## **Réponses aux questions**

1. L'ACC a la conviction que les consommateurs ont fondamentalement droit de regard sur les renseignements qui les concernent. Les principes suivants, qui s'inspirent des lignes directrices de l'OCDE, - peuvent s'appliquer au secteur privé :

- recueillir uniquement les renseignements essentiels;
- recueillir des renseignements uniquement auprès de la personne visée et préciser l'usage auquel ils sont destinés;
- si la personne visée n'a pas consenti à une autre utilisation, utiliser les renseignements uniquement pour l'usage prévu;
- si la personne visée n'a pas donné son consentement ou si aucune règle de droit ne le permet, ne communiquer aucun renseignement à des tiers;
- veiller à ce que les données soient exactes, à jour et complètes dans la mesure du possible;
- protéger les données;
- permettre à la personne visée d'avoir accès aux données et de les corriger;
- détruire les données qui ne sont plus nécessaires;
- charger un responsable de veiller au respect des règles.

L'ACC cite aussi d'autres principes de protection des données, élaborés par M. David Flaherty, qu'elle considère utiles.

2. Il faut adopter des mesures plus énergiques pour protéger la vie privée et les renseignements personnels. On doit à cette fin entreprendre une démarche législative qui réduise le plus possible la bureaucratie et dont le fonctionnement soit aussi économique et efficient que possible. La législation peut prendre appui sur les codes volontaires. Les solutions technologiques et la sensibilisation des consommateurs ont un rôle à jouer.

3. L'intervention législative du gouvernement fédéral est considérée comme étant essentielle à l'établissement de normes nationales qui réduiront la confusion chez les consommateurs et permettront à tous les intervenants de lutter à armes égales. En l'absence de normes nationales, l'ACC doute que les provinces puissent en arriver à s'entendre. Or, cette situation risque de susciter une concurrence entre les provinces pour attirer les entreprises désireuses d'être assujetties à des lignes directrices plus modérées sur la protection de la vie privée.

4. L'élaboration de lignes directrices volontaires par les entreprises serait acceptable uniquement s'il s'agissait d'une étape provisoire, avant l'adoption d'une loi nationale sur la protection de la vie privée.
5. L'autoroute de l'information doit être conçue de manière à très bien protéger la vie privée. Cette préoccupation ne ralentira pas le rythme des innovations technologiques. De fait, il serait plus coûteux de mettre au point rétroactivement des mécanismes de protection de la vie privée.
6. Une participation accrue des Canadiens à la conception de l'autoroute de l'information est fonction de l'efficacité des consultations menées auprès des consommateurs. Les défenseurs de la vie privée doivent avoir voix au chapitre tout au long du processus de conception. En outre, le Comité consultatif devrait compter un plus grand nombre de représentants des consommateurs.
7. L'ACC reconnaît que les Canadiens doivent être mieux renseignés sur les questions touchant la vie privée. Elle ne croit pas qu'il revient aux entreprises de sensibiliser le public. Elle recommande que des cours visant à sensibiliser les consommateurs soient offerts dans les écoles, les collèges et les universités. En outre, les bibliothèques publiques et celles des établissements d'enseignement devraient mettre à la disposition du public des documents d'information dans ce domaine.

Pour terminer, l'ACC présente un extrait tiré du document intitulé *Privacy and Data Protection* qu'elle a produit en 1992. Ce document d'information présente un certain nombre de mécanismes de recours qu'il faut examiner sérieusement si on veut que les consommateurs aient la certitude que les renseignements personnels les concernant sont bien protégés. L'ACC mentionne notamment des dispositions visant à permettre aux consommateurs d'être mieux renseignés quant à l'utilisation des renseignements personnels les concernant, de savoir qui vend ces renseignements et d'exiger qu'ils ne soient pas communiqués; l'établissement de limites concernant l'utilisation de rapports de solvabilité par un employeur; un réexamen des plaintes après 30 jours; la délivrance d'une licence aux agences d'évaluation du crédit par toutes les provinces; la création d'un organisme chargé de la réglementation de la protection de la vie privée; et la mise en place à l'échelle nationale d'un service téléphonique sans frais, financé par le secteur privé, pour la protection des consommateurs.

## **Conseil canadien des consommateurs**

Le Conseil canadien des consommateurs est un organisme autonome à but non lucratif dont le mandat consiste à travailler en collaboration avec les entreprises, le gouvernement et les groupes d'intérêt pour agir sur le marché. Il a été mis sur pied pour renseigner les consommateurs, les entreprises et le gouvernement sur leurs droits et obligations.

Dans l'ensemble, le Conseil est d'avis qu'il faut adopter une loi cadre qui s'appliquerait aux secteurs privé et public et à laquelle pourraient s'ajouter des codes volontaires, des solutions technologiques et des initiatives de sensibilisation des consommateurs qui soient efficaces. Il attend avec impatience de connaître les résultats de l'analyse des commentaires recueillis.

Par ailleurs, il insiste tout particulièrement sur les droits des consommateurs en ce qui touche la vie privée sur l'autoroute de l'information. Sa réaction repose sur la prémisse fondamentale selon laquelle les particuliers ont non seulement un droit de propriété exclusif sur les renseignements personnels les concernant mais aussi le droit d'exercer un contrôle sur leur utilisation.

Parce que les consommateurs ne sont pas très au courant des renseignements les concernant que possèdent diverses institutions, de l'utilisation qu'elles en font, des fins pour lesquelles elles les partagent, de la durée pendant laquelle elles les conservent et du niveau de sécurité qu'elles offrent et aussi parce qu'ils souhaitent pouvoir avoir accès à ces renseignements pour vérifier leur exactitude, les questions liées à la protection de la vie privée suscitent de vives inquiétudes. Les consommateurs se préoccupent particulièrement du contrôle exercé sur les renseignements personnels et de leur utilisation. À cet égard, le Conseil est d'avis que si un particulier a consenti de façon explicite à l'utilisation de renseignements par une institution, sans pour autant conclure un accord contractuel avec cette dernière, il y aurait moins lieu de s'inquiéter.

Compte tenu de ces préoccupations, le gouvernement doit aussi prendre des mesures pour mettre de l'ordre dans ses propres affaires. Il ne faut partager aucun renseignement sans avoir obtenu un consentement à cet égard. De plus, parce qu'à la fois les gouvernements et le secteur privé vendent des renseignements, on doit nommer un commissaire indépendant chargé des données. De surcroît, le gouvernement doit adopter en 1995 une loi type pour protéger la vie privée qui s'appliquerait aux organisations du secteur privé assujetties à une réglementation fédérale.

### **Approches**

- I. Une loi cadre doit établir les normes sur la protection de la vie privée pour l'autoroute de l'information en mettant l'accent sur la prévention des abus, des normes rigoureuses en matière de

protection, un niveau élevé de sécurité et un processus pour donner un consentement en toute connaissance de cause. C'est maintenant qu'il faut agir. Le temps des longues consultations est révolu depuis longtemps.

- II. Il faut montrer que les codes volontaires peuvent permettre aux particuliers d'exercer un contrôle sur les renseignements personnels les concernant. Le Conseil met en doute la capacité des groupes industriels de régir les entreprises membres et d'influencer les autres. Si on arrive à prouver que les codes peuvent protéger les consommateurs, il y a lieu de légiférer pour les appuyer.
- III. La technologie peut offrir des mesures permettant de protéger en partie les renseignements personnels concernant un particulier. Ces mesures de sécurité doivent faire partie intégrante des services offerts et non être une option entraînant des coûts élevés; c'est donc dire que tous doivent y avoir accès. Le gouvernement fédéral doit encourager les progrès technologiques dans ce domaine, ce qui favoriserait l'éclosion au Canada de solutions et de possibilités dont pourrait bénéficier l'industrie nationale.
- IV. Les entreprises, le gouvernement et les groupes d'intérêts doivent s'attaquer en permanence à une lourde tâche, à savoir la sensibilisation des consommateurs. Ces derniers doivent être bien informés pour pouvoir contribuer à prévenir les abus.

#### **Réponses aux questions**

1. Les principes suivants doivent être retenus :
  - la protection de la vie privée est un droit fondamental;
  - chaque particulier est le seul propriétaire des renseignements personnels le concernant;
  - on doit recueillir uniquement les renseignements essentiels;
  - chaque particulier doit consentir de façon explicite à l'utilisation de renseignements le concernant avant qu'on puisse les utiliser;
  - ce consentement ne doit être lié à aucune autre obligation contractuelle;
  - les renseignements doivent servir uniquement aux usages pour lesquels ils ont été recueillis;
  - chaque particulier a le droit de consulter et de corriger les renseignements personnels le concernant;
  - la protection de la vie privée doit faire partie intégrante des nouvelles technologies de l'information avant même que leur application générale soit approuvée;

- aucun coût supplémentaire ne doit être imposé aux consommateurs pour protéger leur vie privée.
- 2. Il faut assurément adopter une loi s'appliquant au secteur privé et rendre plus sévère celle qui vise le secteur public. Le gouvernement doit agir dès maintenant, sans attendre qu'on en soit arrivé à une entente fédérale-provinciale (ce qui pourrait prendre dix ans) ou qu'un « dialogue visant à trouver des solutions » ait porté fruit. La loi doit venir à l'appui des codes volontaires efficaces. Elle doit dans la mesure du possible prévenir les abus. Toutefois, en cas d'abus, les autorités doivent intervenir rapidement pour y mettre fin.
- 3. Il est essentiel d'adopter des normes minimales à l'échelle nationale. Les particuliers sont déconcertés par le méli-mélo de règlements et de codes en vigueur à l'heure actuelle. Une norme nationale permettrait d'élever le marché à un niveau supérieur. Cependant, on ne doit pas abaisser les normes existantes pour qu'elles correspondent à une norme nationale.
- 4. En raison même de leur nature, il semble que les lignes directrices ne peuvent être tout à fait appropriées. Cependant, si les lignes directrices sont des règles et qu'on peut prouver que ces règles fonctionnent, elles peuvent constituer un élément de solution acceptable. C'est à chaque secteur qu'il incombe de prouver l'efficacité de ses lignes directrices.
- 5. Le niveau de protection de la vie privée doit être élevé et sûr. Des normes élevées n'entravent pas l'innovation; toutefois, même si le rythme des innovations s'en trouvait ralenti ou si les coûts étaient plus élevés, il n'y aurait aucune raison de renoncer à un niveau de protection supérieur. L'expérience suédoise en matière de normalisation est un exemple typique. Une fois qu'une norme a été établie, il est presque impossible de la modifier.
- 6. L'autoroute de l'information dépasse les frontières nationales. Il faut mettre en place une instance internationale qui s'occupera de la technologie électronique et de la vie privée et les Canadiens doivent en faire partie pour garantir qu'on tiendra compte de nos valeurs culturelles et nos préoccupations. Les technologies et les services doivent apaiser les inquiétudes des Canadiens concernant la protection de la vie privée et les personnes qui mettent au point les technologies doivent connaître les préoccupations de la population.
- 7. La sensibilisation des consommateurs revêt une importance déterminante et elle doit se faire sur une base permanente. Le gouvernement et les entreprises ont un rôle à jouer, en particulier

dans le contexte des pratiques commerciales quotidiennes. De plus, les défenseurs des consommateurs et les médias doivent s'efforcer de sensibiliser la population.

#### **Propositions et recommandations précises**

La loi doit renfermer des dispositions visant à récupérer tous les produits de la vente de renseignements personnels et rendre cet argent aux particuliers lésés.

Il faut recueillir l'opinion des consommateurs concernant la vie privée et trouver des solutions aux problèmes perçus. Le Conseil serait heureux qu'on lui offre l'occasion d'examiner ce projet et il pourrait faire appel à son réseau de consommateurs canadiens pour effectuer un sondage.

Le risque d'espionnage, de fraude et de harcèlement électroniques est très réel et on ne doit pas le sous-estimer.

***Fédération Nationale des Associations de Consommateurs du Québec (FNACQ)***  
***L'Association Coopérative d'Économie Familiale du Centre de Montréal (ACEF-Centre)***  
***(Présentation conjointe)***

La FNACQ et l'ACEF-Centre sont actives depuis plusieurs années dans le domaine de la vie privée et des renseignements personnels. En participant à l'élaboration de normes de la CSA et à d'autres projets portant sur la protection de la vie privée, elles ont montré leur savoir-faire et leur volonté d'aider à trouver des solutions concrètes aux questions que soulève la vie privée sur l'autoroute de l'information.

En résumé, ces deux organismes sont d'avis qu'il est essentiel de légiférer. Les codes volontaires, les solutions technologiques et la sensibilisation des consommateurs ne peuvent, en soi, garantir un niveau de protection de la vie privée adéquat, mais chacun de ces éléments a un rôle à jouer.

Toutes les études menées au cours des dernières années ont confirmé que les Canadiens se préoccupent beaucoup de la protection de la vie privée et des renseignements personnels. Or, l'essor de l'autoroute électronique vient amplifier ces préoccupations.

#### **Approches**

- I. La FNACQ et l'ACEF-Centre croient que l'adoption officielle par le Canada des lignes directrices de l'OCDE rend nécessaire l'élaboration d'une loi cadre visant à garantir le respect de ces lignes directrices. Il s'agira là d'une démarche très complexe, mais en

s'inspirant de la *Loi sur la protection des renseignements personnels dans le secteur privé* adoptée par le Québec, on pourra mettre en place une loi cadre qui s'appliquera dans l'ensemble du Canada. Il sera par la suite possible de l'adapter, au moyen de règlements et de codes, pour répondre aux besoins des divers secteurs de l'industrie. En outre, cette loi créera un niveau égal d'obligations pour toutes les entreprises et garantira un niveau minimal de protection des particuliers.

À leur avis, puisque le gouvernement fédéral a juridiction sur les secteurs clés (banques, communications et commerce interprovincial et international), il doit prendre les devants en mettant sur pied une initiative uniforme dans l'ensemble du pays pour régler les questions de la protection de la vie privée et des renseignements personnels. De plus, non seulement les provinces ont-elles l'obligation morale de participer à ce processus, mais aussi elles devraient être fortement intéressées par les avantages économiques reliés à une protection adéquate sur leur territoire et dans le contexte international.

- II. Les codes volontaires peuvent offrir certains avantages, mais ils ne suffisent pas à garantir un niveau de protection satisfaisant. D'après l'étude menée par le Centre pour la défense de l'intérêt public, intitulée *Voluntary Codes: a Viable Alternative to Government Legislation*, les codes volontaires présentent plusieurs lacunes : faible participation des consommateurs à leur élaboration; aucune participation des consommateurs à leur administration; participation insuffisante des entreprises et du secteur industriel à leur administration; faible recours à la publicité pour favoriser leur respect; acceptation et champ d'application trop restreints au sein du secteur industriel; surveillance inadéquate en ce qui touche leur respect; sanctions trop peu sévères; et absence de mécanismes de recours efficaces pour les consommateurs.

En règle générale, les codes volontaires sont plus appropriés quand le gouvernement participe à leur mise en application, mais ils n'en présentent pas moins certains problèmes, en particulier l'absence de sanctions efficaces. Alors, les codes volontaires sont généralement mal connus, même au sein du secteur visé; ils sont facultatifs; les consommateurs n'ont participé d'aucune façon à leur élaboration; il n'existe aucun organisme indépendant chargé de veiller à leur respect et de faire office d'arbitre en cas de différend. C'est pourquoi ces codes ne pourront jamais répondre adéquatement aux besoins des consommateurs.

En vertu de la *Loi sur la protection des consommateurs* du Québec, les entreprises peuvent soumettre à l'Office de protection des consommateurs l'équivalent d'un code de conduite et elles doivent s'y conformer si l'Office l'accepte. Cette loi permet aussi au

**gouvernement d'étendre l'application d'un code, élaboré par les membres de l'industrie, à l'ensemble du secteur d'activité économique visé et prévoit l'imposition d'amendes et d'autres sanctions pénales en cas de violation.**

- III. Au moins une partie de la protection doit être offerte par la technologie elle-même. Il faut examiner minutieusement les techniques de chiffrement et de codage; celles-ci doivent permettre un accès protégé et anonyme aux ressources offertes sur l'autoroute de l'information.**

**Il faut absolument que les représentants des groupes de consommateurs et de citoyens participent à l'élaboration, à l'essai et à la mise en oeuvre de nouveaux produits et services. La participation de ces groupes doit être soutenue financièrement pour qu'ils puissent faire appel au savoir-faire approprié et que leur contribution soit de qualité. Dans tous les secteurs de l'économie, il faut évaluer l'impact social des nouvelles technologies et c'est aux organismes de réglementation qu'il incombe de faire cette évaluation avant d'approuver de nouveaux services ou produits. Cette façon de procéder permet d'éviter non seulement des modifications qu'il serait coûteux et long d'apporter ultérieurement, mais aussi des affrontements avec les consommateurs.**

- IV. C'est à toutes les parties prenantes, à savoir le gouvernement, l'industrie et les consommateurs eux-mêmes, que revient la responsabilité de sensibiliser les utilisateurs. On doit élargir le mandat du Commissariat à la vie privée et augmenter les ressources qui lui sont affectées pour lui permettre de s'acquitter de cette responsabilité. Il s'agirait notamment de mettre sur pied un centre d'information, de mener des campagnes de sensibilisation du public sur une base périodique et de coordonner les activités de tous les ministères et organismes qui réglementent l'industrie afin d'assurer le respect des lois et règlements. Il faut produire des documents d'information s'adressant aux élèves de tous les niveaux. En mettant ces documents et ces instruments à la disposition des écoles secondaires, on fera en sorte que les générations futures prendront conscience de leurs droits en matière de vie privée et de renseignements personnels.**

**Il faut avoir recours aux groupes de consommateurs et aux groupes qui se portent à la défense des droits des citoyens pour qu'ils diffusent l'information auprès des consommateurs. On doit donc leur affecter des ressources pour qu'ils demeurent au fait de tous les problèmes et des solutions à y apporter, des innovations technologiques et des mécanismes de résolution des différends dans le domaine.**

L'industrie doit aussi informer les consommateurs des droits que leur accorde la loi et des obligations qu'elle leur impose, des pratiques et lignes directrices concernant le secteur industriel visé et des recours juridiques qu'ils peuvent exercer.

### **Réponses aux questions**

1. Il faut retenir les principes qui sont énoncés dans les lignes directrices adoptées par l'OCDE en 1981 et ceux qui sont issus de la mise en pratique de ces lignes directrices.
2. Le gouvernement doit adopter une loi plus sévère pour contrer le danger de violation de la vie privée de plus en plus grand et apaiser les craintes croissantes des citoyens. Il faut modifier les pratiques dépassées. Seule une approche réfléchie et ayant force exécutoire pourra permettre de résoudre les problèmes.
3. Il faut offrir une protection à l'échelle nationale pour régir les domaines qui ne sont pas de compétence provinciale. Une approche globale est préférable à une approche sectorielle, car les problèmes de fond sont sensiblement les mêmes dans les divers secteurs d'activité.
4. Les codes volontaires peuvent jouer un rôle pourvu qu'ils soient conformes aux normes législatives.
5. L'autoroute de l'information doit être conçue de manière à assurer un niveau élevé de protection de la vie privée. Les faits ont prouvé qu'il est très coûteux de modifier une structure existante. Les méthodes et les techniques utilisées pour assurer un niveau élevé de protection n'auront pas d'incidence négative considérable sur le rythme des innovations et les coûts qui y sont afférents.
6. Les Canadiens doivent participer à la mise en place des systèmes qui auront une incidence sur leur droits fondamentaux. Leur contribution peut prendre plusieurs formes : participation au processus législatif; témoignage devant des organismes administratifs, par exemple, le CRTC, et participation à des tribunes et à des discussions organisées par le gouvernement et l'industrie. Leur contribution pourra être utile dans la mesure où ils seront bien préparés.
7. Les groupes de consommateurs peuvent jouer un rôle important dans le processus qui consiste à informer les Canadiens de leurs droits et obligations concernant la vie privée et les renseignements personnels.

### **Propositions et recommandations précises**

Il faut élargir le mandat du Commissariat à la protection de la vie privée et accroître les ressources qui lui sont affectées pour lui permettre de contribuer à la sensibilisation et à la coordination des institutions publiques qui régissent l'industrie de manière à assurer le respect des lois et règlements visant à protéger la vie privée.

On doit soutenir financièrement les groupes de consommateurs et les groupes qui se portent à la défense des droits des citoyens pour qu'ils participent aux initiatives de sensibilisation et aux audiences publiques.

### ***La Ligue des droits et libertés***

La présentation de la Ligue porte sur deux grands aspects, à savoir ses intérêts généraux et les réponses qu'elle apporte à diverses questions posées dans l'introduction et à la partie 2 (« Les effets de l'autoroute de l'information sur la vie privée ») du Document de travail. En résumé, la Ligue est d'avis qu'il faut adopter une loi assurant un niveau minimal de protection de la vie privée. Les codes volontaires ne peuvent selon elle répondre aux besoins de toutes les parties et les technologies qui donnent lieu à la collecte d'un minimum de renseignements pour accomplir une tâche donnée sont à privilégier. La Ligue attend avec impatience de recevoir les résultats de l'analyse des commentaires recueillis. Par ailleurs, elle déplore que le Comité consultatif accorde relativement peu de poids à l'opinion des particuliers et des groupes de protection des consommateurs en comparaison de celle de l'industrie.

Quant aux intérêts généraux de la Ligue, elle insiste tout particulièrement sur le fait que la définition du concept de « vie privée » donnée dans le Document de travail est à son avis trop limitée, car les enjeux inhérents à la création de l'autoroute de l'information sont beaucoup plus vastes. Elle estime qu'il faut élargir cette définition de manière à englober les concepts suivants :

- la vie privée, en ce qui a trait au droit de vivre en paix sans interruption ni intrusion;
- la réputation, droit reconnu par la Charte québécoise;
- la dignité, droit aussi reconnu par la Charte québécoise;
- la démocratie, au sens de partage du pouvoir et du contrôle des renseignements qui touchent sa propre personne, contrôle qui se manifeste par le consentement éclairé à leur collecte, à leur utilisation et à leur destruction.

Également, il faut mettre fin aux concepts voulant que l'État est le seul protecteur et que l'industrie a mainmise et hégémonie sur une ressource qui ne lui appartient pas, en l'occurrence les renseignements personnels.

Selon la Ligue, les particuliers doivent jouer un plus grand rôle dans la protection des renseignements les concernant et dans la résolution des problèmes que pourrait entraîner leur diffusion. Elle mentionne notamment des domaines tels que le consentement à un acte médical et ou à l'utilisation de renseignements personnels dans l'intérêt public, par exemple, aux fins de la recherche médicale. En outre, il faut s'opposer à un système qui permet aux beaux parleurs ou aux personnes les mieux renseignées de l'emporter, tout simplement en arrivant à convaincre une personne. À cette fin, il n'est pas nécessaire que chaque particulier ait accès à tous les renseignements pertinents (et c'est d'ailleurs impossible). Ce qui est important, c'est que l'infrastructure, les services et les conditions ne favorisent ni les monopoles ni les oligopoles mais plutôt une démocratisation totale. Le défi consiste à assurer l'insertion sociale de tous dans une société complexe.

Toujours d'après la Ligue, pour que les connaissances issues de la science et de la technologie n'aient pas pour effet de mener à l'exclusion sociale d'un particulier ou d'un groupe, nous devons remettre en question la justification de l'exclusion, la fiabilité des renseignements qui conduisent à l'exclusion ainsi que les méthodes employées pour les utiliser. En ce qui touche les renseignements concernant un particulier, il faut pouvoir différencier les faits qu'on sait vrais et les explications plausibles. C'est pourquoi nous devons éviter de consacrer législativement certaines structures qui perpétuent l'inégalité entre l'industrie et les consommateurs ou une certaine conception du pouvoir. De manière générale, la place de la protection des renseignements personnels se trouve à mi-chemin entre la vie privée, la réputation et la dignité.

Quant au deuxième grand aspect, c'est-à-dire les réponses qu'elle apporte aux diverses questions posées dans le Document de travail, la Ligue a formulé les observations suivantes.

Concernant les rôles respectifs du gouvernement, des entreprises et des particuliers, elle estime que les particuliers doivent exercer un contrôle optimal sur les renseignements les concernant. Les lois qui établissent les principes généraux des normes de gestion de l'information sont trop générales. Le gouvernement doit assumer ses responsabilités et adopter des réglementations sectorielles qui soient le fruit des négociations entre l'industrie, le gouvernement et les particuliers.

Sur les questions touchant les données transactionnelles et les profils personnels, la Ligue est d'avis que, compte tenu du déséquilibre des forces en présence, l'équilibre entre les avantages et les dangers ne peut pas se faire de lui-même. Il faut adopter des lois qui assurent un niveau minimal de

protection de la privée. C'est le partage du pouvoir entre les parties en présence qui est l'enjeu. De plus, il faut garantir à tous les particuliers un accès total à tous les renseignements qui les concernent, puisqu'ils sont une partie d'eux-mêmes.

Au sujet des cartes d'identité et des numéros identificateurs uniques, la Ligue croit que l'érosion des libertés individuelles ne découle ni de l'obligation de donner des renseignements sur soi-même pour effectuer une transaction financière ni de l'attribution d'un identificateur unique. En revanche, il y a érosion des libertés lorsqu'un particulier n'exerce plus aucun contrôle sur les renseignements communiqués à une institution.

Par ailleurs, la Ligue a une opinion arrêtée au sujet de la surveillance et du contrôle. Il s'agit en l'occurrence de déterminer quels seront les « espaces communicationnels protégés ». Différents types de renseignements requièrent différentes exigences en matière de sécurité. L'automoteur de l'information doit pouvoir s'adapter à tous les types de renseignements et aux besoins en matière de sécurité qui en découlent, depuis les babillards électroniques non protégés jusqu'aux transactions financières. Cependant, même dans les domaines les moins protégés, il ne saurait être permis d'établir le profil d'une personne sans son consentement. En outre, toutes les formes de surveillance visant à mesurer la productivité des travailleurs doivent être bannies parce qu'elles contribuent à déresponsabiliser le particulier et à déshumaniser le travail. De plus, ces méthodes sont contre-productives. La meilleure mesure de la productivité, c'est le travail effectué. De plus, il faut adopter des règlements stricts interdisant la communication à des tiers de renseignements recueillis au cours du processus visant à protéger un ménage et garantissant qu'on recueille uniquement les renseignements pertinents.

En ce qui a trait à l'intrusion, la Ligue est d'avis que les formes d'intrusion mentionnées dans le Document de travail, par exemple, le télémarketing et le courrier publicitaire ciblé, sont assez inoffensives pour autant que l'intrusion découle directement d'une mesure prise par le particulier. Au Québec, la *Loi sur la protection des renseignements personnels dans le secteur privé* traite cette question de manière adéquate.

### **Approches**

- II. Il est indispensable que tous les codes et les normes soient d'application universelle et que nul ne puisse vendre des renseignements, tout comme il est actuellement illégal de vendre des organes humains, même avec le consentement de la personne visée. Les codes volontaires ne peuvent répondre de manière appropriée aux besoins de toutes les parties, car il y a opposition entre les intérêts des particuliers et ceux des entreprises.

- III. La Ligue est persuadée qu'il faut développer des technologies permettant au particulier de prendre pleinement en charge les renseignements, sa liberté de choix et son consentement éclairé. Ces technologies doivent être assez souples pour assurer la pleine liberté de choix et assez fiables lorsqu'il s'agira de gérer les normes sociales. Il faut favoriser les systèmes qui permettent de recueillir le moins de renseignements personnels possible pour accomplir une tâche donnée. Il faut aussi mettre en place des mécanismes de surveillance pour garantir que toutes les procédures de gestion des renseignements correspondent au niveau de protection requis. De plus, l'audience publique constitue une structure lourde et coûteuse, mais elle procure certains avantages que n'offrent pas d'autres méthodes, par exemple, les enquêtes téléphoniques. Tous les intervenants doivent assumer la responsabilité de protéger la vie privée et les renseignements personnels pour favoriser le développement de technologies ne portant pas atteinte aux libertés civiles. À la lumière de l'expérience acquise, certains aspects de la protection de la vie privée devraient faire l'objet de dispositions législatives, tandis que d'autres pourraient donner lieu au prélèvement de frais auprès des utilisateurs.

### ***Le centre pour la défense de l'intérêt public***

En résumé, le Centre pour la défense de l'intérêt public soutient qu'il faut adopter des lois et des règlements, auxquels s'ajouteraient des codes volontaires, des solutions technologiques et la sensibilisation des consommateurs.

Le Centre craint qu'on n'accorde pas assez d'attention aux préoccupations des Canadiens à faible revenu concernant la vie privée, par exemple, à la perspective de devoir payer pour avoir accès aux renseignements personnels les concernant et pour maintenir le niveau de vie privée existant. Il a aussi signalé que la préoccupation croissante du public à l'égard de la vie privée, révélée par des enquêtes récentes, est justifiée.

#### **Réponses aux questions**

1. Voici une liste des principes de protection de la vie privée à retenir selon le Centre :
  - une définition de l'expression « renseignements personnels » qui englobe tous les renseignements concernant un particulier;
  - les renseignements personnels appartiennent au particulier, au même titre que ses biens privés;

- les particuliers ont le droit d'être informés lorsque des renseignements personnels les concernant sont recueillis, utilisés, partagés, échangés ou diffusés de quelque façon que ce soit;
- les particuliers ont le droit d'avoir accès aux renseignements personnels les concernant et de faire corriger tout renseignement erroné;
- les particuliers ont le droit d'exercer un contrôle sur la collecte, l'utilisation et la diffusion des renseignements personnels les concernant;
- les citoyens ne doivent pas avoir à payer pour maintenir un niveau de protection de la vie privée existant;
- les Canadiens à faible revenu sont particulièrement vulnérables aux incursions dans la vie privée et on doit reconnaître leurs besoins spéciaux.

Par ailleurs, les principes énoncés dans le code type de la CSA constituent aussi une assise sur laquelle peut prendre appui un ensemble de principes directeurs.

2. Les gouvernements fédéral et provinciaux doivent adopter des lois sur la protection de la vie privée s'appliquant à la fois aux secteurs public et privé. Il faut des lois et des règlements, même si l'autoréglementation de l'industrie semble efficace. Le gouvernement fédéral doit d'abord élaborer des lois nationales ou sectorielles pour les domaines qui relèvent de sa compétence. Il doit le faire de concert avec ses homologues provinciaux, y compris tous les commissaires à la protection de la vie privée, de manière à créer un ensemble commun de règles pour tous les secteurs. On pourrait à cet égard s'inspirer de la loi adoptée récemment au Québec.

En outre, le gouvernement fédéral doit modifier la *Loi sur la protection des renseignements personnels* de manière à exiger à l'égard de toutes les nouvelles initiatives gouvernementales une « évaluation de l'impact sur la vie privée » non astreignante. Cette évaluation préalable peut se révéler rentable du fait qu'elle évite de prendre ultérieurement des mesures correctives entraînant des coûts élevés. Il faut aussi envisager d'adopter des lois qui rendraient cette évaluation obligatoire dans le secteur privé.

Les lois doivent être à la fois orientées et complétées par des codes volontaires, mais ces derniers ne peuvent remplacer une réglementation gouvernementale. Dans une étude qu'il a publiée concernant l'efficacité des codes volontaires de l'industrie, le Centre

**fait état de certaines lacunes au chapitre de leur application, de la sensibilisation des consommateurs, des sanctions et des procédures systématiques visant à évaluer et surveiller leur respect.**

**Le gouvernement doit promouvoir énergiquement les nouvelles techniques de cryptographie, par exemple, le chiffrement à « clé révélée ».**

**Le gouvernement a un rôle important à jouer pour faire connaître les lois existantes et les risques qui menacent la vie privée.**

- 3. Il faut adopter des lois nationales et provinciales, de préférence harmonisées. Cependant, des niveaux différents de protection de la vie privée sont préférables à l'absence de protection. Également, une loi générale est préférable à des lois sectorielles. Néanmoins, des lois sectorielles sont préférables à l'absence de loi.**
- 4. Les codes volontaires sont utiles du fait qu'ils sensibilisent l'industrie; qu'ils peuvent permettre de sensibiliser le public; qu'ils aident l'industrie à « prendre de la vitesse » avant l'entrée en vigueur d'une loi; et qu'ils peuvent aider les instances législatives en leur donnant un modèle et une orientation quant aux principes appropriés, aux questions touchant la protection de la vie privée dans un secteur précis et aux mécanismes de mise en oeuvre possibles. Bien que leur efficacité réelle soit moins évidente, il faut les encourager.**
- 5. L'autoroute de l'information doit être conçue de manière à offrir un niveau élevé de protection de la vie privée, même si elle entraîne une augmentation des coûts et ralentit l'innovation. Toutefois, on ne prévoit aucun coût supplémentaire, puisque le fait d'intégrer au départ les mesures de protection de la vie privée permet de réduire les coûts à long terme.**

### **Charles D. Raab**

**M. Charles D. Raab, maître assistant au département des sciences politiques de l'université d'Édimbourg, en Écosse, mène des recherches dans le domaine de la vie privée et de la protection des renseignements.**

**Tout en reconnaissant qu'on doit satisfaire aux obligations constitutionnelles et légales, M. Raab estime qu'il faut adopter une réglementation cadre plus vaste et systématique s'appliquant au secteur privé. Même si les codes volontaires présentent de nombreux avantages, ils ne peuvent à son avis répondre à tous les besoins. Il considère que les solutions technologiques et la sensibilisation du public doivent jouer un rôle partiel mais important. Bref, les diverses approches présentées dans le Document de travail sont d'après lui complémentaires et interreliées.**

## **Approches**

- I. L'adoption d'une loi est un moyen efficace d'accentuer les droits dévolus aux particuliers et les responsabilités confiées aux organisations. Cependant, il faut se doter d'organismes de réglementation énergiques pour que la loi soit appliquée. Il y a lieu de noter que le plus récent projet de directive de l'Union européenne ne reprend pas la distinction peu appropriée entre les secteurs public et privé, puisque les renseignements personnels circulent d'un secteur à l'autre d'une manière qui rend cette distinction de moins en moins pertinente. À cet égard, le fait que la loi du Québec s'applique au secteur privé est de bon augure.
- II. Le recours aux codes volontaires présente de nombreux avantages, comme en témoigne, par exemple, l'expérience au Royaume-Uni et aux Pays-Bas. La détermination des industries et des secteurs pertinents peut poser un problème. Par ailleurs, les nouvelles possibilités multimédia offertes sur l'autoroute de l'information risquent d'estomper la démarcation entre les industries et les secteurs, ce qui remet en question l'applicabilité des codes sectoriels. Cependant, l'approche de la CSA peut être considérée comme une innovation capitale, en particulier parce qu'elle fournit un étalon qui permettrait à la Communauté européenne d'évaluer dans quelle mesure ces codes sont respectés.
- III. Les solutions technologiques présentent aussi un intérêt. Cependant, elles ne permettent de répondre qu'à une partie des exigences en matière de vie privée. En outre, il est important que les mesures de sécurité de nature technologique fassent partie intégrante de l'autoroute de l'information plutôt que de constituer des éléments complémentaires. De plus, il serait utile de mener des évaluations de l'impact sur la vie privée et d'examiner ces évaluations sur une tribune publique.
- IV. La sensibilisation suppose qu'on constate que la protection de la vie privée peut idéalement être le fruit d'une collaboration entre divers participants dont les intérêts diffèrent. Ainsi, la sensibilisation peut entraîner une synergie d'intérêts qui semblent opposés.

### ***Riley Information Services Inc.***

Riley Information Services est une société internationale spécialisée dans l'élaboration de lignes de conduite administratives en matière d'information. Son président, M. Thomas B. Riley, est bien connu dans le domaine de la vie privée et de l'accès à l'information pour les ouvrages qu'il a publiés et les conférences qu'il a organisées sur le sujet.

En réponse au Document de travail, la société Riley Information Services a transmis un exemplaire du document intitulé *Information Technology and Privacy Protection: Practical Suggestions for the Information Age*, qu'elle avait présenté à la Electronic Democracy Conference, en novembre 1994.

Ce document examine les divers types de problèmes que pose la technologie de l'information concernant la protection de la vie privée et décrit en détail l'évolution des principes, des règlements et des lois en la matière au Canada et à l'étranger. Il souligne aussi les lacunes que présentent les innovations mises au point au Canada du fait qu'elles ne satisfont pas aux exigences de l'ère de l'information. Les auteurs ont tenté de soulever certaines questions de fond quant à la nature des principes de protection de la vie privée, aux formes de protection appropriées dans le secteur privé et aux moyens d'améliorer les mesures en vigueur à l'heure actuelle dans le secteur public. Ils considèrent par le fait même la *Loi sur la protection des renseignements personnels* comme étant la référence nationale prédominante en matière de protection de la vie privée et suggèrent qu'on envisage d'y apporter un certain nombre de modifications. Au palier fédéral, ils y examinent, pour le secteur privé, la place qui revient aux industries assujetties à une réglementation fédérale et, pour le secteur public, de quelle manière la protection de la vie privée et la sécurité peuvent être intégrées au moment de l'élaboration des systèmes d'information. Enfin, les auteurs traitent les questions liées à l'utilisation du numéro d'assurance sociale, l'appariement des données, les échanges de renseignements personnels entre les gouvernements fédéral et provinciaux et la commercialisation des renseignements personnels détenus par le secteur public.

C'est des juristes américains Samuel Warren et Louis Brandeis, jusqu'à David Flaherty en passant par Alan Westin, que s'inspire la définition du terme « vie privée ». L'approche de Westin est considérée comme étant à la base des lois fédérale et provinciales actuelles concernant la protection de la vie privée.

De nombreux documents montrent que la protection de la vie privée suscite des préoccupations bien réelles et qu'elle est de plus en plus menacée. La technologie offre maintenant des moyens plus perfectionnés encore de manipuler des données, qu'il s'agisse de « l'enregistrement en double » ou des nouvelles formes de surveillance électronique des employés. Les renseignements personnels sont maintenant commercialisés à de nombreuses fins, notamment pour la promotion commerciale. Les gouvernements partagent de plus en plus les renseignements personnels, au nom de l'efficace et de l'efficacité. Cet état de choses ne manque pas d'amplifier les préoccupations du grand public concernant la protection de la vie privée. Les controverses dont ont récemment fait l'objet, par exemple, le projet Lotus sur CD-ROM aux États-Unis, le réseau d'accès aux renseignements relatifs à l'application des lois en Australie, les propositions en matière d'identification pour les besoins des soins de santé en Ontario et

les propositions du réseau PharmaNet en Colombie-Britannique, témoignent toutes d'une intensification de la menace perçue. Néanmoins, on reconnaît que les clients veulent recevoir des services nouveaux et innovateurs et qu'ils sont favorables à l'utilisation de la technologie pour lutter contre le crime et la fraude. Cet état de choses donne lieu à une étrange ambivalence du fait que les Canadiens réclament davantage la protection de leur propre vie privée que celle de leurs concitoyens. En outre, l'autoroute de l'information apportera des avantages incroyables dans toutes les parties du pays, en particulier dans le domaine de l'accès aux bases aux données, de l'éducation et de la médecine.

En ce qui touche les préoccupations concernant la vie privée, Riley Information Services fait état d'un certain nombre de questions précises. L'utilisation généralisée du numéro d'assurance sociale est considérée comme un problème persistant, du fait qu'elle symbolise la possibilité d'une surveillance exercée par l'État omniprésent. L'appariement des données, dans la mesure où il permet de réprimer les fraudes et de détecter les crimes, par opposition aux possibilités d'incursion dans la vie privée, donne lieu au Canada et à l'étranger à une dichotomie non résolue. L'échange de renseignements personnels entre les gouvernements fédéral et provinciaux pour éliminer le chevauchement des programmes et des services continue de susciter des préoccupations, malgré les avantages qu'il peut offrir. La commercialisation des renseignements personnels, en particulier par le gouvernement dans le but de gagner des revenus supplémentaires, continue de poser un problème. Les auteurs proposent de régler toutes ces questions en modifiant en premier lieu la *Loi sur la protection des renseignements personnels*, et peut-être aussi en adoptant par la suite d'autres lois après avoir consulté les provinces.

Les auteurs examinent aussi en détail l'expérience au Canada et à l'étranger en ce qui touche l'élaboration de la vaste gamme de mesures de protection de la vie privée. Pour le Canada, on mentionne notamment l'évolution de la *Loi sur la protection des renseignements personnels* et des problèmes qu'elle suscite; l'adoption des *Principes de protection de la vie privée dans les télécommunications*, les modifications subséquentes apportées à la *Loi sur les télécommunications* ainsi que les décisions résultantes rendues par le CRTC en matière de protection de la vie privée; la tentative infructueuse d'appliquer la *Loi sur la protection des renseignements personnels* aux organes administratifs du Sénat, de la Chambre des communes, des tribunaux et de toutes les sociétés d'État fédérales; et diverses initiatives provinciales, en particulier la loi adoptée récemment au Québec qui régit la protection des renseignements personnels dans le secteur privé. En ce qui touche l'expérience internationale, le document va des lignes directrices adoptées par l'OCDE au début des années 1980 aux directives sur la protection de la vie privée proposées par la Communauté européenne. Les auteurs se penchent aussi sur certaines initiatives actuellement mises en oeuvre aux États-Unis, par

exemple, la tentative du groupe de travail de la National Information Infrastructure (NII) d'élaborer des principes de protection de la vie privée généraux s'appliquant à un réseau informatique national.

D'après Riley Information Services, ce sont les principes de protection de la vie privée inhérents aux lignes directrices de l'OCDE qui ont eu la plus grande influence sur l'élaboration des initiatives menées au Canada dans le domaine de la vie privée. Cependant, il faut modifier ces principes à la lumière des progrès technologiques récents et des usages plus complexes auxquels servent les renseignements personnels. Les principes proposés par le groupe de travail NII, aux États-Unis, ne semblent pas assez fermes. Les auteurs du document accordent beaucoup de mérite aux critères généraux du Commissariat à la protection de la vie privée du Canada pour l'élaboration de systèmes d'information gouvernementaux renfermant des renseignements personnels, qui supposent les concepts de transparence, de consentement donné en toute connaissance de cause et de sécurité. Également, le *Code type sur la protection des renseignements personnels* proposé pour le secteur privé par la CSA revêt une grande importance à leurs yeux. Ils reconnaissent toutefois qu'on peut y ajouter un principe supplémentaire. Il s'agit de ramener la participation du public à l'étape de la planification ou du lancement des systèmes d'information renfermant des renseignements personnels.

La nécessité d'adopter des lois et des règlements supplémentaires porte principalement sur les modifications proposées à l'égard de la *Loi sur la protection des renseignements personnels* fédérale, qui est considérée comme étant la référence en matière de protection de la vie privée à l'échelle nationale au Canada. Les auteurs mentionnent notamment les modifications suivantes : l'intégration d'un ensemble fondamental de principes de protection de la vie privée; l'inclusion des sociétés d'État et des industries du secteur privé assujetties à une réglementation fédérale, à l'égard desquelles les examens, les approbations et les mécanismes de plainte relèveraient du Commissariat à la protection de la vie privée; une nouvelle définition du terme « renseignements personnels » englobant la surveillance électronique ou autre ainsi que l'information génétique; des dispositions prévoyant un examen annuel du Rapport du Commissariat à la protection de la vie privée par un comité parlementaire, similaire à l'examen du rapport du Vérificateur général par le Comité des comptes publics; un disposition générale concernant les mesures de protection et une exigence plus rigoureuse en matière de sécurité et d'évaluation de l'impact sur la vie privée. Le document fait état de trois options en ce qui touche le contrôle de la protection de la vie privée dans le secteur privé : une loi similaire à celle du Québec, considérée comme étant un « instrument trop contondant »; le maintien des codes volontaires, auxquels s'ajouterait le code type de la CSA; le recours aux enjeux sectoriels pour intervenir en matière de protection de la vie privée au cas par cas. Cependant, Riley Information Services préconise un compromis, selon lequel la *Loi sur la*

*protection de la vie privée* obligerait les entreprises du secteur privé à élaborer des codes de protection de la vie privée s'appuyant sur les normes proposées par la CSA.

Exception faite peut-être du secteur bancaire ainsi que des industries du marketing direct et de la câblodistribution, la présentation semble indiquer que les codes volontaires n'ont pas connu beaucoup de succès jusqu'à présent. Cependant, ils offrent l'avantage de pouvoir s'adapter aux besoins changeants et aux différences entre les secteurs. De plus, les activités d'Industrie Canada laissent entrevoir une approche sectorielle, comme les audiences du Sénat concernant la *Loi sur les banques*. Également, les pressions des consommateurs et les décisions du CRTC en ce qui a trait à la protection de la vie privée pourraient toutes ouvrir la voie à une plus vaste adoption de codes volontaires et à une amélioration de leur efficacité. Il est toutefois à déplorer que ces codes puissent se traduire par une « balkanisation » et laisser des lacunes considérables dans la protection de la vie privée. Néanmoins, les auteurs accordent beaucoup de mérite à l'adoption du *Code type sur la protection des renseignements personnels* de la CSA à titre de norme nationale.

Aux yeux de Riley Information Services, la technologie est considérée comme étant fondamentalement neutre. Néanmoins, à la fois pour ce qui touche les initiatives visant à réinventer le gouvernement et dans le secteur privé en général, des éléments qui risquent de menacer la protection de la vie privée sont évidents. Ils y associent cependant de nombreuses solutions technologiques qui favorisent la protection de la vie privée, par exemple, les cartes à puce et le chiffrement. Quoi qu'il en soit, il ressort de la présentation que c'est le recours à une clé de déchiffrement qui permet de répondre aux préoccupations concernant la vie privée et d'intégrer des mesures de protection au stade de l'élaboration des systèmes d'information. Les auteurs expliquent en détail la méthode employée à cette fin, notamment un processus étape par étape, la participation du Commissariat à la protection de la vie privée et la tenue d'évaluations de la sécurité et de l'impact sur la vie privée.

### **Leslie Regan Shade**

M<sup>me</sup> Leslie Regan Shade fait partie du programme de troisième cycle en communications à l'université McGill.

Sa présentation reprend une partie de l'article portant sur les réseaux informatiques au Canada publié dans le numéro d'hiver 1994 du *Canadian Journal of Communications*. Cet article traite de l'aspect juridique des réseaux ainsi que des plans d'action en matière de protection de la vie privée pour les réseaux aux États-Unis. De plus, il donne quelques suggestions relativement à une loi canadienne concernant la protection de la vie privée dans l'optique des réseaux. Dans ce domaine, l'article propose

que les organismes de réglementation canadiens s'inspirent de la *Electronic Communications Privacy Act (ECPA)* adoptée par les États-Unis en 1986 et du projet de directive de la Communauté européenne sur la protection de la vie privée dans les télécommunications. De plus, à la lumière des initiatives proposées à l'égard du réseau CANARIE, il semblerait avantageux d'étendre aux communications de réseau les Principes de protection de la vie privée dans les télécommunications en adaptant certains aspects de l'ECPA, de la directive de la Communauté européenne sur les télécommunications ou des principes de protection de la vie privée des Computer Professionals for Social Responsibility.

## **GROUPES DE SERVICES FINANCIERS, DE CRÉDIT ET DE MARKETING**

---

### **Canada Trust**

« Canada Trust » est la dénomination sociale utilisée couramment pour désigner les sociétés canadiennes Services financiers CT inc. et Hypothèques Trustco Canada ainsi que sa filiale Société Canada Trust. Canada Trust offre dans les dix provinces des services dans le domaine de l'épargne et des prêts, des fiducies personnelles et des régimes de retraite en fiducie, du courtage immobilier résidentiel et des services financiers au détail.

Canada Trust a toujours accordé une priorité absolue à la protection et à la confidentialité des renseignements personnels concernant ses clients. Elle privilégie l'autoréglementation et les codes volontaires par opposition aux solutions législatives. Elle pourra fournir au besoin des observations plus précises concernant l'industrie des services financiers.

Elle n'est pas en faveur de l'adoption d'une loi concernant la protection de la vie privée. Toutefois, si on estime nécessaire d'adopter une loi, il est important qu'elle permette d'atteindre un juste milieu entre la protection de la vie privée et la libre circulation de l'information indispensable dans une économie de marché. Une loi qui, comme celle du Québec, ne permet pas d'en arriver à un juste milieu n'est pas souhaitable. En vertu de la *Loi sur les banques*, de la *Loi sur les sociétés d'assurances* et de la *Loi sur les compagnies fiduciaires et les compagnies de prêt* adoptées récemment, le gouvernement est autorisé à réglementer l'utilisation des renseignements sur les clients. Comme le gouvernement n'a pas reçu beaucoup de plaintes des acheteurs de produits financiers à l'égard d'abus concernant des renseignements confidentiels, il n'a pas été nécessaire de réglementer en la matière.

En Europe et à l'échelon fédéral au Canada, on est en général favorable à une autoréglementation et à une surveillance de l'industrie qui fassent intervenir l'adoption par les divers secteurs de codes volontaires sur la protection de la vie privée. Les banques ont établi des normes de protection de la vie privée et Canada Trust est en voie de faire de même. Par ailleurs, une approche sectorielle permettrait d'atteindre un équilibre entre, d'une part, les besoins en matière d'information et les besoins liés à l'exploitation de diverses entreprises et, d'autre part, l'efficacité de la protection des consommateurs.

### **Association des banquiers canadiens**

L'Association des banquiers canadiens représente 62 banques à charte du Canada.

En général, l'Association n'est pas en faveur de l'adoption d'une loi. À son avis, l'autoréglementation et les codes volontaires sur la protection de la vie privée constituent une structure reconnue et appropriée, en particulier dans le milieu bancaire électronique en mutation constante. Elle estime que la sensibilisation des consommateurs et les solutions technologiques constituent des éléments importants de l'équation de la vie privée. L'Association aborde aussi les diverses applications bancaires utilisées à l'heure actuelle sur l'autoroute de l'information et elle s'étend sur le sujet dans le document d'accompagnement intitulé *Canadian Banks and the Information Highway*, qui a été présenté à Industrie Canada en 1994.

La protection de la vie privée des consommateurs, la confidentialité et la sécurité sont de première importance pour les activités d'une banque. À cet égard, les banques et leurs clients reconnaissent la nécessité d'utiliser des renseignements concernant les clients pour leur fournir des produits et des services. L'évolution dans le secteur bancaire est dictée par la clientèle. Le succès de l'autoroute de l'information repose donc sur la satisfaction des divers besoins des consommateurs et de leurs attentes en matière de services ainsi que sur les préoccupations de leurs clients en ce qui touche la vie privée. C'est pourquoi l'Association estime qu'il faut évaluer plus en profondeur les questions en jeu avant de prendre des mesures de protection de la vie privée qui auraient des répercussions sur l'évolution de l'autoroute.

D'après l'Association, le fait de légiférer dans le domaine de la vie privée pourrait entraver l'innovation sur le marché, qui constitue l'élément moteur de l'évolution de l'autoroute. En outre, la réglementation par le gouvernement de la vie privée et de l'utilisation de renseignements risquerait d'entraver l'adoption et la promotion de codes d'autoréglementation. De surcroît, une loi est beaucoup moins souple qu'une autoréglementation et elle ne devrait pas viser à exercer une « micro-gestion » des normes commerciales.

Les organisations doivent jouer un rôle de premier plan dans l'autoréglementation et dans la prise en charge de la protection de la vie privée et la sécurité. Pour sa part, le gouvernement doit favoriser l'autoréglementation et amener les consommateurs à prendre des décisions de manière responsable. Les banques sont des chefs de file en matière d'autoréglementation, puisqu'elles ont adopté le *Modèle de code de confidentialité pour les particuliers* de l'Association. En outre de nombreuses banques souscrivent au code sur la protection de la vie privée de l'Association canadienne du marketing direct et au *Code de pratique canadien des services de cartes de débit*. Les banques ont aussi mis en place un service téléphonique sans frais permettant aux clients de formuler des plaintes et de faire valoir leurs préoccupations. De plus, l'autoréglementation permet de surmonter les difficultés liées au partage des domaines de compétence dans les cas où les intérêts du gouvernement fédéral et ceux des provinces risquent d'entraver l'adoption d'un ensemble

de règles; de plus, les codes volontaires peuvent aider les entreprises à établir des normes de service minimales. Par ailleurs, c'est l'autoréglementation qui offre la plus grande flexibilité lorsqu'il s'agit d'adapter les pratiques en fonction de l'évolution des besoins et des attentes de la clientèle et il semble sage de la favoriser à un moment où le gouvernement fédéral rationalise le processus de réglementation. Essentiellement, les codes propres à chaque banque constituent des documents « vivants » qui font systématiquement l'objet d'examen et de modifications de manière à refléter les changements observés sur le marché et dans les attitudes de la clientèle concernant la protection de la vie privée dans les activités bancaires, par exemple, les nouvelles dispositions permettant d'exiger la non-communication de renseignements personnels. L'Association des banquiers canadiens a aussi participé à l'élaboration du *Code type sur la protection des renseignements personnels* de la CSA, mais c'est à son avis le comité de la CSA qui devrait examiner les questions touchant le rôle de cette dernière en matière de certification.

L'Association donne de nombreux exemples qui illustrent de quelle façon elle-même et l'industrie bancaire participent à la mise au point de technologies innovatrices. Ainsi, elles ne perdent jamais de vue la vie privée, la confidentialité et la sécurité quand il s'agit de développer de nouveaux produits et de nouveaux services bancaires. Non seulement ont-elles recours à la technologie pour protéger les renseignements et les systèmes, mais aussi elles y font de plus en plus appel pour permettre aux clients d'exercer leur droit de mieux protéger leur vie privée. L'Association remet en question le principe selon lequel les organismes de réglementation doivent tenir des audiences publiques avant qu'une nouvelle technologie soit lancée sur le marché. De plus, elle se préoccupe du fait que l'innovation sur le marché doive être sanctionnée par le gouvernement.

Dans un contexte d'autoréglementation, il incombe aux organisations de fournir assez de renseignements pour aider les clients à comprendre la nature des produits et des services en général et leur permettre de faire un choix éclairé, au moment où ils décident d'utiliser ou non un service donné. À cet égard, l'industrie bancaire étend aussi aux systèmes technologiques ses initiatives de sensibilisation des consommateurs, qui faisaient traditionnellement appel aux documents imprimés. Par ailleurs, les clients doivent comparer les produits et les services offerts, comprendre leurs propres obligations et prendre des précautions raisonnables pour protéger leur vie privée. Quant au gouvernement, son rôle consiste à favoriser la sensibilisation des consommateurs.

### ***Association canadienne du marketing direct (ACMD)***

L'Association canadienne du marketing direct représente 575 entreprises réparties dans plusieurs industries qui pratiquent le marketing direct de produits et services partout au Canada. Cette organisation fondée en 1967

regroupe des institutions financières, des éditeurs, des entreprises de vente par catalogue, des organismes de bienfaisance, des services de téléachat, des agences de publicité, des agences de marketing direct, des sociétés d'informatique, de gestion des données et de télécommunications, des centres de traitement à façon, des imprimeurs et des services de livraison de lettres et de colis.

La présentation fait une large place au rôle croissant du marketing direct sur l'autoroute de l'information. L'Association est très favorable à l'autoréglementation par l'industrie et souhaite fortement que cette dernière adopte des codes volontaires. De plus, elle préconise l'application de solutions technologiques pour appuyer ces mécanismes.

L'Association fait valoir quelques points touchant des facteurs généraux qu'elle considère importants dans l'évolution de l'autoroute de l'information. En outre, elle donne de nombreux détails sur des sujets tels que les éléments qui influent sur la croissance du marketing direct; l'impact de l'autoroute de l'information sur le marketing direct; les consommateurs et la technologie; les entreprises de marketing direct et l'autoroute de l'information; la volonté éventuelle des Canadiens de faire des achats sur l'autoroute de l'information à partir de leur domicile; la prise de décisions éclairées par les consommateurs; la personnalisation des services.

Les renseignements détaillés présentés par l'Association indiquent que le marketing direct constitue une très vaste industrie (200 000 employés et des ventes de 9 milliards de dollars en 1993) en plein essor. À mesure qu'évoluera l'autoroute de l'information, on assistera à l'apparition d'un grand nombre de nouveaux services et à l'ouverture de nouveaux marchés, dont le plus important pourrait être celui des achats à domicile au moyen d'une technologie interactive. Dans une enquête récente menée aux États-Unis, 89 p. 100 des répondants se sont déclarés très favorables aux achats à domicile. De plus, à mesure que la technologie sera mise en place, le marketing direct deviendra moins intrusif et plus informatif tout en protégeant mieux la vie privée. En dernière analyse, l'avenir de l'industrie repose sur sa capacité de gagner et de conserver la confiance des clients en ce qui touche la sécurité des données transactionnelles.

D'après l'Association, les renseignements qu'utilise l'industrie du marketing direct, principalement des registres d'achat, ne sont pas au cœur de la question de la vie privée. Le débat dans ce domaine est en règle générale centré sur la collecte et l'utilisation de renseignements personnels, par exemple, des dossiers médicaux et financiers, en fonction desquels les grandes organisations des secteurs public et privé prennent des décisions qui influent sur la vie des particuliers.

En fait de mesures de protection de la vie privée, l'Association est très favorable aux codes volontaires et cite certains points de son propre code à titre d'exemple. Le *Code de protection de la vie privée* adopté en 1992 par

**L'Association, dont les membres enregistrent 82 p. 100 des activités de marketing direct pratiquées au Canada, a contribué à convaincre les consommateurs qu'ils ont le droit d'exercer un contrôle sur l'utilisation et la communication de renseignements figurant, par exemple, dans les registres d'achat. Ce code renferme des dispositions qui permettent aux consommateurs de limiter ou d'interdire l'accès de certaines agences de marketing direct aux renseignements commerciaux; il leur confère aussi le droit non seulement de savoir quels renseignements possède l'agence de marketing direct et d'où ils proviennent mais aussi de les corriger. D'après l'Association, si on leur donne le choix, les consommateurs soucieux de la protection de leur vie privée préféreront traiter avec des organisations qui respectent leur droit de limiter l'utilisation des renseignements personnels les concernant. En dernière analyse, les renseignements les plus utiles sont ceux qu'on fournit volontairement, puisqu'ils sont plus exacts et que leur degré de détail supérieur se prête mieux au marketing sélectif. En outre, l'Association a participé à l'élaboration du *Code modèle sur la protection des renseignements personnels* de la CSA et elle croit que toute campagne de marketing direct menée de façon responsable peut satisfaire aux critères établis dans ce code.**

**D'après l'Association, on aura recours à un système de chiffrement pour protéger les données contre les pirates informatiques et pour préserver les transactions financières et diverses formes de paiement électronique. Par ailleurs, la sécurité des données transactionnelles est non seulement dans l'intérêt des consommateurs mais aussi dans celui de l'industrie dans son ensemble.**

### ***Association Interac***

**L'Association Interac a été créée pour faciliter l'échange de transactions électroniques entre les institutions canadiennes qui reçoivent des dépôts. Cette association exploite par l'entremise de guichets automatiques d'un bout à l'autre du pays un service de retrait en mode partagé ainsi que le service Paiement direct Interac.**

**Des sondages menés auprès de clients révèlent que la protection de la vie privée et la sécurité revêtent une grande importance à leurs yeux et qu'elles ont de ce fait une incidence déterminante sur le succès de tout réseau électronique. À cet égard, les deux services offerts par Interac protègent la vie privée, notamment parce qu'ils font appel à un numéro d'identification personnel (NIP). Dans le cadre des services offerts par le réseau Interac, les transactions des clients sont protégées du début à la fin. Il est donc évident que des systèmes très efficaces figurent parmi les solutions qui peuvent et doivent être intégrées à l'étape du développement des technologies. Par ailleurs, Interac est favorable à l'approche de la CSA, car**

le *Code modèle sur la protection des renseignements personnels* proposé permettra aux divers secteurs d'élaborer des codes précis adaptés à leur situation particulière.

### ***Equifax Canada Inc.***

Equifax Canada est une société de services d'information qui recueille, conserve et regroupe des renseignements concernant des particuliers et des entreprises et qui les communique à ses clients pour faciliter les transactions financières. Elle exploite dans l'ensemble du Canada un réseau informatisé de services d'information de crédit et un service de recouvrement de créances. De plus, elle gère des bases de données distinctes sur les demandes d'indemnité présentées en vertu d'une assurance-automobile, d'une assurance-habitation ou par suite d'une assurance visant un autre type d'une de sinistre. Toutes ses activités sont indépendantes les unes des autres et les renseignements qu'elle gère sont stockés dans des bases de données distinctes.

D'après Equifax, les codes de conduite volontaires permettront probablement de régler la plupart des problèmes que pose la protection des renseignements personnels sur l'autoroute de l'information. Toutefois, si l'adoption de lois et de règlements s'avère nécessaire, ceux-ci doivent être clairs et homogènes pour que les industries puissent exercer leurs activités partout au pays. Ils doivent aussi être adaptés à la nature évolutive de l'autoroute de l'information tout en permettant d'éviter les problèmes au moment de la mise en place d'un nouveau service ou d'un progrès technologique. De plus, Equifax est persuadée que la technologie peut offrir des solutions à certains problèmes, en particulier ceux qui touchent la sécurité et le contrôle d'accès. Par ailleurs, il revient aux promoteurs de l'autoroute de faire valoir auprès du public canadien les avantages qu'elle offre sur le plan du contrôle exercé par les citoyens sur les renseignements personnels les concernant, de l'accès à l'information ainsi que du traitement uniforme et de la sécurité des données.

D'après des études menées par Equifax, qu'elle a publiées en 1993, les Canadiens se préoccupent réellement de leur vie privée. Ainsi, ces études ont révélé qu'une grande majorité de Canadiens souhaitent qu'on ajoute à la *Charte des droits* une disposition visant à protéger la vie privée, considèrent la vie privée comme un droit fondamental, et s'inquiètent de la protection de leur propre vie privée. Ils se préoccupent particulièrement de la façon dont les entreprises et les organismes gouvernementaux peuvent utiliser la technologie informatique pour recueillir, compiler et échanger des renseignements personnels au sujet d'un particulier. Les mesures de sécurité, les utilisations incompatibles, les profils personnels des clients, les transferts transfrontières et les renseignements inexacts suscitent des préoccupations particulières. Toutefois, une grande majorité de répondants ont déclaré que non seulement l'informatique facilite l'accès aux

renseignements et aux services utiles, mais aussi qu'elle a amélioré la qualité de vie. Par ailleurs, une proportion équivalente de répondants se sont dits favorables à l'utilisation de renseignements personnels pour l'établissement des primes d'assurance-automobile, l'approbation d'emprunts, l'émission de cartes de crédit ou l'établissement de limites de crédit. De surcroît, même si les Canadiens considèrent que la protection de la vie privée constitue un droit fondamental, ils conviennent qu'il faut aussi tenir compte de l'intérêt public, notamment pour prévenir les fraudes et le crime ainsi que pour réduire les dettes et les faillites. Les auteurs du rapport en sont arrivés à la conclusion que 62 p. 100 des «Canadiens adoptent une approche pragmatique quant à l'atteinte d'un équilibre entre les intérêts liés à la vie privée et l'accès à des avantages appréciés des consommateurs». De plus, la reconnaissance du droit d'accès à leurs dossiers et la possibilité de corriger les erreurs ou d'ajouter des observations apaisent considérablement les préoccupations des particuliers. D'après Equifax, on doit en arriver au bout du compte à exercer les mesures de contrôle nécessaires tout en laissant place à la vitesse d'exécution et au principe d'interconnexion, qui sont l'essence même de l'autoroute de l'information.

Equifax est d'avis qu'il faut respecter certains principes dans le but de protéger les renseignements personnels sur l'autoroute de l'information. On doit adopter des normes ou des règles cadres portant sur la collecte, la conservation et la communication de renseignements personnels et permettant non seulement d'y avoir accès mais aussi de les corriger. Cependant, il faut en arriver à un équilibre entre les règles et la nature évolutive de l'autoroute de l'information. D'ailleurs, les intervenants chargés de l'élaboration de ces règles doivent prendre en considération le degré de sensibilité de l'information; par exemple, les renseignements financiers sont de nature plus délicate que le profil des clients. Néanmoins, dans ce dernier cas, les consommateurs doivent avoir le droit de consulter leur profil et d'y ajouter des observations. Enfin, d'après Equifax, il ne faut pas interdire formellement l'appariement de données, mais les particuliers doivent avoir le droit de demander que leur nom ne figure pas sur les listes d'envoi.

Si l'on décide d'adopter une loi pour le secteur privé, elle doit édicter des règles claires et homogènes permettant aux industries d'exercer leurs activités partout au Canada sans être mises en cause pour des considérations d'ordre constitutionnel. Le gouvernement fédéral pourrait s'inspirer du modèle européen et adopter un cadre général auquel les provinces seraient invitées à souscrire. Les banques de données des organismes gouvernementaux et des entreprises du secteur privé doivent donc être assujetties aux mêmes règles, puisqu'elles seront raccordées au même réseau.

Equifax n'est pas en faveur de l'adoption d'une nouvelle loi. De fait, elle permet depuis plus de trente ans à ses clients d'avoir accès à leurs dossiers et de corriger les renseignements inexacts et elle informe les entreprises des corrections apportées. C'est pourquoi elle a facilement

satisfait aux exigences de la loi adoptée par le Québec concernant la protection des renseignements personnels dans le secteur privé. De plus, il sera essentiel d'adapter à la nouvelle nature instantanée des transactions sur l'autoroute de l'information les lois et règlements applicables.

Compte tenu de ses trente années d'expérience dans la protection de la vie privée, Equifax considère qu'elle exploite de manière efficace un système d'autoréglementation conforme aux normes et aux règlements cadres susmentionnés. Aux fins de l'élaboration des codes volontaires, on devrait tenir compte de la situation particulière des divers utilisateurs après avoir consulté les clients. De plus, ces codes doivent être assez souples pour tenir compte de la nature évolutive de l'autoroute de l'information, sans ériger d'obstacles quasi juridiques inutiles.

Même si la technologie suscite des inquiétudes parmi les consommateurs, Equifax est persuadée que les nouvelles technologies peuvent répondre aux préoccupations du public. Les bases de données informatisées sont plus sûres que les dossiers sur support papier, car des mesures telles que les codes d'accès et les cartes à puce permettent de contrôler électroniquement tout usage et tout accès non autorisé. Equifax a mis en place des mesures de sécurité rigoureuses, portant à la fois sur l'accès des clients au système et sur l'exploitation de ce dernier. Elle s'est dotée d'un code de conduite interne à l'intention de ses employés, auxquels elle offre par ailleurs une formation approfondie. Lorsqu'il s'agit de mettre au point de nouvelles technologies, la tenue de consultations préalables auprès de groupes de consommateurs permettrait de prévenir le blocage de nouveaux projets et la prolifération de poursuites judiciaires. Le protecteur du citoyen ou une autre instance similaire pourrait se charger de ces consultations. Equifax mentionne à titre d'exemple le débat actuel quant à savoir si la liaison par fibres optiques servant à la prestation de services doit être établie jusqu'au domicile même ou se terminer à une distance de 100 mètres de celui-ci pour ensuite être relayée au moyen d'un dispositif de transmission sans fil. Cette dernière option permettrait de réduire les coûts, mais elle aurait des répercussions sur la protection de la vie privée.

## **COMMISSAIRES À LA PROTECTION DE LA VIE PRIVÉE**

### ***Commission d'accès à l'information du Québec***

La Commission examine les effets de l'autoroute de l'information et fait valoir le rôle primordial que remplissent les lois en la matière. Quant aux codes volontaires et à la technologie, ils seront efficaces uniquement dans la mesure où ils seront régis par les lois. À cet égard, la Commission a joint à l'étude menée par le consortium UBI une copie de sa présentation.

D'après la Commission, l'autoroute de l'information modifiera considérablement le mode de vie des Canadiens. De nombreuses personnes s'accordent pour dire qu'elle constitue une menace pour la vie privée et notamment pour les renseignements personnels qui vont y circuler. De nouveaux consortiums, regroupant principalement des entreprises privées qui ont pour but de mettre en place des systèmes d'information, détiendront des renseignements de toute nature sur les citoyens, en particulier sur leurs habitudes et leur mode de vie, qui s'avéreront d'une grande valeur pour les entreprises. En raison du mode de circulation et de diffusion de l'information, il pourra être difficile pour les citoyens de protéger ces renseignements personnels.

Dans sa présentation au consortium UBI, la Commission examine les avantages de l'autoroute de l'information. Elle mentionne, par exemple, sa contribution au développement économique; le fait qu'elle constitue pour le gouvernement un moyen sans précédent de communiquer avec les citoyens et pour ces derniers d'avoir accès aux renseignements que détient le gouvernement; le télémarketing et le téléenseignement; l'exécution des transactions financières. Toutefois, elle signale qu'il faudra en arriver à un équilibre entre, d'une part, ces avantages et, d'autre part, des mesures qui protégeront les particuliers contre les intrusions dans leur vie personnelle (création de profils personnels) et leur domicile (surveillance) ainsi que des mesures qui leur permettront d'exercer un contrôle sur la collecte et l'utilisation des renseignements personnels les concernant (consentement éclairé). En ce qui touche le Québec, la Commission explique en détail les dispositions des lois québécoises qui protègent les renseignements personnels à la fois dans les secteurs public et privé et qu'ils doivent tous deux respecter.

#### **Approches**

- I. La Commission fait remarquer que peu de provinces exercent une juridiction sur le secteur privé au regard de la protection de la vie privée et des renseignements personnels. Tout en étant consciente des difficultés de nature juridictionnelle que peut présenter une démarche législative, la Commission considère que pour l'autoroute de l'information, comme dans tout autre domaine, c'est la seule

solution qui, jumelée à des sanctions efficaces, garantira le respect des droits des citoyens quant à la protection de la vie privée et des renseignements personnels. Un cadre légal contribuera en outre à la sensibilisation de la population, puisqu'il fera connaître les droits et les obligations de toutes les parties. Les mesures prévues dans la loi québécoise montrent qu'il est possible de protéger la vie privée des citoyens et les renseignements personnels les concernant sans nuire à la compétitivité des entreprises et sans créer des obligations qui peuvent les empêcher de fonctionner.

- II. On dit souvent que les codes d'éthique volontaires sont moins contraignants pour les entreprises qu'un cadre réglementaire. Cependant, la Commission considère que ces codes comportent certaines lacunes dans plusieurs domaines clés. L'adhésion à un code est volontaire et certaines entreprises refuseront d'y adhérer; aucune autorité indépendante et impartiale n'est chargée d'en assurer le respect; le citoyen ne dispose d'aucun recours autre que ceux dont fait état le code.
- III. Quant à l'application de solutions technologiques, la Commission est d'avis qu'elles peuvent fonctionner uniquement dans un contexte où le principe de confidentialité a déjà été enchâssé dans un texte légal. Il faut doter l'autoroute de l'information de tous les moyens techniques nécessaires pour assurer la protection des renseignements personnels. À cet égard, la sécurité constitue un aspect important et il faut notamment avoir recours au chiffrement pour assurer la confidentialité des renseignements de nature délicate, par exemple, l'information médicale. Il faut veiller à ce que les employés du réseau prennent conscience des obligations qui leur sont imposées au regard de la protection des renseignements personnels et qu'ils signent un protocole de confidentialité. On doit prévoir la mise en place de mesures de sécurité, notamment, dans le cas des employés, un code d'accès et un mot de passe, un accès limité et la journalisation des consultations de renseignements personnels; dans le cas des usagers, une carte d'accès et un code d'accès spécifique (NIP) avec rejet de la carte après entrées invalides, un code d'accès qui peut être modifié uniquement à des points de service, l'identification au moment de l'émission de la carte ou de son remplacement. De plus, tous les citoyens, y compris les personnes qui manquent de connaissances techniques ou les personnes handicapées, doivent avoir accès au réseau de manière à éviter qu'on crée deux classes de citoyens. De plus, avant d'introduire dans le réseau des renseignements provenant du secteur public ou privé, on doit procéder à une évaluation de l'impact sur la vie privée.

## **Commissariat à l'information et à la protection de la vie privée de la Colombie-Britannique**

Selon le commissariat à l'information et à la protection de la vie privée de la Colombie-Britannique, la solution la plus probable en ce qui touche la protection de la vie privée sur l'autoroute de l'information serait une combinaison de réglementations fédérale et provinciales, auxquelles s'ajouteraient des codes établis par le secteur privé, qui en arriveraient à avoir force de loi et à faire l'objet d'une surveillance indépendante. En outre, à son avis, le recours à des solutions technologiques visant à protéger les données et la sensibilisation des consommateurs sont essentielles.

L'établissement de profils ainsi que la liaison et l'appariement de données suscitent de vives préoccupations compte tenu de la très grande valeur des renseignements personnels pour les entreprises. Une préoccupation plus précise porte sur la capacité des particuliers d'effectuer des transactions sur la base d'un consentement éclairé. Le manque d'intérêt des gouvernements et des entreprises à l'égard de la préservation du droit à la vie privée pourrait entraîner un risque considérable de réaction hostile des consommateurs face aux progrès technologiques. À cet égard, certains défenseurs de la protection de la vie privée croient que l'automatisation continue des registres publics traditionnels (par exemple, les données relatives à l'immatriculation des véhicules et aux permis de conduire avec leurs utilisations et liaisons multiples) menace gravement la vie privée des particuliers. La capacité des nouvelles technologies de permettre une surveillance physique des particuliers soulève aussi certaines appréhensions, à la plupart desquelles permet de répondre l'application de pratiques équitables en matière d'information.

La Colombie-Britannique, l'Alberta, l'Ontario et le Québec ont adopté des lois sur la vie privée, tandis que certaines autres provinces ont opté pour des lois d'une portée moindre. Toutefois, seul le Québec s'est doté d'une loi protégeant la vie privée dans le secteur privé. Cette situation se compare à ce qui se produit en Europe, où l'élaboration de la directive de la Communauté européenne sur la protection de la vie privée en est à sa dernière étape. La protection des renseignements personnels constitue un droit fondamental en vertu de cette directive qui s'applique à la fois aux registres manuels et automatisés dans les secteurs public et privé. Elle établit des pratiques équitables en matière d'information et prévoit l'examen indépendant de leur respect et des mécanismes de recours. De plus, les dispositions de protection des données qu'elle renferme pourraient avoir une incidence négative sur les partenaires commerciaux de la Communauté européenne qui n'ont pas mis en place des mesures de protection similaires.

**Le commissariat retient douze grands principes de protection des données, en l'occurrence des pratiques en matière de traitement des renseignements personnels.**

- **transparence des systèmes d'information du gouvernement qui renferment des renseignements personnels, par exemple, aucune banque de données secrètes;**
- **collecte et stockage de renseignements personnels uniquement lorsqu'ils sont nécessaires et pertinents;**
- **réduction de la collecte, de l'utilisation et du stockage des renseignements personnels dans toute la mesure du possible;**
- **établissement préalable de la finalité des renseignements personnels et de leur utilisation ultime à des fins administratives;**
- **désignation de personnes chargées de la tenue des systèmes d'information renfermant des renseignements personnels;**
- **exercice d'un contrôle sur les liaisons, les communications et les interconnexions portant sur des renseignements personnels;**
- **consentement en toute connaissance de cause exigé pour la collecte de renseignements personnels;**
- **exactitude et exhaustivité des renseignements personnels stockés dans les systèmes d'information;**
- **adoption de dispositions concernant l'accès non autorisé à des données, y compris des sanctions civiles et criminelles en cas d'abus;**
- **adoption de règles particulières pour la protection des renseignements personnels de nature délicate;**
- **droit d'accéder aux renseignements personnels et de les corriger;**
- **droit d'être «oublié», notamment la dépersonnalisation ou la destruction de presque tous les renseignements personnels.**

**Plus précisément, des données peuvent être communiquées à des tiers uniquement si le particulier visé en a autorisé la communication, laquelle ne saurait être justifiée du simple fait qu'il ne s'y est pas opposé, comme le souhaite le secteur privé. De plus, le consentement éclairé doit être donné le plus possible «en toute connaissance de cause» et on doit maximiser les possibilités de permettre le libre choix.**

**Il existe une entente selon laquelle on doit éviter les «refuges de données» et les obstacles au commerce interprovincial découlant d'exigences différentes en matière de protection de la vie privée.**

Selon le commissariat, il n'est pas nécessaire d'avoir recours à une **intervention législative fédérale uniforme** face à tous les problèmes que pose la protection de la vie privée sur l'autoroute de l'information. On pourrait s'attendre à ce qu'une solution canadienne type fasse appel à des réglementations fédérale et provinciales. L'application de la *Loi sur la protection des renseignements personnels* à toutes les institutions du secteur privé assujetties à la réglementation du gouvernement fédéral constituerait un bon point de départ. De plus, on pourrait adopter des lois et des règlements progressistes pour régir l'énorme réserve de renseignements détenus par les divers ordres de gouvernement. Toutefois, avant même de réglementer, il faut déployer des efforts constants pour comprendre les utilisations proposées à l'égard de la technologie et les méthodes qui seront mises en oeuvre.

Tous les organismes et les organisations qui possèdent des renseignements personnels doivent s'engager le plus possible dans une autoréglementation volontaire en adoptant des codes sur la protection de la vie privée qui englobent des pratiques équitables en matière d'information. Cependant, aucun de ces codes n'a force de loi et aucun ne répond entièrement aux préoccupations des particuliers concernant la vie privée. À cet égard, le commissariat recommande d'examiner avec attention les résultats des recherches actuelles du professeur Colin Bennett (pour le compte de la CSA) portant sur l'adoption de codes volontaires dans les sociétés industrielles évoluées. En dernière analyse, il faudrait que ces codes volontaires aient force de loi et qu'un organisme indépendant soit chargé de veiller à leur respect.

On doit absolument déterminer dans quelle mesure toute nouvelle technologie pose un problème en matière de protection de la vie privée. La formulation d'énoncés concernant l'impact sur la vie privée doit être un préalable à la promotion et à l'application d'une nouvelle technologie et de nouveaux produits et services dans les secteurs public et privé. À tout le moins, il faudrait cerner dans toute la mesure du possible les intérêts opposés en présence et proposer des moyens, s'il en est, d'arriver à un équilibre. Bien que la plupart des nouvelles technologies menacent la vie privée, elles peuvent aussi offrir des mesures de protection des renseignements personnels, par exemple, en faisant appel au chiffrement et aux cartes à puce.

### ***Commissaire à l'information et à la protection de la vie privée de l'Ontario***

Le commissaire à l'information et à la protection de la vie privée estime nécessaire d'adopter une loi fédérale s'appliquant au secteur privé et de mettre en place à l'échelle provinciale des mesures de protection des données équivalentes. Les codes volontaires sur la protection de la vie privée dans le secteur privé ne constituent selon lui qu'une première étape.

Les solutions technologiques peuvent aussi permettre de régler une partie du problème. De plus, toujours selon le commissaire, la sensibilisation des consommateurs constitue un besoin fondamental.

Selon une enquête menée en 1994 par Gallup Canada pour Andersen Consulting Canada, la majorité (67,7 p. 100) des répondants ont déclaré que l'autoroute de l'information est une «bonne idée», mais une proportion plus forte encore (83,7 p. 100) se sont dits très préoccupés ou quelque peu préoccupés par l'incidence que peut avoir cette autoroute sur leur vie privée. Il faut donc veiller à ce qu'on puisse profiter des avantages qu'offre l'évolution de l'autoroute, sans pour autant qu'elle mine rapidement la vie privée des particuliers.

### Réponses aux questions

1. Il faut établir des principes clairs de portée générale. Le commissaire est d'avis qu'une protection efficace de la vie privée sur l'autoroute de l'information peut prendre appui sur les principes suivants.

- *Il faut respecter et protéger la vie privée.*

La complexité croissante de l'autoroute de l'information permettra de retracer, de regrouper et d'analyser des volumes considérables de renseignements personnels. Il sera ainsi possible de créer des profils personnels et d'exercer une surveillance sur les particuliers. Dans la mesure où ces derniers considèrent que les avantages obtenus ne font pas contrepois à cette menace à la vie privée, l'information et les services accessibles sur l'autoroute ne seront pas utilisés à pleine capacité.

- *Avant d'introduire une nouvelle technologie ou un nouveau service, il faut examiner son impact sur la vie privée.*

On doit tenir compte des préoccupations concernant la vie privée dès le début de la conception et de la mise en place d'une technologie ou d'un service. Il est plus coûteux et plus difficile d'intervenir lorsqu'un mécanisme est déjà opérationnel.

- *La collecte, le stockage, l'utilisation et la communication de renseignements personnels doivent être régis par des pratiques équitables en matière d'information établies par la loi.*

Le code de pratiques équitables en matière d'information le plus connu fait partie des Lignes directrices de l'OCDE, dont s'inspire la loi canadienne. On trouve un certain nombre de codes volontaires sectoriels, mais ils ne satisfont pas toujours aux Lignes directrices de l'OCDE. Cet état de choses pourrait constituer un obstacle à l'échange d'information entre les pays

ainsi qu'entre les secteurs public et privé. L'adoption d'une loi fédérale s'appliquant au secteur privé constituerait le meilleur moyen d'éviter ce problème. Des lois provinciales similaires à la loi du Québec concernant la protection de la vie privée dans le secteur privé pourraient s'y ajouter. Ces lois doivent édicter des normes régissant la collecte, l'utilisation, la communication et la correction des renseignements personnels, l'accès à ces renseignements et l'avis de communication. Il faut préciser clairement la finalité de la collecte; cette dernière doit en général faire suite à une demande du particulier et celui-ci doit absolument en être informé et y consentir. Le particulier doit donner son consentement éclairé pour que des renseignements puissent faire l'objet d'une utilisation secondaire ou être communiqués à des tiers. De plus, il doit avoir le droit d'accéder aux renseignements personnels le concernant et de les corriger. Enfin, il doit être informé des raisons à l'origine de la collecte et de la règle de droit qui s'applique, qu'elle soit obligatoire ou volontaire, de la façon dont les renseignements seront utilisés et divulgués, des conséquences de la transmission ou de la retenue des renseignements et de la personne à qui s'adresser pour poser des questions.

- *Les technologies ou les services d'information susceptibles de menacer la vie privée doivent renfermer des mesures de protection appropriées sans que le particulier ait à en assumer le coût.*

Les nouvelles technologies et les nouveaux services ne doivent pas porter atteinte à la vie privée. À tout le moins, il faut pouvoir maintenir les niveaux de protection de la vie privée existants sans que des coûts supplémentaires en découlent.

- *Il faut sensibiliser le public à toutes les questions de sécurité ou de protection de la vie privée entourant l'automatisation de l'information et lui offrir une formation dans ce domaine.*

C'est aux fournisseurs de services qu'il doit incomber d'informer le public de toute incidence sur la vie privée que peuvent avoir leurs services.

- *Il faut protéger les renseignements personnels en mettant en place des mesures de sécurité appropriées.*

En règle générale, les solutions techniques (par exemple, les mots de passe et le chiffrement) ainsi que les procédures de sécurité doivent être proportionnées aux risques en jeu. On doit envisager le chiffrement des renseignements personnels de nature délicate et des renseignements présentant un risque élevé d'accès non autorisé.

- *Il faut trouver un moyen de traiter les plaintes et de réparer les torts subis.*

Pour favoriser le respect d'un code commun de pratiques équitables en matière d'information, on doit mettre en place un mécanisme indépendant pour traiter les plaintes et, s'il y a lieu, imposer des sanctions et accorder un dédommagement en cas d'utilisation non autorisée de renseignements personnels.

2. D'après le commissaire, tous les ordres de gouvernement doivent participer à l'élaboration et à la mise en place de mesures plus rigoureuses de protection de la vie privée. Ces mesures peuvent s'inspirer des quatre approches présentées dans le Document de travail.

Comme il a déjà été mentionné, le commissaire se montre favorable à une loi fédérale et à des lois provinciales complémentaires s'appliquant au secteur privé, qui renfermeraient des dispositions concernant les plaintes et les mécanismes de recours. De plus, à titre d'instance de réglementation, le gouvernement doit remplir un rôle permanent, similaire à celui que joue le CRTC à l'heure actuelle. Les organismes de réglementation doivent exiger une évaluation de l'impact sur la vie privée chaque fois qu'on offre de nouveaux services. De cette façon, les intervenants seraient tenus d'envisager des mesures de protection de la vie privée dès le début du processus d'élaboration, et cette pratique se révélerait rentable.

Le commissaire préconise l'adoption de codes volontaires comme première étape de la protection des données dans le secteur privé. Toutefois, à son avis, leur portée n'englobe pas l'ensemble du secteur privé; il est possible qu'ils ne répondent pas à la norme de protection «adéquate» de la vie privée adoptée par la Communauté européenne; il se peut aussi que leur application pose des problèmes, et l'on observe souvent des lacunes en ce qui touche l'apport de la personne visée et le contrôle qu'elle exerce. À long terme, c'est donc une loi s'appliquant à la fois au secteur public et au secteur privé qui constituerait la solution la plus efficace.

On convient que certaines technologies peuvent permettre de protéger la vie privée au lieu d'y porter atteinte, par exemple, des signatures aveugles faisant appel à un chiffrement à clé révélée. Une nouvelle technologie doit aussi offrir aux particuliers la possibilité d'exercer un contrôle sur les renseignements personnels les concernant. De plus, la protection de la vie privée doit être primordiale dès le début plutôt qu'après coup. Par défaut, les consommateurs se trouvent en position de réaction, ce qui peut donner lieu à des modifications coûteuses ou au rejet absolu d'un produit, comme dans le cas du logiciel Lotus

**Marketplace: Households.** C'est pourquoi la protection de la vie privée doit constituer un critère fondamental en ce qui touche la technologie et les services.

La sensibilisation des entreprises aux incidences sur la vie privée et la prise de conscience des consommateurs constituent des besoins fondamentaux. Toutes les parties doivent assumer la responsabilité de la sensibilisation. Cependant, il ne suffit pas de sensibiliser le public. On doit adopter une approche intégrée pour que toutes les parties qui interviennent sur l'autoroute de l'information soient informées également.

3. Le commissaire est favorable à une approche axée sur une coordination des lois à tous les paliers. La combinaison d'un cadre législatif et de codes sectoriels, un peu comme ce que l'on a fait en Nouvelle-Zélande, pourrait garantir le respect du droit à la vie privée, tout en permettant de s'adapter aux caractéristiques uniques des différents secteurs. La loi canadienne doit aussi être harmonisée avec les faits nouveaux sur la scène internationale, car l'autoroute de l'information ne prend pas fin à la frontière.
4. Il est important d'amener les entreprises à comprendre que la protection de la vie privée doit faire partie intégrante de leurs activités. Cependant, comme l'indique la réponse à la question n° 2, les codes volontaires sur la protection de la vie privée tels qu'ils sont appliqués à l'heure actuelle n'offrent pas une protection entière de la vie privée. Le commissaire à l'information et à la protection de la vie privée de l'Ontario est en faveur uniquement de lignes directrices élaborées par les entreprises, qui constitueraient une étape vers une législation de portée générale s'appliquant au secteur privé.
5. Il ne faut pas considérer la protection de la vie privée isolément, mais bien l'intégrer au processus décisionnel concernant l'autoroute de l'information. De plus, comme l'acceptabilité de cette autoroute sur le plan social figurera parmi les aspects clés de sa concrétisation, elle doit permettre de bien protéger la vie privée. L'autoroute doit donc être conçue de manière à offrir un niveau élevé de protection de la vie privée. L'intégration des mesures de protection dès le début de la conception ne devrait ni ralentir les progrès ni entraîner une augmentation indue du coût des innovations. Il est reconnu que les systèmes protégés coûtent en général plus cher que ceux qui ne le sont pas. Toutefois, le prix à payer en dignité humaine et en autonomie est trop élevé pour que l'intégration d'un niveau élevé de protection de la vie privée ne constitue pas une exigence.
6. Des initiatives telles que la production du Document de travail, les audiences du CRTC et les vastes consultations menées par la

coalition pour l'information du public favorisent toutes la participation de ce dernier aux décisions de principe concernant l'autoroute de l'information. Cependant, les consultations ont été limitées en ce qui touche les progrès technologiques et les pratiques dans une optique fondamentale, par exemple, en vue de déterminer leur incidence sur la société plutôt que l'augmentation éventuelle de leur efficience. Les entreprises doivent donc consulter les citoyens et tenir compte de leur opinion lorsqu'elles développent des produits et des services susceptibles de menacer la vie privée. Il s'agit peut-être d'un changement fondamental, mais nécessaire, dans les pratiques commerciales au Canada.

7. Tous les ordres de gouvernement doivent accorder la priorité à la sensibilisation du public et veiller à ce qu'on y affecte les fonds et les ressources nécessaires. Les fournisseurs de services et d'information du secteur privé doivent aussi partager cette responsabilité. De plus, les Canadiens doivent s'efforcer de devenir des consommateurs mieux renseignés. Pour leur part, les commissaires à la protection de la vie privée et les autres intervenants qui participent à l'évolution de l'autoroute de l'information doivent avoir à coeur de protéger les intérêts du public, de soulever les préoccupations liées à la vie privée et de favoriser le débat public dans le domaine.

### ***Commissariat à la protection de la vie privée du Canada***

Le Commissariat à la protection de la vie privée du Canada est l'organisme fédéral chargé de protéger les citoyens. Le parlement lui a confié le mandat d'examiner les plaintes liées à la collecte, à l'utilisation et à la divulgation par le gouvernement fédéral de renseignements personnels concernant les Canadiens. Il surveille aussi l'application de la *Loi sur la protection des renseignements personnels*, qui repose sur les codes de pratiques équitables en matière d'information acceptés à l'échelle internationale.

Après avoir procédé à un vaste examen des grandes questions touchant la protection de la vie privée sur l'autoroute de l'information, le Commissariat en arrive à la conclusion qu'il est essentiel de mettre en place un cadre législatif ferme (aux paliers provincial, fédéral et international). À son avis, les codes volontaires, les solutions technologiques et la sensibilisation des consommateurs ont aussi leur place dans l'équation de la vie privée, mais ces éléments ne permettent pas de régler à eux seuls l'enchevêtrement de préoccupations concernant la vie privée et d'intérêts commerciaux que soulève l'autoroute de l'information.

Les renseignements personnels appartiennent au particulier visé. Ce principe de base s'applique, que l'information soit traitée au moyen d'une plume d'oie ou d'un ordinateur. De surcroît, la protection de la vie privée

n'est pas un produit issu uniquement de l'ère de l'informatique. Il y a longtemps que des lois interdisent de pratiquer l'écoute électronique et de consulter le courrier destiné à une autre personne qui ne lui a pas été remis.

Le Commissariat s'inquiète du fait que certains milieux acceptent de faire des sacrifices sur le plan de la protection de la vie privée en contrepartie de la rapidité et de l'aspect pratique de l'autoroute de l'information. Toutefois, il s'oppose lui-même à cette attitude, même si la protection de la vie privée sur l'autoroute de l'information peut poser certaines difficultés. Sans cette protection, le public risque de ne pas pouvoir utiliser pleinement l'autoroute, au détriment de l'augmentation de l'efficacité du gouvernement et de la compétitivité du secteur privé. Dans sa présentation, le Commissariat se préoccupe particulièrement de la protection de la vie privée des particuliers qui ont recours au courrier électronique. Le courrier électronique est considéré comme une communication privée et il ne peut être divulgué en l'absence de consentement explicite. On doit donc s'efforcer de le protéger contre les interceptions. Toutefois, dans les cas où c'est impossible, il faut informer les utilisateurs que leur courrier électronique n'est pas protégé. En outre, le Commissariat s'inquiète de la vulnérabilité de certains types particuliers de renseignements, à savoir l'information médicale et les données transactionnelles. La nature particulièrement délicate de l'information médicale exige des mesures de protection supplémentaires. Par ailleurs, les transactions électroniques laissent derrière elles des données qui peuvent permettre de connaître les croyances d'une personne, ses goûts, sa situation financière ou sa solvabilité. C'est pourquoi il faut les protéger. La surveillance et le contrôle des utilisateurs de téléphones portatifs, au moyen de satellites de géopositionnement inquiètent aussi le Commissariat. L'utilisation de cette technologie, souvent désignée par le terme «laisse électronique» présente certains avantages pratiques. Toutefois, en l'absence d'une règle de droit autorisant cette pratique, les renseignements acquis doivent servir uniquement à faciliter les liaisons techniques.

Contrairement aux lignes directrices de l'OCDE s'appliquant à l'échelle internationale, la *Loi sur la protection des renseignements personnels* adoptée par le gouvernement fédéral et les lois provinciales équivalentes, exception faite de celle du Québec, ne régissent pas en général la protection de la vie privée dans le secteur privé.

Le Commissariat recommande d'intégrer les principes suivants aux lois s'appliquant aux secteurs public et privé.

- On ne peut recueillir que les renseignements personnels nécessaires pour fournir le produit ou le service visé.
- L'entreprise de télécommunication et le maître du fichier doivent expliquer à leurs clients les pratiques qu'ils appliquent en matière de

protection des données et les répercussions des nouvelles technologies sur la protection de la vie privée.

- Les particuliers doivent avoir le droit d'exercer un contrôle sur les renseignements personnels les concernant transmis sur l'autoroute de l'information.
- La divulgation de renseignements personnels sans le consentement explicite du particulier doit être interdite.
- Les particuliers doivent avoir accès aux renseignements personnels les concernant; l'entreprise de télécommunication et le maître du fichier doivent s'assurer qu'ils sont exacts et à jour.
- Il doit être interdit d'imposer des frais pour la protection de la vie privée.
- Il faut mettre en place un mécanisme de supervision indépendant qui protège la vie privée et offre un processus de recours.

La distinction entre les secteurs public et privé s'estompe de plus en plus en raison, par exemple, de l'impartition et du recours à des entreprises de télécommunication du secteur privé pour effectuer des transactions commerciales pour le compte du gouvernement.

Il faut harmoniser les lois sur la protection de la vie privée aux échelons fédéral et provincial, sans quoi certains intervenants pourraient tenter de se soustraire à des mesures de protection de la vie privée en s'établissant sur le territoire des secteurs de compétence les moins sévères au détriment des autres. De plus, il pourrait alors devenir nécessaire de créer par voie législative des distinctions artificielles quant à l'« emplacement » des renseignements.

La protection de la vie privée ne saurait être tributaire des caprices du marché. C'est pourquoi le gouvernement fédéral doit non seulement légiférer pour protéger la vie privée sur l'autoroute de l'information dans les secteurs public et privé, mais aussi inciter les provinces à adopter des lois complémentaires. Ces lois doivent reposer sur des pratiques équitables en matière d'information et sur les principes susmentionnés et prévoir des sanctions appropriées.

Les codes volontaires ne peuvent fournir un niveau de protection adéquat. Du fait de leur nature volontaire, ils n'ont pas force exécutoire et risquent de ne pas être respectés par les intervenants qui possèdent un intérêt financier ou souhaitent obtenir un avantage concurrentiel. Comme toute chaîne, ils ont la force du plus faible de leurs maillons. De plus, les codes volontaires constituent souvent des demi-mesures et il est possible qu'ils ne confèrent aux particuliers aucun droit à exercer. Ils ont néanmoins leur place dans un contexte général, notamment à des fins de sensibilisation.

Quant aux solutions technologiques, elles ont aussi leur place mais ne sauraient suffire en soit. À cet égard, la sécurité des renseignements revêt une grande importance et la mise en place de mécanismes de chiffrement efficaces et d'installations de transmission protégées ont aussi un rôle important à jouer. Le Commissariat souligne toutefois que le chiffrement soulève un problème important. En effet, doit-on permettre qu'il soit efficace à un point tel que les organismes chargés de l'application de la loi ne puissent en trouver la clé? Même s'il incombe aux entreprises de télécommunication de veiller à ce que leurs circuits de transmission soient fondamentalement sûrs, elles ne peuvent être tenues responsables de la protection des renseignements personnels qui y circulent. De fait, elles doivent avoir l'obligation de ne pas examiner les renseignements diffusés. La sécurité des renseignements proprement dits incombe au maître du fichier. Sa protection peut passer par le chiffrement de renseignements personnels de nature délicate, par exemple, l'information médicale. Le maître de fichier doit avoir l'obligation d'informer la personne visée lorsqu'il ne peut assurer cette sécurité. De plus, la protection de la vie privée doit être intégrée à l'élaboration des nouvelles technologies. À cette fin, les évaluations de l'impact sur la vie privée doivent être mises à la disposition des organismes de réglementation et du public.

De même, la sensibilisation doit jouer un rôle important. Les consommateurs doivent être informés de l'impact des nouvelles technologies sur leur vie privée et des moyens permettant de la protéger. La sensibilisation de la population quant à l'éthique dans l'acquisition et le traitement des renseignements personnels constitue un besoin tout aussi important. À cet égard, le Commissariat à la protection de la vie privée et les organismes provinciaux homologues peuvent jouer un rôle important. Les fournisseurs de services ont aussi l'obligation de laisser les consommateurs libres de choisir d'utiliser ou non les services fournis et d'opter pour le niveau de sécurité exigé.

### **Gouvernement de la Colombie-Britannique**

Le ministère de l'Emploi et de l'Investissement de la Colombie-Britannique fait la présentation au nom du gouvernement de la Colombie-Britannique.

Cette province estime qu'il faut consulter tous les ordres de gouvernement au sujet du rôle législatif et réglementaire que doivent jouer les gouvernements dans la protection de la vie privée des particuliers. Cette consultation doit aussi englober le secteur public en général, les milieux de l'enseignement et le secteur privé. Toutefois, il faut en arriver à un équilibre entre l'autoréglementation et l'intervention des gouvernements, au besoin, dans la réglementation des activités.

Le gouvernement de la Colombie-Britannique reconnaît les énormes possibilités qu'offre l'autoroute de l'information. Toutefois, les progrès technologiques dans la communication, la collecte et le traitement des renseignements risquent de porter atteinte à la vie privée des particuliers. On observe un accroissement des problèmes liés à l'appariement des données, aux données transactionnelles, à la sécurité des réseaux et à la diffusion générale des données. Pour répondre à ces préoccupations, il faut adopter sans tarder des mesures de protection de la vie privée au Canada.

#### **Réponses aux questions**

1. La province souscrit aux *Principes de protection de la vie privée dans les télécommunications* adoptés par le gouvernement fédéral. En outre, elle est en accord avec les éléments énoncés par le Commissaire à la protection de la vie privée du Canada pour décrire le droit à la vie privée.

- Le droit à l'autonomie individuelle.
- Le droit de vivre en paix.
- Le droit à l'intimité.
- Le droit d'exercer un contrôle sur les renseignements qui touchent sa personne.
- Le droit de limiter l'accessibilité aux renseignements qui touchent sa personne.
- Le droit de réduire les intrusions.
- Le droit de s'attendre à la confidentialité.
- Le droit à la solitude.

En outre, les décisions concernant la vie privée doivent reposer sur le principe selon lequel les intervenants qui possèdent des renseignements personnels concernant les particuliers exercent un pouvoir sur ces derniers, que l'utilisation de ces renseignements peut causer du tort et qu'il faut donc utiliser l'information de manière responsable.

2. Des lois fédérale et provinciales sont nécessaires pour protéger les renseignements personnels que possède le gouvernement. Ces lois doivent intégrer les douze grands principes de protection des données énoncés dans la présentation du commissariat à l'information et à la vie privée de la Colombie-Britannique. Elles doivent en outre prévoir le consentement à la collecte et à la diffusion de renseignements, la divulgation des types de données détenues, un droit d'accès et l'obligation de veiller à la mise en place de mesures de sécurité appropriées.

Les divers secteurs de compétence doivent examiner en toute objectivité l'adoption éventuelle d'une loi s'appliquant au secteur privé. Le cas échéant, cette loi doit être harmonisée entre les secteurs de compétence, sans quoi le transfert de données entre les provinces ou entre les échelons fédéral et provincial posera des problèmes.

Avant même d'adopter une loi, il faut inciter l'industrie à adopter des codes sur la protection de la vie privée. Si elle est efficace, l'autoréglementation est plus efficace et plus économique. En outre, des codes pourraient se révéler efficaces dans les domaines où des organismes centraux sont chargés de l'accréditation ou de la délivrance de licences. Même si les codes sur la protection de la vie privée adoptés par l'industrie sont plus souples, une norme nationale pouvant servir de modèle pour l'élaboration de ces codes permettrait de garantir une démarche commune et globale. C'est pourquoi la province est favorable au code élaboré par la CSA concernant la protection de la vie privée.

Les progrès technologiques peuvent servir à protéger la vie privée tout autant qu'ils peuvent la menacer. Il est important d'avoir recours à des codes d'accès et au chiffrement.

5. La question de la vie privée est trop importante pour qu'on la néglige au profit d'un développement non contrôlé.
6. Les gouvernements doivent adhérer aux principes généraux selon lesquels une consultation prend place à l'étape de l'élaboration des systèmes qu'ils utiliseront. Lorsque la vie privée est gravement menacée, le processus de consultation doit être similaire à ceux qui s'appliquent pour les autres types de réglementation.

7. Tous les secteurs doivent contribuer à sensibiliser le public à la protection de la vie privée. Les organismes de réglementation, par exemple, le CRTC, diverses entités gouvernementales des secteurs de la consommation et des sociétés commerciales ainsi que les commissaires à l'information et à la protection de la vie privée peuvent tous y participer. En ce qui touche les commissaires, cette sensibilisation doit faire partie intégrante de leur mandat. Les groupes de consommateurs, les établissements d'enseignement et le secteur privé doivent aussi assumer cette responsabilité.

## **Santé et Bien-être social Canada**

Dans sa présentation, Santé et Bien-être Canada examine le concept général de la protection de la vie privée et de la confidentialité ainsi que ses diverses conséquences, l'utilisation des données à des fins administratives et statistiques, le caractère confidentiel des dossiers médicaux et les codes et normes volontaires. Il aborde ces éléments dans sa propre perspective en tant qu'autorité nationale en matière de santé au Canada.

La définition du terme «vie privée» qui figure dans le Document de travail peut donner lieu à une interprétation erronée. La protection de la vie privée est un droit fondamental, mais il ne s'agit pas d'un droit absolu. On doit aussi tenir compte des droits de la société en général. De plus, la question des «droits» peut susciter beaucoup d'émotion. C'est pourquoi la confidentialité et l'imposition aux organisations de l'exigence de rendre compte des renseignements personnels sur lesquels elles ont la haute main sont considérées comme des questions déterminantes.

Le Ministère se préoccupe fortement du fait qu'on établisse une distinction entre l'utilisation de renseignements personnels à des fins administratives (pour les besoins d'un processus décisionnel qui influera directement sur le particulier) et son utilisation à des fins statistiques ou pour la recherche. Dans les cas où la confidentialité revêt une importance primordiale et où les mesures de protection sont tout à fait adéquates, l'utilisation de renseignements à des fins statistiques ou pour la recherche ne doit pas être limitée. Il s'agit là d'un principe primordial, dans la mesure où il permet d'acquérir de nouvelles connaissances sur les maladies et les risques pour la santé à l'échelle nationale et internationale. De plus, Santé et Bien-être social estime que le public est très conscient de l'importance de la recherche dans ces domaines.

La confidentialité des dossiers médicaux est aussi un aspect d'intérêt majeur. Même si la *Loi sur la protection des renseignements personnels* semble traiter cette question de manière adéquate, les soins de santé sont de compétence provinciale et ce ne sont pas toutes les provinces qui ont adopté une loi sur la protection de la vie privée. De plus, le secteur privé, qui n'est pratiquement assujéti à aucune réglementation en la matière,

possède aussi des dossiers médicaux, et cette situation risque d'entraîner des abus. Plusieurs solutions sont possibles. Le Ministère mentionne notamment l'adoption par les provinces de lois uniformes concernant la protection des données, à savoir des lois qui s'appliqueraient au secteur de la santé dans son ensemble et aux autres utilisateurs de renseignements sur les soins de santé. Les législateurs pourraient s'inspirer de la *Data Protection Act* du Royaume-Uni et de la *Uniform Health Care Information Act* des États-Unis. Une autre solution consiste à élaborer des codes modèles pour la protection des renseignements sur les soins de santé. Certains codes similaires existent déjà dans plusieurs secteurs et on ne doit pas sous-estimer leur importance même s'ils n'ont pas force de loi.

Santé et Bien-être social est en accord avec l'objectif des codes volontaires sur la protection de la vie privée, en particulier le projet de code modèle de la CSA. Toutefois, certains principes énoncés dans le code de la CSA suscitent des préoccupations. Ces principes se rapportent au « consentement », à la « détermination des finalités » et à la « limitation de l'utilisation, de la communication et de la conservation ». L'application à la lettre de ces principes pourrait entraver considérablement ou restreindre des activités de recherche légitimes. Dans le domaine de la recherche épidémiologique et des autres champs de recherche médicale, on a besoin de volumes considérables de renseignements personnels pour l'appariement de données statistiques, et cette exigence exclut l'application stricte des principes mentionnés ci-dessus. Toutefois, les chercheurs et les organismes de recherche du secteur de la santé, par exemple, le Conseil de recherches médicales et l'Institut canadien d'information en matière de santé, ont adopté des principes fondés sur les lignes directrices de l'OCDE; ils ont aussi élaboré des politiques visant à protéger la confidentialité des dossiers personnels et des mesures de protection contre la divulgation par inadvertance de données de faible grandeur.

### ***Ministère de la Santé et des Services sociaux de l'Île-du-Prince-Édouard***

Le Ministère se préoccupe du fait qu'une loi visant à protéger la vie privée pourrait entraver la recherche pharmacoépidémiologique. Il est à son avis important de prévoir des dispositions à l'égard de ces études qui font appel à des renseignements dépersonnalisés qui demeurent confidentiels. Force est de reconnaître à la fois l'importance de la protection de la vie privée et la nécessité d'obtenir des renseignements aux fins de la recherche médicale.

### ***Secrétariat provincial de la Saskatchewan***

Cette présentation est faite au nom du service des politiques en matière de télécommunications et de radiodiffusion du secrétariat provincial de la

**Saskatchewan. Elle n'exprime pas le point de vue du gouvernement de cette province.**

**Il est primordial de reconnaître l'importance des questions relatives à la protection de la vie privée pour l'essor et l'évolution de l'autoroute de l'information. Si l'on néglige ces questions, les utilisateurs ne pourront intégrer cette autoroute dans leurs activités quotidiennes.**

**La Saskatchewan se fera un plaisir de mener des consultations à l'égard de toutes les propositions et recommandations découlant des délibérations du Comité consultatif.**

### **Congrès du travail du Canada**

En résumé, le Congrès du travail du Canada considère qu'il est essentiel de légiférer, car les codes volontaires se sont révélés inadéquats. Il remet en question le sens prêté couramment au terme «vie privée» dans le secteur privé et formule plusieurs préoccupations. Il propose aussi un certain nombre de principes sur lesquels pourrait prendre appui une protection efficace de la vie privée.

En règle générale, le public et les entreprises assimilent la vie privée à la confidentialité. Ils ne tiennent alors pas compte du précepte fondamental selon lequel les particuliers doivent pouvoir exercer un contrôle sur les renseignements personnels les concernant.

Le Congrès exprime plusieurs préoccupations à l'égard de l'invasion de la vie privée qui pourrait se produire en raison du volume considérable de renseignements personnels que possèdent les gouvernements, les employeurs et le secteur privé. Il s'inquiète également de la communication de renseignements personnels, dans le cadre de partenariats entre les secteurs public et privé, ainsi que de leur transfert à l'étranger.

Une loi de portée générale doit intégrer les principes suivants :

- Les particuliers doivent exercer un contrôle sur les renseignements personnels les concernant.
- Les renseignements doivent être communiqués uniquement au moment prévu et aux destinataires ciblés.
- Il faut recueillir uniquement les détails essentiels pour fournir un service.
- La divulgation doit être interdite sans le consentement explicite.
- Il faut expliquer clairement aux clients les procédures de collecte des données.
- Il doit être interdit d'avoir recours à des enregistrements qui montrent de quelle façon et à quel moment un particulier a utilisé l'autoroute de l'information, à moins que celui-ci y ait consenti en toute connaissance de cause.
- L'utilisation de dossiers transactionnels doit être limitée aux usages qui ont fait l'objet d'un consentement et sont permis par la loi.
- Des méthodes de chiffrement appropriées et d'autres moyens techniques visant à protéger la confidentialité des communications électroniques doivent être obligatoires.

- Il doit être interdit de réclamer des frais pour la protection de la vie privée.
- Le gouvernement doit exercer une surveillance en ce qui touche la protection de la vie privée sur l'autoroute.
- Il faut adopter par voie législative un code de pratiques équitables en matière d'information qui régira l'autoroute de l'information.
- Il faut prévoir des sanctions sévères pour dissuader les contrevenants éventuels.

D'après le Congrès, il est essentiel aux fins de la protection de la vie privée d'adopter une loi de portée générale s'appliquant au secteur privé, notamment aux entreprises, ainsi qu'au gouvernement. Cette loi doit reposer sur les principes déjà mentionnés et servir de cadre pour tous les intervenants visés. À l'exception du Québec, qui a adopté un modèle de loi sur la protection de la vie privée dans le secteur privé, le Canada semble l'un de rares pays fortement industrialisés qui ne protège pas de manière adéquate les renseignements personnels détenus par le secteur privé. La loi doit faire en sorte que tous les utilisateurs de renseignements personnels soient assujettis aux mêmes lignes directrices.

Le méli-mélo de codes volontaires sur la protection de la vie privée s'est révélé tout à fait inadéquat, en particulier du fait que, dans de nombreux cas, ces codes ne prévoient aucun mécanisme indépendant pour le traitement des plaintes et ils servent les intérêts des entreprises plutôt que ceux des consommateurs. De plus, l'agence de protection de la vie privée en matière de télécommunications n'a jamais vraiment pris son essor. Le projet de code modèle sur la protection de la vie privée de la CSA semble prometteur, s'il peut faire échec aux possibilités d'incursion dans la vie privée et suivre le rythme des changements technologiques.

### ***Association canadienne de normalisation (CSA)***

D'après la CSA, les dix principes énoncés dans son *Code modèle sur la protection de la vie privée* forment la base même d'une protection efficace de la vie privée. Les solutions technologiques et la sensibilisation des consommateurs ont aussi un rôle à jouer.

Le code de la CSA a été élaboré par consensus. Les codes volontaires accroîtront l'efficacité des trois autres approches présentées dans le Document de travail. De plus, ils peuvent faire appel à des mesures non législatives pour garantir leur respect. En 1995, la CSA étudiera diverses options pour la mise en oeuvre de son propre code. Par ailleurs, les codes ont souvent une incidence favorable sur les entreprises, parce qu'ils leur permettent d'améliorer la qualité de la gestion de l'information.

Il faudra protéger la vie privée sur l'autoroute de l'information. À tout le moins, le réseau doit atténuer la vulnérabilité du courrier électronique ainsi que du télécopieur et prévoir le chiffrement des renseignements. La CSA participe déjà à l'élaboration de normes sur la technologie de l'information, notamment sur les dispositifs de sécurité et les cartes à puce.

Le bien-fondé de la sensibilisation des consommateurs à la protection de la vie privée ne fait aucun doute. Cette responsabilité doit être assumée conjointement par tous les intervenants qui recueillent de l'information. La publication du code de la CSA constitue à son avis un moyen de sensibiliser les consommateurs.

#### **Proposition et recommandation précise**

En sa qualité d'agent de consensus, la CSA serait bien préparée à participer à la sensibilisation des consommateurs.

### ***COMSEC Services Inc.***

COMSEC Services est une entreprise qui exerce ses activités dans le domaine de la sécurité des communications.

Sa présentation porte principalement sur la sécurité technique dans le contexte de l'autoroute de l'information. Elle établit un parallèle entre l'incursion de la vie privée au moyen de dispositifs de balayage des ondes de téléphones cellulaires et d'incursions similaires éventuelles sur l'autoroute de l'information en raison des normes de sécurité inadéquates adoptées à l'égard des circuits téléphoniques actuels. Le Comité consultatif doit examiner les possibilités d'atteinte à la sécurité des données sur l'autoroute de l'information. Lorsque leur sécurité est en cause, l'entreprise de télécommunication doit informer les abonnés de la situation ou, à tout le moins, des lacunes que présentent les normes techniques et des risques de compromission.

### ***Bill Doskoch***

M. Bill Doskoch est un journaliste de Regina. Il fait partie de l'Association canadienne des journalistes et a participé à la création de son réseau de journalisme d'enquête assisté par ordinateur. Cependant, c'est à titre de citoyen qu'il fait sa présentation.

Il est essentiel d'en arriver à un équilibre entre, d'une part, la protection de la vie privée et, d'autre part, l'importance d'assurer la transparence du gouvernement et des dispositions de la *Charte des droits et libertés* qui garantissent la liberté d'expression. Il craint qu'on restreigne l'accès aux renseignements détenus par le gouvernement en vertu des lois protégeant la vie privée, mais cette restriction n'est pas nécessaire si l'on

dépersonnalise les renseignements. Néanmoins, M. Doskoch souhaite que l'on prévoie la diffusion des renseignements dans les cas où il y va de l'intérêt public.

Il propose en outre que les bases de données des médias qui sont commercialisées auprès du public et renferment des renseignements personnels soient assujetties à des pratiques équitables en matière d'information. Néanmoins, cette mesure soulève d'autres problèmes, par exemple, la vérification de l'impartialité et de l'exactitude de ces renseignements, ainsi que la nécessité éventuelle d'établir des liens hypertextuels entre les lettres au rédacteur et toute correction ou explication se rapportant à un article en particulier.

### ***Eridani Productions Ltd.***

M. Robin Rowland est un producteur de télévision et un écrivain indépendant qui donnera le premier cours de journalisme d'enquête assisté par ordinateur à l'université Ryerson Polytechnic, à Toronto.

Il exhorte le Comité consultatif à produire un rapport qui reconnaît la nécessité de protéger la vie privée tout en recommandant fortement la transparence du droit relatif aux documents. M. Rowland en est arrivé à cette opinion à la lumière de l'expérience du réseau de journalisme d'enquête assisté par ordinateur, qui fait appel à des bases de données et à des tableurs pour trouver les faits qui se cachent derrière l'histoire. Il cite en exemple des cas où cette méthode a été employée avec succès aux États-Unis, par exemple, pour mettre au jour des fraudes électorales ou découvrir les dossiers de chauffeurs d'autobus scolaires reconnus coupables de conduite dangereuse ou de conduite avec facultés affaiblies. Le livre intitulé *Investigative Reporters and Editors: 101 Computer Assisted Stories from the IRE Morgue* fait état de nombreuses autres histoires similaires. Il est essentiel que le public et plus particulièrement les médias aient accès aux renseignements du gouvernement. C'est pourquoi M. Rowland se préoccupe du fait que les mesures de protection de la vie privée puissent servir à limiter l'accès à un volume considérable d'enregistrements, même si l'on pourrait dans la plupart des cas supprimer les renseignements personnels.

### ***Curtis E.A. Karnow***

M. Curtis E.A. Karnow est membre du cabinet Landels, Ripley & Diamond, de la Californie. Cet avocat est un spécialiste de la technologie informatique et des questions juridiques connexes. Il présente des articles qu'il a publiés dans diverses revues spécialisées ainsi que le texte d'une allocution qu'il a prononcée à Londres et dans laquelle il fait allusion à la nature planétaire de la question.

À son avis, les renseignements personnels concernant un particulier qui peut être identifié lui appartiennent, sous réserve d'exceptions très précises, par exemple, les médias ne doivent pas se voir interdire l'accès à des renseignements en raison du principe du droit de propriété si ces derniers sont dépersonnalisés.

Il souligne le caractère fondamental du principe voulant que les données recueillies par une entité pour une fin déterminée ne doivent pas être utilisées à une autre fin ni par une autre entité en l'absence de consentement explicite.

Par ailleurs, M. Kamow est très favorable au concept selon lequel c'est le gouvernement fédéral qui doit légiférer au Canada, notamment en ce qui touche la garantie absolue de la vie privée, puisque ce droit est à la fois de nature nationale et internationale. Cependant, il signale que les dispositions législatives détaillées seront dépassées avant même qu'elles puissent entrer en vigueur. La législation doit plutôt mettre l'accent sur des propositions telles que la définition de la vie privée et du droit de propriété sur les données en tant que concepts fondamentaux. De plus, le gouvernement doit protéger le droit à la vie privée en vertu de la *Charte*.

D'après M. Kamow, ni le gouvernement ni aucun autre groupe ne peut concevoir une autoroute de l'information, parce que celle-ci est en pleine évolution. Le gouvernement peut uniquement mettre en place les conditions appropriées, notamment la liberté d'expression, l'accès à des mécanismes de chiffrement puissants, l'abolition des restrictions portant sur l'innovation et une tribune offrant un mécanisme de recours aux personnes ou aux organisations lésées sur l'autoroute de l'information. De plus, comme le monde électronique ne se limite pas à une province, un État ou un pays, il est inutile que le gouvernement tente de restreindre la diffusion de l'information au Canada ou vers l'étranger. En effet, les progrès technologiques accomplis ailleurs dans le monde auraient préséance sur toute démarche législative. En ce qui touche le chiffrement, le gouvernement doit permettre et encourager la pleine accessibilité à des logiciels de chiffrement puissants sans imposer quelque restriction que ce soit sur leur importation ou leur exportation.

### **Veronica Lacey**

M<sup>me</sup> Lacey est la présidente du groupe d'étude du Comité consultatif sur l'autoroute de l'information qui est chargé de l'apprentissage et de la formation.

Elle s'inquiète des nombreux types d'incursions dans la vie privée que peuvent entraîner l'utilisation des dossiers d'études et l'accès à ces dossiers sans autorisation. À son avis, les dossiers d'apprentissage, les libertés des étudiants, le suivi des particuliers, les didacticiels multimédias, les dossiers

transactionnels, la formation des enseignants, la fraude ainsi que la collaboration entre les gouvernements fédéral et provinciaux méritent tous qu'on y porte une attention particulière. Il faut en arriver à un équilibre entre, d'une part, l'utilisation et l'accès qui sont essentiels à la saine administration des programmes d'enseignement et, d'autre part, l'utilisation et l'accès qui peuvent porter atteinte au droit à la vie privée légitime d'un particulier.

#### **Propositions et recommandations précises**

- Il faut chiffrer les dossiers d'apprentissage et les partager uniquement après avoir obtenu un consentement. De plus, il faut se prémunir contre la création d'enregistrements de la naissance à la mort.
- Les dossiers d'apprentissage et de formation transmis sur l'autoroute de l'information doivent être chiffrés.
- Les dossiers transactionnels relatifs à l'apprentissage et à la formation doivent demeurer dépersonnalisés et seuls les intervenants des réseaux d'enseignement et de formation doivent y avoir accès.
- La formation des enseignants doit sensibiliser ces derniers à la protection de la vie privée et englober un volet consacré à cet aspect.
- Les gouvernements fédéral et provinciaux devront entreprendre des discussions en vue de déterminer la meilleure façon de protéger sur l'autoroute de l'information les données de nature délicate concernant l'apprentissage et la formation.
- Les représentants des milieux de l'apprentissage et de la formation doivent se joindre au comité de la CSA chargé de la vie privée pour faire valoir la perspective de l'enseignement aux fins de l'élaboration et de la mise en oeuvre de normes sur la protection de la vie privée.

#### ***Detective Superintendent Ken Grange***

M. Ken Grange, Detective Superintendent au sein du service de police métropolitain de New Scotland Yard, à Londres, en Angleterre, s'est intéressé aux aspects de la protection de la vie privée se rapportant aux activités policières.

Sa présentation vise à exprimer le point de vue personnel d'un agent de police actif dans les domaines de la protection des données et de la recherche théorique. Il met l'accent sur les problèmes liés à la *Data Protection Act*, adoptée par le Royaume-Uni en 1994 ainsi que sur les lacunes qu'elle présente. À son avis, il serait utile de se pencher sur ces

éléments au moment de déterminer l'orientation à prendre au Canada. De plus, il propose l'adoption de mesures plus fermes pour protéger la vie privée et la sécurité des renseignements personnels, au moyen d'une combinaison de lois, de codes volontaires, de solutions technologiques et d'initiatives de sensibilisation.

La *Data Protection Act* pose à son avis plusieurs problèmes d'ordre pratique et opérationnel. En vertu de la loi britannique, le processus d'enregistrement des données est beaucoup trop bureaucratique, la vaste majorité des intervenants n'en tiennent pas compte et le bureau du registraire de la protection des données doit y consacrer beaucoup trop de temps. C'est pourquoi tout enregistrement de données doit être limité aux données considérées comme étant de nature délicate, ce qui permettrait au bureau de traiter uniquement les plaintes concernant ce type de données et d'autres cas de violation plus graves de la loi.

M. Grange considère que le droit d'accès par les particuliers donne lieu à de graves abus. Ainsi, 99 p. 100 de toutes les demandes d'accès présentées au service de police métropolitain portent sur des cas où un employeur a obligé ses employés ou des employés potentiels à donner leur consentement. Cette pratique va à l'encontre des principes de la loi et contourne les mécanismes d'application de la *Rehabilitation of Offenders Act*.

Le principe de consentement à la collecte et à la divulgation pose parfois des problèmes, car la loi britannique ne renferme aucune disposition prévoyant des exemptions dans l'intérêt public lorsque des données recueillies pour un usage servent à un autre. Il s'agit là d'un problème particulier en ce qui touche la divulgation aux organismes de soutien des victimes, aux autorités locales, aux services sociaux, etc., lorsqu'un crime a été commis. En outre, de nombreuses autres organisations effectuent des enquêtes et peuvent avoir des raisons légitimes d'obtenir des renseignements personnels. Or, à une époque où les ressources affectées aux services de police sont très limitées, cet état de choses pourrait rendre l'industrie inapte à agir de manière efficace dans les cas de fraude.

Le principe de la protection de la sécurité des données est plutôt vague dans la loi britannique. Ainsi, le problème du «piratage» n'est pas mentionné. On ne s'est pas attaqué à ce problème avant l'adoption en 1990 de la *Computer Misuse Act*. Par conséquent, en raison de l'évolution rapide de l'autoroute de l'information, les dispositions législatives portant sur la technologie proprement dite ne sont pas des outils efficaces lorsqu'il s'agit de régler des problèmes à court terme.

## **Approches**

- I. **Toute loi doit avoir pour objet d'établir des mesures uniformes à l'échelle du Canada, c'est-à-dire l'adoption de normes communes, car il s'agit là d'un problème constant au sein de la Communauté européenne. La loi doit viser à protéger les données et non la technologie ni l'infrastructure du réseau. Autrement, non seulement la loi ne fonctionnerait pas et elle serait inacceptable aux yeux des secteurs public et privé, mais aussi elle désavantagerait le Canada sur le plan commercial dans un monde de concurrence. De plus, une telle loi pourrait atténuer les avantages évidents que la technologie apporte au public.**
- II. **Une démarche axée sur des codes et des normes volontaires offrirait aux groupes sectoriels la possibilité de prendre appui sur les grands principes énoncés dans la loi, comme dans le cas de la loi du Royaume-Uni. En vertu de la loi britannique, le secteur des politiques harmonise ses codes internes avec les règles du registraire des données et, s'il contrevient à ces codes, il est passible de sanctions par le registraire.**
- III. **M. Grange accorde beaucoup de mérite aux solutions technologiques. Même si une loi ne doit pas aller à l'encontre de la technologie dans le contexte de la protection de la vie privée, la technologie peut contribuer considérablement à cette protection. C'est pourquoi il faut persuader l'industrie de la technologie de mettre au point des solutions techniques aux problèmes touchant la protection de la vie privée et d'accroître ainsi la viabilité commerciale des réseaux.**
- IV. **Au Royaume-Uni, les particuliers sont considérés comme étant très ambivalents face aux questions de la protection des données, à moins qu'ils soient directement touchés par une contravention à cet égard ou par l'inexactitude de renseignements les concernant. M. Grange en donne pour preuve le faible taux des demandes d'accès à des renseignements personnels. Il reconnaît néanmoins que la sensibilisation est un domaine qui peut avoir une grande incidence, peut-être même conduire à l'intégration de la protection de la vie privée dans une forme de charte des clients ou des citoyens.**

## **Réponses aux questions**

2. **D'après M. Grange, il est nécessaire d'adopter des mesures plus fermes, mais elles doivent être à la fois réalistes et réalisables. L'expérience britannique indique bien selon lui ce qu'il faut faire et ce qu'il ne faut pas faire. Il considère que la démarche idéale**

consiste à combiner les quatre approches (loi, codes volontaires, solutions technologiques et sensibilisation).

**Proposition et recommandation précise**

Toute loi doit proscrire le recours à un consentement forcé pour obtenir l'accès à des renseignements personnels concernant un particulier.

**ASSOCIATION CANADIENNE DE NORMALISATION (CSA)  
PROJET DE CODE MODÈLE SUR LA PROTECTION DES  
RENSEIGNEMENTS PERSONNELS**

**LES PRINCIPES EN BREF**

---

**1. Responsabilité**

Un organisme est responsable des renseignements personnels qui relèvent de lui et devra désigner une personne qui s'assurera que les principes énoncés ci-dessous y sont respectés.

**2. Détermination des finalités**

Les finalités pour lesquelles des renseignements personnels sont recueillis doivent avoir été déterminées par l'organisme et ce, préalablement ou au moment de la collecte.

**3. Consentement**

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

**4. Limitation de la collecte**

L'organisme ne peut recueillir que les renseignements personnels nécessaires aux fins déterminées et doit procéder par des moyens licites et honnêtes.

**5. Limitation de l'utilisation, de la communication et de la conservation**

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

**6. Exactitude**

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

## **7. Mesures de sécurité**

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

## **8. Transparence**

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

## **9. Accès aux renseignements personnels**

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

## **10. Possibilité de porter plainte contre le non-respect des principes**

Toute personne doit être en mesure d'éprouver le respect par un organisme des principes énoncés ci-dessus en s'adressant à la personne désignée comme responsable.

