

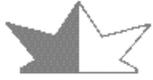
Le Groupe de travail
sur l'avenir du
secteur des services
financiers canadien

La protection des renseignements personnels dans le secteur des services financiers au Canada

par
Richard C. Owens
Smith Lyons

Septembre 1998

Document de recherche préparé pour le Groupe de travail
sur l'avenir du secteur des services financiers canadien



Le Groupe de travail
sur l'avenir du
secteur des services
financiers canadien

La protection des renseignements personnels dans le secteur des services financiers au Canada

par
Richard C. Owens
Smith Lyons

Septembre 1998

Document de recherche préparé pour le Groupe de travail
sur l'avenir du secteur des services financiers canadien

**Les points de vue exprimés dans ces documents
de recherche n'engagent que leurs auteurs;
ils ne reflètent pas nécessairement l'opinion du Groupe de
travail sur l'avenir du secteur des services financiers canadien.
Le chercheur a produit en anglais la version originale
du document, et l'auteur n'a pas
été en mesure d'en réviser la traduction.**

Numéro de catalogue : BT22-61/3-1998F-11
ISBN 0-662-83162-4

Pour obtenir d'autres exemplaires de ce document,
veuillez vous adresser au :
Centre de distribution
Ministère des Finances
300, avenue Laurier ouest
Ottawa K1A 0G5

Téléphone : (613) 995-2855
Télécopie : (613) 996-0518

Également disponible sur Internet à l'adresse
<http://groupetravailsservfin.fin.gc.ca>

This publication is also available in English.



Avant-propos

Il me fait plaisir de présenter cette étude au Groupe de travail sur l'avenir du secteur des services financiers au Canada.

Le secteur des services financiers canadiens évolue à un rythme étourdissant. Ces transformations touchent plusieurs éléments – la concurrence, la structure, le régime de propriété et la technologie. Toutes ces tendances ont une incidence sur la protection des renseignements personnels.

Je remercie le Groupe de travail de m'avoir permis d'exposer mes idées sur cette question d'actualité et j'espère que mes propos sauront aider les membres à s'acquitter de leur mandat.

Cette étude a été réalisée en grande partie avant le 23 février 1998. Les renseignements qu'on y retrouve reflètent donc la situation à cette date.

Juin 1998

Remerciements

J'assume l'entière responsabilité de la structure et du contenu de cette étude ainsi que de ses conclusions. Toutefois, il me faut préciser que cet ouvrage est le fruit d'un travail d'équipe et, en particulier, qu'il aurait été impossible à réaliser sans la collaboration soutenue de certains de mes collègues de travail chez Smith Lyons. Je me dois tout d'abord de souligner les efforts de M. Thomas Onyshko, associé de Smith Lyons, et les nombreuses heures qu'il a consacrées à ce document. Les connaissances spécialisées de Tom ont été très utiles à la réalisation de cette étude, tant par les entretiens qu'il m'a été donné d'avoir avec lui que par ses apports aux travaux de recherche et à l'étape de la rédaction. Tom a lui-même rédigé une grande partie de la version préliminaire de ce document et a aussi dirigé l'étude lorsque mes dossiers juridiques exigeaient ma présence. M. Neil Guthrie, un autre associé de Smith Lyons, a également rédigé des parties importantes de cette étude et participé aux travaux de recherche, tout comme M. William Schnurr, étudiant en droit. D'autres étudiants en droit, notamment MM. Bryce Kraeker, Simon Crawford et Ned Djordjevic, ont aussi prêté leur concours à la préparation de ce document et aux travaux de recherche. Nombre d'entre eux, Tom surtout, ont participé à la correction des textes et à la préparation des notes de bas de page. Les étudiants nous ont aussi prêté main-forte au chapitre de la correction d'épreuves. M^{me} Tammie Savoie a participé aux travaux de recherche et à la préparation des textes. Je dois également cette réussite à mon adjointe, M^{me} Rosemary Haight, dont les efforts sans cesse renouvelés et le souci du détail m'ont permis de venir à bout de ce projet, comme de tant d'autres au cours des trois dernières années. Je sais gré à tous ces gens de leur professionnalisme, de leur énergie et de leur grande lumière. Mais ces remerciements ne seraient pas complets sans mentionner la contribution et le soutien de nombreux représentants d'institutions financières et de défenseurs des droits des consommateurs. M. Thomas Wright, ancien Commissaire à la protection des renseignements personnels de l'Ontario, nous a prodigué de fort utiles conseils pendant nos recherches. Il nous a fourni de la documentation et a mis son expérience et son savoir-faire à profit en annotant la version préliminaire de ce rapport. Je tiens aussi à souligner la contribution de MM. Fred Gorbert, H.H. MacKay et John Chant, ainsi que du personnel du Groupe de travail, qui nous ont fait part de remarques des plus pertinentes tout en participant à de nombreuses étapes de la préparation de ce document. Je remercie également M. Tom Smee, consultant chez Deloitte & Touche, de ses précieux conseils sur les subtilités de la technologie de l'information. Enfin, je tiens à témoigner toute ma gratitude à une personne qui a fait preuve d'une patience exemplaire à mon égard et m'a accordé un soutien moral et intellectuel inconditionnel : mon épouse adorée, Elizabeth Brubaker.

Table des matières

Sommaire

I. Introduction	17
Toile de fond de cette étude	17
Principes de base de cette étude	18
Droit à la vie privée et questions liées à la protection des renseignements personnels.....	19
Le principe du droit à la vie privée.....	19
Le fondement de la protection des renseignements personnels.....	21
L'informatisation des renseignements personnels	22
Problèmes relatifs à la protection des renseignements personnels.....	24
Évolution de la perception du droit à la vie privée dans le secteur des services financiers au Canada.....	27
Les années quatre-vingt : Premières démarches visant la mise en œuvre des principes adoptés par l'OCDE	27
Le début des années quatre-vingt-dix : Réforme des lois fédérales sur les institutions financières et des lois du Québec en matière de protection de la vie privée	29
La fin des années quatre-vingt-dix : le code de l'Association canadienne de normalisation, les réformes complémentaires des lois sur les institutions financières fédérales et les propositions pour une législation fédérale relative à la protection de la vie privée	33
Préoccupations du grand public à l'égard de la protection des renseignements personnels et plaintes afférentes.....	39
Sondages sur la protection des renseignements personnels	39
Sondage Ekos réalisé en 1992	39
Sondage Louis Harris/Equifax Canada Inc. réalisé en 1994	40
Sondage FNACQ/CDIP 1994	42
Plaintes au sujet d'institutions financières.....	43
Commission québécoise.....	43
L'Ombudsman bancaire canadien et les ombudsmans des banques.....	45
Associations sectorielles d'assureurs	47
Interprétation des données.....	47
Caractéristiques du secteur des services financiers au Canada	48

II. Mesures en vigueur en matière de protection des renseignements personnels.....	51
Introduction	51
Aperçu des mesures de protection des renseignements personnels en common law et dans le cadre des actions d'équité.....	51
Actions liées à l'intrusion	52
Actions liées à la divulgation ou à l'utilisation de renseignements personnels	54
Droit contractuel.....	57
Les carences de mesures fondées sur l'équité et la common law	61
L'exigence contractuelle implicite de confidentialité	62
<i>Tournier</i> et l'exigence implicite de confidentialité.....	62
Dispositions implicites et politiques relatives à la vie privée	67
Dispositions législatives visant les institutions financières et la protection des renseignements personnels	69
Lois fédérales sur les institutions financières	69
Pouvoir de réglementation en matière de renseignements sur les clients.....	70
Protection et exactitude des dossiers	71
Politiques de la direction en matière de protection des renseignements personnels	72
Restrictions concernant l'utilisation des renseignements personnels.....	72
Conservation et traitement des renseignements personnels des clients	73
Lois provinciales et questions connexes	74
La loi québécoise sur la protection des renseignements personnels dans le secteur privé...	79
Codes des associations industrielles.....	83
Association des banquiers canadiens	83
Association des compagnies de fiducie du Canada.....	90
Associations de l'industrie de l'assurance.....	90
Centrale des caisses de crédit du Canada	94
Observations concernant les codes des associations	95
III. Problèmes relatifs à la protection de la vie privée.....	98
Inquiétudes des consommateurs	98
Le partage et l'utilisation des renseignements personnels.....	98
Consentement implicite par opposition à consentement explicite	102
Méthodes de règlement des différends et transparence	103
Établissements non réglementés par la loi fédérale.....	106
Tendances et technologies nouvelles	106
Recoupement des données.....	106
Marketing ciblé et exploration de données.....	108
Cartes de valeur	110
Opérations bancaires sur Internet et logiciels de gestion de fonds au Canada	112
Échange de renseignements et prestation de services à l'échelle internationale	113

IV. Conventions internationales, directive UE et textes de loi à l'étranger comme au pays	115
Ententes et conventions internationales touchant le Canada.....	115
Directive de l'Union européenne	116
La démarche européenne en matière de lois sur la protection des renseignements personnels	116
Mise au point de la directive de l'Union européenne.....	118
Convention du Conseil de l'Europe	118
Avant-projet de directive UE	119
Harmonisation des lois sur la protection des données dans l'Union européenne ..	121
Aperçu de la directive UE	122
Protection « adéquate » et transfert de données vers des pays tiers en vertu de la directive UE.....	124
Protection « adéquate » et lois en vigueur dans les pays tiers	124
Protection « adéquate » et dispositions contractuelles	127
Législation de la vie privée au Royaume-Uni	129
Aperçu du <i>Data Protection Act 1984</i>	130
Amendements envisagés par suite de la directive UE.....	132
Loi québécoise sur la protection des données dans le secteur privé.....	133
Lois sur la confidentialité des données en Nouvelle-Zélande	135
Aperçu du <i>Privacy Act 1993</i> néo-zélandais.....	135
Justification pour l'élargissement de la confidentialité au secteur privé.....	139
Révision du <i>Privacy Act</i>	140
Évolution de la législation australienne	141
V. Protection de la vie privée, pouvoirs constitutionnels et collaboration entre le gouvernement fédéral et les provinces	145
Pouvoirs constitutionnels en matière de protection de la vie privée	145
Articles 91 et 92 de la <i>Loi constitutionnelle</i>	146
Pouvoirs fédéraux en matière de trafic et de commerce.....	147
Paix, ordre et bon gouvernement.....	148
Conclusion.....	151
Modèles pour une collaboration entre les instances fédérales et provinciales	153

VI. Réponses circonstanciées aux questions posées	159
1. Les lois canadiennes sur la protection de la vie privée qui régissent les prestataires de services financiers répondent-elles aux besoins des consommateurs de ces services? Dans l’affirmative, répond-on à ces besoins de manière uniforme à travers tout le secteur des services financiers, ou plutôt selon des modalités limitées à certains types de prestataires ou à certaines juridictions?.....	159
Adéquation de la protection existante	159
Homogénéité dans l’ensemble du secteur	160
Les possibilités d’améliorations	161
2. Dans quelle mesure l’avènement des nouvelles technologies ou l’internationalisation de la prestation des services financiers provoqueront-ils le besoin d’une protection accrue de la vie privée?	162
3. Dans quelle mesure faut-il personnaliser la réglementation en fonction du secteur des services financiers?	163
4. La directive UE, ou éventuellement n’importe quel texte de loi exigeant la réciprocité pour la protection de la vie privée, crée-t-elle le besoin d’une réglementation accrue dans ce domaine pour faciliter le flux transfrontières des données?	164
5. S’il devait s’avérer nécessaire de réglementer davantage la protection de la vie privée dans le secteur des services financiers, de quelle structure de réglementation devrait-on s’inspirer pour le contexte canadien?.....	165
Modèles de réglementation potentiels	165
Sélection du modèle approprié	167
6. Le Canada a-t-il des leçons à tirer des efforts déployés pour l’introduction d’un mécanisme de protection élargie dans un cadre multijuridictionnel?	169
7. Quels sont les risques que pourraient constituer, pour la protection de la vie privée, le phénomène de propriété réciproque entre institutions financières, ainsi que la prestation de différents services financiers par une même entité?	169
VII. Conclusions	172
Introduction	172
Intérêts en matière de confidentialité et besoin de réglementation	172
Codes de conduite pour la confidentialité	173
Imprimés types et renseignements sur l’état de santé.....	175
Agences d’évaluation du crédit et compagnies d’assurances.....	176
Implications de la directive UE	177
Tendances, technologies, et propriété réciproque	177
Annexe A	178
Table de jurisprudence	202
Bibliographie	207

Sommaire

Aperçu

Cette étude porte sur les inquiétudes que soulèvent la collecte et l'utilisation des renseignements personnels par les fournisseurs de services financiers. Il y est également question de nouvelles mesures à mettre en oeuvre, le cas échéant, pour assurer aux clients de ces établissements toute la confidentialité à laquelle ils ont droit. Ce mémoire est divisé en sept parties.

La Partie I présente le contexte global de la présente étude. On y traite de la protection des renseignements personnels d'un point de vue social et juridique ainsi que des divers problèmes liés à la collecte et à l'utilisation de ce genre de renseignements. Vient ensuite un bref aperçu de l'évolution de la protection des renseignements personnels par rapport aux institutions financières pendant les années quatre-vingt et quatre-vingt-dix. La Partie I se termine par un examen des diverses facettes du secteur des services financiers canadiens dont il faut tenir compte pour définir les nouvelles mesures à mettre en oeuvre pour assurer la protection des renseignements personnels.

La Partie II porte sur les mécanismes de protection des renseignements personnels actuellement en vigueur. Elle débute par un examen des dispositions de la common law et des mesures d'équité qui assurent, à certains égards, la protection des renseignements personnels, ainsi que des grandes lacunes de ces mesures. Elle traite ensuite de l'exigence implicite de confidentialité à laquelle sont tenus les banquiers, comme l'a statué un tribunal britannique dans l'affaire *Tournier c. National Provincial & Union Bank of England*. Nous examinons ensuite les mécanismes de protection des renseignements personnels adoptés par les gouvernements fédéral et provinciaux. Il sera question des dispositions législatives fédérales visant les institutions bancaires, les compagnies d'assurance, les sociétés de fiducie et les associations de caisses de crédit, ainsi que des lois provinciales visant les fournisseurs de services financiers, y compris les bureaux de crédit. Cette section de la Partie II traite aussi des dispositions de la *Loi sur la protection des renseignements personnels dans le secteur privé*, la première mesure législative de protection des renseignements personnels au Canada visant l'ensemble du secteur privé. Nous terminerons par un examen approfondi des politiques des associations d'institutions bancaires, de sociétés de fiducie et de compagnies d'assurance en matière de protection des renseignements personnels, ainsi que par un aperçu de celles que l'association des coopératives de crédit songe à adopter.

La Partie III porte sur les menaces à la protection des renseignements personnels. Elle commence par un examen des principales préoccupations des associations de consommateurs et des spécialistes en la matière, lesquelles ont essentiellement trait à la diffusion et à la consultation des renseignements personnels, au recours au consentement implicite (par opposition à explicite), aux mécanismes de résolution des différends et au fait que nombre de fournisseurs de services financiers ne sont assujettis à aucune loi fédérale. Nous poursuivons avec l'étude des technologies et des tendances commerciales ayant une incidence sur la protection des renseignements personnels, comme le recoupement des données, le marketing ciblé et l'exploration de données, les cartes à puce, les opérations bancaires sur Internet et les

logiciels de gestion de fonds, de même que l'échange de renseignements et la prestation de services financiers à l'échelle internationale.

La Partie IV porte sur les lois et les accords internationaux qui assurent la protection des renseignements personnels dans le cadre de certaines activités au pays et à l'étranger. Elle débute par un examen des conventions et des accords internationaux de protection des renseignements personnels dont le Canada est signataire. Elle se penche ensuite de façon plus détaillée sur la directive UE en la matière, notamment sur les restrictions relatives à la divulgation de renseignements personnels. Le reste de cette partie traite des lois sur la protection des renseignements personnels dans le secteur privé que l'on retrouve dans trois pays et de l'expérience d'un quatrième pays qui s'est refusé à adopter une loi en ce sens. Aux termes du *Data Protection Act*, qu'a adopté le Royaume-Uni en 1944, toute personne ou société détentrice de renseignements personnels est tenue de s'inscrire auprès d'un organisme central. La *Loi sur la protection des renseignements personnels dans le secteur privé*, qui a été adoptée au Québec, est un exemple de mécanisme qui ne comporte aucune exigence d'inscription mais stipule des mesures à prendre pour assurer la protection de ce genre de renseignements. Le *Privacy Act* de la Nouvelle-Zélande, adopté en 1993, impose l'observation d'exigences réglementaires qui s'appuient certaines politiques en la matière que l'on retrouve dans le secteur privé. Enfin, l'Australie nous fournit un exemple de juridiction qui a songé, puis a refusé, d'adopter des dispositions législatives visant à étendre les mécanismes de protection des renseignements personnels au secteur privé.

La Partie V examine les liens entre la Constitution du Canada et la protection des renseignements personnels. Elle porte sur les avantages de la rivalité fédérale-provinciale en matière de compétences relatives à la protection des renseignements personnels et conclut que ces pouvoirs sont probablement partagés par ces deux paliers de gouvernement. Elle se penche ensuite sur quelques modèles conceptuels et historiques de collaboration fédérale-provinciale susceptibles d'inspirer une nouvelle approche réglementaire commune en la matière.

La Partie VI répond en détail à sept questions précises qui ont été posées aux auteurs de la présente étude. Elle traite notamment de la pertinence des lois sur la protection des renseignements personnels qui régissent actuellement les institutions financières, de la nécessité de mettre en œuvre de nouvelles mesures de protection à la lumière des nouvelles technologies et des tendances des services financiers, de la mesure dans laquelle il est nécessaire d'adapter les règlements sur la protection des renseignements personnels au secteur des services financiers, de la mesure dans laquelle la directive UE et les autres mécanismes étrangers de même nature exigent la mise en place de nouveaux règlements en matière de protection des renseignements personnels compte tenu de leurs dispositions à cet égard, du modèle qui serait le plus approprié pour guider l'avènement de nouveaux règlements en la matière au Canada, des leçons qu'il est possible de tirer des démarches antérieures visant à mettre en œuvre des mécanismes de protection des renseignements personnels dans un cadre multijuridictionnel ainsi que des risques que pourraient constituer, pour la protection de la vie privée, le phénomène de propriété réciproque entre institutions financières et la prestation de services multiples par une même entité.

La Partie VII relate les conclusions des auteurs au sujet de la réglementation sur la protection des renseignements personnels par rapport aux fournisseurs des services financiers. Il y est, entre autres, question des intérêts relatifs à la protection des renseignements personnels et de la nécessité d'adopter de nouveaux règlements en la matière, des politiques en vigueur dans le secteur des services financiers, des formulaires qu'emploient couramment les fournisseurs de services financiers, de la diffusion, par les compagnies d'assurance, de renseignements personnels sur l'état de santé de leurs clients, de la réglementation des bureaux de crédit et des compagnies d'assurance, des conséquences de la directive UE, ainsi que des répercussions des nouvelles tendances et technologies, et de la propriété réciproque entre fournisseurs de services financiers.

Voici maintenant de brefs résumés des réponses offertes aux questions qui ont été posées aux auteurs de cette étude ainsi que des conclusions générales du présent mémoire. Le texte intégral desdites réponses et conclusions se trouve aux Parties VI et VII.

Résumé des réponses

- ***Les lois canadiennes sur la protection de la vie privée qui régissent les prestataires de services financiers répondent-elles aux besoins des consommateurs de ces services? Dans l'affirmative, répond-on à ces besoins de manière cohérente à travers tout le secteur des services financiers, ou plutôt selon des modalités limitées à certains types de prestataires ou à certaines juridictions?***

À l'heure actuelle, la loi qui régit les fournisseurs de services financiers à charte fédérale n'est pas très exhaustive, mais elle est étoffée par des dispositions de common law et les codes de déontologie dont se sont dotés certains de ces fournisseurs. La cohérence des mesures de protection des renseignements personnels varie quelque peu d'un établissement à l'autre et ce sont surtout les grandes institutions, plus précisément les grandes banques, qui assument la plus grande cohérence en la matière. En règle générale, la faible proportion de plaintes des consommateurs relativement à la protection des renseignements personnels et l'étendue des dispositions de common law, de l'équité et des codes portent à croire que les mesures de protection actuelles sont adéquates. À l'extérieur du Québec, les lois sur la protection des renseignements personnels ne sont pas aussi cohérentes que les experts le souhaiteraient, mais les coûts associés à l'imposition de nouvelles exigences en la matière doivent être évalués en fonction de leurs retombées probables. Il y aurait bien des façons d'améliorer les codes existants afin d'atteindre un niveau idéal de protection des renseignements personnels. Enfin, il faut tenir compte du fait que la réglementation fédérale ne s'applique qu'aux établissements à charte fédérale et qu'une grande partie du secteur des services financiers n'est pratiquement assujéti à aucune mesure de protection des renseignements personnels, sauf au Québec.

- ***Dans quelle mesure l'avènement des nouvelles technologies ou l'internationalisation de la prestation des services financiers provoqueront-ils le besoin d'une protection accrue de la vie privée?***

Les nouvelles technologies bancaires (comme les transactions par l'entremise d'ordinateurs personnels et du réseau Internet) peuvent soulever des inquiétudes relatives à la sécurité des données transmises par les réseaux informatiques. Cependant, comme les fournisseurs de services financiers prennent en général des moyens très sophistiqués pour assurer la protection de ces données, il n'est pas nécessaire d'adopter d'autres règlements en la matière. D'ici quelques années, on peut s'attendre à ce que les institutions financières pratiquent « l'exploration des données » de façon plus soutenue à des fins de marketing. Afin de s'assurer de conserver un certain contrôle des renseignements personnels, les gens devraient être autorisés à faire rayer leur nom de toute liste nominative dressée dans le cadre d'activités de marketing. La mondialisation du secteur des services financiers peut également soulever des inquiétudes relatives à la protection des renseignements personnels s'il devenait nécessaire d'adhérer aux normes plus strictes dont s'est dotée l'Union européenne ou si les institutions financières qui exercent des activités commerciales au Canada se mettaient à vouloir traiter leurs données à l'étranger, dans des pays où les lois en la matière sont moins exigeantes. Enfin, on doit également songer aux conséquences de la possibilité qu'une institution financière étrangère offre ses services aux Canadiens par le réseau Internet sans tenir compte de nos dispositions en matière de protection des renseignements personnels. Toutefois, il existe si peu de mesures réglementaires à cet effet qu'il est probable que la règle de *caveat emptor* continuera de s'appliquer.

- ***Dans quelle mesure faut-il personnaliser la réglementation en fonction du secteur des services financiers?***

À vrai dire, il vaudrait mieux se demander *s'il est opportun* de personnaliser la réglementation en fonction du secteur des services financiers. En règle générale, les enjeux relatifs à la collecte et au traitement des renseignements personnels sont les mêmes pour les institutions financières que pour toute autre entreprise. Les tenants de la réglementation personnalisée pourront faire valoir que les institutions financières utilisent des données qui ont trait à l'état de santé et à la situation financière de leurs clients, deux catégories de renseignements qui suscitent le plus d'inquiétudes en matière de confidentialité. Par ailleurs, puisqu'il s'agit justement de renseignements de nature délicate, ils font déjà l'objet de dispositions législatives exhaustives qui rendent inopportune toute nouvelle réglementation.

- ***La directive UE, ou tout autre texte de loi éventuel exigeant la réciprocité pour la protection de la vie privée, crée-t-elle le besoin d'une réglementation accrue dans ce domaine pour faciliter le flux transfrontières des données?***

L'article 25 de la directive UE stipule que le transfert vers un pays tiers de données à caractère personnel faisant l'objet d'un traitement ne peut avoir lieu que si le niveau de protection offert par le pays tiers est « adéquat » au regard des circonstances relatives à un transfert ou à une catégorie de transferts de données. Toutefois, l'article 26 de cette même

directive permet de transférer, dans des circonstances précises dont la liste se trouve dans ce même document, des données à un pays tiers qui ne s'est pas doté de mesures de protection « adéquates ». Les organismes chargés de l'élaboration des politiques au Canada auront de la difficulté à formuler un dosage de réglementation nationale, de dispositions législatives et de codes de déontologie de l'industrie capable de satisfaire aux exigences de l'article 25. En outre, la directive UE s'appuie largement sur les traditions sociales et juridiques de l'Europe, lesquelles ne font pas nécessairement bon ménage avec les traditions canadiennes. Par conséquent, le Canada aurait probablement intérêt à se doter d'une politique qui ne soit pas une imitation des modèles et des objectifs européens en matière de protection des renseignements personnels. Quoiqu'il en soit, nombre de transferts de renseignements personnels pourront être effectués entre l'Europe et le Canada après l'entrée en vigueur de la directive UE en se fondant sur des mesures contractuelles de protection des renseignements personnels.

- ***S'il devait s'avérer nécessaire de réglementer davantage la protection de la vie privée dans le secteur des services financiers, de quelle structure de réglementation devrait-on s'inspirer pour le contexte canadien?***

Il existe plusieurs modèles de réglementation. Par exemple, le Royaume-Uni s'est doté d'un système qui exige que l'on s'enregistre avant de traiter des renseignements personnels. Le Québec a adopté une loi qui ne comporte pas d'exigence en matière d'enregistrement mais qui comporte des dispositions détaillées en matière de protection des renseignements personnels dans le secteur privé. La Nouvelle-Zélande offre un exemple de loi qui énonce des principes généraux sur la protection des renseignements personnels, lesquels peuvent être appliqués par le biais des codes de déontologie en vigueur dans le secteur privé. Le modèle (ou l'amalgame des éléments tirés de divers modèles) retenu devrait tenir compte de divers facteurs, dont l'ampleur des coûts, de la protection et des examens indépendants que visent les organismes chargés de l'élaboration des politiques.

En choisissant un modèle de réglementation adéquat pour le Canada, on peut présumer qu'un mécanisme à grande échelle et aux modalités d'application plutôt strictes qui se traduirait par l'obligation d'engager des dépenses considérables serait moins opportun qu'un régime plus souple et moins lourd. L'adoption d'une approche moins rigide va d'ailleurs dans le sens des conclusions de la présente étude au sujet de la nécessité de mettre en œuvre des règlements sur la protection des renseignements personnels dans le secteur des services financiers au Canada. Compte tenu du nombre peu élevé de plaintes que l'on reçoit à cet égard et de la nature des règlements de protection que l'on retrouve aujourd'hui dans le secteur des services financiers, la situation n'appelle, du moins pour l'instant, aucune modification. Il suffirait probablement d'adopter un système qui permettrait d'élaborer des règlements adaptés à l'industrie. En gros, l'approche d'autoréglementation en vigueur au Canada a donné de bons résultats et peut servir de modèle dans l'avenir.

Si nous décidions d'adopter des mesures législatives plus rigides en matière de protection des renseignements personnels, il serait préférable de s'inspirer de l'approche privilégiée par la Nouvelle-Zélande. Les principes de protection des renseignements personnels devraient être énoncés dans la loi. Ces principes pourraient alors être mis en œuvre par l'entremise de codes dont se doterait l'industrie, lesquels devraient être approuvés, plutôt que par le biais de la loi elle-même. Cette approche permettrait de s'assurer que les codes de l'industrie seraient conformes aux exigences, faisant ainsi échec à toute mesure visant à satisfaire ses propres intérêts. En outre, nous estimons que le système actuel de surveillance de l'information est adéquat et qu'il devrait faire partie intégrante d'un tel système. L'Ombudsman bancaire canadien devrait être chargé d'examiner, à titre de tierce partie indépendante, les plaintes que les consommateurs adressent aux banques. D'autres industries devraient être invitées à adopter des mesures de résolution des différends qui permettraient de faire appel à un médiateur ou à un arbitre indépendant pour trouver des solutions aux problèmes qui ne peuvent être réglés à l'interne par les institutions.

- ***Le Canada a-t-il des leçons à tirer des efforts déployés pour l'introduction d'un mécanisme de protection élargie dans un cadre multijuridictionnel?***

Les résultats de la mise en œuvre de la directive EU démontrent que l'application d'une norme unique à plusieurs États exige que l'on fasse des compromis. Au Canada, il semble que la meilleure façon de procéder consisterait à élaborer des politiques de protection des renseignements personnels de concert avec les gouvernements provinciaux, en raison des limites que la Constitution impose au gouvernement fédéral à cet égard. Il se peut que d'importants problèmes surviennent dans le cas du Québec puisque cette province s'est déjà dotée d'une loi détaillée en la matière, laquelle ne ralliera peut-être pas les conditions avec lesquelles le gouvernement fédéral et les gouvernements des autres provinces doivent composer. Idéalement, toutes les provinces devraient offrir le même niveau de protection des renseignements personnels afin que les établissements qui possèdent des succursales partout au pays ne soient pas tenus d'adhérer à différentes normes.

- ***Quels sont les risques que pourraient constituer, pour la protection de la vie privée, le phénomène de propriété réciproque entre institutions financières, ainsi que la prestation de différents services financiers par une même entité?***

La propriété réciproque entre institutions financières ouvre la voie à la mise en commun de l'information entre les organismes qui mettent en marché divers genres de services financiers pour cibler plus précisément leurs clientèles. Cette capacité de partager l'information entre fournisseurs de services financiers pourrait se traduire par une amélioration des services et une diminution des coûts pour les consommateurs. Les questions relatives à la protection des renseignements personnels dans les différents paliers du secteur des services financiers sont, d'un point de vue physique, à peu près les mêmes. La séparation des services en entités juridiques distinctes n'a pas vraiment d'incidence sur la protection des renseignements personnels mais traduit plutôt une capacité accrue de réglementer, des facteurs de prudence ou, le plus souvent, l'efficacité des démarches qu'entreprennent les groupes de pression pour protéger leurs intérêts économiques. Par conséquent, le consentement implicite qu'appellent

les contrats avec les consommateurs en matière de transmission de renseignements personnels entre membres d'un groupe de sociétés est parfaitement acceptable. Des associations de consommateurs ont fait valoir que l'utilisation de renseignements personnels à des fins de marketing pourrait amener les consommateurs à se sentir forcés d'acheter des produits par souci de continuer d'entretenir de bons rapports avec leurs institutions financières. D'après nous, cette hypothèse n'a pas été suffisamment étayée pour être fondée.

Résumé des conclusions

- **Les intérêts en matière de protection des renseignements personnels et la nécessité d'adopter une réglementation :** L'ensemble des dispositions législatives, de la common law et des codes sur la protection des renseignements personnels auxquels sont présentement assujettis les fournisseurs de services financiers au Canada englobe les principes et les aspects convenant à un régime moderne de protection des renseignements personnels. Compte tenu du nombre relativement peu élevé de plaintes liées à la protection des renseignements personnels et au raffinement des meilleurs éléments du système en vigueur, une analyse de rentabilité ferait valoir les avantages qu'il y aurait à faire preuve de prudence quant aux modifications qui seront apportées à ce système. Si l'on jugeait opportun de renforcer les mesures de protection des renseignements personnels, il serait préférable de faire preuve de souplesse pour permettre au nouveau régime de s'adapter aux impératifs avec lesquels l'industrie doit composer. La protection des renseignements personnels n'est pas un enjeu qui touche uniquement le secteur des services financiers, bien que ce soit celui-ci qui soulève le plus d'inquiétudes de la part des consommateurs, compte tenu de la nature délicate des renseignements sur l'état de santé et la situation financière. En ce qui a trait aux mesures mises en œuvre pour protéger les renseignements personnels, on constate qu'il y a peu de différence entre les organismes à charte fédérale, les organismes régis par les gouvernements provinciaux et les fournisseurs de services financiers qui ne sont assujettis à aucune réglementation.
- **Les codes de protection des renseignements personnels :** Les codes de protection des renseignements personnels dont se sont dotés les associations d'institutions financières et leurs membres correspondent aux normes modernes en la matière. Il s'agit en général de documents fouillés qui accordent une grande importance à la protection des renseignements des clients. Toutefois, ces codes pourraient être améliorés en les enrichissant de dispositions plus précises relativement au consentement implicite, à la finalité de la collecte de l'information, aux circonstances dans lesquelles il est possible de divulguer des renseignements à des tiers et à celles dans lesquelles on pourra refuser aux clients le droit de consulter leurs dossiers personnels. Les codes de protection des renseignements personnels devraient permettre aux gens de faire rayer leur nom de toute liste constituée à des fins de marketing. Cette approche nous semble raisonnable, compte tenu du fait que les problèmes liés à cette pratique ne sont pas monnaie courante. Le public devrait pouvoir se procurer ces codes sans difficulté. La plupart des régimes de protection des renseignements personnels prévoient la possibilité de recourir à un médiateur ou à un arbitre indépendant pour résoudre les différends qui n'ont pu être réglés à l'interne. Dans le cas des banques, ce rôle est imparti à l'Ombudsman bancaire canadien. Les autres associations sectorielles devraient aussi se

nommer un ombudsman ou encore se doter de méthodes de médiation ou d'arbitrage qui permettraient de résoudre les différends compliqués. Les présentes observations sur les codes de protection des renseignements personnels ne veulent pas témoigner de carences significatives mais uniquement souligner les éléments de ces codes qui se prêteraient à certaines améliorations aux fins d'atteindre l'idéal en matière de protection des renseignements personnels. Ces codes constituent un point de départ raisonnable à l'élaboration d'un mécanisme d'autoréglementation dans le secteur des services financiers.

- **Les formulaires types et les renseignements médicaux :** L'industrie devrait se pencher sur le libellé des articles que l'on retrouve dans les formulaires types qu'utilisent les fournisseurs de services financiers. Dans certaines circonstances, les formulaires qui autorisent la collecte et la mise en commun de l'information sont parfois libellés en termes trop vagues. Les renseignements médicaux recueillis à des fins d'assurance ne devraient pas être utilisés pour prendre des décisions d'une autre nature, comme celles qui ont trait au crédit.
- **Les bureaux de crédit et les compagnies d'assurance :** Les bureaux de crédit soulèvent bien des inquiétudes en matière de protection des renseignements personnels. Les lois visant la production de rapports de solvabilité traitent également de ces établissements, mais elles devraient faire l'objet d'un examen visant à les rendre plus cohérentes et complètes. De plus, la mise en commun de renseignements médicaux par les assureurs, grâce au Bureau de renseignements médicaux, devrait être assujettie à une loi appropriée.
- **Les répercussions de la directive UE :** Nous aurions tort de nous appuyer totalement sur la directive UE aux fins de l'élaboration d'une politique nationale de protection des renseignements personnels au Canada. Les mesures actuellement en vigueur dans le secteur des services financiers pourraient être « adéquates » et répondre aux exigences de l'article 25 de la directive UE en matière de transfert de l'information, surtout si elles étaient sanctionnées par les projets de règlements qu'étudie présentement le gouvernement fédéral. Quoi qu'il en soit, il règne une grande incertitude quant aux mesures à prendre pour se conformer à l'article 25 et il serait préférable de faire preuve de prudence.
- **Les tendances, les technologies et la propriété réciproque :** Les technologies de pointe et les nouvelles tendances ne soulèvent pas vraiment de problèmes de protection des renseignements personnels appelant une solution réglementaire. L'utilisation accrue de « l'exploration de données » et les programmes de marketing direct nous amènent à conclure que les gens devraient avoir la possibilité de faire rayer leur nom de toute liste utilisée dans de tels programmes en faisant une demande à cet effet à leur institution financière. La propriété réciproque entre institutions financières pourrait donner lieu à l'utilisation, par des fournisseurs de services connexes, de renseignements personnels à des fins autres que celles pour lesquelles ils ont été recueillis à l'origine. Ces fins devraient être communiquées aux intéressés. Toutefois, la propriété réciproque ne pose pas un risque suffisamment important à la protection des renseignements personnels pour susciter une réaction autre que celle qui a déjà été suggérée relativement à l'utilisation des renseignements de nature médicale et à la possibilité de faire rayer son nom de toute liste dressée à des fins de marketing.

I. Introduction

La Partie I présente le contexte global de la présente étude. On y traite de la protection des renseignements personnels d'un point de vue social et juridique ainsi que des divers problèmes liés à la collecte et à l'utilisation de ce genre de renseignements. Vient ensuite un bref aperçu de l'évolution de la protection des renseignements personnels par rapport aux institutions financières pendant les années quatre-vingt et quatre-vingt-dix. La Partie I se termine par l'examen des diverses facettes du secteur des services financiers canadiens dont il faut tenir compte pour définir les nouvelles mesures à mettre en œuvre pour assurer la protection des renseignements personnels.

Toile de fond de cette étude

Cette étude sur la protection des renseignements personnels dans le secteur des services financiers a été commandée par le Groupe de travail sur l'avenir du secteur des services financiers au Canada, dit « le **Groupe** », à l'automne 1997. Entre autres éléments de notre mandat, nous devions répondre à des questions précises :

1. Les lois canadiennes sur la protection de la vie privée qui régissent les prestataires de services financiers répondent-elles aux besoins des consommateurs de ces services? Dans l'affirmative, répond-on à ces besoins de manière cohérente à travers tout le secteur des services financiers, ou plutôt selon des modalités limitées à certains types de prestataires ou à certaines juridictions?
2. Dans quelle mesure l'avènement des nouvelles technologies ou l'internationalisation de la prestation des services financiers provoqueront-ils le besoin d'une protection accrue de la vie privée?
3. Dans quelle mesure faut-il personnaliser la réglementation en fonction du secteur des services financiers?
4. La directive UE, ou n'importe quel texte éventuel de loi exigeant la réciprocité pour la protection de la vie privée, crée-t-elle le besoin d'une réglementation accrue dans ce domaine pour faciliter le flux transfrontières des données?
5. S'il devait s'avérer nécessaire de réglementer davantage la protection de la vie privée dans le secteur des services financiers, de quelle structure de réglementation devrait-on s'inspirer dans le contexte canadien?
6. Le Canada a-t-il des leçons à tirer des efforts déployés pour l'introduction d'un mécanisme de protection élargie dans un cadre multijuridictionnel?
7. Quels sont les risques que pourraient constituer, pour la protection de la vie privée, le phénomène de propriété réciproque entre institutions financières, ainsi que la prestation de différents services financiers par une même entité?

Principes de base de cette étude

Cette étude repose sur certains principes. Mentionnons tout d'abord qu'elle porte sur l'ensemble du secteur des services financiers. Cela englobe les institutions financières régies par le gouvernement fédéral comme les banques, les sociétés de fiducie, certaines sociétés d'assurance ainsi que des caisses de crédit. Ce secteur comprend également d'autres organismes assujettis, à divers degrés, à des règlements fédéraux et provinciaux, de même que des fournisseurs de services financiers qui ne font l'objet d'aucune réglementation. Le secteur des services financiers compte aujourd'hui une vaste gamme d'organismes. Certains de ces organismes sont des représentants bien connus des quatre grands piliers : les banques, les compagnies d'assurance, les courtiers en valeurs mobilières et les sociétés de fiducie. D'autres ne font l'objet de presque aucune mesure de réglementation. Les organismes non réglementés qui offrent des services aux consommateurs comprennent les sociétés commerciales qui exploitent des services de prêt garanti par des actifs et des programmes de rachat de comptes-clients, comme la Newcourt Credit, ou des entreprises privées de cartes de crédit, ou encore des fournisseurs de services financiers aux consommateurs. Nombre de ces entreprises appartiennent à des intérêts étrangers.

Deuxièmement, le « droit à la vie privée », tel que nous l'entendons ici, est un principe qui s'applique aux particuliers et non pas aux entreprises. Nos entretiens avec des représentants de fournisseurs de services financiers nous ont mené à la conclusion que les entreprises confondent le droit à la confidentialité, relevant davantage des données commerciales, et le droit à la vie privée. Une bonne partie des moyens et des précautions mis en place servent ces deux objectifs, mais la protection de ces deux catégories de renseignements repose sur des justifications théoriques différentes. Dans le cas des consommateurs, la justification s'appuie, en partie, sur le fait que la protection de la dignité personnelle embrasse le respect de la vie privée, alors que dans le cas des entreprises commerciales, on se soucie davantage d'assurer la protection de renseignements qui, s'ils étaient divulgués, pourraient servir les intérêts de la concurrence. Quoiqu'il en soit, cette étude ne porte que sur la protection des renseignements personnels.

Troisièmement, le droit à la vie privée est une valeur humaine importante que l'on ne doit pas sacrifier à la convenance des utilisateurs de données. En se fondant sur ce principe, cette étude cherche à voir dans quelle mesure la confidentialité peut être compromise par la prestation de services financiers et, de façon plus précise, les risques qu'encourent les consommateurs qui utilisent ces services. Nous examinons le fondement théorique du droit à la vie privée ainsi que des données empiriques sur les menaces à la protection des renseignements dans le secteur des services financiers. Nous examinons aussi certains mécanismes mis en œuvre à l'étranger, des recommandations tirées d'autres études ainsi que les tendances internationales en matière de réglementation des données. Nous examinons aussi toutes les lois en vigueur en matière de protection des renseignements personnels dans le cadre de la prestation de services financiers. Nous nous sommes efforcés d'approfondir la question dans la mesure du possible, tout en respectant les modalités énoncées au début de l'étude, et de formuler des conclusions s'appuyant sur une évaluation objective du problème.

Droit à la vie privée et questions liées à la protection des renseignements personnels

Le principe du droit à la vie privée

En 1890, deux avocats de Boston, Samuel D. Warren et Louis D. Brandeis, signaient un article historique dans une revue juridique. Celui-ci portait sur le droit à la vie privée dans les actions fondées sur un délit.¹ Ce faisant, ils avaient, sans le savoir, formulé ce qui allait devenir une des définitions les plus populaires du droit à la vie privée, c'est-à-dire « le droit d'être laissé en paix ». Les deux hommes se souciaient alors bien davantage d'assurer la protection des particuliers contre la presse qui s'immisciait de plus en plus dans la vie privée des gens, ne reculant devant rien pour relater le déroulement d'événements privés et mettant à profit la nouvelle technologie de la photographie en noir et blanc « instantanée ».

La conception qu'avaient Warren et Brandeis du droit à la vie privée découlait de l'analyse de la loi traditionnelle sur la propriété, laquelle laissait entendre qu'il était du devoir de toute société de respecter certaines limites fondées sur la propriété, dont l'inviolabilité du domicile. Cette approche convenait probablement fort bien à la société de la fin des années 1800, mais elle ne répond plus aux besoins de l'ère moderne, qui met de plus en plus l'accent sur l'importance et le pouvoir économique de l'information.

La définition de « vie privée » la plus généralement acceptée de nos jours est essentiellement axée sur la protection des renseignements personnels. Dans son livre *Privacy and Freedom*, Alan F. Westin a défini la vie privée comme « le droit d'une personne, d'un groupe de personnes ou d'un établissement de choisir quand, comment et dans quelle mesure les renseignements les concernant peuvent être divulgués »². La définition de Westin est fréquemment citée dans les ouvrages didactiques et les décisions des tribunaux.³ Elle offre une conception suffisamment souple de la vie privée qui dépend, du moins en partie, des préférences de l'individu.⁴ Bien que la définition de Westin constitue un bon point de départ, elle n'accorde pas assez d'importance au traitement des renseignements personnels après leur divulgation initiale. En effet, la protection des renseignements personnels s'entend de la nécessité d'informer une personne

¹ S.D. Warren et L.D. Brandeis, « The Right to Privacy » (1890) 4 *Harvard Law Review* 193. Pour une critique de l'article de Warren et Brandeis, voir : W.L. Prosser, « Privacy » (1960) 48 *California Law Review* 383.

² A.F. Westin, *Privacy and Freedom* (New York, Atheneum, 1967), p. 7.

³ Voir, par exemple : P. Burns, « The Law and Privacy: The Canadian Experience » (1976) 54 *Canadian Bar Review*, p. 5 et M. Rankin, « Privacy and Technology: A Canadian Perspective » (1984) 22 *Alberta Law Review* 323, p. 325. Voir aussi : *La Reine c. Duarte* (1990) 65 D.L.R. (4th) 240 (S.C.C), p. 252, et *United States Department of Justice c. Reporters Committee for Freedom of the Press*, 489 U.S. 749 (1989), p. 763.

⁴ Comme le suggère un rapport pour la commission ontarienne sur la liberté de l'information et le droit à la vie privée, la vie privée s'entend d'un équilibre entre la fermeture et la transparence, et le droit à la vie privée s'entend du droit de la personne à déterminer les modalités de cet équilibre. Voir : *Privacy and Personal Data Protection: Research Publication No. 15*, Ontario, Commission on Freedom of Information and Individual Privacy, (mars 1980), p. 13. Toutefois, la capacité d'une personne à gérer l'information devrait avoir certaines limites. Parfois, le droit à la vie privée doit céder le pas aux intérêts de la société.

lorsqu'on prévoit colliger et utiliser des renseignements personnels la concernant à des fins susceptibles de modifier ses rapports avec autrui. En définitive, la protection des renseignements personnels est une mesure qui permet de calibrer nos rapports et de fixer des limites quant à l'utilisation légitime des renseignements qui nous concernent.

De nos jours, nous estimons que les renseignements personnels d'un individu lui appartiennent en propre; que c'est là une des composantes essentielles du droit à la vie privée. Toutefois, les renseignements personnels ne sont pas des biens tangibles, d'où la difficulté d'en faire l'objet d'articles sur les droits de propriété.⁵ Alors que la valeur des biens tangibles tient à ce que leurs propriétaires puissent les soustraire aux autres personnes, un simple renseignement peut appartenir à plusieurs parties en même temps sans que sa valeur n'en souffre. En outre, le bien commun nécessite la libre circulation de certains types de renseignements personnels. En fait, il arrive parfois que des renseignements personnels soient aussi importants pour un tiers que pour la personne concernée. Par exemple, mon nom et mon adresse sont des renseignements qui présentent une certaine mesure de confidentialité, mais s'ils n'étaient pas connus, personne ne pourrait venir me remettre ce qui m'est dû ou communiquer avec moi au besoin. Par contre, mes titres de propriétés et intérêts sont des renseignements à circulation plus restreinte. Je pourrais, par exemple, vouloir éviter que ma femme, une environmentaliste, apprenne que je possède des intérêts considérables dans une usine de pâtes et papier (purement hypothétique), alors que je n'aurais évidemment aucun intérêt à dissimuler ce renseignement à mon comptable. Il y a également une catégorie très vaste de renseignements personnels qui sont en même temps de type institutionnel.

La vie privée est un concept qui comporte bien des volets que l'on ne doit pas confondre. La confidentialité peut revêtir plusieurs définitions selon le contexte qui prévaut. Par exemple, aux États-Unis, le droit constitutionnel à la vie privée constitue le fondement du droit à l'avortement.⁶ Par ailleurs, on s'est beaucoup penché sur la notion de l'utilisation des renseignements personnels par les gouvernements, et sur la menace que cela comporte pour les libertés individuelles. La confidentialité n'est pas un concept unique mais bien un regroupement de plusieurs concepts et toute analyse rigoureuse se doit de préciser quel genre de confidentialité elle vise. Dans notre cas, il sera question de questions liées à la protection des renseignements personnels dans un secteur donné (les fournisseurs de services financiers) et dans une région géographique précise (le Canada).

⁵ Voir, de façon générale : R.J. Roberts, « Is Information Property? » (1987) *Intellectual Property Journal* 209 et R.G. Hammond, « Quantum Physics, Econometric Models and Property Rights to Information » (1981) *27 Revue de droit de McGill* 47.

⁶ Pour des exemples des premières décisions de la Cour Suprême des États-Unis reconnaissant le droit constitutionnel à la vie privée, lequel protégeait la capacité de prendre certaines décisions personnelles sans l'intervention de l'État, voir : *Griswold c. Connecticut*, 381 U.S. 479 (1965), *Eisenstadt c. Baird*, 405 U.S. 438 (1972) et *Roe c. Wade*, 410 U.S. 113 (1973). Dans l'affaire *Roe c. Wade*, le tribunal a statué que le droit à la vie privée constituait un fondement au droit à l'avortement; la portée de ce jugement a été limitée par d'autres décisions plus récentes de la Cour suprême des États-Unis, mais celles-ci ne l'ont pas invalidé. Pour un aperçu de la loi constitutionnelle des États-Unis en matière de droit à la vie privée, voir par exemple : Ken Gormley, « One Hundred Years of Privacy » (1992) *Wisconsin Law Review* 1335.

Le fondement de la protection des renseignements personnels

Il y a bien des raisons pour lesquelles les renseignements personnels doivent faire l'objet de mécanismes de protection officiels. Plusieurs auteurs ont avancé que la protection des renseignements personnels est nécessaire à l'épanouissement de l'individu. L'intimité laisse à l'individu la latitude physique et intellectuelle dont il a besoin pour faire des tentatives, apprendre et croître.⁷ D'autres font valoir que l'intimité est un élément prépondérant des rapports personnels soutenus, comme ceux que l'on entretient avec son conjoint ou ses proches.⁸ Des études psychologiques ont démontré les bienfaits du temps passé hors du cadre des responsabilités professionnelles et à l'écart des rôles que nous impose la société.⁹ En outre, la société et l'État reconnaissent l'importance du droit à la vie privée. L'intimité est le fondement d'une citoyenneté autonome, capable d'évaluer les actes de ses gouvernements, ce qui est la pierre angulaire de toute véritable démocratie.¹⁰ Le droit à la vie privée permet aux gens de nourrir et de faire valoir des points de vue impopulaires et même d'en parler librement, ce qui donne naissance à la formation d'opinions diversifiées et à l'expression de points de vue divergents.¹¹ Quoiqu'il en soit, selon les résultats des sondages, l'ensemble des membres de la société semblent s'entendre sur la nécessité d'assurer la protection des renseignements personnels et du droit à la vie privée.

Ces raisons ne sont cependant pas implicites lorsqu'il est question de protection des renseignements personnels dans le secteur des services financiers. En fait, trois raisons précises motivent l'intérêt relié à la protection des renseignements personnels dans ce secteur. Dans un premier temps, un individu a le droit de savoir que les renseignements de nature délicate sur sa situation financière, son état de santé aux fins d'assurance et ses actifs demeureront confidentiels. La divulgation de tels renseignements risquerait de le gêner, d'en faire l'objet d'envie ou de tentatives frauduleuses, ou de nuire à sa capacité de négocier avec des tiers. Par exemple, la divulgation de renseignements sur des transactions pourrait témoigner d'associations privées avec des organismes religieux ou politiques, ou encore de son orientation sexuelle. De même, la divulgation de renseignements sur son état de santé pourrait en faire la cible de préjugés ou lui faire perdre des possibilités d'emploi, de logement ou d'autres avantages. Deuxièmement, une personne a tout intérêt à veiller à ce que les renseignements personnels qu'un établissement financier recueille à son sujet, et sur lesquels elle s'appuie pour effectuer des transactions avec elle, sont exacts et à jour. Troisièmement, les gens veulent parfois éviter de faire l'objet de campagnes de marketing ciblé. Bien que les produits que l'on cherche à vendre puissent intéresser l'individu, certaines personnes s'objectent à une telle utilisation de leurs renseignements personnels.

⁷ Voir, par exemple : R. Gavison, « Privacy and the Limits of Law » (1980) 89 *Yale Law Journal* 42.

⁸ Voir : C. Fried, « Privacy » (1968) 77 *Yale Law Journal* 475 et S.I. Benn, *Privacy, Freedom and Respect for Persons* (Lieber-Atherton, 1971).

⁹ Westin, *supra*, note 2, p. 32ff.

¹⁰ Voir, par exemple : Gavison, *supra*, note 7, et E.R. Ryan, « Privacy, Orthodoxy and Democracy » (1973) 51 *Canadian Bar Review* 84.

¹¹ Gavison, *supra*, note 7.

Il est important de faire valoir que le concept de droit à la vie privée n'est pas un principe absolu. La société exige qu'il s'établisse un juste équilibre entre les intérêts individuels et les intérêts publics; une société où le droit à la vie privée primerait sur tout le reste serait constituée d'ermites et non de personnes menant leurs vies de concert. Le droit à la vie privée doit être pondéré par d'autres valeurs afin d'atteindre des objectifs sociaux. Par exemple, il faut lever le voile sur certains détails de la vie privée pour permettre aux assureurs d'obtenir tous les renseignements dont ils ont besoin pour régler les demandes d'indemnité, aux courtiers en valeurs mobilières de tenir des registres exacts et de respecter la règle qui exige que l'on « connaisse le client », ou à une banque ou à une société en fidéicommiss de se procurer l'adresse à laquelle elle doit faire parvenir les rentes annuelles ou les renseignements sur son compte. La société a également intérêt à formuler des règles relatives aux mécanismes d'obtention et de stockage des renseignements personnels généraux sous forme d'éléments de base de tous les contrats. Cela permet d'épargner les frais de négociations individuelles rendues nécessaires pour satisfaire aux intérêts de chaque consommateur. Enfin, si nous, en tant que consommateurs, exigeons que les institutions financières adoptent une approche plus personnelle et se fassent plus soucieuses de nos besoins et de nos désirs, il faut s'attendre à ce qu'elles recueillent et utilisent des renseignements personnels à cette fin.

Un autre point à souligner est le fait que le droit à la vie privée est un concept qui varie sensiblement selon la culture où l'on évolue. Par exemples, certains auteurs font valoir les différences marquées entre les mécanismes de protection des renseignements personnels qu'utilisent les gouvernements américain et européens.¹² Ainsi, Westin affirme que l'histoire des États-Unis a mené son peuple à s'opposer plus vigoureusement à la mise en œuvre de fichiers d'identification nationaux, lesquels sont monnaie courante en Europe.¹³ Alors que le concept de vie privée varie d'une société à l'autre, il évolue aussi avec le temps, à mesure que les conditions sociales se transforment. Les concepts actuels du droit à la vie privée au Canada découlent en grande partie des changements sociaux que l'on observe depuis environ un siècle. Ces changements structurels ont mené à une toute autre définition de la famille, à une migration de la population de la campagne à la ville, à l'élargissement des sphères d'activités de l'État et à une plus grande importance stratégique de la multitude de renseignements personnels que doivent posséder les secteurs public et privé. Par ailleurs, les personnes qui habitent dans les grands centres urbains jouissent probablement de beaucoup plus d'intimité que celles qui vivent dans de petites collectivités.

L'informatisation des renseignements personnels

La préoccupation du public à l'égard du droit à la vie privée et de la divulgation des renseignements personnels est un mouvement qui a pris de l'ampleur au cours des années soixante, lorsque les gouvernements et les grandes entreprises ont commencé à tenir des registres

¹² Voir, par exemple : Herbert J. Spiro, « Privacy in Comparative Perspective » dans *Privacy: Nomos XIII*, éd. par J. Rolland Pennock et John W. Chapman (New York, Atherton Press, 1971).

¹³ Alan F. Westin, « Privacy, Technology and Regulation » dans *The Computer Culture*, éd. par Denis P. Donnelly (London, Associated University Press, 1985), pp. 138-139.

informatiques. L'informatisation des dossiers personnels permettait de trier, de recouper, de transmettre et d'utiliser des renseignements personnels à d'autres fins plus facilement que jamais auparavant. Rapidement, l'informatisation et la montée de la société de l'information ont mené à la naissance de nouvelles entreprises dont le seul mandat consistait à recueillir, à analyser et à utiliser des renseignements personnels.¹⁴ Les sociétés commerciales, dont les institutions financières, ont mis au point de nouvelles méthodes de mise en marché de leurs produits et services, méthodes qui s'appuient sur les renseignements qu'elles recueillent à propos de leurs clients dans le cadre des transactions courantes. Cette capacité « d'entreposer » une quantité phénoménale de renseignements personnels élémentaires et d'aller ensuite puiser à même cette banque de données pour en extraire des groupes cibles est extrêmement importante pour les entreprises parce qu'elle leur confère un avantage considérable en matière de marketing.

Pendant les années soixante et soixante-dix, le public a également commencé à prendre conscience de la progression de la technologie informatique, ce qui a mené à l'élaboration de principes sur le traitement équitable des renseignements personnels. Bien que ces principes visent une foule de questions, ils traitent essentiellement de la protection de la vie privée. Les lignes directrices de l'Organisation de coopération et de développement économique (OCDE) élaborées en 1980 offrent ce qui est peut-être le meilleur ensemble de principes de protection du droit à la vie privée dont on dispose à l'heure actuelle. Jetons un coup d'oeil à ces principes :

Principe de la limitation en matière de collecte : Il conviendrait d'assigner des limites à la collecte des données de caractère personnel et toute donnée de ce type devrait être obtenue par des moyens licites et loyaux et, le cas échéant, après en avoir informé la personne concernée ou avec son consentement.

Principe de la qualité des données : Les données de caractère personnel devraient être pertinentes par rapport aux finalités en vue desquelles elles doivent être utilisées et, dans la mesure où ces finalités l'exigent, elles devraient être exactes, complètes et tenues à jour.

Principe de la spécification des finalités : Les finalités en vue desquelles les données de caractère personnel sont collectées devraient être déterminées au plus tard au moment de la collecte des données et lesdites données ne devraient être utilisées par la suite que pour atteindre ces finalités ou d'autres qui ne soient pas incompatibles avec les précédentes et qui seraient déterminées dès lors qu'elles seraient modifiées.

Principe de la limitation de l'utilisation : Les données de caractère personnel ne devraient pas être divulguées ni fournies, ni utilisées à des fins autres que celles spécifiées conformément au paragraphe [sur le principe de la spécification des finalités], si ce n'est avec le consentement de la personne concernée ou lorsqu'une règle de droit le permet.

Principe des garanties de sécurité : Il conviendrait de protéger les données de caractère personnel, grâce à des garanties de sécurité raisonnables, contre des risques tels que la perte des données ou leur accès, destruction, utilisation, modification ou divulgation non autorisés.

¹⁴ Pour un aperçu de l'industrie des renseignements personnels, voir : Anne Wells Branscomb, *Who Owns Information? From Privacy to Public Access* (New York, BasicBooks, 1994). Voir aussi : Joseph P. Bigus, *Data Mining with Neural Networks* (New York, McGraw-Hill, 1996).

Principe de la transparence : Il conviendrait d'assurer, d'une façon générale, la transparence des progrès, pratiques et politiques, ayant trait aux données de caractère personnel. Il devrait être possible de se procurer aisément les moyens de déterminer l'existence et la nature des données de caractère personnel et les finalités principales de leur utilisation, de même que l'identité du maître de fichier et le siège habituel de ses activités.

Principe de la participation individuelle : Toute personne physique devrait avoir le droit :

- a) d'obtenir du maître de fichier, ou par d'autres voies, confirmation du fait que le maître de fichier détient des données la concernant;
- b) se faire communiquer les données la concernant i) dans un délai raisonnable; ii) moyennant, éventuellement, une redevance modérée; iii) selon des modalités raisonnables; et iv) sous une forme qui lui soit aisément intelligible;
- c) d'être informée des raisons pour lesquelles une demande qu'elle aurait présentée conformément aux alinéas a) et b) est rejetée et de pouvoir contester un tel rejet; et
- d) de contester les données la concernant et, si la contestation est fondée, de les faire effacer, rectifier, compléter ou corriger.

Principe de la responsabilité : Tout maître de fichier devrait être responsable du respect des mesures donnant effet aux principes énoncés ci-dessus.¹⁵

Les principes de l'OCDE ont été approuvés à l'unanimité par les membres de cet organisme et s'inspirent de démarches effectuées par nombre des pays membres en vue de modifier leurs lois en matière de protection des renseignements personnels. Ces principes ont joué un rôle prépondérant dans les débats entourant la protection des renseignements personnels au Canada. Ils ont d'ailleurs récemment servi de toile de fond à la rédaction du *Code type sur la protection des renseignements personnels* de l'Association canadienne de normalisation.¹⁶

Problèmes relatifs à la protection des renseignements personnels

On considère aujourd'hui le droit à la vie privée comme un amalgame de principes relatifs à la protection des renseignements personnels. Premièrement, le droit à la vie privée a une incidence sur les mécanismes de cueillette et d'utilisation des renseignements personnels. Une des grandes préoccupations des années soixante et soixante-dix tenait au projet de création, par le gouvernement, d'un dossier « du berceau à la tombe » sur chaque citoyen.¹⁷ Plus récemment, des spécialistes en protection des renseignements personnels ont commencé à lever le voile sur les problèmes liés à la collecte et à l'utilisation des renseignements personnels dans le secteur

¹⁵ Pour consulter le texte intégral des lignes directrices de l'OCDE, voir, par exemple : James Michael, *Privacy and Human Rights* (Paris, UNESCO Publishing, 1994), p. 139ff.

¹⁶ Association canadienne de normalisation, *Code type de protection des renseignements personnels*, CAN/CSA-Q830-96 (Etobicoke, ACNOR, 1996).

¹⁷ Voir, par exemple : Westin, *supra*, note 2, et Arthur R. Miller, *The Assault on Privacy: Computers, Data Banks and Dossiers* (Ann Arbor, University of Michigan Press, 1971).

privé.¹⁸ Les entreprises commerciales recueillent aujourd'hui des renseignements fournis par les consommateurs lorsque ces derniers font des achats et prennent des décisions, et analysent d'autres renseignements de notoriété publique comme ceux que l'on peut obtenir auprès des bureaux de recensement. Les renseignements personnels sont considérés comme des biens que l'on peut utiliser pour améliorer la mise en marché des produits et services que l'on destine aux consommateurs. Les spécialistes font valoir que cette tendance porte atteinte à la capacité des consommateurs de gérer les renseignements qui les concernent. Ils avancent que les individus devraient pouvoir exercer un certain contrôle sur ces renseignements et être capables, du moins dans une certaine mesure, de décider de la façon et du moment où ils seront utilisés, ainsi que des raisons pour lesquelles ils pourraient l'être. La capacité d'une personne d'influencer la nature de ses rapports avec le gouvernement et les établissements commerciaux constitue le fond de la question.

En deuxième lieu viennent les problèmes liés à la divulgation et à la transmission des renseignements personnels. Un organisme gouvernemental ou commercial qui a colligé des renseignements auprès d'une personne peut transmettre ou divulguer ces renseignements de manière à ce que d'autres parties y aient accès, parties auxquelles ces renseignements n'étaient pas destinés en premier lieu et qui n'ont pas été autorisées à en prendre connaissance. Par exemple, un éditeur de revue peut vendre sa liste d'abonnés à une entreprise qui désire mettre en marché des produits ou des services susceptibles d'intéresser les lecteurs de cette revue. La divulgation et la transmission de ce genre de renseignements soulèvent les mêmes problèmes que la collecte et l'utilisation des données. Sans mécanisme de contrôle sur la transmission des renseignements, les gens risquent de perdre le contrôle des renseignements qui les concernent ainsi que leur capacité d'influencer les rapports qu'ils entretiennent avec autrui. Dans le cas des fournisseurs de services financiers, divers secteurs d'un même organisme peuvent utiliser les renseignements que les clients auront fournis aux fins de l'obtention d'un produit ou d'un service précis dans le but de les sensibiliser, dans le cadre d'une campagne de marketing, à d'autres produits et services. Toutefois, les institutions financières ne peuvent transmettre ces renseignements à un tiers sans le consentement de l'intéressé. Le cas le plus fréquent de transmission de tels renseignements à l'extérieur de l'institution est probablement celui du bureau d'évaluation de crédit. Les fournisseurs de services financiers transmettent aux bureaux de crédit des renseignements au sujet de la capacité de crédit de leurs clients, et ces bureaux mettront ensuite ces renseignements à la disposition d'autres établissements à la recherche de personnes à qui offrir des services de crédit.¹⁹ Un autre exemple de transmission à un tiers est le partage de renseignements médicaux entre assureurs. Les assureurs transmettent fréquemment

¹⁸ Voir, par exemple : Willis H. Ware, « The New Faces of Privacy » (1993) 9 *Information Society* 195, et Branscomb, *supra*, note 14.

¹⁹ Pour de plus amples renseignements au sujet des bureaux de crédit, voir : Partie II, notes de bas de page 201 à 210 ainsi que le texte auquel ces notes se rattachent.

des renseignements médicaux de base au sujet de leurs clients à une base de données située au Massachusetts, laquelle fournit ces renseignements à d'autres assureurs sur demande.²⁰

Troisièmement, le stockage inopportun de renseignements personnels peut porter atteinte au droit à la vie privée d'une personne. En règle générale, il est préférable d'effacer les renseignements personnels lorsque les rapports qui unissent une entreprise et son client n'existent plus. On prendra cependant soin de les conserver quelque temps de manière à permettre au client de consulter son dossier au besoin afin de connaître, par exemple, les raisons motivant une décision à son sujet. En outre, il serait souhaitable d'éliminer les renseignements pertinents mais défavorables au client après de longues périodes données. Cette théorie s'appuie sur le fait que les renseignements personnels ne devraient pas nuire indéfiniment au dossier d'une personne et qu'après un certain laps de temps, les gens devraient être dégagés des conséquences négatives liées à certains genres de renseignements. Par exemple, la loi ontarienne qui régit les bureaux de crédit stipule que certains renseignements ne doivent plus apparaître au dossier de crédit des gens après une période donnée. Ainsi, les renseignements au sujet, par exemple, d'une première faillite d'un individu, d'une omission de paiement de taxes ou de pénalités, ou encore les condamnations pour actes criminels doivent être éliminés du dossier de crédit des gens sept ans après la date à laquelle l'événement s'est produit.²¹

Quatrièmement, les renseignements personnels doivent faire l'objet de mesures de protection adéquates afin d'éviter qu'ils ne soient utilisés ou divulgués sans autorisation. Ces mesures de protection peuvent revêtir diverses formes : des politiques au sujet des personnes autorisées à les consulter, des mesures de restriction physique de l'accès à l'information, des circuits et réseaux réservés à la télécommunication de l'information, ainsi que des mesures de sécurité informatique (matériel et logiciels), comme l'encryptage, qui permettent d'éviter que les renseignements ne soient consultés par des employés non autorisés. De même, on doit disposer des renseignements personnels de manière à ce que les renseignements de nature délicate ne puissent être consultés par le public. Par exemple, il est de mise de disposer de renseignements de nature délicate sur support papier à l'aide d'une déchiqueteuse plutôt que de se contenter de les jeter à la poubelle ou dans un bac de recyclage. Bien que les mesures appropriées représentent un volet important du protocole de protection des renseignements personnels, ils ne posent pas, du moins en majorité, de problème technique. La présente étude ne s'y attarde donc pas outre mesure.

Cinquièmement vient le droit d'une personne à consulter et à corriger les renseignements personnels la concernant. Dans la mesure où les renseignements de nature personnelle sont utilisés pour prendre des décisions qui ont des conséquences pour l'intéressé, ce dernier a intérêt à veiller à ce que ces renseignements soient aussi exacts que faire se peut. Les politiques de

²⁰ Le Bureau de renseignements médicaux (MIB) de Westwood, au Massachusetts, conserve les renseignements médicaux sous forme codée que les compagnies d'assurance lui transmettent au sujet de leurs clients. Pour se faire une meilleure idée des activités du Bureau de renseignements médicaux, voir : Partie II, notes de bas de page 212 à 215 ainsi que le texte d'accompagnement.

²¹ *Loi sur les renseignements concernant le consommateur*, L.R.O. 1990, c. C-33, a. 9.

transmission de ces renseignements entre établissements rendent ce droit de consultation et de correction encore plus important, de manière à prévenir les effets néfastes de la divulgation, à plus ou moins grande échelle, de renseignements erronés. Le droit à la consultation et à la rectification de l'information doit être inséré dans une loi visant les gouvernements fédéral et provinciaux au Canada.²² Ce droit a d'ailleurs récemment été reconnu par le gouvernement du Québec, qui a voté une loi à cet effet, ainsi que par diverses associations industrielles, qui ont adopté des politiques en ce sens.²³

Évolution de la perception du droit à la vie privée dans le secteur des services financiers au Canada

Les années quatre-vingt : Premières démarches visant la mise en œuvre des principes adoptés par l'OCDE

Toute analyse de l'évolution du dossier de la protection des renseignements personnels dans le secteur des services financiers au Canada²⁴ se doit de débiter par l'examen des lignes directrices adoptées par l'OCDE, le document le plus important à ce sujet de nos jours. Adoptées par l'OCDE à la fin des années quatre-vingt, ces lignes directrices étaient destinées à servir de point de départ à l'élaboration de mesures législatives sur la protection des renseignements personnels dans les pays membres de l'organisme. Elles ont été formulées en réponse aux préoccupations que suscitaient la protection des renseignements personnels et plus particulièrement le flux transfrontières de ces renseignements à des fins commerciales. L'esprit de ces lignes directrices se trouve dans les huit principes qu'elles énoncent et qui visent à la fois les secteurs public et privé, soit : 1) le principe de la limitation en matière de collecte, 2) le principe de la qualité des données, 3) le principe de la spécification des finalités, 4) le principe de la limitation de l'utilisation, 5) le principe des garanties de sécurité, 6) le principe de la transparence, 7) le principe de la participation individuelle et 8) le principe de la responsabilité. La définition intégrale de ces principes a été donnée dans les pages qui précèdent.²⁵

²² Pour un aperçu général des mesures législatives de protection des renseignements personnels dans le secteur public au Canada, voir : Colin H.H. McNairn et Christopher D. Woodbury, *Government Information: Access and Privacy* (Scarborough, Ontario, Carswell, 1992).

²³ La loi régissant la protection des renseignements personnels et les codes afférents adoptés par les associations sectorielles du domaine des services financiers au Québec font l'objet d'un examen plus poussé dans la Partie II de la présente étude.

²⁴ Le traitement des questions abordées sous cette rubrique s'inspire largement d'un autre document : Richard C. Owens, Tom Onyshko et Peter C. Goode, « Reform Proposals Relating to Customer Privacy and Tied Selling in the Federally-Regulated Financial Services Sector » dans *The Regulation of Financial Institutions: Issues and Perspectives* (Scarborough, Ontario, Carswell, 1997) 143, p. 153ff.

²⁵ Voir la rubrique « Droit à la vie privée et questions liées à la protection des renseignements personnels », dans les pages précédentes de cette Partie.

En 1984, le gouvernement du Canada a annoncé qu'il avait officiellement adhéré aux *Lignes directrices* de l'OCDE. Plutôt que d'adopter une loi visant la mise en oeuvre de ces principes, le gouvernement s'est engagé « à encourager les entreprises du secteur privé à élaborer leur propre code de protection des données à caractère personnel ». ²⁶ En 1985, le ministère fédéral de la Justice a publié un document sur les incidences des lignes directrices de l'OCDE. ²⁷ En 1987, un comité parlementaire chargé d'examiner la *Loi sur la protection des renseignements personnels* a recommandé que cette loi soit modifiée de manière à viser les organismes à charte fédérale qui exercent des activités commerciales dans le secteur privé. ²⁸ Cependant, le gouvernement fédéral n'a pas jugé bon de poser un geste en ce sens. ²⁹ À la fin des années quatre-vingt, le ministre des Affaires extérieures a demandé avec insistance aux entreprises du secteur privé d'adhérer aux lignes directrices de l'OCDE. ³⁰ Le Commissariat à la protection de la vie privée s'est entretenu avec des sociétés de transport aérien, des institutions financières et des sociétés de télécommunication au sujet des codes de protection des renseignements personnels. ³¹ Des fonctionnaires fédéraux ont également rencontré leurs vis-à-vis des provinces pour discuter de stratégies destinées à inciter le secteur privé à se doter de codes de protection des renseignements personnels. ³²

À cette époque, John Grace occupait le poste de commissaire à la protection des renseignements personnels. L'évolution de sa perception du dossier mérite qu'on s'y attarde. Immédiatement après l'annonce de l'engagement du gouvernement fédéral en 1984, il a déclaré être en faveur d'une approche visant à encourager les entreprises du secteur privé à élaborer leur propre code de protection de données à caractère personnel. Il a écrit que l'autoréglementation était préférable à la réglementation gouvernementale et que les codes de protection des renseignements personnels

^{26.} *Commissaire à la protection de la vie privée au Canada, Rapport annuel 1984-1985* (Ottawa, Approvisionnement et Services, 1985), p. 11. Formulant son opinion au sujet de la décision du gouvernement fédéral, le commissaire a écrit ce qui suit : « Cet engagement important devrait faire l'objet de mesures énergiques de mise en œuvre dès à présent ». Cependant, un an plus tard, le commissaire se plaignait, dans son rapport, de ce que le gouvernement fédéral avait fait bien peu de choses pour mettre en œuvre les lignes directrices de l'OCDE. Voir : *Commissaire à la protection de la vie privée au Canada, Rapport annuel 1985-1986* (Ottawa, Approvisionnement et Services Canada, 1986), p. 12.

^{27.} Gouvernement du Canada, ministère de la Justice, *Les lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel de l'OCDE : Incidences pour le Canada* (Ottawa, ministère de la Justice, 1985).

^{28.} *Open and Shut: Enhancing the Right to Know and the Right to Privacy: Report of the Standing Committee on Justice and Solicitor General on the Review of the Access to Information Act et the Privacy Act* (Ottawa, Imprimeur de la Reine, 1987), p. 77.

^{29.} Voir : Gouvernement du Canada, ministère de la Justice, *The Steps Ahead* (Ottawa, ministère de la Justice, 1987).

^{30.} Voir : *Commissaire à la protection de la vie privée au Canada, Rapport annuel 1987-1988* (Ottawa, Approvisionnement et Services Canada, 1988), p. 8 : « Le ministre des Affaires extérieures a souligné l'engagement pris par le Canada à l'intention des grandes sociétés canadiennes et leur a demandé avec insistance d'adhérer aux lignes directrices de l'OCDE. »

^{31.} *Commissaire à la protection de la vie privée au Canada, Rapport annuel, 1989-1990* (Ottawa, Approvisionnement et Services Canada, 1990), p. 13.

^{32.} *Commissaire à la protection de la vie privée au Canada, Rapport annuel, 1988-1989* (Ottawa, Approvisionnement et Services Canada, 1989), p. 9.

comportaient également des avantages pour les entreprises.³³ Suite au dépôt du rapport du comité parlementaire sur la *Loi sur la protection des renseignements personnels*, il a déclaré appuyer le gouvernement dans sa décision de ne pas élargir la portée de la Loi au secteur privé. Il a déclaré qu'il ne semblait pas y avoir d'abus à grande échelle dans le secteur privé, qu'on pouvait douter de la capacité de la *Loi sur la protection des renseignements personnels* à couvrir les multiples facettes des diverses industries auxquelles elle était destinée et que la mise en œuvre d'une telle mesure de réglementation nécessiterait une augmentation considérable des ressources du Commissariat à la protection de la vie privée.³⁴ Le commissaire a toutefois dénoncé la lenteur avec laquelle les entreprises du secteur privé élaboraient leurs propres codes.³⁵ Enfin, dans son rapport 1989-1990, il a demandé que la *Loi sur la protection des renseignements personnels* soit modifiée de manière à exiger des organismes à charte fédérale qu'ils élaborent des codes et les présentent au Commissariat. M. Grace a fait valoir que son bureau pourrait se charger de la surveillance de ces codes, bien qu'il ne voulait jouer aucun rôle dans le processus de mise en œuvre des dispositions qu'on y retrouvait.³⁶

Le début des années quatre-vingt-dix : Réforme des lois fédérales sur les institutions financières et des lois du Québec en matière de protection de la vie privée

Au début des années quatre-vingt-dix, les pressions se faisaient de plus en plus fortes pour que les institutions financières à charte fédérale adoptent des mesures de protection des renseignements personnels. Des réformes des lois fédérales régissant les institutions financières ont amélioré les perspectives de réglementation de la protection des renseignements personnels relatifs aux clients. Bruce Phillips, nommé commissaire fédéral à la protection de la vie privée en 1991, en remplacement de M. Grace, plaidait en faveur d'une réglementation relative à la protection des renseignements personnels visant les institutions financières et d'une législation étendue relative à la protection de la vie privée visant le secteur privé. Le Québec a adopté une législation relative à la protection de la vie privée pour l'ensemble du secteur privé. Dès lors, de plus en plus d'associations industrielles représentant des institutions financières

^{33.} *Commissaire à la protection de la vie privée au Canada, Rapport annuel 1984-1985* (Ottawa, Approvisionnement et Services Canada, 1985), p. 11.

^{34.} Voir : *Commissaire à la protection de la vie privée au Canada, Rapport annuel 1986-1987* (Ottawa, Approvisionnement et Services Canada, 1987), p. 6; *Commissaire à la protection de la vie privée au Canada, Rapport annuel 1987-1988* (Ottawa, Approvisionnement et Services Canada, 1988), p. 7; *Commissaire à la protection de la vie privée au Canada, Rapport annuel 1988-1989* (Ottawa, Approvisionnement et Services Canada, 1989), p. 9.

^{35.} Voir, par exemple : *Commissaire à la protection de la vie privée au Canada, Rapport annuel 1988-1989* (Ottawa, Approvisionnement et Services Canada, 1989), p. 9.

^{36.} *Commissaire à la protection de la vie privée au Canada, Rapport annuel 1989-1990* (Ottawa, Approvisionnement et Services Canada, 1990), p. 14.

réglementées et des institutions privées se mirent à adopter leurs propres codes de protection des renseignements personnels.³⁷

Au début des années quatre-vingt-dix, le gouvernement fédéral a considérablement modifié la loi régissant le secteur des services financiers. Ces modifications, entrées en vigueur en 1992, constituaient le point de départ d'une évolution qui allait marquer le secteur des services financiers. Dans le cadre de ces modifications, un nouveau pouvoir est venu renforcer la *Loi sur les banques*, la *Loi sur les compagnies d'assurance*, ainsi que la *Loi sur les sociétés de fiducie et de prêt*, donnant au Cabinet fédéral la possibilité d'élaborer des règlements relatifs à la protection des renseignements personnels reliés aux clients.³⁸ Par exemple, l'article 459 de la *Loi sur les banques* donnait au gouverneur en conseil le pouvoir d'élaborer des règlements régissant l'utilisation par une banque de tout renseignement lui étant fourni par ses clients. Le gouvernement y a inclus des dispositions permettant d'établir des règlements pour répondre aux inquiétudes relatives à l'échange de renseignements entre les institutions financières, leurs filiales et d'autres établissements.³⁹

Faisant également partie du cadre des modifications de 1992, des règlements fédéraux régissant les banques et les compagnies de fiducie interdisaient à des telles institutions de se lancer dans la vente au détail de la plupart des produits d'assurance — ainsi que d'utiliser des renseignements sur les clients à ces fins.⁴⁰ En vertu de ces règlements, il était interdit aux banques et aux compagnies de fiducie de faire la promotion de la plupart des types d'assurance et de fournir des renseignements sur des clients à une compagnie d'assurance.⁴¹ L'interdiction d'utiliser les renseignements sur les clients à des fins d'assurance était motivée par le souci de protéger l'industrie de l'assurance d'une concurrence des banques et des compagnies de fiducie. Guy David et Louise Pelly avaient noté que : « au cœur de l'interdiction concernant les assurances

³⁷ Il sera question, à la Partie II, des codes de l'Association des banquiers canadiens, de l'Association des compagnies de fiducie du Canada, de l'Association canadienne des compagnies d'assurance de personnes (ACCAP) et du Bureau d'assurance du Canada (BAC). Soulignons que l'ACCAP s'est dotée de son propre code de protection des renseignements personnels bien avant les autres associations, soit dès 1980. En 1986, le BAC a à son tour présenté un modèle de code à ses membres, mais ceux-ci l'ont rejeté.

³⁸ Voir : *Loi sur les banques*, L.C. 1991, ch. 46, art. 459; *Loi sur les sociétés de fiducie et de prêt*, L.C. 1991, ch. 45, art. 444; et *Loi sur les sociétés d'assurance*, L.C. 1991, ch. 47, art. 489.

³⁹ Voir : John W. Teolis et Jeffrey S. Graham, *Financial Institutions Reform Package: Phase Two / New Banking Legislation Annotated* (Toronto, CCH Canadian, 1991) p. 302. Les notes explicatives officielles relatives au projet de loi ne contenaient pas beaucoup de renseignements sur les objectifs des articles. Par exemple, les annotations officielles de l'article 459 de la *Loi sur les banques* disent simplement que cet article contient des dispositions afférentes à la réglementation de l'utilisation des renseignements personnels des clients et que ces règlements seront élaborés de concert avec l'industrie et d'autres intéressés. Voir : Gouvernement du Canada, ministère des Finances, *Notes explicatives de la Loi sur les banques* (Ottawa, ministère des Finances, hiver 1990), p. 55.

⁴⁰ Voir *Loi sur les banques*, L.C. 1991, ch. 46, art. 416; *Règlement sur les activités d'assurance (banques)*, DORS/92-330, tel que modifié; *Loi sur les sociétés de fiducie et de prêt*, L.C. 1991, ch. 45, art. 16; et *Règlement sur les activités d'assurance (sociétés de fiducie et de prêt)*, DORS/92-331, tel que modifié.

⁴¹ Voir *Règlement sur les activités d'assurance (banques)*, DORS/92-330, al. 7 et 8; *Règlement sur les activités d'assurance (sociétés de fiducie et de prêt)*, DORS/92-331, al. 7 et 8.

[dans la *Loi sur les banques* et sa réglementation], on retrouve les questions de marketing ciblé et de circulation des renseignements » et que « le gouvernement acceptait le point de vue de l'industrie de l'assurance selon lequel les banques disposeraient d'un avantage indu si on leur permettait de concurrencer les compagnies d'assurance ». ⁴² L'impertinence d'une cohabitation intellectuelle entre des mesures de protection des renseignements personnels et des mesures pouvant contribuer à l'inefficacité concurrentielle est abordée plus loin dans cette étude.

Après l'entrée en vigueur des réformes de 1992, le comité sénatorial permanent des banques et du commerce (le « **Comité des banques du Sénat** ») a tenu des audiences afin d'étudier la possibilité pour le gouvernement fédéral d'utiliser le pouvoir qui lui a été conféré par la loi pour élaborer des règlements relatifs à la protection des renseignements personnels sur les clients qui sont conservés dans les institutions. Le Commissaire à la protection de la vie privée, M. Phillips, s'est présenté devant le comité pour défendre cette idée. ⁴³ Le Comité des banques et du commerce du Sénat chargeait M. David H. Flaherty (alors professeur à l'Université Western Ontario et ayant acquis une expertise en matière de protection de la vie privée) du développement d'un avant-projet de règlement. L'avant-projet de règlement, présenté en juillet 1992, proposait une variété de règles similaires à celles contenues dans les directives de l'OCDE sur la protection de la vie privée. ⁴⁴ Les règlements exposaient surtout des principes relatifs à la limitation de la collecte, la qualité des données, les fins de la collecte, la limitation de l'utilisation, la communication des renseignements, les mesures de sécurité, le consentement de toute personne concernée, la responsabilité, la transparence, l'exactitude et la possibilité d'un examen externe. Les règlements de l'avant-projet sont remarquables à l'égard des limitations strictes relatives à la communication des renseignements personnels, de l'obligation pour les institutions d'apporter les corrections appropriées s'il y a lieu aux renseignements personnels d'un dossier et de les communiquer à tous ceux qui l'ont consulté, et de leur engagement à accepter un examen externe sur des plaintes relatives à la protection des renseignements personnels. ⁴⁵ Le Comité des

⁴². Guy David et Louise S. Pelly Q.C., Version annotée de la *Loi sur les banques 1996* (Toronto, Carswell, 1995) p. 296.

⁴³. Comité sénatorial permanent des banques et du commerce, Rapport provisoire sur la loi de 1992 concernant les institutions financières (août 1995), p. 9.

⁴⁴. Règlement sur l'utilisation, par une institution financière, des renseignements qui lui sont fournis par ses clients, préparé par le Comité sénatorial permanent sur les banques et le commerce (Ottawa, Service de recherche de la Bibliothèque du Parlement, 30 juillet 1992).

⁴⁵. Flaherty a proposé ce qui suit au sujet de la divulgation : en règle générale, aucun renseignement personnel ne devrait être divulgué sans le consentement exprès ou écrit du client; les banques devraient aviser les clients dont le dossier personnel est visé par une ordonnance des tribunaux; toutes les demandes de divulgation de renseignements adressées par des tiers devraient être présentées par écrit et préciser le motif de la requête; les institutions financières ne devraient pas être habilitées à utiliser des renseignements personnels à des fins de marketing sans l'autorisation expresse ou écrite du client; en règle générale, les institutions financières ne devraient pas être autorisées à divulguer des renseignements personnels à des sociétés affiliées et les renseignements personnels divulgués à des tiers pour vendre des produits et des services (comme l'impression de chèques personnalisés) devraient faire l'objet de mesures contractuelles d'observation du règlement. En ce qui a trait au règlement des différends, Flaherty suggère que le Bureau du Surintendant des institutions financières soit tenu de faire enquête au sujet des plaintes relatives à la protection des renseignements personnels et investi du pouvoir d'ordonner aux banques de prendre les mesures opportunes pour remédier à la situation.

banques et du commerce du Sénat concluait finalement, dans son rapport de 1993, que le gouvernement fédéral devait adopter les règlements. Ce rapport faisait ressortir le besoin d'examen des plaintes concernant la protection de la vie privée par un organisme indépendant et recommandait la création d'une nouvelle agence de protection de la vie privée dans le secteur financier pour exercer cette fonction.⁴⁶

En janvier 1994, la *Loi sur la protection des renseignements personnels dans le secteur privé* (projet de loi 68) entra en vigueur au Québec.⁴⁷ La Loi s'applique à un large éventail d'établissements du secteur privé incluant : des corporations, des entreprises individuelles, des sociétés de personnes, des organismes et des associations.⁴⁸ Plusieurs dispositions régissent la collecte, l'utilisation et la communication de renseignements personnels; la Loi établit également le droit d'accès de toute personne aux renseignements personnels qui la concernent et son droit d'exiger des corrections à son dossier s'il contient des inexactitudes. Des dispositions spéciales s'appliquent dans le cas de listes nominatives utilisées à des fins commerciales et aussi dans le cas de communication à des tiers, à l'extérieur du Québec, de renseignements concernant des personnes résidant au Québec.⁴⁹ Les désaccords pouvant survenir dans le cadre de cette Loi doivent être réglés par la Commission d'accès à l'information, l'organisme public responsable de résoudre les différends relatifs au droit de consultation dans les services publics et aux règlements sur la protection de la vie privée. Sur la question de savoir si l'application de la Loi aux banques est constitutionnelle, au moins un commentateur a émis l'opinion qu'elle survivrait à une poursuite d'ordre constitutionnel.⁵⁰ On note également que cette Loi a soulevé d'importantes questions touchant l'ensemble du pays puisque que le Canada devenait « le seul pays dans lequel la compétence de juridiction d'une de ses provinces en matière de protection de la vie privée surpasse celle du gouvernement fédéral ».⁵¹

Au milieu des années quatre-vingt-dix, le Commissaire à la protection de la vie privée, M. Phillips, a demandé que la *Loi fédérale sur la protection de la vie privée* soit étendue aux industries du secteur privé réglementées par le gouvernement fédéral. Dans son rapport annuel de 1995, il écrivait qu'il ne pouvait plus soutenir une approche basée sur des codes volontaires de réglementation. Ses motifs comprenaient la croissance de l'industrie des renseignements personnels, le rythme rapide des changements technologiques et la menace pour la protection de la vie privée dans le secteur public que constitue « l'interconnectivité entre les systèmes de

^{46.} Règlement sur l'utilisation, par une institution financière, des renseignements qui lui sont fournis par ses clients, Rapport final du Comité sénatorial permanent sur les banques et le commerce (Ottawa, Imprimeur de la Reine, juin 1993), pp. 1 et 3.

^{47.} La Loi étouffe les dispositions du nouveau *Code civil du Québec*, adopté en 1991 : L.Q. 1991, ch. 64, art. 35 à 41.

^{48.} Voir : L.R.Q. ch. P-39.1, art. 1 et le *Code civil du Québec*, art. 1525.

^{49.} Voir : L.R.Q. ch. P-39.1, art. 17 et al. 22-26.

^{50.} Voir : Étienne Dubreuil, « Québec Bill 68: Is It Sufficient for the Federal Canadian Financial Institutions Sector? » (Le projet de loi 68 est-il suffisant pour le secteur des institutions financières du Canada?) dans *Privacy in Financial Services* (Toronto, Canadian Institute, 1994).

⁵¹ Colin J. Bennett, *Implementing Privacy Codes of Practice* (Toronto, ACNOR, 1995), p. 10.

transmission et les bases de données du secteur public et du secteur privé ». ⁵² Le Commissaire proposait une nouvelle législation pouvant s'appliquer tant au secteur public qu'au secteur privé et qui créerait un mécanisme de surveillance indépendant.

La fin des années quatre-vingt-dix : le code de l'Association canadienne de normalisation, les réformes complémentaires des lois sur les institutions financières fédérales et les propositions pour une législation fédérale relative à la protection de la vie privée

À la fin des années quatre-vingt-dix, nous avons connu de nouveaux développements dans le domaine de la protection de la vie privée. Ces nouveaux développements incluent : le code type de l'Association canadienne de normalisation (en anglais, Canadian Standards Association, ou CSA) sur la protection de la vie privée, des réformes législatives fédérales sur les institutions financières qui comportaient un pouvoir étendu de réglementation en matière de protection de renseignements personnels, ainsi que les dernières propositions fédérales pour une législation sur la protection de la vie privée destinée au secteur privé.

En 1996, l'Association canadienne de normalisation (ACNOR) a adopté son *Code type sur la protection des renseignements personnels*. ⁵³ Le code type de l'ACNOR a été rédigé par un comité regroupant des représentants du milieu des affaires, du gouvernement et de groupes de consommateurs. Il comprend dix principes relatifs à la protection de la vie privée et au droit d'accès des individus aux renseignements personnels qui proviennent en grande partie des directives de l'OCDE :

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

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

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

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

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

^{52.} *Commissaire à la protection de la vie privée du Canada, Rapport annuel 1994-1995* (Ottawa, Groupe des communications du Canada, 1995), p. 4.

^{53.} L'Association canadienne de normalisation (CSA) est un organisme sans but lucratif qui élabore des normes dans des domaines comme la santé, la sécurité et la protection de l'environnement.

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

Mesures de sécurité : les renseignements personnels doivent être protégés par des mesures de sécurité correspondant à leur degré de délicatesse.

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.

Accès aux renseignements personnels : un organisme doit informer toute personne qui en fait la demande de l'existence de renseignements personnels qui la concernent, de l'usage qui en est fait et de leur communication à des tiers (s'il y a lieu), et lui permettre de les consulter. Il sera aussi possible de contester l'exactitude et l'état complet des renseignements et d'y faire apporter les corrections appropriées.

Possibilité de porter plainte contre l'inobservance des principes : toute personne doit être en mesure de se plaindre de l'inobservance des principes énoncés ci-dessus en communiquant avec le ou les individus responsables de les faire respecter au sein de l'organisme concerné.⁵⁴

Le code type de l'ACNOR est proposé comme un modèle pouvant être choisi volontairement par une entreprise lorsque des modifications correspondant à son secteur d'activités y auront été apportées. Ce modèle a été reconnu comme étant fonctionnel par le Commissaire fédéral à la protection de la vie privée et les autres fonctionnaires concernés.⁵⁵ Après la publication du code type, les associations industrielles représentant les banques et les compagnies d'assurance générale ont révisé leurs codes types sur la protection des renseignements personnels afin de se conformer à la nouvelle norme de l'ACNOR.

Encore en 1996, le ministère fédéral des Finances publiait son Livre Blanc sur le projet de remaniement des lois fédérales régissant les institutions financières en 1997. Ce document traitait de la possibilité de réformer plusieurs aspects du problème de la protection des consommateurs incluant la protection des renseignements personnels. Le document soutenait que la protection de la vie privée était devenue un enjeu capital depuis que des nouvelles technologies permettaient de facilement amasser et analyser des renseignements personnels.⁵⁶ En même temps qu'il reconnaissait les efforts du secteur des services financiers pour répondre aux problèmes relatifs à la protection des renseignements personnels, le document soutenait qu'il fallait faire plus. Il proposait une réglementation gouvernementale qui obligerait les institutions financières à adopter des codes de conduite réglementant la collecte, l'utilisation, la conservation et la communication de renseignements personnels. De plus, la réglementation proposée exigerait que les institutions financières désignent des cadres supérieurs devant mettre en oeuvre

^{54.} Association canadienne de normalisation, *Code type sur la protection des renseignements personnels – Norme nationale du Canada*, CAN/CSA-Q830-96 (Etobicoke, Ontario, ACNOR, 1996), p. ix.

^{55.} Voir, par exemple : *Commissaire à la protection de la vie privée du Canada, Rapport annuel 1994-1995* (Ottawa, Groupe des communications du Canada, 1995), pp. 14-15.

^{56.} Gouvernement du Canada, ministère des Finances, *1997 Review of Financial Sector Legislation: Proposals for Changes*, document portant sur les modifications qu'on proposait d'apporter en 1997 aux lois régissant le secteur financier (Ottawa, ministère des Finances, juin 1996), p. 15.

des procédures de traitement des plaintes et qu'elles soumettent un rapport annuel portant sur les plaintes reçues concernant les renseignements personnels et sur les mesures prises pour accueillir et traiter celles-ci. Ultérieurement, des observateurs ont maintenu que les propositions sur la protection des renseignements personnels étaient inutiles et qu'étant donné le manque de preuves relatives à des problèmes sur la protection des renseignements personnels dans le secteur des services financiers, elles causaient même un tort à la réputation de l'industrie.⁵⁷

Le Comité permanent des finances de la Chambre des communes (le « **Comité des finances de la Chambre** ») et le Comité des banques du Sénat ont tous deux produit des rapports contenant des observations relatives aux problèmes de la protection de la vie privée soulevés dans le Livre Blanc. Le rapport du Comité des banques du Sénat recommandait que les réglementations gouvernementales obligent les institutions financières à fournir à leurs clients une documentation écrite décrivant leurs codes de protection des renseignements personnels et la démarche à suivre pour porter plainte.⁵⁸ Le rapport recommandait également qu'un nouvel organisme fédéral – l'Office de la protection du consommateur – soit créé afin d'instruire les plaintes relatives à la protection des renseignements personnels. Le rapport recommandait finalement que « l'enjeu que constitue la position dominante acquise par les institutions financières sur le marché grâce à l'énorme quantité de données et de renseignements mis à leur disposition, devrait être pris en considération par le groupe de travail sur l'accès à l'information et la protection des renseignements personnels »⁵⁹ Le Comité des banques du Sénat a appuyé les recommandations du gouvernement présentées dans le Livre Blanc.⁶⁰

Un autre développement survenu en 1996 mérite d'être pris en considération. Les ministres fédéraux de l'Industrie et de la Justice se sont engagés à élaborer une nouvelle législation pour protéger le caractère confidentiel des renseignements personnels dans le secteur privé. Le rapport *Organiser la société de l'information* d'Industrie Canada faisait remarquer que pour répondre aux inquiétudes publiques sur la mauvaise utilisation des renseignements personnels, la nouvelle législation devait reconnaître le droit de chacun à la protection de la vie privée dans le monde de l'électronique. « Le droit à la protection de la vie privée doit être reconnu par la loi, particulièrement dans l'univers électronique des bases de données où il est tellement facile de recueillir et d'exploiter des renseignements personnels sur chaque citoyen. »⁶¹ Le rapport mentionnait que les ministres fédéraux de l'Industrie et de la Justice consulteraient les provinces pour élaborer des propositions dans le but d'établir un « cadre législatif » pour la protection des

⁵⁷ Voir : Owens, Onyshko et Goode, *supra*, note 24.

⁵⁸ *Quatrième rapport du Comité permanent des finances de la Chambre des communes, (1997 Review of Financial Sector Legislation: Proposals for Changes)*, document sur les modifications que l'on se proposait d'apporter en 1997 aux lois régissant le secteur financier (octobre 1996), pp. 3-4.

⁵⁹ *Idem*, p. 4.

⁶⁰ *Comité sénatorial permanent sur les banques et le commerce*, document sur la réforme des institutions financières en 1997 : *Lowering the Barriers to Foreign Banks* (octobre 1996), p. 32.

⁶¹ Gouvernement du Canada, ministère de l'Industrie, *Building the Information Society: Moving Canada into the 21st Century* (Ottawa, ministère de l'Industrie, 1996), p. 25.

données personnelles dans le secteur privé. Plus tard, le ministre de la Justice promettait de faire adopter la nouvelle législation en matière de protection de la vie privée avant l'an 2000.⁶²

En 1997, le parlement adoptait une législation contenant les réformes proposées sur la protection de la vie privée présentées en 1996 dans le Livre Blanc du ministère des Finances. Parmi d'autres modifications, il y avait le projet de loi C-82 qui ajoutait à la *Loi sur les banques*, la *Loi sur les sociétés de fiducie et de prêt* et à la *Loi sur les sociétés d'assurance*, un pouvoir étendu d'élaborer des règlements.⁶³ Ce nouveau pouvoir permettait au gouvernement d'émettre des règlements exigeant qu'une institution financière établisse des procédures relatives à la collecte, la conservation, l'utilisation et la communication de tout renseignement sur ses clients. Ce nouveau pouvoir permettait aussi d'établir des règlements obligeant les institutions à mettre en œuvre des procédures de traitement des plaintes relatives à la protection de la vie privée et de préparer des rapports sur les plaintes reçues pour un organisme de réglementation. Il faut s'attendre à ce que le gouvernement émette de nouveaux règlements en vertu de ce nouveau pouvoir dès l'été 1998.

À la fin de l'année 1997, le ministère de la Santé de l'Ontario publiait une proposition de *Loi sur la protection des renseignements personnels dans le domaine de la santé*.⁶⁴ La Loi proposait la réglementation de l'utilisation des renseignements personnels sur la santé des personnes par divers organismes incluant le ministère de la Santé de la province, les hôpitaux et les compagnies d'assurance autorisées par la *Loi sur les assurances* de l'Ontario.⁶⁵ De tels organismes seraient alors obligés de se conformer aux règles de la protection de la vie privée concernant la collecte, l'utilisation et la communication de renseignements personnels dans le domaine de la santé ainsi que l'obligation de donner à chaque personne des droits d'accès aux renseignements sur leur propre santé. L'industrie de l'assurance a exprimé son inquiétude à savoir que si l'Ontario et les autres provinces adoptaient des lois relatives à la protection des renseignements personnels dans le domaine de la santé, ces lois ne seraient-elles pas assujetties aux différents pouvoirs législatifs relatifs à la protection de la vie privée dans chaque province?⁶⁶ (Les gouvernements du

⁶² Notes d'une allocution de l'Honorable Allan Rock, ministre de la Justice et Procureur général du Canada, prononcée dans le cadre de la dix-huitième Conférence internationale sur le droit à la vie privée et la protection des renseignements personnels (Ottawa, 18 septembre 1996).

⁶³ L.C. 1991, ch. 46, art. 459 telle que modifiée par 1997, ch. 15, art. 55; L.C. 1991, ch. 45, art. 444 telle que modifiée par 1997, ch. 15, art. 385; L.C. 1991, ch. 47, art. 489 telle que modifiée par 1997, ch. 15, art. 263.

⁶⁴ Gouvernement de l'Ontario, ministère de la Santé, *Loi sur la protection des renseignements médicaux, 1997 : Document de consultation* (novembre 1997); voir : <http://www.gov.on.ca/health>. Voir aussi : Gouvernement de l'Ontario, ministère de la Santé, *Version préliminaire de la loi sur la protection des renseignements médicaux, 1997 : Aperçu* (novembre 1997).

⁶⁵ Pour une liste des parties visées par cette disposition, voir la définition de « health information custodian » à l'article 2 de la version préliminaire de la Loi.

⁶⁶ Association canadienne des compagnies d'assurances de personnes inc., *Privacy and Financial Institutions: Input to Mr. Owens and Mr. Wright Re Task Force Research Project* (décembre 1997), p. 6: « Il y a lieu de se demander si une nouvelle réglementation provinciale en la matière ne risque pas de donner lieu à certaines incohérences [traduction libre] ».

Manitoba et de l'Alberta ont présenté des projets de loi sur la protection des renseignements médicaux, quoique les dispositions de ces projets de loi ne semblent pas s'appliquer aux assureurs.⁶⁷⁾ Cependant, des compagnies d'assurance ont déjà échangé par le passé des renseignements par le truchement d'organismes centraux tel que le Bureau de renseignements médicaux (en anglais, Medical Information Bureau, ou MIB) du Massachusetts. Tout comme les bureaux de crédit sont réglementés à cause du risque encouru par un consommateur dans le cas où des renseignements détenus à son sujet seraient inexacts, il serait approprié de réglementer les activités de mise en commun de renseignements par les assureurs.

En janvier 1998, les ministères fédéraux de l'Industrie et de la Justice publiaient un document de travail sur la législation fédérale relative à la protection de la vie privée dans le secteur privé.⁶⁸ Le document de travail propose une nouvelle loi fédérale s'appliquant à tout le secteur privé réglementé par le fédéral, associée à une nouvelle législation provinciale s'appliquant au secteur privé réglementé par le provincial. Ceci voudrait dire que le secteur des services financiers réglementé par le fédéral tomberait sous la juridiction de la loi fédérale de la protection de la vie privée.⁶⁹ Le document de travail soulève une série de questions relatives à la forme que prendrait la nouvelle législation et réclame l'avis du public sur ces questions.

Le document fédéral de travail suggère que les dix règles contenues dans le modèle de code de l'Association canadienne de normalisation constituent la base d'une nouvelle législation. Cependant, cela pose le problème de savoir si le langage utilisé dans ces règles est suffisamment précis pour être utilisé dans la législation et si d'autres attributions non incluses dans ces règles devraient être prises en considération. Le document soulève aussi la question du rôle que les codes de protection de la vie privée pourraient jouer dans le nouvel environnement législatif. Il souligne que si les codes étaient approuvés, ils pourraient servir d'outil d'interprétation de la loi ou même remplacer les fonctions de protection de la vie privée exposées dans la loi, comme dans le cas des législations respectives des Pays-Bas et de la Nouvelle-Zélande. D'un autre côté, il

⁶⁷ Voir : Manitoba's *Personal Health Information Act 1997* (Bill 51) (loi du Manitoba sur les renseignements médicaux personnels, 1997, projet de loi 51) et Alberta's *Health Information Protection Act 1997* (Bill 30), (loi de l'Alberta sur la protection des renseignements médicaux, 1997, projet de loi 30). Dans le projet de loi manitobain, la définition d'un « trustee » (fiduciaire), que l'on trouve à l'article 1 laisse entendre que ce projet de loi ne s'applique pas à un organisme du secteur privé comme une compagnie d'assurance. Dans le cas du projet de loi albertain, il semble viser essentiellement les organismes gouvernementaux et les établissements de soins de santé. La définition d'un « custodian of health information » (gardien des renseignements à caractère médical) que l'on trouve à l'article 1 comprend toute société ou autre organisme réputé être un gardien aux termes du règlement. Par conséquent, il serait possible de désigner, par voie de réglementation, les compagnies d'assurance et d'autres organismes comme étant des gardiens. Un document de travail sur le projet de loi de l'Alberta ne précise pas si l'on envisage d'ajouter les compagnies d'assurance à la liste des gardiens. Voir <http://www.health.gov.ab.ca/whatsnew/releases/protect.htm>.

⁶⁸ Gouvernement du Canada, ministères de l'Industrie et de la Justice, *La protection des renseignements personnels : Pour une économie et une société de l'information au Canada* (Ottawa, ministère de l'Industrie, janvier 1998); voir : <http://strategis.ic.gc.ca/privacy>. Voir aussi : Jeff Sallot, « Ottawa Weaving Tight Web Privacy Law », *Globe & Mail*, 27 janvier 1998, pp. A1 et A12.

⁶⁹ *La protection des renseignements personnels, supra*, note 68, p. 16. Selon ce document, le modèle de code de confidentialité de l'Association des banquiers canadiens de 1996 est un exemple intéressant d'autoréglementation. On n'y suggère cependant pas que la nouvelle loi fédérale ne s'appliquerait pas aux banques.

souligne que la nouvelle loi pourrait tout simplement ignorer les codes ou ne leur donner aucun effet juridique. Finalement, le document aborde plusieurs éléments de mise en application. À ce sujet, il suggère un processus qui verrait les plaintes concernant la protection sur la vie privée d'abord prises en charge par l'établissement puis, si la personne concernée demeure insatisfaite, dirigées vers un organisme gouvernemental d'examen des plaintes. En suggérant que l'entité responsable de l'examen des plaintes devrait être soit la personne responsable de la réglementation pour l'établissement particulier ou un directeur général d'examen des plaintes sur la protection de la vie privée comme le Commissaire à la protection de la vie privée du gouvernement fédéral, le document ne clôt pas le débat quant à l'identité de l'entité en question.

Le document de travail mentionne que l'organisme national de réforme du droit connu sous le nom de Conférence sur l'uniformisation des lois du Canada (en anglais, Uniform Law Conference of Canada, ou ULCC) est en train de rédiger un modèle de loi sur la protection de la vie privée qui pourrait servir de base pour de nouvelles législations fédérales et provinciales. Les travaux de la Conférence sur l'uniformisation des lois du Canada (ULCC) ont débuté en 1995, alors qu'elle entreprenait des discussions sur les besoins d'avoir un modèle de loi pour réglementer l'utilisation des renseignements personnels dans le secteur privé.⁷⁰ En mars 1998, des avocats chargés de développer le modèle de loi pour l'ULCC ont produit un deuxième avant-projet basé sur les règles de l'ACNOR.⁷¹ Le deuxième avant-projet impose des devoirs généraux aux organismes du secteur privé et suggère que des procédures détaillées pour obtenir le consentement des particuliers et imposer des frais donnant accès aux dossiers personnels soient élaborées dans les règlements. Le deuxième avant-projet donne aussi à un commissaire à la protection de la vie privée le pouvoir d'enquêter sur les plaintes et de formuler des recommandations aux parties impliquées. Si une plainte n'était pas réglée par ce procédé, la personne lésée aurait alors la possibilité de soumettre l'affaire à un tribunal de la protection de la vie privée. Ce dernier aurait le pouvoir d'émettre des arrêts exécutoires incluant une ordonnance de dédommagement pour les torts causés par une violation de la Loi. On s'attend à ce que le deuxième avant-projet soit de nouveau modifié; finalement, l'avant-projet remanié sera présenté à la réunion annuelle de l'ULCC prévue pour le mois d'août 1998 où il devrait être adopté par les membres de l'organisme. En supposant que le modèle de loi soit adopté par l'ULCC, il pourrait servir de point de départ pour la réforme des lois fédérales et provinciales.

⁷⁰ Pour un aperçu du premier rapport de l'ULCC au sujet du concept d'une loi servant de modèle, voir : Denis C. Kratchanov, *Conférence pour l'harmonisation des lois au Canada : Protection de la vie privée dans le secteur privé* (1995), disponible sur le site <http://www.law.ualberta.ca/alri/ulc/95pro/f95m.htm>.

⁷¹ Télécopie de Denis C. Kratchanov, ministère de la Justice (Canada) à T.S. Onyshko, 5 mars 1998, à laquelle était annexée la version préliminaire de la *Loi sur la protection des renseignements personnels dans le secteur privé*. La première version du deuxième avant-projet, qui traitait de la plupart des dispositions de cette loi en tant que modèle, à l'exception de celles qui avaient trait aux modalités d'observation, est parue à l'automne 1997. Voir la télécopie de Denis C. Kratchanov à T.S. Onyshko, 15 décembre 1997.

Préoccupations du grand public à l'égard de la protection des renseignements personnels et plaintes afférentes

Sondages sur la protection des renseignements personnels

Des sondages récents ont révélé que la protection des renseignements personnels était un sujet qui inquiétait beaucoup le grand public. Cependant, la gravité des atteintes à la vie privée que les personnes interrogées ont réellement subies reste à clarifier. Ces enquêtes ont aussi dévoilé des attitudes contradictoires quant à la confiance que les Canadiens accordent à la capacité du secteur privé à s'autoréglementer dans ce domaine. Trois études réalisées au Canada méritent un examen attentif : le sondage effectué en 1992 par la société Ekos Research Associates (Les Associés de recherche Ekos inc.) à la demande de divers clients, l'enquête menée en 1995 par la maison Louis Harris & Associates pour le compte d'Equifax Canada Inc., ainsi que l'étude réalisée en 1994 par les associations de protection des consommateurs FNACQ et CDIP Inc.

Sondage Ekos réalisé en 1992

En 1992, Les Associés de recherche Ekos inc. a réalisé un sondage auprès de 3 000 ménages canadiens au nom de divers clients des secteurs public et privé.⁷² L'étude a révélé que les préoccupations liées à la protection de la vie privée étaient « très grandes » : 92 p. 100 des personnes interrogées exprimaient des inquiétudes d'intensité modérée ou plus élevée au sujet de la protection de la vie privée.⁷³ La recherche a démontré une préoccupation particulière à l'égard de la protection des renseignements personnels. Les répondants étaient invités à évaluer l'importance de cinq domaines de la vie privée; les données recueillies ont, par la suite, été réparties en fonction du nombre de répondants qui avaient exprimé de très grandes inquiétudes à propos des sujets mentionnés. Deux aspects touchant les renseignements personnels se sont classés respectivement au deuxième et troisième rangs des préoccupations (le « contrôle des bénéficiaires des renseignements » et le « contrôle de la nature des renseignements recueillis »), devant les questions liées à l'intimité au foyer et à l'atmosphère en milieu de travail (le « fait d'être dérangé chez soi » et le « fait d'être surveillé au travail »).⁷⁴

Le sondage de la maison Ekos a aussi mis au jour des préoccupations ciblées en matière de renseignements portant sur les aspects financiers et sur la santé. Les répondants étaient invités à qualifier leur niveau de préoccupation à l'égard de dix catégories de renseignements; les données recueillies ont, par la suite, été réparties en fonction du nombre de répondants qui avaient exprimé de très grandes inquiétudes par rapport à des catégories précises de renseignements. Le classement a révélé de très grandes préoccupations à l'égard des renseignements liés à la situation financière, au dossier médical et aux habitudes d'achat des individus.⁷⁵ Il importe toutefois de noter que l'intensité de la préoccupation associée à la divulgation de renseignements

⁷² Les Associés de recherche Ekos inc., *Privacy Revealed: The Canadian Privacy Survey* (Ottawa, Les Associés de recherche Ekos inc., 1993).

⁷³ *Ibid.*, p. i.

⁷⁴ *Ibid.*, p. 10.

⁷⁵ *Ibid.*, p. 20.

personnels variait selon la nature des solliciteurs. Parmi treize catégories d'entreprises ou d'organismes, cette analyse a relégué les compagnies d'assurance et les banques au septième et huitième rangs, respectivement.⁷⁶ Les organismes qui suscitaient les plus grandes préoccupations étaient les entreprises de vente qui sollicitent les gens chez eux, les maisons de sondage, les entreprises de téléphonie, les commerces de vente au détail, les agences d'évaluation de crédit et les câblodistributeurs.

Quand on a demandé aux répondants de qualifier leur expérience personnelle en la matière, 18 p. 100 des personnes interrogées ont indiqué avoir déjà subi une atteinte « importante » à leur vie privée.⁷⁷ Les incidents vécus appartenaient aux huit grandes catégories suivantes : menaces physiques ou incidents criminels; nuisances ou perturbations; harcèlement verbal ou psychologique; utilisation abusive de renseignements, intrusion gouvernementale ou divulgation de renseignements sans consentement préalable; incidents de nature financière ou reliés au crédit; incidents impliquant les forces de l'ordre; espionnage ou entrée sans permission; en dernier lieu, incidents reliés au milieu de travail. Certaines de ces expériences semblent, à tout le moins, être assez éloignées des grands enjeux préoccupant les experts en matière de protection de la vie privée. De plus, comme l'étude elle-même l'a indiqué, la vaste majorité des Canadiens n'ont pas fait l'objet d'une véritable atteinte à leur vie privée; cette situation laisse supposer que les préoccupations de plusieurs personnes sont fondées sur d'autres facteurs. Ces facteurs peuvent être les suivants : questions de principe, situations hypothétiques, inquiétude de voir ce genre d'ennuis leur arriver ou se produire dans leur famille, ou encore les expériences de leurs amis et des membres de leur famille.⁷⁸

Enfin, l'étude Ekos a démontré que le grand public souhaite que l'on agisse dans ce domaine et qu'il accorde son soutien le plus ferme à l'action gouvernementale, initiée par les gouvernements eux-mêmes ou en collaboration avec le secteur privé.⁷⁹ Une majorité de répondants se disent d'accord avec des énoncés voulant que les gouvernements fassent adopter des lois assurant la protection de la vie privée, que les règlements liés à la protection de la vie privée s'appliquent à la fois aux gouvernements et au secteur privé, et que les gouvernements collaborent avec le milieu des affaires pour élaborer des lignes directrices en matière de protection de la vie privée. Par ailleurs, une minorité de répondants croient que la protection de la vie privée ne sera pas menacée si le secteur privé assume la responsabilité de s'autoréglementer.

Sondage Louis Harris/Equifax Canada Inc. réalisé en 1994

En août et en septembre 1994, la maison Louis Harris a effectué une enquête auprès de 1 250 Canadiens pour le compte d'Equifax Canada Inc., une importante agence d'évaluation du crédit.⁸⁰ Le sondage a démontré des niveaux élevés d'inquiétude à propos de la protection de la

⁷⁶ *Ibid.*

⁷⁷ *Ibid.*, p. 15.

⁷⁸ *Ibid.*

⁷⁹ *Ibid.*, p. 28.

⁸⁰ Le sondage effectué par la société Louis Harris & Associates en 1994 constituait un suivi d'un sondage réalisé en 1992 pour Equifax Canada Inc. par la même maison.

vie privée : 70 p. 100 des répondants ont approuvé l'énoncé suivant : « Les consommateurs ont perdu tout contrôle sur la circulation des renseignements personnels qui les concernent et qui sont utilisés par les entreprises ». ⁸¹ Cependant, faisant écho au sondage de 1992 de la maison Ekos, l'enquête Harris a démontré qu'une minorité de répondants (22 p. 100) ont déjà subi des atteintes à leur vie privée.

Le sondage a fourni des preuves que le grand public approuve certains usages des renseignements personnels. La collecte et l'utilisation de renseignements personnels à des fins d'évaluation des risques de crédit bénéficient d'un vaste soutien. Des majorités substantielles de répondants acceptent que les agences de crédit doivent recueillir et fournir des renseignements personnels en vue d'évaluer correctement les risques reliés aux prêts bancaires, aux prêts hypothécaires et à l'obtention de cartes de crédit. ⁸² Le sondage a aussi laissé entendre que les préoccupations des consommateurs reliées à l'utilisation des renseignements personnels portaient davantage sur la transmission des renseignements à l'extérieur de l'institution que sur l'utilisation des renseignements par l'institution à d'autres fins. ⁸³ Par exemple, 79 p. 100 des répondants accepteraient qu'une banque renseigne ses clients par courrier à propos des taux hypothécaires, même si ceux-ci n'ont rien demandé. Toutefois, 69 p. 100 des répondants n'accepteraient pas qu'une entreprise de services financiers, avec laquelle ils font affaires, transmettent leurs nom et adresse à une société de placement affiliée pour permettre à cette-ci de leur poster des offres de placement.

Certains résultats appuient l'idée d'une autoréglementation par les intervenants concernés pour répondre aux attentes en matière de protection des renseignements personnels. Une majorité de 74 p. 100 des répondants approuvent l'énoncé suivant : « Il serait préférable que les entreprises et les associations sectorielles adoptent volontairement des politiques de protection de la vie privée, plutôt que de s'en remettre à une intervention gouvernementale ». ⁸⁴ Un plus grand nombre de répondants se disaient plus inquiets des atteintes à la vie privée perpétrées par les gouvernements que des atteintes à la vie privée perpétrées par le secteur privé ⁸⁵, et une majorité de répondants

⁸¹ *The Equifax Canada Report on Consumers and Privacy in the Information Age*, rapport préparé pour Equifax Canada et portant sur les consommateurs et la vie privée à l'âge de l'information (Equifax Canada Inc., 1995), p. 17.

⁸² *Ibid.*, p. 43.

⁸³ *Ibid.*, pp. xiii et 20-22.

⁸⁴ *Ibid.*, p. 17.

⁸⁵ *Ibid.*, p. 18 : « Lorsqu'on leur demande quelles sont les atteintes à la vie privée qui les inquiètent le plus, 51 p. 100 des Canadiens interrogés répondent que ce sont les atteintes découlant d'activités d'organismes gouvernementaux, tandis que 37 p. 100 des répondants sont d'avis que les atteintes découlant d'activités commerciales sont plus préoccupantes. [traduction libre] ».

ont laissé entendre que, pour eux, le choix d'une banque ou d'une compagnie pouvant leur offrir de l'assurance maladie dépendait énormément de la vigueur de la politique de protection des renseignements personnels adoptée par les institutions en question.⁸⁶

Sondage FNACQ/CDIP 1994

Deux groupes de pression, l'un de Montréal, soit la Fédération nationale des associations de consommateurs du Québec (FNACQ) et l'autre d'Ottawa, soit le Centre de défense de l'intérêt public (CDIP), ont mené une étude auprès de 2 000 Canadiens en décembre 1994.⁸⁷ L'enquête laissait voir qu'en dépit des conclusions des recherches précédentes, les individus pouvaient témoigner de nombreuses atteintes personnelles à leur vie privée :

Des études antérieures ont tenté de démontrer que de nombreux Canadiens ressentent de très grandes inquiétudes devant la possibilité théorique d'atteintes insidieuses, camouflées, ou par des voies détournées, à la vie privée. Cette nouvelle étude démontre que de nombreuses atteintes à la vie privée sont passablement répandues et, de fait, remarquées par les individus. D'autre part, il est assez clair que la quantité de personnes lésées est inversement proportionnelle à la gravité de l'atteinte. En d'autres termes, des envahissements relativement bénins (par exemple, être « victime » d'activités de télé-marketing) sont très répandus, tandis que des activités plus graves en matière d'atteinte à la vie privée, telles que la vente de dossiers médicaux à des compagnies d'assurance ou l'enregistrement de conversations téléphoniques d'un employé par son employeur, sont plutôt rares.⁸⁸

Le sondage FNACQ/CDIP a cerné plusieurs activités ayant des implications en matière d'atteinte à la vie privée dont 50 p. 100 des répondants avaient déjà fait l'objet ou croyaient avoir fait l'objet : appels téléphoniques non sollicités d'entreprises, nécessité de fournir des renseignements sur ses occupations professionnelles au moment d'ouvrir un compte bancaire, appels non sollicités d'organismes de bienfaisance, entreprises vérifiant des renseignements personnels à des fins de marketing, et appels d'organismes où l'individu avait appelé sans laisser de message.⁸⁹ Parmi les autres activités dont un grand nombre de répondants avaient déjà fait l'expérience (ou le croyaient), on peut parler des ventes de renseignements personnels par certaines entreprises, du partage de renseignements personnels auprès d'entreprises associées, et

⁸⁶ *The Equifax Canada Report on Consumers and Privacy in the Information Age*, rapport préparé pour Equifax Canada et portant sur les consommateurs et la vie privée à l'âge de l'information (Equifax Canada Inc., 1995), pp. 19-20.

⁸⁷ Centre de défense de l'intérêt public et Fédération nationale des associations de consommateurs du Québec, *Des frontières à définir, la population canadienne et les renseignements personnels*, (Ottawa et Montréal, CDIP et FNACQ, 1995)

⁸⁸ *Ibid.*, pp. x-xi.

⁸⁹ *Ibid.*, p. 6.

de ventes de listes de noms par des organismes de bienfaisance.⁹⁰ Cependant, plusieurs de ces atteintes, y compris les plus courantes (par exemple, des sollicitations d'entreprises non désirées et des appels d'organismes de bienfaisance), étaient perçues comme étant « très importantes » par une minorité de consommateurs seulement.

Au sujet des moyens de protéger la vie privée, le sondage FNACQ/CDIP laisse supposer que le grand public préfère, et de loin, une intervention gouvernementale, même si l'on a constaté une méfiance à l'égard des gouvernements comme du secteur privé. En effet, 87 p. 100 des répondants ont affirmé que la protection des renseignements personnels devrait constituer une « priorité » pour les gouvernements. Cependant, une vaste majorité rejetait l'idée d'avoir à payer des impôts plus élevés pour bénéficier d'une meilleure protection de la vie privée.⁹¹ Les responsables du sondage ont tenté d'expliquer le mouvement de soutien en faveur d'une autoréglementation des intervenants concernés qui était ressorti du sondage Harris/Equifax de 1994 en précisant que la question posée à ce moment-là était conditionnelle (par exemple, : « Si les entreprises et les associations sectorielles adoptaient volontairement des politiques de protection *efficaces*, [...] »).

Plaintes au sujet d'institutions financières

Bien que les sondages évoqués précédemment laissent entrevoir de grandes inquiétudes au sujet de la protection de la vie privée, il semble y avoir peu ou pas de preuves que les consommateurs éprouvent de sérieux problèmes d'atteintes à la vie privée lorsqu'ils transigent avec les institutions financières. On peut citer trois sources principales de renseignements et de statistiques au sujet des plaintes en matière d'atteinte à la vie privée : la Commission d'accès à l'information du Québec, l'Ombudsman bancaire canadien et les ombudsmans des banques respectives, ainsi que les associations sectorielles dans le domaine de l'assurance. Toutes ces sources font état d'un nombre peu élevé de plaintes en matière d'atteinte à la vie privée.

Commission québécoise

La Commission d'accès à l'information du Québec est l'organisme gouvernemental chargé de recevoir les plaintes, d'enquêter sur celles-ci et de trouver des solutions conformément à la loi provinciale régissant la protection des renseignements personnels dans le secteur privé. En 1995 - 1996, la commission a reçu 151 plaintes touchant l'ensemble du secteur privé, dont 13 p. 100 (20 plaintes) concernaient des institutions financières et 14 p. 100 (21 plaintes), des

⁹⁰ *Ibid.*, p. 6. Un pourcentage oscillant entre 25 et 39 p. 100 des répondants ont dit qu'ils avaient subi ou cru subir ce genre d'activités.

⁹¹ Centre de défense de l'intérêt public et Fédération nationale des associations de consommateurs du Québec, *Des frontières à définir, la population canadienne et les renseignements personnels*, (Ottawa et Montréal, CDIP et FNACQ, 1995), pp. 36-37.

compagnies d'assurance.⁹² D'après la nature des plaintes reçues, il semble que deux grandes catégories se dessinent : les plaintes ayant trait à la collecte ou à la divulgation des renseignements sans autorisation préalable, et celles qui se rapportent au libellé des formulaires de consentement des individus.⁹³

À titre d'exemple de plainte de la première catégorie, une banque avait présumément colligé des renseignements personnels au sujet d'une femme qui avait fait une demande de prêt automobile, dont des renseignements sur ses pensions alimentaires et son loyer, en plus de transmettre ces renseignements à son employeur. La Commission a statué que la plainte était fondée, étant donné que le formulaire utilisé ne permettait pas à la personne concernée de fournir un consentement éclairé en matière de divulgation des renseignements, et a ordonné à la banque de prendre des mesures correctives. Dans un autre cas, une société de fiducie a révélé à l'épouse du plaignant que celui-ci disposait de trois certificats de placements garantis de divers montants. La société de fiducie voulait avertir le plaignant qu'elle s'apprêtait à fermer la succursale où il faisait affaires. Même si on ne peut taxer cette société de fiducie de mauvaise foi, son geste contrevenait à la loi québécoise puisque la société avait divulgué des renseignements à une tierce partie. Dans un autre dossier impliquant une Caisse populaire, la Commission a démontré que l'institution avait divulgué le contenu du livret de banque du plaignant à un avocat, après que celui-ci eut fait émettre un bref d'assignation concernant ces mêmes renseignements. La Commission a fait remarquer que l'avocat ne pouvait exiger la divulgation de ces renseignements, et qu'un représentant de l'institution aurait dû comparaître en cour et révéler ces renseignements à cet endroit. D'autres cas impliquent des institutions financières qui ont effectué des vérifications de crédit sans consentement éclairé ou ont divulgué des renseignements personnels à l'ex-épouse d'un plaignant ou à une tierce partie.⁹⁴

⁹² Commission d'accès à l'information du Québec, *Vie privée et transparence administrative au tournant du siècle* (juin 1997), article 1.3.3 et graphique 10, disponible sur le site Web suivant : <http://www.cai.gouv.qc.ca/sunset1.htm>. Le document n'expose pas la définition de l'expression « institution financière » au sens de la Commission; par ailleurs, les compagnies d'assurance ne semblent pas faire partie de cette catégorie.

⁹³ Les commentaires qui suivent à propos des plaintes déposées à la Commission sont étayés par des documents reliés à des enquêtes, et transmis aux auteurs de cette étude par la Commission d'accès à l'information du Québec en décembre 1997. Veuillez consulter la lettre adressée à B. Schnurr par Christiane Cliche de ladite commission le 9 décembre 1997. Un représentant de la Commission nous a précisé que ces documents pouvaient être publiés dans le cadre de cette étude.

⁹⁴ Par exemple, un plaignant prétendait qu'une banque avait divulgué des renseignements personnels à son ex-épouse (p. ex. son solde de compte en banque) et que cette indiscretion lui avait causé de gros problèmes. La Commission a statué que l'institution avait enfreint la loi et devait prendre des mesures pour s'assurer qu'une telle situation ne se reproduise plus. Dans un autre cas, le plaignant avait reçu des renseignements personnels transmis par une banque à propos d'une tierce partie, probablement par erreur. Après avoir été mise au courant de la situation, la banque a pris des mesures appropriées pour que la situation ne se reproduise plus. Dans d'autres cas, une Caisse populaire et une compagnie d'assurance n'ont pas réussi à obtenir un consentement éclairé avant de procéder à des vérifications de crédit au sujet de certaines personnes. La compagnie d'assurance a rétorqué que l'individu concerné avait consenti verbalement, ce que la personne contestait. Toutefois, la Commission fait remarquer qu'en cas de doute, le fardeau de la preuve revient à l'institution qui doit démontrer qu'elle a obtenu un consentement éclairé.

À titre d'exemple de plainte appartenant à la seconde catégorie, un regroupement de consommateurs a déposé une plainte contre une compagnie d'assurance à propos d'un formulaire de consentement qu'un assuré devait signer pour demander un remboursement de frais médicaux. Le formulaire autorisait n'importe quel médecin, hôpital, clinique ou organisme gouvernemental à fournir à l'assureur tout renseignement demandé à propos du dossier médical du patient. La Commission a statué que l'assureur n'avait pas besoin de pouvoir disposer de tout le dossier médical d'un client pour pouvoir traiter la demande de celui-ci. L'assureur a reçu l'ordre de modifier le formulaire.

Dans un autre cas de ce genre, le plaignant désirait effectuer une demande d'indemnité auprès de son assureur et devait signer un formulaire permettant à la compagnie d'assurance de recueillir et de communiquer tout renseignement personnel relié à l'assuré. La Commission a statué que le formulaire de demande d'indemnité contenait des dispositions trop vastes pour assurer un consentement éclairé et l'assureur a reçu l'ordre de reformuler les dispositions du formulaire. Dans un autre cas, le plaignant a défié une politique bancaire qui obligeait un nouveau client à produire trois pièces d'identité, c'est-à-dire un numéro d'assurance sociale, une carte d'assurance maladie et une carte de crédit. La Commission a statué que le plaignant avait en partie raison : même si la banque pouvait demander des pièces d'identité, elle ne pouvait exiger spécifiquement les pièces susmentionnées.

L'Ombudsman bancaire canadien et les ombudsmans des banques

Le bureau de l'Ombudsman bancaire canadien (« l'Ombudsman ») a été mis sur pied en 1996 par le secteur bancaire. Le bureau de l'Ombudsman est financé par les grandes banques qui ont des activités au Canada et il relève d'un conseil d'administration composé de cinq banquiers et de cinq autres membres indépendants.⁹⁵ Le mandat original de l'Ombudsman consistait à résoudre les plaintes provenant des petites entreprises; cependant, le mandat a été élargi pour inclure les plaintes des individus, lesquelles sont acceptées depuis le mois de mars 1997. L'Ombudsman peut enquêter sur une plainte d'un consommateur à l'égard d'une banque si le consommateur a déjà déposé une plainte auprès de la banque en question, a suivi les procédures requises et demeure insatisfait. Après enquête, l'Ombudsman peut émettre une recommandation non exécutoire à la banque concernée. Des statistiques sur le nombre et la nature des plaintes des consommateurs déposées au bureau de l'Ombudsman ont été publiées en juillet 1997 et démontrent qu'au cours des cinq premiers mois de service aux particuliers, le bureau a reçu 198 plaintes de ce genre.⁹⁶ Parmi celles-ci, deux seulement, soit 1 p. 100 du total, relevaient du domaine de la protection de la vie privée.

⁹⁵ L'Ombudsman bancaire canadien, *Rapport annuel 1996*; L'Ombudsman bancaire canadien, *Mémoire présenté au Groupe de travail sur l'avenir du secteur des services financiers au Canada* (North York, octobre 1997).

⁹⁶ L'Ombudsman bancaire canadien, *Rapport des neuf mois terminés le 31 juillet 1997* (1997).

Une de ces deux plaintes faisait état de la situation suivante.⁹⁷ M. X avait fait une demande pour obtenir une marge de crédit auprès de la succursale bancaire où, avec son épouse, M^{me} X, il avait contracté un emprunt hypothécaire et ouvert un compte conjoint. Mme X n'accorda pas son consentement pour que la banque obtienne un rapport de solvabilité à son sujet; toutefois, la banque montra, par la suite, un rapport de solvabilité de M^{me} X à M. X. M^{me} X se plaignit ensuite d'atteinte à sa vie privée. La banque s'est défendue en disant qu'étant donné que les autres transactions bancaires du couple avaient été conjointes, elle présumait que la demande d'une marge de crédit était conjointe aussi. L'Ombudsman a fait enquête et statué que la banque avait enfreint les principes de ses propres politiques, ainsi que plusieurs principes de protection des renseignements personnels exposés dans le modèle de code de l'Association des banquiers canadiens. Les infractions étaient reliées, entre autres, aux activités suivantes : avoir montré un rapport de solvabilité à une tierce partie extérieure à la banque et s'être contenté d'un consentement vieux de dix ans pour obtenir un rapport de solvabilité. Le conflit s'est réglé lorsque la banque a décidé de verser une somme de 4 000 \$ à M^{me} X, en guise de compensation pour les dépenses encourues et les revenus de travail perdus au cours d'une période de lutte d'un an pour amener la banque à reconnaître qu'elle avait violé sa vie privée.

L'autre plainte avait trait à une demande de prêt pour un REER effectuée au téléphone.⁹⁸ Le représentant de la banque demanda au client le nom de son employeur afin de communiquer avec celui-ci, sans toutefois obtenir le consentement du demandeur à cet effet. La banque communiqua ensuite avec l'employeur en question et se défendit en affirmant que le demandeur aurait dû savoir que la vérification d'emploi faisait partie des procédures de prêt. L'Ombudsman a conclu que la banque avait enfreint ses propres principes d'obtention du consentement des clients. La plainte a été réglée lorsque la banque a versé une somme de 500 \$ au client, en guise de compensation pour le bris de confidentialité.

Le bureau de l'Ombudsman tient aussi des statistiques sur les plaintes reçues par les ombudsmans et les responsables des plaintes des banques elles-mêmes. La plupart des banques ont maintenant leur propre ombudsman ou des responsables des plaintes chargés d'enquêter à cet effet et de résoudre les griefs des consommateurs. Les ombudsmans et les responsables de plaintes des banques règlent la grande majorité de celles-ci, comme en fait foi le nombre relativement modeste de dossiers qui se rendent jusqu'au bureau de l'Ombudsman. En juillet 1997, le bureau de l'Ombudsman a publié des statistiques sur les plaintes déposées auprès des onze banques participantes.⁹⁹ Au cours des cinq mois recensés par le rapport, les banques participantes ont reçu 1 626 plaintes de clients, mais 1 p. 100 seulement de celles-ci relevaient de la vie privée et de la confidentialité. Des entrevues menées par les auteurs de la présente étude auprès de nombreux ombudsmans et responsables des plaintes des banques ont confirmé que

⁹⁷ L'Ombudsman bancaire canadien, résumé d'incidents d'atteintes à la vie privée, (17 novembre 1997); il s'agit d'un bref document transmis aux auteurs de la présente étude par l'Ombudsman et résumant divers incidents d'atteintes à la vie privée résolus. L'Ombudsman a précisé aux auteurs qu'ils pouvaient utiliser les éléments factuels contenus dans le résumé à condition que les parties soient identifiées de façon anonyme (p. ex., M. X et M^{me} X).

⁹⁸ *Ibid.*

⁹⁹ Voir L'Ombudsman bancaire canadien, *supra*, note 96.

celles-ci reçoivent très peu de plaintes de ce type, la moyenne se situant autour de 1 p. 100, ou un peu plus, du total de toutes les plaintes reçues.¹⁰⁰ Toutes les plaintes, sauf quelques-unes, ont rapidement été résolues à la satisfaction du client.

Associations sectorielles d'assureurs

En outre, l'Association canadienne des compagnies d'assurances de personnes et le Bureau d'assurance du Canada (BAC) maintiennent des centres d'information qui acceptent les appels des consommateurs sur des questions reliées à l'assurance vie ou à l'assurance maladie. Les statistiques liées aux appels des consommateurs démontrent qu'un tout petit pourcentage des appels concernent la vie privée. Dans le cas de l'Association, 15 appels seulement sur les 75 000 reçus en 1996 relevaient véritablement de la sphère de la vie privée.¹⁰¹ « On a remarqué une certaine augmentation dans ce domaine au cours des dernières années, probablement due à une prise de conscience plus aiguë des enjeux reliés à la vie privée et à une publicité accrue autour de ces questions, mais le nombre de demandes reste très modeste », selon les dires de l'Association elle-même.¹⁰² En ce qui concerne le BAC, sur les 113 000 demandes de renseignements de consommateurs enregistrées en 1997 dans les cinq centres d'information régionaux du BAC, seuls 342 appels étaient reliés à la vie privée.¹⁰³ Règle générale, ces appels portaient sur des questions telles que le droit d'un assureur d'obtenir le dossier associé à un véhicule automobile ou un historique d'accidents, ou encore d'exercer une surveillance de l'assuré lorsqu'une demande d'indemnité pour dommages corporels était présentée.

Interprétation des données

Les commentaires qui suivent analysent le genre de plaintes reçues au sujet de la vie privée. Deux observations s'imposent. Premièrement, comme nous l'avons déjà mentionné, le nombre de plaintes est extrêmement modeste comparativement au nombre de transactions bancaires que les individus effectuent régulièrement. Les grandes institutions financières emploient des dizaines de milliers de personnes et traitent annuellement des centaines de millions de transactions reliées aux clients. Le faible taux de plaintes s'explique sans doute en partie par le fait que les individus ne savent pas ce que l'on fait de leurs renseignements personnels ou ne savent pas à qui s'adresser pour se plaindre. Cependant, le nombre négligeable de plaintes par rapport au nombre de transactions laisse supposer que les clients sont relativement satisfaits de la

¹⁰⁰ Au cours de l'automne 1997, nous avons communiqué avec les ombudsmans ou les responsables de plaintes des institutions bancaires suivantes : Banque Canadienne Impériale de Commerce, Banque Toronto Dominion, Canadian Western Bank, Banque de Nouvelle-Écosse, Banque Laurentienne du Canada, Banque HongKong du Canada, Citibank Canada, Banque de Montréal, Banque Nationale du Canada, Banque AMEX du Canada et Banque Royale du Canada. MM. Richard C. Owens et Thomas S. Onyshko ont rencontré la plupart des personnes concernées ou leur ont parlé au téléphone, en plus d'échanger de la correspondance.

¹⁰¹ Association canadienne des compagnies d'assurances de personnes inc., *Privacy and Financial Institutions: Input to Mr. Owens and Mr. Wright Re Task Force Research Project* (décembre 1997), p. 5.

¹⁰² *Ibid.*

¹⁰³ Télécopie transmise par Steven Lingard du Bureau d'assurance du Canada à T.S. Onyshko, le 22 mai 1998.

manière dont les institutions financières traitent les renseignements personnels. Deuxièmement, les plaintes déposées relatent des incidents survenus dans des circonstances diversifiées et singulières et, bien que ces événements puissent sans aucun doute préoccuper les individus concernés, ils ne témoignent pas d'une faillite systémique généralisée des mécanismes de protection de la vie privée mis en place.

Malgré tout, une mise en garde est de mise. Au cours de la réalisation de cette étude, nous avons parlé à divers intervenants du secteur des services financiers ainsi qu'à des membres d'associations sectorielles et d'associations de consommateurs; nous nous sommes penchés sur des documents portant sur la vie privée et les services financiers, et nous avons étudié des cas particuliers qui se rapportaient à notre recherche. Nous avons déployé tous les efforts nécessaires pour bien étayer nos observations et nos conclusions, mais notre recherche empirique était évidemment limitée par des contraintes raisonnables, liées à l'échéancier et aux ressources financières dont nous disposions. Donc, bien que les conclusions de notre étude s'appuient sur les recherches effectuées, nos travaux ne constituent pas une enquête exhaustive et statistiquement fiable sur la satisfaction des consommateurs.

Caractéristiques du secteur des services financiers au Canada

Avant de terminer cette introduction, il convient de se pencher sur les cinq caractéristiques du secteur des services financiers au Canada qui ont une incidence sur le dossier de la protection des renseignements personnels. Ces caractéristiques comptent parmi les principaux éléments autour desquels se sont articulées les observations et les conclusions formulées dans cette étude.

En premier lieu, la plupart des institutions financières à charte fédérale sont habilitées à offrir des services partout au Canada. En règle générale, ces organismes sont assujettis à la réglementation provinciale et, par conséquent, visés par les lois provinciales. Seules les banques sont, dans une certaine mesure, exonérées de la portée des lois provinciales.¹⁰⁴ Toutefois, les fournisseurs de services financiers qui exercent des activités commerciales au Québec peuvent être tenus de se conformer à la loi de cette province à propos de la protection des renseignements personnels dans le secteur privé.¹⁰⁵ Dans le même esprit, les assureurs établis en Ontario seraient assujettis à toute loi qui serait adoptée dans cette province relativement à la protection des renseignements à caractère médical. Il se peut donc que les institutions faisant affaires partout au pays soient aux prises avec une multitude de lois provinciales à observer, lesquelles prescriraient leurs propres normes. La situation risquerait de s'envenimer si les provinces devaient adopter des normes conflictuelles ou incompatibles. Dans un monde idéal, la réglementation en matière de renseignements personnels (pour ne pas dire tous les règlements) visant les fournisseurs nationaux de services financiers serait cohérente partout au pays.

¹⁰⁴ Pour de plus amples renseignements au sujet des mesures de réglementation provinciales visant les institutions financières et au sujet de la compétence exclusive du gouvernement fédéral en matière d'institutions bancaires, voir : Peter W. Hogg, *Constitutional Law of Canada*, format feuilles mobiles, volume 1 (Scarborough, Ont., Carswell, mise à jour reflétant la situation jusqu'en 1997), pp. 24-1ff.

¹⁰⁵ Voir, par exemple : Dubreuil, *supra*, note 50.

Deuxièmement, la protection des renseignements personnels fait, depuis toujours, partie intégrante de la tradition des banques, des sociétés de fiducie, des coopératives de crédit et des assureurs. Règle générale, les gens ne craignent pas de révéler des renseignements au sujet de leur situation financière, de leurs revenus et de leur état de santé aux institutions financières puisqu'ils estiment pouvoir leur faire confiance. Le climat de confidentialité qui règne dans ces établissements a été renforcé par les dispositions de common law qui énoncent en toutes lettres le devoir de confidentialité auquel sont tenues les banques.¹⁰⁶ En outre, une institution financière aurait bien peu à gagner et beaucoup à perdre en divulguant des renseignements personnels de nature délicate à des tiers. Si une telle pratique venait à être connue du public, les consommateurs éviteraient de faire affaires avec l'établissement en question et chercheraient à confier leurs renseignements à des institutions financières plus dignes de confiance.

Troisièmement, le secteur des services financiers du Canada est le théâtre d'une concurrence de plus en plus féroce, situation que l'on peut, du moins en partie, attribuer aux modifications qui ont été apportées aux lois fédérales qui régissent les institutions financières. Dans un tel contexte, les institutions financières ont tout à gagner en faisant savoir au public que la protection des renseignements personnels est une question qui leur tient à cœur, dans le but de gagner de nouveaux clients et de s'assurer de la loyauté des clients qu'elles possèdent déjà.

Quatrièmement, les fournisseurs de services financiers ont également déployé bien des efforts pour répondre aux préoccupations du public en matière de protection des renseignements personnels. L'industrie de l'assurance a été la première à se doter de codes en la matière, soit dès le début des années quatre-vingt. Plus récemment, les banques et les sociétés de fiducie ont emboîté le pas en réponse aux demandes pressantes que leur avaient adressées les organismes de réglementation fédéraux en ce sens. En règle générale, ces codes s'inspirent des principes énoncés dans les lignes directrices de l'OCDE et le code type de l'ACNOR. En outre, le secteur bancaire a nommé un ombudsman chargé de régler les plaintes des clients, dont celles qui ont trait à la protection des renseignements personnels. Dès lors, les clients insatisfaits des mesures mises en œuvre par une banque pour régler leur plainte peuvent porter le dossier en appel auprès de l'Ombudsman bancaire canadien. Pris un à un, ces codes comportent bien certaines carences, sans compter le fait qu'il soit, dans certains cas, plutôt difficile pour le public de s'en procurer un exemplaire. Toutefois, il ne faudrait pas laisser ces menus problèmes obscurcir le fait que les institutions financières ont fait plusieurs grands pas dans la bonne direction.

Cinquièmement, à ce jour, il n'existe que bien peu de preuves tangibles étayant l'hypothèse que le secteur des services financiers fasse l'objet d'un très grand nombre de plaintes relatives à la protection des renseignements personnels. Ainsi, les statistiques établies par l'Ombudsman bancaire canadien (dont nous traitons de façon plus détaillée ailleurs dans cette Partie) laissent entendre qu'environ un pour cent à peine des plaintes reçues sont liées à la protection des

¹⁰⁶ Pour de plus amples renseignements au sujet de l'exigence implicite de confidentialité en common law, voir la rubrique « L'exigence contractuelle implicite de confidentialité », à la Partie II.

renseignements personnels.¹⁰⁷ Étant donné la situation, les organismes de réglementation devraient faire preuve de prudence lorsqu'ils adoptent de nouveaux règlements.

En fait, compte tenu de l'ensemble de ces caractéristiques, les organismes chargés de formuler des politiques ne devraient pas se presser d'adopter de nouvelles lois et de nouveaux règlements en matière de protection des renseignements personnels. Ils devraient se montrer particulièrement soucieux des coûts inhérents à la mise en œuvre de nouvelles mesures de protection des renseignements personnels. Les institutions financières devraient en effet engager des dépenses considérables pour observer ces nouveaux règlements (par exemple, les coûts liés à l'embauche et à la formation de nouveaux employés, à l'impression de nouveaux documents, aux expéditions postales, etc.). Mais ces dernières ne seront pas les seules à devoir assumer des dépenses supplémentaires. Les contribuables feront eux aussi les frais de la mise en place des rouages d'un nouveau système de réglementation, comme les coûts liés à l'affectation d'organismes de réglementation aux questions qui ont trait à la protection des renseignements personnels. Bien sûr, ces dépenses n'entraîneront pas la faillite des institutions financières et chevaucheront parfois les dépenses que doit engager un établissement tenu d'agir avec grande circonspection pour protéger les renseignements de ses clients. Mais bien qu'ils ne soient peut-être pas matériels, ces coûts seraient extrêmement importants puisqu'ils correspondraient à des sommes considérables. Par conséquent, il serait préférable, dans une optique générale, de veiller à ce que tous les règlements que l'on songera à adopter en matière de protection des renseignements personnels soient évalués à la lumière des mécanismes existants et de la nécessité véritable d'en élargir la portée.

¹⁰⁷ Pour de plus amples renseignements au sujet de ces statistiques, voir la rubrique « Préoccupations du grand public à l'égard de la protection des renseignements personnels et plaintes afférentes », dans la présente Partie I.

II. Mesures en vigueur en matière de protection des renseignements personnels

Introduction

La Partie II porte sur les mécanismes de protection des renseignements personnels actuellement en vigueur. Elle débute par un examen des dispositions de la common law et des mesures d'équité qui assurent, à certains égards, la protection des renseignements personnels, ainsi que des grandes lacunes de ces mesures. Elle traite ensuite de l'exigence implicite de confidentialité à laquelle sont tenus les banquiers, comme l'a statué un tribunal britannique dans l'affaire *Tournier c. National Provincial & Union Bank of England*. Nous examinons ensuite les mécanismes de protection des renseignements personnels adoptés par les gouvernements fédéral et provinciaux. Il sera question des dispositions législatives fédérales visant les institutions bancaires, les compagnies d'assurance, les sociétés de fiducie et les associations de caisses de crédit, ainsi que des lois provinciales visant les fournisseurs de services financiers, y compris les bureaux de crédit. Cette section de la Partie II traite aussi des dispositions de la Loi sur la protection des renseignements personnels dans le secteur privé, la première mesure législative de protection des renseignements personnels au Canada visant l'ensemble du secteur privé. Nous terminerons par un examen approfondi des politiques des associations d'institutions bancaires, de sociétés de fiducie et de compagnies d'assurance, en matière de protection des renseignements personnels, ainsi que par un aperçu de celles que l'association des coopératives de crédit songe à adopter.

Aperçu des mesures de protection des renseignements personnels en common law et dans le cadre des actions d'équité

Le Québec est la seule province canadienne à avoir adopté une loi sur la protection des renseignements personnels visant l'ensemble du secteur privé. À l'extérieur de cette province, les personnes qui désirent obtenir réparation pour ce qu'elles estiment être une utilisation à mauvais escient de leurs renseignements personnels doivent s'en remettre aux dispositions de la common law ou aux actions en équité, à une disposition précise d'une loi fédérale ou provinciale liée à la protection des renseignements personnels, ou encore au code en la matière dont se sera doté l'établissement faisant l'objet d'une plainte. Ce paragraphe offre un bref aperçu de certaines dispositions de common law et des actions d'équité qui sont destinées à protéger certains aspects de la vie privée.¹⁰⁸ Dans ce chapitre, il sera également question de droit contractuel, de dispositions précises des lois fédérales et provinciales, de la loi du Québec sur la protection des renseignements personnels ainsi que des codes dont se sont dotées les institutions du secteur financier.

¹⁰⁸ Soulignons que cette Partie reprend certains éléments du texte de Thomas Steven Onyshko, *Informational Privacy and the Law in Canada*, thèse de maîtrise en droit (Université de Toronto, faculté de droit, automne 1995).

Les actions en responsabilité délictuelle et en équité liées à la question peuvent être classées dans deux grandes catégories : tout d'abord, les actions liées à l'atteinte à la vie privée d'une personne et, deuxièmement, les actions liées à la divulgation ou à l'utilisation des renseignements personnels. Les actions relevant de la première catégorie comprennent l'intrusion, la nuisance et l'atteinte à la vie privée, alors que celles de la deuxième catégorie comprennent la diffamation, la négligence, la décision rendue dans l'affaire *Rylands c. Fletcher*, l'abus de confiance et la violation d'une obligation fiduciaire. Toutefois, lorsque les rapports qu'entretiennent les parties sont fondés sur un contrat, ce dernier peut contenir des dispositions restreignant la capacité des intéressés à exercer un recours devant les tribunaux dans le cadre d'actions en common law ou en équité. En outre, la jurisprudence reconnaît, aux termes des dispositions implicites des contrats liant un client à une institution financière, l'exigence juridique de confidentialité à laquelle cette dernière est tenue envers son client. Par conséquent, le droit contractuel est un facteur particulièrement important dans l'étude des activités du secteur des services financiers.

Actions liées à l'intrusion

Quiconque porte physiquement atteinte à la personne, au bien ou au terrain d'une autre personne commet un délit civil d'intrusion. La jurisprudence fait état d'affaires en justice où les dispositions relatives à l'intrusion ont été invoquées pour protéger le droit à la vie privée du plaignant. Par exemple, dans les causes *Sheen c. Clegg*¹⁰⁹ et *Grieg c. Grieg*,¹¹⁰ les tribunaux ont conclu que les défendeurs avaient commis un délit civil d'intrusion lorsqu'ils avaient installé des microphones dans les domiciles des plaignants. Par ailleurs, le fait de prendre des photographies aériennes n'est pas réputé constituer une intrusion puisqu'on ne porte pas physiquement atteinte au terrain.¹¹¹ Dans le contexte des institutions financières, si une banque fouillait le coffre de sécurité d'un client sans la permission de celui-ci, elle commettrait probablement une intrusion.¹¹² En outre, une affaire entendue par les tribunaux ontariens laisse entendre que l'envoi par la poste de matériel de marketing non sollicité pourrait être une forme d'intrusion

¹⁰⁹ Non publiée. La cause a déjà été décrite dans l'édition du 22 juin 1961 du Daily Telegraph. Voir : Burns, « The Law and Privacy: The Canadian Experience », (1976) 54 *Canadian Bar Review* 1, p. 13, note de bas de page 85.

¹¹⁰ [1966] V.R. 376 (S.C).

¹¹¹ *Bernstein of Leigh c. Skyviews & General Ltd.*, [1978] 1 Q.B. 479. Voir aussi : *Malone c. Commissioner of Police (No. 2)*, [1979] 2 All E.R. 620 (Ch.D.). Le tribunal a conclu que la surveillance des conversations téléphoniques des plaignants par des responsables gouvernementaux ne constituait pas une effraction, aucune intrusion matérielle n'ayant été perpétrée sur les lieux occupés par le plaignant.

¹¹² Il est peu vraisemblable que l'utilisation non autorisée de renseignements personnels par l'institution puisse être considérée comme une intrusion sur la propriété d'un individu. Pour prouver qu'il y a eu intrusion, le client devrait démontrer qu'il possède un droit de propriété quelconque sur les renseignements personnels détenus par la banque et que les activités reprochées constituaient, pour sa personne ou sa propriété, une intervention *physique* ayant eu une incidence matérielle négative.

lorsque le matériel en question est livré au domicile de la personne.¹¹³ Cette décision ne semble toutefois pas relever de la portée du droit délictuel.

Le délit civil de nuisance a été défini dans le but de permettre au plaignant d'utiliser sa propriété et d'en jouir. Jusqu'à présent, les actions à cet égard ont été exercées pour remédier à des intrusions en série, comme le bruit, les odeurs et les vibrations, lesquelles empêchaient, dans une mesure importante et déraisonnable, le plaignant de jouir de sa propriété. Toutefois, la Cour d'appel de l'Alberta a statué que le harcèlement téléphonique pouvait également être reconnu comme une forme de nuisance lorsque poussé à l'extrême. Dans l'affaire *Motherwell c. Motherwell*,¹¹⁴ le tribunal a statué qu'il y avait bel et bien eu délit lorsque le défendeur a placé jusqu'à trente appels en une heure au domicile du plaignant. On peut aussi se demander dans quelle mesure une campagne de télémarketing comprenant plusieurs appels au même numéro ne constitue pas une forme de nuisance.

L'Ontario a reconnu le délit d'atteinte à la vie privée sans toutefois l'avoir défini en détail. La Cour de justice de l'Ontario a été la première à reconnaître cette forme de délit dans l'affaire *Saccone c. Orr*,¹¹⁵ lorsqu'elle accorda des dommages-intérêts au plaignant dont les conversations privées avec l'accusé avaient été rendues publiques par ce dernier. Ce jugement a par la suite été appuyé par deux autres décisions rendues par le juge Mandel de la Cour de justice de l'Ontario et par la Division générale de la Cour de l'Ontario.¹¹⁶ Dans l'affaire *Palad c. Pantaleon*,¹¹⁷ le juge Mandel a accordé un dédommagement de 2 500 \$ pour atteinte à la vie privée alors qu'un créancier avait harcelé son débiteur au téléphone et s'était rendu fréquemment à son domicile et à son lieu de travail. Dans l'affaire *Roth c. Roth*,¹¹⁸ le juge a accordé 25 000 \$ pour angoisse découlant d'atteinte à la vie privée, de même que 5 000 \$ en dommages exemplaires. Dans cette affaire, un des défendeurs avait attaqué un des plaignants, retiré des objets qui se trouvaient dans la résidence d'été du plaignant et verrouillé le portillon donnant accès à la route menant au chalet.

¹¹³ Dans *Allan Mather c. Columbia House*, une cause non publiée dans le cadre de laquelle la Division Générale de la Cour de l'Ontario a rendu une décision le 6 août 1972, le plaignant a intenté une poursuite en vertu de dispositions contractuelles contre la société de marketing direct Columbia House afin d'amener celle-ci à cesser d'envoyer du courrier chez lui. Le plaignant avait demandé en vain à plusieurs reprises que son nom soit retiré des listes d'envoi de cette maison. Le tribunal a jugé que la société Columbia House était tenue de ne pas envoyer de courrier inutile aux personnes qui effectuaient une demande à cet effet. Pour en arriver à cette conclusion, le tribunal s'appuyait sur le fait que Columbia House appartenait à une association nationale et souscrivait à un code de déontologie qui l'obligeait à retirer des listes d'envoi les noms des personnes qui ne voulaient pas y figurer, lorsque celles-ci en faisaient la demande. Le tribunal a déclaré Columbia House coupable d'effraction et a accordé des dommages-intérêts généraux et punitifs au plaignant. La cause est intéressante, étant donné que le tribunal a donné une portée plus grande aux arguments juridiques afin de dédommager un propriétaire très ennuyé, et qu'il a suggéré qu'un code dont l'adhésion était facultative, puisse devenir exécutoire.

¹¹⁴ [1976] 6 W.W.R. 550, 1 A.R. 47, 73 D.L.R. (3d) 62 (C.A.)

¹¹⁵ (1981), 34 O.R. (2d) 317.

¹¹⁶ Pour en savoir plus long sur l'élaboration du délit d'atteinte à la vie privée, voir : Ian Lawson, *Privacy and Free Enterprise: The Legal Protection of Personal Information in the Private Sector* (Ottawa, Centre de défense de l'intérêt public, 1992), p. 226ff.

¹¹⁷ (14 juin 1989), Ontario District Court, procès n° 266930/86 (non publié).

¹¹⁸ (1991), 4 O.R. (3d) 740 (O.C.G.D.).

Il est possible, mais peu probable, que le délit d'atteinte à la vie privée invoqué par les tribunaux ontariens puisse également s'appliquer à la collecte et à l'utilisation des renseignements personnels. En théorie, on peut avancer que la collecte et l'utilisation de renseignements personnels constituent des formes d'atteinte à la vie privée, particulièrement lorsque ces renseignements sont ensuite utilisés à l'insu ou sans le consentement de l'intéressé. Cependant, la majorité des cas de jurisprudence de l'Ontario traitent de circonstances comportant un élément d'entrée avec effraction, c'est-à-dire où le défendeur s'est physiquement introduit dans le domicile, le chalet ou le lieu de travail du plaignant. Pour l'instant, on ignore si le délit d'atteinte à la vie privée peut s'appliquer à l'information. Aux États-Unis, où la jurisprudence en la matière est beaucoup plus étoffée, la décision rendue dans l'affaire *Dwyer c. American Express*¹¹⁹ laisse entendre qu'en territoire américain, le délit d'atteinte à la vie privée ne peut être invoqué à l'égard de l'utilisation de renseignements fournis par des clients lors d'un achat.

Actions liées à la divulgation ou à l'utilisation de renseignements personnels

Le délit de diffamation peut ouvrir droit à des dommages-intérêts lorsque le défendeur publie (c'est-à-dire fournit à une ou plus d'une personne) des renseignements personnels défavorables et erronés au sujet du plaignant. Pour être réputé diffamatoire, les renseignements doivent amener le plaignant à faire l'objet de haine, de jalousie ou de ridicule, ou être susceptibles de l'humilier aux yeux de membres raisonnables de la société.¹²⁰ La diffamation ne s'applique que lorsque les allégations ne sont pas fondées; par conséquent, on ne peut l'invoquer que lorsque le comportement du défendeur comporte un élément d'erreur ou de mauvaise conduite, mais non lorsque des renseignements de nature délicate mais exacts sont divulgués à des tiers. Dans l'affaire *Gillett c. Nissen*,¹²¹ le plaignant a traduit en justice son ancien employeur. Ce dernier avait affirmé (à tort) à une entreprise qui se proposait d'offrir un poste à son ancien employé que celui-ci avait été congédié pour malhonnêteté. De même, une personne pourrait traduire en justice une institution financière qui fournirait des renseignements erronés au sujet de sa solvabilité, lesquels pourraient porter atteinte à sa réputation. Par exemple, dans l'affaire *Cossette c. Dun*,¹²² la Cour suprême du Canada a statué qu'une société établie au Québec était passible de dommages-intérêts pour avoir produit de faux renseignements au sujet de la situation

¹¹⁹ 652 N.E. 2d 1351 (1995, Ill. App. Ct.). Dans *Dwyer*, plusieurs détenteurs de cartes American Express prétendaient que la vente de renseignements sur les achats des consommateurs par ladite société constituait une atteinte à la vie privée. La Cour d'appel de l'Illinois a rejeté la plainte en disant que l'utilisation d'une carte de crédit était volontaire et que la pratique de la société se comparait aux ventes de listes d'abonnés de magazines, pratiques qui avaient été confirmées dans d'autres causes aux États-Unis.

¹²⁰ Pour en savoir plus long sur le droit en matière de diffamation, voir : Raymond E. Brown, *The Law of Defamation in Canada*, vol. I (Toronto, Carswell, 1994), pp. 1-16.1ff.

¹²¹ (1976), 58 D.L.R. (3d) 104 (Alta. S.C.).

¹²² (1891), 18 S.C.R. 22.

financière du plaignant, lequel s'est ensuite retrouvé au bord de la faillite en raison de ces faux renseignements.¹²³

La décision rendue dans l'affaire *Rylands c. Fletcher* ouvrait droit à des dommages-intérêts pour maux découlant du déversement de certaines substances dangereuses ou nocives. Dans cette affaire¹²⁴, la Chambre des lords a conclu que le défendeur, propriétaire d'une usine, était en tous points responsable lorsque le contenu d'un réservoir lui appartenant s'est déversé dans la mine du plaignant, endommageant gravement la propriété de ce dernier. Les tribunaux britanniques ont associé une responsabilité absolue au principe voulant que : « Une personne qui, à ses propres fins, apporte et garde sur un terrain lui appartenant quoi que ce soit qui soit susceptible de causer des dommages en s'en échappant doit le conserver à ses risques et, à défaut de le faire, sera tenue responsable de tous les dommages naturels que cela aura entraînés. »¹²⁵ [traduction libre]. Quelques observateurs canadiens ont fait remarquer que le jugement rendu dans l'affaire *Rylands c. Fletcher* pourrait s'appliquer à des bases de données contenant des renseignements de nature délicate, de sorte que la personne qui a la garde de telles bases de données pourrait être tenue responsable des dommages découlant de l'utilisation ou de la divulgation non autorisée de ces renseignements.¹²⁶ Par conséquent, aux termes de cette décision, une personne qui subirait des dommages suite à la divulgation non autorisée de renseignements financiers provenant de la banque de données d'une institution financière pourrait traduire cette dernière en justice. Cependant, on peut se demander si cette décision peut être interprétée comme ayant une portée telle qu'elle englobe également les renseignements personnels emmagasinés dans les banques de données. Jusqu'ici, les cas de jurisprudence ont essentiellement traité de dommages attribuables à la fuite d'objets physiques, à des incendies et à des vibrations; il pourrait s'avérer difficile de faire la preuve que la fuite de quelque chose d'aussi impalpable que des renseignements devrait être traitée de la même façon.

L'action en équité pour abus de confiance peut ouvrir droit à des dommages-intérêts aux plaignants dont les renseignements personnels ont été utilisés ou divulgués sans leur autorisation. Cette action s'applique lorsque trois conditions sont satisfaites : tout d'abord, les renseignements

¹²³ Le Juge Ritchie souligna la nécessité pour les sociétés d'évaluation du crédit de fournir des efforts raisonnables pour établir la vérité sur les renseignements de crédit, étant donné que les individus n'avaient pas accès à leurs propres dossiers. (La décision a été rendue en 1891, bien avant l'existence de lois provinciales en matière d'évaluation de crédit qui accordaient aux individus un droit d'accès à leurs propres renseignements.) Cependant, dans la cause *Cossette c. Dun*, la décision du tribunal s'appuyait sur le principe de la responsabilité délictuelle énoncé dans le *Code civil du Québec*, de sorte que le tribunal n'a pas eu à juger la cause à la lumière des grands principes de droit liés à la diffamation.

¹²⁴ (1866) L.R. 1 Ex 265, confirmée par (1868) L.R. 3 H.L. 330.

¹²⁵ (1866) L.R. 1 Ex 265, pp. 279-280. Dernièrement, la Chambre des lords a confirmé que le principe de prévisibilité s'appliquait à la règle voulant que le défendeur ne puisse être tenu responsable du déversement de matériaux que l'on ne savait pas dangereux au moment de leur déversement : *Cambridge Water Company c. Eastern Counties Leather*, [1994] 1 All E.R. 53.

¹²⁶ Voir : Dale Gibson, « Regulating the Personal Reporting Industry » dans *Aspects of Privacy Law: Essays in Honour of John M. Sharp*, éd. par Dale Gibson (Toronto, Butterworths, 1980) 111, p. 127; et Chris Dockrill, « Computer Data Banks and Personal Information: Protection Against Negligent Disclosure », (1988) 11 *Dalhousie Law Journal* 546, pp. 564-566.

doivent être réputés confidentiels; deuxièmement, les renseignements doivent avoir été confiés dans des circonstances caractérisées par une exigence de confidentialité; et, troisièmement, les renseignements doivent avoir été utilisés à des fins non autorisées ou autres que celles prévues à l'origine.¹²⁷ Il semble que les dommages-intérêts accordés aux termes d'actions en common law et en équité peuvent être octroyés aux plaignants qui remportent leur cause.¹²⁸ À ce jour, la principale affaire à avoir été entendue par les tribunaux au Canada portait sur la divulgation de renseignements commerciaux,¹²⁹ mais dans quelques causes britanniques, des poursuites ont été intentées pour assurer la protection de divers genres de renseignements personnels. Par exemple, dans l'affaire *Duchess of Argyll c. Duke of Argyll*,¹³⁰ le tribunal a émis une injonction interdisant au Duc d'Argyll de publier des renseignements que lui avait révélés en confiance son ancienne épouse bien qu'elle ait, depuis, obtenu le divorce. Et dans l'affaire *X. c. Y.*,¹³¹ le tribunal a émis une injonction interdisant à un journal de publier les noms de deux médecins infectés par le virus du sida. Si une institution financière se proposait d'utiliser, sans autorisation à cette fin, des renseignements personnels au sujet de ses clients, ces derniers pourraient exercer une action pour abus de confiance, selon la nature des renseignements et les circonstances dans lesquelles ils ont été confiés à l'institution.

Enfin, la possibilité de recourir à une action en équité pour violation d'une obligation fiduciaire peut éviter l'utilisation non autorisée de renseignements dans le cadre de certains rapports. En règle générale, les obligations fiduciaires s'appliquent à la partie qui exerce un rôle dominant au sein de relations comportant un élément particulier de confiance ou d'autorité, comme celles qui unissent l'avocat à son client ou le médecin à son patient.¹³² En outre, certains tribunaux ont également convenu d'impartir de telles responsabilités à des parties liées par des rapports autres que ceux qui sont fondés sur le principe de confiance traditionnelle, en fonction des circonstances particulières de l'affaire en cause.¹³³ L'obligation fiduciaire force le fiduciaire à

¹²⁷ Voir : Mistrale Goudreau, « Protecting Ideas and Information in Common Law Canada and Quebec », (1994) 8 *Intellectual Property Journal* 189, p. 192

¹²⁸ Voir, par exemple, les commentaires du juge Sopinka dans *LAC Minerals c. International Corona Resources Ltd.*, [1989] 2 R.C.S. 574, p. 615.

¹²⁹ *LAC Minerals c. International Corona Resources Ltd.*, [1989] 2 S.C.R. 574; *Pharand Ski Corporation c. Alberta* (1991), 7 C.C.L.T. 225 (Alta. Q.B.).

¹³⁰ [1967], Ch.D. 302.

¹³¹ [1988], 2 All E.R. 648.

¹³² Pour en savoir plus long sur le droit en matière d'obligations fiduciaires, voir : *Special Lectures of the Law Society of Upper Canada, 1991: Fiduciary Duties* (Toronto, Richard De Boo, 1991).

¹³³ La méthode générale d'essai adoptée par différents membres de la Cour Suprême du Canada fut d'abord proposée par le juge Wilson dans *Frame c. Smith*, [1987] 2 S.C.R. 99, pp. 135-136. Cette méthode d'essai suggère que des obligations fiduciaires soient imposées aux parties qui correspondent aux trois grandes caractéristiques suivantes : « 1) Le fiduciaire possède un pouvoir discrétionnaire. 2) Le fiduciaire peut exercer ce pouvoir unilatéralement et influencer sur les intérêts juridiques et sociaux du bénéficiaire. 3) Le bénéficiaire est particulièrement vulnérable ou à la merci d'un représentant détenant un pouvoir discrétionnaire. » [traduction libre]. Voir : *LAC Minerals c. International Corona Resources Ltd.*, [1989] 2 S.C.R. 574, p. 599, par le juge Sopinka. Veuillez remarquer, cependant, que les juges ont insisté pour que les obligations fiduciaires soient imposées de manière souple et qu'un lien puisse être un lien fiduciaire à certaines fins et non pour d'autres. Voir : *LAC Minerals c. International Corona Resources Ltd.*, [1989] 2 S.C.R. 574, p. 648, par le juge La Forest.

agir de bonne foi envers le bénéficiaire. Par conséquent, le fiduciaire ne saurait utiliser les renseignements qui lui sont transmis dans le cadre de ses rapports avec le bénéficiaire à des fins non autorisées. Il est possible que, dans certaines circonstances, une banque, un assureur, une société de fiducie ou une coopérative de crédit soit réputée entretenir des rapports fiduciaires avec une personne.

Droit contractuel

Le droit contractuel est une arme à double tranchant. D'une part, les termes utilisés ou sous-entendus implicitement dans un contrat peuvent assurer la confidentialité de l'information et le droit à la vie privée du client. Par ailleurs, les termes exprès d'un contrat peuvent limiter la portée des mesures de protection des renseignements personnels dont un client pourrait bénéficier autrement.

Le droit contractuel est particulièrement important dans le cas des institutions financières. En se fondant sur le précédent établi par la Cour d'appel britannique dans l'affaire *Tournier*,¹³⁴ les tribunaux ont reconnu le devoir d'assurer la confidentialité comme un élément implicite de tout contrat entre les banques et leurs clients. Cette obligation implicite limite considérablement la marge de manœuvre des institutions financières, à moins d'être levée par contrat. Cela dit, il arrive que la politique d'une institution bancaire fasse implicitement partie des contrats qu'elle offre à ses clients, de manière à ce qu'une infraction aux politiques en question constitue un bris de contrat. (Nous traitons, un peu plus loin, de l'affaire *Tournier* et de la possibilité que la politique d'une institution financière en matière de protection des renseignements personnels fasse implicitement partie d'un contrat.)¹³⁵

Cependant, les contrats entre les institutions financières et leurs clients comprennent habituellement des dispositions habilitant la banque, par consentement du signataire tel que l'exige la politique, à utiliser certains renseignements personnels. Ces textes désignent habituellement des tiers auprès desquels l'institution financière désire se procurer des renseignements ou encore auxquels elle entend fournir des renseignements au sujet de son client. Ces dispositions sont parfois très vagues, laissant place à une interprétation excessive. Il vaut la peine d'examiner le libellé de certaines de ces dispositions telles qu'on les retrouve au verso des formulaires de demande d'ouverture de compte de bien des banques. (Cette référence aux formulaires utilisés par les banques est à la fois pratique et éloquente, mais nous ne cherchons d'aucune manière à insinuer que ces dispositions sont le propre des institutions bancaires puisqu'on les retrouve également chez les assureurs, les sociétés de fiducie et les courtiers en valeurs mobilières.) Voici le libellé de dispositions que l'on retrouve au verso du formulaire Demande de services de dépôt de la Banque Scotia :

¹³⁴ [1924], 1 K.B. 461 (C.A.).

¹³⁵ Pour en savoir plus long sur l'affaire *Tournier* et des codes sur la protection des renseignements personnels, voir la rubrique « Exigence contractuelle implicite de confidentialité », dans la présente Partie II.

Les renseignements que la Banque Scotia obtient de ses clients servent à établir avec eux une relation durable, à leur proposer et fournir ses produits et services, à prendre des décisions en matière de crédit, à réaliser des études de marketing, à assurer l'observation de la réglementation, ainsi qu'à protéger leurs intérêts et ceux de la Banque. Ils peuvent également être utilisés à toute autre fin jugée compatible.

En apposant votre signature au recto de cette demande, vous confirmez que les renseignements que vous nous avez fournis sont complets et véridiques. Vous nous autorisez à donner, à obtenir, à vérifier et à échanger des renseignements sur votre solvabilité et toute autre information vous concernant avec des tiers, notamment avec des bureaux de renseignements, les filiales de la Banque et avec toute personne avec qui vous entretenez des relations financières ou avec toute autre personne, lorsque la loi le permet ou l'exige. Vous autorisez également toute personne que nous pourrions contacter à cet égard à fournir de tels renseignements. Vous nous autorisez à vous envoyer des renseignements sur les produits de la Banque et de ses filiales et vous acceptez que nous utilisions l'information vous concernant à des fins de marketing, même après que la relation établie aux termes du présent document ait pris fin.¹³⁶

Voici le libellé des dispositions que l'on retrouve dans la Demande de compte personnel et de services de la Banque Canadienne Impériale de Commerce, au-dessus de la ligne de signature :

Vous pouvez à l'occasion fournir des informations de crédit ainsi que d'autres informations me concernant, notamment celles figurant sur la présente formule : a) à toute agence de renseignements sur le crédit ou organisme chargé de communiquer les renseignements; b) à toute personne avec laquelle j'entretiens ou je me propose d'entretenir des rapports d'ordre financier; et c) à toute personne relativement à tout rapport que j'ai ou que je me propose d'avoir avec vous. Vous pouvez également à l'occasion recevoir de telles informations émanant de ces sources. J'accepte que vous puissiez utiliser ces informations pour établir et maintenir mes relations avec vous et m'offrir à l'occasion tous services permis par la loi.¹³⁷

Voici le libellé des dispositions que l'on retrouve dans la Convention de services financiers de la Banque Toronto Dominion, au-dessus de la ligne de signature :

Vous nous autorisez à obtenir des renseignements concernant votre solvabilité, ainsi que tout autre renseignement pertinent tel que prescrit ou autorisé par la loi. Vous nous autorisez à transmettre à d'autres établissements et bureaux de crédit les renseignements inscrits dans la présente demande, de même que les données relatives à votre solvabilité dans notre établissement.¹³⁸

¹³⁶ Banque Scotia, *Demande de services de dépôts*, formulaire apparemment daté du mois de septembre 1996, obtenu à l'automne 1997 auprès d'une succursale de la Banque Scotia située au centre-ville de Toronto. Signalons que ce formulaire renvoie à la brochure *Convention bancaire personnelle*, qui ne contient pas d'autres dispositions en matière de protection des renseignements personnels.

¹³⁷ Banque Canadienne Impériale de Commerce, *Demande de compte personnel et de services – Renseignements sur le compte*, formulaire apparemment daté du mois d'août 1995, obtenu à l'automne 1997 auprès d'une succursale de la CIBC située au centre-ville de Toronto.

¹³⁸ Banque Toronto Dominion, *Convention de services financiers*, formulaire apparemment daté du mois de juin 1995 et obtenu à l'automne 1997 auprès d'une succursale de la Banque TD située au centre-ville de Toronto.

Voici le libellé des dispositions que l'on retrouve à la deuxième page du formulaire d'ouverture d'un compte d'épargne personnel à la Banque Royale, au-dessus de la ligne de signature :

Vous pouvez vous procurer des renseignements concernant ma solvabilité ou ma situation financière (les « renseignements ») en consultant les conventions de services que j'ai passées avec vous ou par votre intermédiaire, ou par l'intermédiaire de bureaux de crédit, d'autres institutions financières ou des références que je vous ai fournies. Vous pouvez transmettre ces renseignements à des bureaux de crédit, à d'autres institutions financières et, avec mon consentement, à des tiers. Vous pouvez également utiliser ces renseignements pour déterminer ma situation financière et les conserver dans vos dossiers aussi longtemps qu'il est nécessaire pour assurer la prestation des services ci-dessus.¹³⁹

En outre, un formulaire de convention-client annexé à la demande de services contient les dispositions suivantes sur la collecte et l'utilisation des renseignements personnels :

Au besoin, vous pourrez :

- (a) vous procurer des renseignements concernant ma solvabilité ou ma situation financière (les « renseignements »), en m'en faisant la demande, en consultant les conventions de services que j'ai passées avec vous ou par votre intermédiaire, ou par l'intermédiaire de bureaux de crédit, d'autres institutions financières et des références que je vous ai fournies;**
- (b) utiliser les renseignements de la manière suivante :**
 - i) les transmettre à des bureaux de crédit et à d'autres institutions financières et, avec mon consentement, à des tiers;**
 - ii) les mettre à profit pour déterminer ma solvabilité;**
 - iii) les utiliser à toute fin reliée à la prestation des services que je vous demande. Vous pouvez également les donner à toute personne qui travaille avec ou pour vous, mais seulement aux fins de la prestation de ces services;**
 - iv) vous pouvez utiliser mon numéro d'assurance sociale aux fins des déclarations de l'impôt sur le revenu si je vous ai communiqué ce numéro; et**
- (c) utiliser également les renseignements pour les fins suivantes :**
 - i) pour faire la promotion de vos services auprès de moi. Vous pouvez également les intégrer aux listes de clients que vous dressez et utilisez à cette fin;**
 - ii) en faire part à d'autres membres du Groupe Financier Banque Royale (si la loi vous y autorise) pour leur permettre de faire la promotion de leurs services auprès de moi; et**

¹³⁹ Banque Royale, *Demande de compte de dépôt personnel*, formulaire apparemment daté du mois d'octobre 1997, obtenu à l'automne 1997 auprès d'une succursale de la Banque Royale située au centre-ville de Toronto.

- iii) **utiliser également mon numéro d'assurance sociale pour établir mon identité auprès des bureaux de crédit et d'autres institutions financières aux fins du rapprochement des dossiers de crédit.**

Je peux vous demander de cesser d'utiliser les renseignements aux fins indiquées en (c) ci-dessus à tout moment en communiquant avec ma succursale ou en appelant, sans frais, au numéro 1 800 ROYAL 9-9.

Vous reconnaissez que l'autorisation d'utiliser ces renseignements aux fins décrites en (c) ci-dessus relève de mon entière discrétion et que des services de crédit ou autres ne me seront pas refusés uniquement parce que je vous ai demandé de cesser d'utiliser ces renseignements à ces fins.

Pour les fins de l'alinéa (c)ii), les autres membres du Groupe Financier Banque Royale comprennent vos sociétés affiliées qui offrent à la population canadienne un ou plusieurs des services suivants : services de dépôt, des prêts et autres services financiers personnels ; services de carte de crédit et de paiement; services de fiducie et de garde des valeurs; services de valeurs mobilières et de courtage; services d'assurance.

Même si notre relation d'affaires ou la présente convention prend fin, vous pouvez conserver les renseignements dans vos dossiers et vous en servir aux fins indiquées en (b) ci-dessus.¹⁴⁰

À la lecture de ces formulaires, nous constatons qu'en règle générale, elles offrent une assez grande marge de manœuvre en ce qui a trait à la collecte et à la divulgation des renseignements personnels.

Les formulaires ci-dessus soulèvent certaines questions quant à l'interprétation des dispositions autorisant la collecte et la divulgation des renseignements personnels. (Nous pourrions aussi citer en exemple les formulaires de demande d'indemnité des assureurs, qui accordent une toute aussi vaste marge de manœuvre en matière de collecte et de divulgation de renseignements personnels.¹⁴¹) Comme nous venons de le mentionner, ces dispositions confèrent souvent aux banques une grande latitude, à tel point qu'elles constituent un risque à la protection des renseignements personnels. En outre, elles créent un déséquilibre entre les pouvoirs de l'institution et ceux de leurs clients. Les simples citoyens appelés à signer ce genre de formulaire ne possèdent pas toujours les connaissances nécessaires pour en modifier le libellé de manière à mieux se protéger. La banque refusera sans autre explication toute modification aux contrats types qu'elle utilise dans le cadre de transactions courantes avec ses clients. De plus, les gens ne sont parfois pas au courant du fait que les formulaires types des différentes banques ne sont pas tous libellés de la même façon, bien qu'ils se recoupent souvent par l'esprit du texte. À la défense des banques, on comprendra pourquoi, d'un point de vue juridique, le libellé de ces formulaires est si vague. Il serait difficile de prévoir toutes les situations dans lesquelles il est

¹⁴⁰ Banque Royale, *Convention avec le client*, formulaire apparemment daté du mois de novembre 1996 et obtenu auprès d'une succursale de la Banque Royale située au centre-ville de Toronto à l'automne 1997.

¹⁴¹ De nombreuses plaintes adressées à la Commission d'accès à l'information du Québec ont mené à la conclusion que les modalités des formulaires qu'utilisent des compagnies d'assurance de cette province sont beaucoup plus vagues que ne l'exigent les circonstances. Voir la rubrique « Préoccupations du grand public à l'égard de la protection des renseignements personnels et plaintes afférentes », à la Partie I.

nécessaire de divulguer de l'information; c'est pourquoi les avocats rédigent parfois ces documents en des termes aussi vagues, particulièrement lorsqu'il n'y a aucune négociation en cause pour les forcer à adopter une approche plus circonscrite. Du fait, en partie, que les formulaires types ne font l'objet d'aucune négociation au moment de la signature, les tribunaux ont tendance à les interpréter en faveur du client. Par exemple, alors que le formulaire de la Banque Scotia semble, à première vue, être rédigé en des termes qui permettent la divulgation de pratiquement tout renseignement, il y a fort peu de chances qu'un tribunal accepte que cette institution fasse valoir de telles dispositions pour justifier des actes dont la portée excéderait, du point de vue du client, les pouvoirs que ce dernier estimerait avoir conférés à l'institution lorsqu'il a apposé sa signature sur ce document.

Voilà qui illustre les limites du droit contractuel en matière de protection des renseignements personnels. Cependant, il faut également tenir compte du volume des services que fournissent les banques et les assureurs. Les problèmes et les coûts qui seraient liés à la négociation de chaque contrat signé avec chaque client seraient respectivement si complexes et prohibitifs que la quasi-totalité des consommateurs ne pourraient plus faire affaires avec les banques et les compagnies d'assurance. Par conséquent, un contrat, au même titre qu'un mécanisme d'application lors d'une poursuite devant les tribunaux, ne doit pas être considéré comme un document exhaustif servant à assurer la protection des renseignements personnels.

Les carences de mesures fondées sur l'équité et la common law

Le droit de la responsabilité délictuelle et de l'équité, de même que le droit contractuel, protègent certains aspects de la vie privée. Cependant, les mesures fondées sur le droit et l'équité comportent deux carences majeures dont il faut tenir compte. En premier lieu, il est parfois difficile de faire la preuve des préjudices que le plaignant affirme avoir subis suite à la divulgation non autorisée ou de la mauvaise utilisation de renseignements personnels.¹⁴² Si le plaignant ne parvient pas à en établir la preuve de façon satisfaisante, sa demande sera rejetée ou les tribunaux ne lui accorderont qu'un dédommagement minime, selon la nature du recours. Cela peut être juste dans les circonstances, mais ne contribue pas vraiment à la mise en place de normes de conduite. Deuxièmement, le coût prohibitif d'un recours en justice découragera bien des gens d'emprunter cette voie pour obtenir un dédommagement. D'ailleurs, la divulgation ou la mauvaise utilisation de renseignements personnels donne souvent lieu à des dédommagements minimes, bien que le plaignant ait dû engager des sommes considérables pour porter l'affaire devant les tribunaux.

¹⁴² Voir, par exemple, l'affaire en diffamation *Gillett c. Nissen* (1976), 58 D.L.R. (3d) 104 (Alb. S.C.). Dans cette affaire, le plaignant s'est vu refuser un nouvel emploi parce que son ancien employeur avait fait de fausses déclarations au sujet de son honnêteté; le plaignant n'a cependant pas réussi à faire la preuve que ces déclarations étaient à l'origine du refus de lui accorder l'emploi pour lequel il avait postulé.

L'exigence contractuelle implicite de confidentialité

Tournier et l'exigence implicite de confidentialité

Selon la jurisprudence de la common law, tous les rapports professionnels entre une banque et son client sont assujettis à une exigence contractuelle implicite de confidentialité. Par le fait même, cette exigence devrait également s'appliquer aux rapports qu'entretiennent d'autres institutions financières avec leurs clients. Les exigences de la common law ont une incidence directe sur la façon dont les institutions financières traitent les renseignements personnels qu'elles possèdent au sujet de leurs clients. Aux termes de la common law, elles ne disposent que d'une partie de la marge de manœuvre accordée aux autres genres de sociétés, ce qui restreint considérablement leur capacité de divulguer des renseignements personnels à des tiers.

L'exigence implicite de confidentialité a été établie dans une affaire qui a fait jurisprudence au Royaume-Uni, *Tournier c. National Provincial & Union Bank of England*.¹⁴³ Dans cette affaire, une banque avait divulgué des renseignements au sujet d'un de ses clients, M. Tournier, à son employeur. De façon plus précise, la banque avait révélé que le compte de M. Tournier était souvent à découvert et qu'il avait endossé un chèque pour le compte d'un preneur de paris. Lorsque l'employeur refusa d'embaucher M. Tournier à la fin de son stage, ce dernier intenta une poursuite contre la banque. Il alléguait qu'une disposition contractuelle implicite interdisait à la banque de divulguer des renseignements au sujet de son compte à des tiers.

La Cour d'appel britannique a fait valoir qu'il n'existait aucune disposition contractuelle tenant la banque à une confidentialité absolue. Par contre, elle a reconnu qu'un contrat entre une banque et son client comporte une exigence implicite de confidentialité assujettie à quatre conditions. Le tribunal, composé de trois juges, a refusé de formuler une définition exhaustive des devoirs de la banque en la matière, mais a traité de l'étendue, de la qualité opportune et de la nature de ces exigences.

En ce qui a trait à la qualité opportune et à l'étendue de la confidentialité, le juge Bankes a statué ce qui suit :¹⁴⁴

¹⁴³ [1924] 1 K.B. 461 (C.A.).

¹⁴⁴ Les trois juges de la Cour d'appel ont formulé des raisons différentes, bien que celles de Bankes aient souvent été citées par la suite dans des affaires de même nature. Compte tenu des différentes raisons, la véritable portée du jugement dans l'affaire *Tournier* n'est pas aussi précise qu'on pourrait le souhaiter. En fait, un juge a même adopté une approche beaucoup plus étroite. Alors que Bankes et Atkin étaient d'avis que l'exigence contractuelle implicite de confidentialité englobait tous les renseignements recueillis auprès du client ou dans le cadre des rapports que celui-ci entretient avec la banque, Scrutton estimait que cette exigence ne s'appliquait qu'au compte bancaire du client et aux transactions s'y rattachant, mais non aux renseignements provenant d'autres sources. De plus, bien que Banks et Atkin étaient d'avis que cette exigence ne pourrait éventuellement entraîner la fermeture d'un compte, Scrutton estimait qu'elle ne s'appliquait pas aux renseignements recueillis avant l'établissement de rapports contractuels entre la banque et son client, non plus qu'après la fin de ces rapports.

- l'exigence de confidentialité n'est pas levée du seul fait qu'un compte soit fermé; les renseignements sur un compte demeurent confidentiels à moins que la banque ne soit dégagée de ses devoirs aux termes d'une autre condition;
- les renseignements réputés confidentiels ne se limitent pas qu'à l'état du compte; ils comprennent également toute information associée à ce compte, comme l'adresse du client et les autres renseignements personnels qu'on y retrouve; et
- l'exigence de confidentialité ne se limite pas qu'aux renseignements obtenus auprès des clients; elle comprend également les renseignements recueillis auprès de tiers, sous réserve que ces renseignements aient été obtenus par des employés de la banque dans le cadre de leurs fonctions officielles.

Le juge Bankes a ensuite formulé les quatre conditions relatives à l'exigence de confidentialité, lesquelles sont encore pertinentes aujourd'hui. Il a statué qu'une banque peut divulguer des renseignements personnels au sujet de ses clients :

- lorsque la loi exige qu'ils soient divulgués;
- lorsque l'intérêt public le justifie;
- lorsque les intérêts de la banque le justifient; et
- lorsque la divulgation est effectuée avec le consentement exprès ou implicite du client.

L'exigence implicite de confidentialité reconnue dans l'affaire *Tournier* a été invoquée et interprétée par d'autres tribunaux en Angleterre, au Canada, aux États-Unis et dans d'autres pays membres du Commonwealth.¹⁴⁵ Par exemple, dans l'affaire *Hull c. Childs & Huron and Erie Mortgage Corp.*, la Haute Cour de l'Ontario a statué que la divulgation du montant de la marge de crédit à un tiers constituerait une infraction à l'exigence implicite de confidentialité, même si cette personne présentait un chèque en blanc autorisant son bénéficiaire à retirer le solde total du compte.¹⁴⁶ Et, dans l'affaire *Guertin c. la Banque Royale du Canada*, la Haute Cour de l'Ontario

¹⁴⁵ Le jugement rendu dans l'affaire *Tournier* a récemment été appuyé par une décision du Judicial Committee of the English Privy Council, *Robertson c. Canadian Imperial Bank of Commerce*, [1995] 1 All E.R. 824 (P.C.). Exemples de jugements rendus en Australie : *Smorgen c. Australia and New Zealand Banking Group Ltd* (1976), 134 C.L.R. 475; *Re Peter Lawrence Crawley et al* (1981), 52 F.L.R. 123; *Re Kingston Thoroughbred Horse Stud and Australian Tax Office No. N85/130* (1986) (Administrative Appeals Tribunal); *Kabwand Pty. Ltd. c. National Australian Bank Limited* (1989), No. G355, Fed. No. 195 (Aust. F.C.); *Australian Securities Commission c. Westpac Banking Corporation* (1991), A.C.S.R. 350, 32 F.C.R. 546. Exemples de jugements rendus aux États-Unis : *Jacobsen c. Citizens State Bank* (1979), 587 SW2d 480 (Tex. Civ. App.); *Suburban Trust Co.* (1979), 408 A.2d, p. 758; *State c. McCray* (1976) 15 Wash. App. 810, 551 P.2d 1376; *Burrows c. Superior Court of San Bernardino County* (1974), 13 Cal. 3d 238, 118 Cal. Rptr. 166, 529 P.2d 590; *Pigg c. Robertson* (1977), 549 SW2d 597; *Taylor c. Commercial Bank* (1903) 174 NY 181, 66 NE 726.

¹⁴⁶ *Hull c. Childs & Huron and Erie Mortgage Corp.*, [1951] O.W.N. 116.

a statué que l'exigence de confidentialité d'une banque envers son client comprend également un volet interdisant aux employés de cette banque d'utiliser les renseignements concernant leurs clients à des fins personnelles.¹⁴⁷ D'autres jugements ont laissé entendre que la divulgation de renseignements personnels à des tiers dans le cadre d'une société de portefeuille ou entre filiales d'une même société pourrait aussi constituer une infraction à l'exigence de confidentialité.¹⁴⁸

La jurisprudence interprète également l'étendue des quatre conditions énoncées par le juge Banks. La première condition traite de la nécessité de divulguer des renseignements personnels dans le cadre d'un procès ou à la suite d'une ordonnance du tribunal.¹⁴⁹ Il est aussi parfois nécessaire de divulguer de tels renseignements aux termes de dispositions des lois canadiennes ou étrangères.¹⁵⁰ Lorsqu'une banque doit divulguer des renseignements personnels au sujet d'un de ses clients dans le cadre d'un procès, elle devrait prendre des mesures raisonnables pour l'en informer, bien qu'elle n'y soit pas formellement tenue, compte tenu du fait qu'il est parfois difficile de communiquer avec les clients dans des délais aussi courts.¹⁵¹

¹⁴⁷ (1983), 43 O.R. (2d) 363, p. 374. Voir aussi le jugement rendu récemment dans l'affaire *Hongkong Bank of Canada c. Phillips*, [1997] M.J. No. 134 (Man. Q.B.), dans lequel la Cour du banc de la Reine du Manitoba a fait valoir que la confidentialité à laquelle une banque est tenue envers son client ne modifiait pas son devoir d'aviser un autre client de son droit de faire appel à un service juridique ou financier indépendant à l'égard d'une transaction comportant des risques dont la banque est tout à fait consciente.

¹⁴⁸ [1987] A.C. 45 pp. 53-54, [1986] 3 All E.R. 468 pp. 475-476 (C.A.); *Bhogal c. Punjab National Bank*, [1988] 2 All E.R. 296, p. 305 (C.A.).

¹⁴⁹ Voir : Bradley Crawford, *Crawford and Falconbridge on Banking and Bills of Exchange*, 8^e édition (Toronto, 1989), pp. 806 à 811. Le droit canadien ne reconnaît aucun privilège en matière de renseignements bancaires. Voir, par exemple : *La Reine c. Spencer* (1983), 2 C.C.C. (3d) 526 (C.A.), par McKinnon A.C.J.O. Dans l'affaire *Haughton c. Haughton*, [1965] 1 O.R. 481, le tribunal a fait valoir qu'une ordonnance à comparaître n'était pas suffisante pour forcer le directeur/la directrice d'un établissement bancaire à témoigner, mais qu'une ordonnance de divulgation comportait un élément de « force de loi » qui aurait préséance sur le devoir de confidentialité auquel la banque était tenue. Par la suite, le jugement rendu dans l'affaire *Haughton* a été appuyé par la décision rendue dans l'affaire *Royal Bank of Canada c. Art's Welding & Machine Shop* (1989), 34 C.P.C. (2d) 190.

¹⁵⁰ Voir : *CIBC c. A.-G. Can.* (1962), 35 D.L.R. (2d) 49 (S.C.C) et Rosemary Regan, « You Don't Say » (1982) 89 *Canadian Banker* 32. Voir aussi : *Budzich c. Toronto Dominion Bank*, [1996] 2 C.T.C. 278, affaire dans laquelle les parties ont reconnu qu'une demande de Revenu Canada présentée aux termes d'un pouvoir réglementaire avait « force de loi »; et *Park c. Bank of Montreal*, [1997] B.C.J. N° 787, où le tribunal a conclu que la banque avait agi conformément à la loi en divulguant, par l'entremise d'une succursale située en Corée, des renseignements à un procureur coréen, puisque la loi coréenne exigeait que ces renseignements soient divulgués. Il y avait donc « force de loi ».

¹⁵¹ *Robertson c. Canadian Imperial Bank of Commerce*, supra, note 145 par Lord Nolan. Il peut également y avoir des circonstances où une banque a le droit de ne pas aviser son client, c'est-à-dire aux termes d'un consentement ou lorsque cela s'impose pour protéger les intérêts de la banque ou encore par devoir public : voir *ibid.*; *X A.-G. c. A Bank*, [1983] 2 All E.R. 464; et *Marcel c. Commissioner of Police of the Metropolis*, [1992] 1 All E.R. 72, Ch. 225. Des tribunaux canadiens se sont également penchés sur la question. Voir : *Budzich c. Toronto Dominion Bank*, [1996] 2 C.T.C. 278, affaire dans laquelle le tribunal a tenu compte de la décision *Robertson* et suggéré qu'une banque peut être obligée de prévenir un client lorsqu'elle est forcée, par Revenu Canada, de divulguer des renseignements au sujet de son compte bancaire. Voir aussi : *Foundation Co. of Canada Ltd. c. Dhillon*, [1995] O.J. 3211 (Division générale de la Cour de l'Ontario), où le tribunal a déclaré que la banque n'était pas tenue d'aviser le client dans le cas des prétentions établies prima facie voulant que ce client ait commis un abus de confiance, une fraude ou ait accepté des pots-de-vin. Voir aussi : *Park c. Bank of Montreal*, [1997] B.C.J. N° 787, où le tribunal a fait valoir que lorsque la situation a un lien avec une question de nature autre que criminelle, la banque a le devoir de faire de son mieux pour aviser le client de la nécessité de divulguer des renseignements personnels à son sujet. Par contre, dans le cas de divulgations ayant un lien avec une enquête criminelle, il n'existe aucune disposition obligeant la banque à prévenir le client avant de divulguer les renseignements.

La deuxième condition porte sur la nécessité de divulguer des renseignements personnels dans l'intérêt public.¹⁵² On a suggéré que cette condition pourrait s'appliquer dans le cas de banques qui devraient fournir des renseignements à la police au sujet de personnes soupçonnées d'activités criminelles ou de collaboration avec l'ennemi en temps de guerre. Cependant, cette condition n'a été invoquée que très rarement.¹⁵³ Dans l'affaire *La Reine c. Lillico*, la divulgation de renseignements à la police aux fins d'une enquête judiciaire sur des actes commis par le client était justifiée puisqu'elle servait l'intérêt public.¹⁵⁴ Dans cette même affaire, on a également fait valoir que bien que la possession de tels renseignements s'accompagne de devoirs de confidentialité qui pourraient être invoqués aux termes de l'article 8 de la *Charte canadienne des droits et libertés*, l'intérêt public en matière d'application de la loi par le biais de la divulgation de renseignements bancaires généraux (par exemple, la confirmation qu'un chèque donné a été déposé dans le compte du client) a préséance sur toute atteinte à la vie privée du client tel que l'entend l'article 8 de la *Charte*.¹⁵⁵ Toutefois, bien qu'une banque puisse être tenue de divulguer des renseignements au sujet d'un de ses clients pour satisfaire à une enquête judiciaire, le fait d'affirmer qu'un client est habituellement « malhonnête » ne se justifie pas au nom de l'intérêt public.¹⁵⁶

La troisième condition s'applique lorsqu'une banque se voit dans l'obligation de divulguer des renseignements personnels pour répondre à ses propres intérêts, comme lorsqu'elle doit poursuivre un client dont le compte est à découvert ou qu'elle prend des mesures de protection contre des activités criminelles ou frauduleuses.¹⁵⁷ En pareil cas, une telle divulgation doit s'avérer raisonnablement nécessaire pour assurer la protection de la banque et n'est évidemment pas permise aux seules fins de tirer profit de la situation.¹⁵⁸ L'affaire *Montgomery c. Ryan* constitue un excellent exemple de ce genre de situation, alors que la banque avait eu raison de prévenir une personne intéressée à acheter un bien que ce bien avait été donné en garantie d'une

¹⁵² *Tournier, supra*, note 143, p. 473. Voir aussi : *Weld-Blundell c. Stephens*, [1920] A.C. 956, p. 965.

¹⁵³ *Crawford & Falconbridge, supra*, note 149, p. 811. Voir, par exemple : *Libyan Arab Foreign Bank c. Bankers Trust Co.*, [1988] 1 Lloyd's Rep. 259.

¹⁵⁴ (1994), 92 C.C.C. (3d) 90 (Division générale de la Cour de l'Ontario)

¹⁵⁵ *Ibid.*, pp. 93-94 et 95.

¹⁵⁶ *Murano c. Bank of Montreal* (1995), 31 C.B.R. (3d) 1, 20 B.L.R. (2d) 61, affaire dans laquelle le tribunal a rejeté l'argument voulant que le fait qu'une banque puisse qualifier un client de « malhonnête » auprès des associés de ce dernier, de ses fournisseurs et d'autres prêteurs était une pratique justifiée par le devoir public. Cependant, il faudrait voir aussi : *Canadian Deposit Insurance Corp. c. Canadian Commercial Bank* (1989), 64 Alta. L.R. (2d) 329, 71 C.B.R. (N.S.) 239, 95 A.R. 24, A.W.L.D. 367, affaire dans laquelle le tribunal a statué que parce que la Société d'assurance-dépôt du Canada devait consulter des comptes de banque confiés au séquestre, l'intérêt public exigeait que la divulgation des renseignements soit d'une ampleur qui dépasse les résultats d'une recherche documentaire.

¹⁵⁷ *Tournier, supra*, note 143, p. 473, *par* Bankes; p. 481, *par* Scrutton; p. 486, *par* Atkin.

¹⁵⁸ *Ibid.*, p. 481, *par* Scrutton.; p. 486, *par* Atkin. Aussi, dans l'affaire *Park c. Bank of Montreal*, [1997] B.C.J. N° 787, le tribunal a statué que la condition invoquée devait être interprétée avec circonspection; par contre, dans l'affaire *Royal Bank of Canada c. Brattberg* (1993), 11 Alta. L.R. (3d) 190, 8 W.W.R. 139, 143 A.R. 131, A.W.L.D. 684, la banque a été autorisée à révéler qu'elle avait acquis un droit de sûreté dans la propriété du client dans le but de protéger ses intérêts. Voir aussi : *Crawford & Falconbridge, supra*, note 149, pp. 812 à 814.

note représentant un endettement.¹⁵⁹ Dans l'affaire de la *Canadian Imperial Bank of Commerce c. Sayani*, la Cour d'appel de la Colombie-Britannique a statué qu'il était « inconcevable qu'un banquier honnête accepte de transiger avec une personne à condition de ne révéler à qui que ce soit des renseignements qui permettrait à son client de duper un tiers ». ¹⁶⁰ Et dans l'affaire *Sutherland c. Barclays Bank Ltd.*, il a été statué que le défendeur (la banque) avait agi de façon adéquate et dans son propre intérêt en divulguant à l'époux de la plaignante que le compte de celle-ci était à découvert et que la plupart des chèques imputés à ce compte étaient rédigés à l'ordre de preneurs de paris.¹⁶¹

La quatrième et dernière condition traite du consentement exprès ou implicite du client à ce que la banque divulgue des renseignements personnels à son sujet.¹⁶² Cette situation se produit couramment lorsque le client autorise la banque à communiquer des renseignements à son sujet à un tiers aux fins d'établir sa solvabilité. Bien que les circonstances dans lesquelles le client consent expressément à la divulgation de tels renseignements soient relativement simples, celles où il est question de consentement implicite sont parfois plus difficiles à démêler par les tribunaux. Les tribunaux canadiens ont statué qu'un simple chèque en blanc ne constitue pas une autorisation implicite, de la part du signataire, à divulguer des renseignements personnels à des tiers.¹⁶³ Par ailleurs, dans l'affaire *Royal Bank of Canada c. Art's Welding & Machine Shop*, le tribunal a statué que lorsqu'un client sait pertinemment que le gagne-pain d'une autre personne est tributaire de leurs rapports contractuels, ce client consent à ce que la banque fournisse des renseignements au sujet de son compte à la personne en question.¹⁶⁴ Soulignons également que bien que l'exigence de confidentialité ne s'applique pas aux renseignements divulgués dans ces conditions, la banque peut quand même faire l'objet d'une poursuite pour dommages-intérêts si ladite divulgation devait se traduire par des pertes financières ultérieures.¹⁶⁵

Le jugement rendu dans l'affaire *Tournier* restreint la marge de manœuvre des banques et, par conséquent, des autres institutions financières en matière de divulgation des renseignements personnels à des tiers. Cependant, il ne couvre pas tous les aspects de la question. Par exemple, il n'impose aucune restriction quant au genre de renseignements qu'il est possible de recueillir au sujet d'un client. Il ne traite d'aucune façon de la nature des démarches qu'une banque peut

¹⁵⁹ (1907), 9 O.W.R. 572 (H.C.), inf. (1908), 16 O.L.R. 75 (C.A.).

¹⁶⁰ (1993), 83 B.C.L.R. (2d) 167, p. 172, par Taylor.

¹⁶¹ (1938) 5 L.D.A.B. 163, par Du Parcq. Ce juge a également statué que la plaignante avait donné son consentement implicite à la divulgation.

¹⁶² *Tournier*, supra, note 143, p. 473, par Bankes. Le consentement du client relève des faits : *ibid.*, p. 468, par Atkin.

¹⁶³ Voir *Hull c. Childs*, supra, note 146.

¹⁶⁴ *Royal Bank of Canada c. Art's Welding & Machine Shop*, (1989), 34 C.P.C. (2d) 190, A.W.L.D. 653, C.L.D. 895. Voir aussi : *Hong Kong Bank of Canada c. Phillips*, [1997] M.J. N° 134 (Man. Q.B.). Dans cette affaire, le tribunal a statué que lorsqu'un client d'une banque où son compte est en souffrance amène de nouveaux clients pour qu'ils puissent contracter un prêt et investir dans son entreprise, ce même client est réputé avoir consenti implicitement à ce que la banque divulgue des renseignements que ce dernier lui avait fournis relativement à cette entreprise commerciale.

¹⁶⁵ Voir supra, note 150.

entreprendre en ce sens, à savoir ce qui est acceptable et ce qui outrepassé les limites d'une enquête justifiable. Ce jugement ne traite pas non plus des fins auxquelles une banque peut utiliser les renseignements qu'elle possède au sujet d'un client. Il n'empêcherait pas une banque d'utiliser ces renseignements à d'autres fins, comme la promotion d'un service bancaire qui n'a aucun lien avec les fins pour lesquelles le client avait fourni des renseignements personnels en premier lieu. Enfin, ce jugement ne confère aucun droit d'accès à des renseignements personnels, ni droit de rectification de renseignements personnels erronés. Pourtant, de nos jours, les principes régissant la collecte, l'utilisation ou la divulgation de renseignements personnels et les droits d'accès à ces renseignements font partie intégrante des mesures de protection de la vie privée.

Dispositions implicites et politiques relatives à la vie privée

Les politiques relatives à la vie privée qu'ont volontairement adoptées nombre d'institutions financières peuvent être interprétées comme les dispositions implicites des contrats que ces établissements concluent avec leurs clients. Aux termes de la common law, un tribunal peut affecter une disposition implicite à tout contrat dans le but de préciser la nature des rapports qui unissent les intéressés¹⁶⁶ ou lorsque les pratiques commerciales habituelles¹⁶⁷ démontrent que de telles dispositions sont réputées faire partie intégrante du contrat. Cependant, même si les tribunaux sont prêts à reconnaître que les politiques relatives à la vie privée correspondent à des dispositions contractuelles implicites, le plaignant devra tout de même prouver qu'il y a eu atteinte à ses droits contractuels et qu'il serait justifié de lui accorder un dédommagement de nature financière ou autre. En outre, lorsqu'un client signe un contrat contenant des dispositions autorisant spécifiquement la divulgation ou l'utilisation de renseignements personnels, lesdites dispositions auront probablement préséance sur toute mesure implicite. Par conséquent, les éléments des politiques relatives à la vie privée sont mieux servis par un mécanisme de résolution des différends, comme l'ombudsman de la banque.

On peut se demander si les modalités de la politique d'une institution financière en matière de respect de la vie privée sont nécessaires pour faire le point sur les rapports contractuels qui unissent l'établissement à ses clients. Comme l'a écrit le professeur G.H.L. Fridman au sujet du concept de l'efficacité commerciale : « La théorie derrière cette doctrine veut que si un tiers avait attiré l'attention des parties vers le problème à résoudre, elles auraient convenu que la solution aurait dû se trouver dans le contrat de la façon suggérée subséquentement, pour les différends

¹⁶⁶ « La loi stipule clairement que lorsqu'il est raisonnable de s'y attendre, compte tenu des circonstances, ou qu'il existe une pratique commerciale courante susceptible d'avoir une incidence sur les rapports qu'entretiennent les parties, le contrat peut être réputé comporter une disposition d'accord implicite entre ces parties. » [traduction libre] Voir : *Midland Doherty Limited c. Rohrer*, (1984) 62 N.S.R. (2d) 205 p. 212 (N.S.T.D.).

¹⁶⁷ « L'usage, lorsqu'il est bien établi évidemment, peut avoir une incidence sur le libellé d'un contrat; mais on doit en être raisonnablement assuré et il doit faire à tel point partie des règles de l'art que l'on peut assumer qu'il est un élément implicite de tout contrat. » [traduction libre] Voir : *Georgia Construction c. Pacific Great Eastern R. Co.*, [1929] 4 D.L.R. 161, p. 163 (S.C.C.)

ultérieurs, comme une disposition implicite. »¹⁶⁸ Si le tiers avait fait part au client de la politique de l'établissement en matière de protection des renseignements personnels au moment de signer le contrat, ce dernier aurait probablement perçu cette politique comme faisant partie intégrante du contrat. Par contre, l'institution financière ne verrait pas la situation du même œil. De même, on pourra faire valoir que les modalités de la politique de l'institution en matière de protection des renseignements personnels ne font pas partie des rouages du mécanisme contractuel à proprement parler, puisque nombre de ces contrats ont été ratifiés avant que les institutions financières canadiennes n'adoptent de telles politiques.

En outre, les tribunaux peuvent reconnaître la validité d'une disposition implicite en s'appuyant sur les pratiques commerciales habituelles d'une entreprise, d'un corps de métier et d'une profession. Toutefois, à venir jusqu'à présent, les tribunaux ont fait preuve d'une certaine rigidité quant à la reconnaissance de ce principe. L'usage doit, pour être reconnu comme faisant partie intégrante d'un contrat, être accepté et mis en pratique par la majorité des entreprises qui exercent des activités dans ce domaine.¹⁶⁹ Il est possible que ce soit le cas de la politique de l'Association des banquiers canadiens en matière de protection des renseignements personnels. Cette politique est appliquée, à quelques modalités près, depuis 1990 et a fait l'objet d'une grande campagne de sensibilisation destinée au public et au gouvernement; elle se voulait la réponse de l'industrie aux inquiétudes relatives à l'utilisation des renseignements personnels par les institutions financières. De même, la politique emploie des expressions réglementaires pour qualifier les devoirs auxquels les banques sont tenues. Ces faits portent à croire que l'ensemble de l'industrie bancaire accepte cette politique et la met en œuvre.

Au Canada, les tribunaux ont peu statué jusqu'à maintenant dans des causes où il était précisément question de l'insertion, dans un contrat, des modalités d'une politique à laquelle les intéressés sont libres d'adhérer.¹⁷⁰ Dans l'affaire *Banks c. Biensch*,¹⁷¹ le tribunal a appuyé sa décision sur le code de déontologie qu'a publié une association d'éleveurs de taureaux et de vaches Charolais, lequel garantissait que les animaux vendus étaient en état de se reproduire. Le tribunal a statué que les pratiques commerciales habituelles de cette industrie étaient si courantes qu'elles étaient réputées faire partie intégrante de tout contrat de vente d'animaux reproducteurs. Dans l'affaire *Smith c. Kamloops et la District Elizabeth Fry Society*,¹⁷² une travailleuse sociale avait été mise à pied en raison des rapports qu'elle entretenait avec un client qui recevait des consultations dans l'établissement où elle travaillait. La poursuite pour mise à pied injustifiée a été rejetée parce que le contrat d'embauche de l'employée exigeait implicitement qu'elle respecte le code de déontologie de l'Association des travailleurs sociaux de la Colombie-Britannique. Ces deux affaires tendent à démontrer que les modalités des politiques en matière de protection

¹⁶⁸ Voir : G.H.L. Fridman, *The Law of Contract in Canada*, 3^e édition (Scarborough, Carswell, 1994), p. 476.

¹⁶⁹ *Georgia Construction Co. c. Pacific Great Eastern R. Co.*, [1929] 4 D.L.R. 161 p. 163 (S.C.C.).

¹⁷⁰ Les tribunaux ont déjà traité de nombreuses causes où l'application de normes réglementaires à des codes de construction ou des codes du travail a été reconnue comme faisant partie des modalités implicites des contrats, mais ces affaires n'ont qu'un lien très mince avec la question qui nous intéresse ici.

¹⁷¹ (1977) 5 A.R. 83 (S.C.).

¹⁷² [1995] B.C.J. N° 516 (B.C.S.C.), confirmée par (1996) 136 D.L.R. (4th) 644 (C.A.).

des renseignements personnels peuvent être considérées comme faisant implicitement partie de certains contrats. De même, plus le public sera sensibilisé aux modalités de ces politiques, plus on pourra les invoquer comme faisant partie intégrante des ententes contractuelles.

Il est possible d'éviter la plupart des problèmes inhérents à l'analyse des modalités puisque, bien qu'on puisse en débattre, les institutions financières adhèrent à des politiques de protection des renseignements personnels qui régissent leurs rapports avec les clients et que, par conséquent, ces politiques font partie intégrante de leurs contrats. L'application, dans les faits, de cette théorie dépend des conventions que le client aura signées auprès de l'institution financière; à savoir si elles comportent, en noir sur blanc, des dispositions affirmant exclure toute modalité autre que celles apparaissant dans le contrat. Toutefois, il est peu probable qu'un tribunal reconnaisse la validité d'un contrat qui n'a fait l'objet d'aucune négociation significative, ce qui est le cas de la plupart des contrats types, lesquels ne sauraient vraisemblablement prévoir toutes les modalités des transactions entre l'établissement et ses clients, de manière à interdire le recours à une solution fondée sur la politique en matière de protection des renseignements personnels quand les circonstances s'y prêtent.

Un autre argument à cet effet laisse entendre que les politiques en matière de protection personnelle ont été adoptées en réponse aux dispositions des lois visant les services financiers, dans le but d'en faire des instruments à l'application quasi-réglementaire ayant force de droit public.

Dispositions législatives visant les institutions financières et la protection des renseignements personnels

Lois fédérales sur les institutions financières

Au Canada, quatre lois régissent le statut des personnes morales ainsi que la direction et la réglementation des institutions financières : la *Loi sur les banques*¹⁷³, la *Loi sur les sociétés d'assurance*¹⁷⁴, la *Loi sur les sociétés de fiducie et de prêt*¹⁷⁵ et la *Loi sur les associations coopératives de crédit*.¹⁷⁶ Ces lois protègent les renseignements personnels des consommateurs de cinq façons différentes. Tout d'abord, trois d'entre elles permettent au gouverneur en conseil d'adopter des règlements sur l'utilisation de ce genre de renseignements. Deuxièmement, elles obligent les institutions financières à prendre des mesures raisonnables pour assurer la protection et l'exactitude des données qui se trouvent dans leurs dossiers. Troisièmement, les responsables d'une institution financière sont tenus de formuler et de mettre en œuvre des mécanismes limitant l'utilisation des renseignements personnels. Quatrièmement, les règlements adoptés aux termes

¹⁷³ L.C. 1991, ch. 46 ainsi modifiée.

¹⁷⁴ L.C. 1991, ch. 47 ainsi modifiée.

¹⁷⁵ L.C. 1991, ch. 45 ainsi modifiée.

¹⁷⁶ L.C. 1991, ch. 48 ainsi modifiée.

de ces lois restreignent la mesure dans laquelle certaines institutions financières peuvent divulguer à des tiers les renseignements qu'elles possèdent au sujet de leurs clients. Enfin, les institutions financières sont tenues de conserver certains registres au Canada, bien que les renseignements puissent être traités à l'étranger si le Bureau du Surintendant des institutions financières y consent par le biais d'un décret d'exonération.

Pouvoir de réglementation en matière de renseignements sur les clients

Jusqu'au début des années quatre-vingt-dix, aucune disposition dans les lois fédérales régissant les institutions financières ne permettait au gouvernement d'adopter des règlements sur la protection des renseignements personnels et de l'information en général.¹⁷⁷ En 1991, les anciennes lois ont été révoquées et remplacées par les lois actuelles. Les nouvelles *Loi sur les banques*, *Loi sur les sociétés d'assurance*, et *Loi sur les sociétés de fiducie et de prêt* comprennent une disposition selon laquelle « le gouverneur en conseil peut adopter des règlements régissant l'utilisation, par une société, de tous les renseignements fournis à celle-ci par ses clients. »¹⁷⁸ (Remarquons que la nouvelle *Loi sur les associations coopératives de crédit* ne comporte aucune disposition à cet effet.)

En 1997, le pouvoir de réglementation conféré par la *Loi sur les banques*, la *Loi sur les sociétés d'assurance* et la *Loi sur les sociétés de fiducie et de prêt* a été révoqué et remplacé par une disposition accordant au gouverneur en conseil des pouvoirs plus précis en matière de réglementation de l'utilisation de l'information. Les nouvelles dispositions de ces trois lois stipulent que le gouverneur en conseil est habilité à adopter des règlements :

- exigeant d'une institution financière qu'elle établisse une marche à suivre relative à l'obtention, au stockage, à l'utilisation et à la divulgation de tout renseignement au sujet de ses clients ou de toute catégorie de clients;
- exigeant d'une institution financière qu'elle établisse une marche à suivre relative au traitement des plaintes formulées par les clients au sujet de l'obtention, du stockage, de l'utilisation et de la divulgation de renseignements les concernant;
- concernant la divulgation, par une institution financière, des renseignements ayant trait à la marche à suivre pour le traitement des renseignements personnels et des plaintes;

¹⁷⁷ La législation en vigueur se composait des lois suivantes : la *Loi sur les banques*, L.R.C. 1985, ch. B-1, la *Loi sur les sociétés de prêt*, L.R.C. 1985, ch. L-12, la *Loi sur les sociétés de fiducie*, L.R.C. 1985, ch. T-20, la *Loi sur les compagnies d'assurance canadiennes et britanniques*, L.R.C. 1985, I-12, la *Loi sur les compagnies d'assurance étrangères*, L.R.C. 1985, I-13, et la *Loi sur les associations coopératives de crédit*, L.R.C. 1985, ch. C-41.

¹⁷⁸ L.C. 1991, ch. 46, art. 459; L.C. 1991, ch. 47, art. 489; et L.C. 1991, ch. 45, art. 444.

- exigeant d'une institution financière qu'elle affecte des cadres et des employés à la mise en œuvre de la marche à suivre concernant le traitement de l'information et à l'accueil et au traitement des plaintes formulées par les clients;
- exigeant d'une institution financière qu'elle signale les plaintes formulées par les clients au sujet du traitement de leurs renseignements personnels, ainsi que les mesures adoptées pour régler la situation; et
- définissant les termes « renseignements », « obtention » et « stockage » aux fins des règlements.¹⁷⁹

Dans les faits, cette disposition détaillée permet au gouvernement fédéral d'adopter des règlements qui forceraient une institution financière à se doter d'une politique en matière de traitement des renseignements personnels.

Au moment d'écrire le présent mémoire (printemps 1998), les cadres fédéraux préparaient des projets de règlements aux termes de cette disposition. On s'attend à ce que ces règlements contiennent les éléments suivants : les institutions financières régies par le gouvernement fédéral seront tenues d'établir des marches à suivre sur l'obtention, l'utilisation et le stockage des renseignements personnels de leurs clients, ainsi que sur le traitement des plaintes à ce sujet; les institutions seront tenues de fournir aux clients, voire même à *tous* leurs clients, un résumé écrit de leur marche à suivre concernant le traitement des renseignements personnels et des plaintes s'y rattachant; et il y aura quelque exigence relative à la production d'un rapport annuel permettant aux responsables de la réglementation de surveiller le nombre de plaintes adressées aux institutions financières. On s'attend à ce que ces projets de règlements soient publiés au printemps 1998 et que leurs versions définitives soient adoptées dès l'été de la même année. La consultation des intervenants de l'industrie avant la parution de la version préliminaire de ces règlements n'a pas donné les résultats espérés, c'est-à-dire que les intéressés ne les ont pas appuyés d'emblée. Certaines dispositions de ces règlements, dont l'obligation d'envoyer par la poste à tous les clients une note les avisant de la nouvelle politique en matière de traitement des renseignements personnels, ont fait l'objet d'une certaine opposition qui faisait valoir que de telles mesures entraîneraient des coûts importants qu'il n'était pas justifié d'engager pour l'instant.

Protection et exactitude des dossiers

Avant 1991, le paragraphe 157(3) de la *Loi sur les banques* stipulait qu'une banque et ses mandataires étaient tenus de prendre des précautions raisonnables pour : « a) éviter la perte ou la destruction de, b) éviter la falsification des données dans, [et] c) faciliter la détection et la correction des erreurs dans les registres et les dossiers dont la tenue et la mise à jour sont exigées

¹⁷⁹ L.C. 1991, ch. 46, art. 459 modifié par 1997 ch. 15, art. 55; L.C. 1991, ch. 47, art. 489 modifié par 1997 ch. 15, art. 263; et L.C. 1991, ch. 45, art. 444 modifié par 1997, ch. 15, art. 385. Cette disposition est reprise dans la *Loi sur les sociétés d'assurance* dans le but de donner au gouverneur en conseil le pouvoir d'adopter des règlements semblables visant également les sociétés étrangères. Voir : L.C. 1991, ch. 47 art. 607 modifié par L.C. 1997, ch. 15, art. 314.

ou autorisées par cette Loi ». En 1991, l'article de la *Loi sur les banques* a été modifié de manière à y ajouter le paragraphe d), qui stipulait que les institutions financières devaient prendre des précautions raisonnables pour « éviter que le personnel non autorisé n'ait accès ou n'utilise les renseignements » consignés dans les registres et les dossiers.¹⁸⁰ Des dispositions identiques à celles que l'on retrouve dans la nouvelle version du paragraphe 157(3) ont également été ajoutées, pour la première fois, dans les *Loi sur les sociétés d'assurance*, *Loi sur les sociétés de fiducie et de prêt* et *Loi sur les associations coopératives de crédit*.¹⁸¹ Toutes ces Lois comportent maintenant cette disposition.

Politiques de la direction en matière de protection des renseignements personnels

Avant 1991, ces Lois ne comportaient aucune disposition spécifique obligeant la direction des institutions financières à formuler des politiques internes relatives à l'utilisation des renseignements personnels. Toutefois, depuis 1991, toutes les lois fédérales visant les institutions financières exigent que la direction de ces établissements « mettent en œuvre des mécanismes de résolution des conflits d'intérêts, y compris des techniques [...] visant à restreindre l'utilisation des renseignements personnels. »¹⁸²

Restrictions concernant l'utilisation des renseignements personnels

Le gouvernement fédéral a adopté deux règlements restreignant la divulgation des renseignements personnels aux termes des lois fédérales sur les institutions financières. Le *Règlement sur le commerce de l'assurance (banques)*¹⁸³, adopté en vertu de la *Loi sur les banques*, interdit à une banque et à toutes ses filiales de communiquer quelque renseignement que ce soit à propos d'un client ou d'un employé de la banque ou de la filiale à une compagnie, un agent ou un courtier d'assurance. En fait, ce règlement restreint la capacité des banques à communiquer des renseignements au sujet de leurs clients à d'autres sociétés et même à leurs filiales à des fins d'assurance et cela, même si le client y a consenti. Le *Règlement sur les renseignements sur le crédit (sociétés d'assurance)*¹⁸⁴, adopté en vertu de la *Loi sur les sociétés d'assurance*, empêche, pour sa part, les compagnies d'assurance d'utiliser des renseignements sur la solvabilité des clients obtenus auprès de ces derniers dans le but de faire la publicité d'une

¹⁸⁰ L.C. 1991, ch. 46, paragr. 157(3).

¹⁸¹ L.C. 1991, ch. 47, art. 267; L.C. 1991, ch. 45, art. 249; L.C. 1991, ch. 45, art. 241, respectivement.

¹⁸² L.C. 1991, ch. 46, al. 157(2)(c); L.C. 1991, ch. 47, al. 165(2)(c); L.C. 1991, ch. 45, al. 161(2)(c) et L.C. 1991, ch. 48, al. 167(2)(c).

¹⁸³ SOR/92-330, dicté en application de l'article 416 de la *Loi sur les banques*.

¹⁸⁴ SOR/97-11, dicté en application de l'article 489 de la *Loi sur les sociétés d'assurance*.

compagnie, d'un agent, d'un courtier ou d'une police d'assurance, à moins de satisfaire à certaines conditions. Ce règlement interdit également aux compagnies d'assurance et à leurs filiales de communiquer directement ou indirectement des renseignements concernant la solvabilité d'un client à une autre compagnie d'assurance, un agent ou un courtier.

Conservation et traitement des renseignements personnels des clients

Aux termes des dispositions des lois fédérales, une institution financière est tenue de conserver, au Canada, un registre quotidien de chaque transaction effectuée avec les clients ainsi que le solde créditeur ou débiteur du client.¹⁸⁵ En règle générale, l'institution financière doit traiter toutes les données liées à la préparation et à la mise à jour de ces registres au Canada. Cependant, ces données peuvent également être traitées à l'étranger sous réserve d'obtenir un décret d'exonération auprès du Surintendant des institutions financières.¹⁸⁶ Le cas échéant, les activités de traitement sont assujetties aux modalités et aux conditions stipulées dans le décret d'exonération. Bien que ces dispositions soient susceptibles de protéger les renseignements personnels de clients, on notera que de tels décrets ont jusqu'ici été principalement accordés dans le but d'assurer la protection et la sécurité des données elles-mêmes.

Le Surintendant des institutions financières a formulé des lignes directrices définissant les circonstances dans lesquelles il est possible d'obtenir un décret d'exonération.¹⁸⁷ Les institutions qui désirent obtenir un tel décret doivent satisfaire à trois conditions.¹⁸⁸ Tout d'abord, le Surintendant doit avoir accès à ces données de façon raisonnable. Les lois du pays où les données seront traitées, ainsi que les contrats et les autres mesures juridiques s'y rattachant, doivent habiliter le Surintendant à consulter les données de l'institution financière en tout temps, de façon opportune. Deuxièmement, le traitement des données à l'étranger ne doit avoir aucune conséquence négative sur les activités de l'institution, ni sur les services qu'elle offre à ses clients au Canada. Cette disposition vise essentiellement à éviter que les clients ne fassent les frais de retards indus attribuables à l'absence d'un mécanisme adéquat de sauvegarde des données sur place. Troisièmement, les lois du pays où les renseignements sont traités et conservés doivent être compatibles avec les lois canadiennes. Ces lois ne doivent pas empêcher l'institution financière d'effectuer elle-même certaines activités avec les données, activités que les institutions financières canadiennes effectuent couramment. Le Surintendant stipule également qu'un décret d'exonération peut faire l'objet d'une limite de temps et comporter toutes les modalités et les conditions qu'il juge nécessaires, incluant la nécessité de satisfaire aux dispositions de tout contrat ou procédure de traitement et de stockage de données et de renseignements à l'étranger.¹⁸⁹

¹⁸⁵ L.C. 1991, ch. 46, art. 238; L.C. 1991, c. 47, art. 261; L.C. 1991, ch. 45, art. 243; L.C. 1991, ch. 48, art. 235.

¹⁸⁶ L.C. 1991, ch. 46, art. 245(1); L.C. 1991, ch. 47, paragr. 268(1); L.C. 1991, ch. 45, paragr. 250(1); L.C. 1991, ch. 48, paragr. 242(1).

¹⁸⁷ L.C. 1991, ch. 46, paragr. 245(7); L.C. 1991, ch. 47, paragr. 268(7); L.C. 1991, ch. 45, paragr. 250(7); L.C. 1991, ch. 48, paragr. 242(6).

¹⁸⁸ Bureau du Surintendant des institutions financières du Canada, *Ligne directrice E-3, Traitement de l'information à l'extérieur du Canada*, mai 1992; voir le site Web à l'adresse : <http://www.osfi-bsif.gc.ca>.

¹⁸⁹ *Ibid.*

Lois provinciales et questions connexes

Les institutions financières peuvent faire l'objet de diverses lois provinciales destinées à assurer la protection des renseignements personnels dans des circonstances précises. Ces lois relèvent essentiellement de trois catégories : les lois qui régissent les coopératives de crédit et les associations coopératives, les lois en matière de protection des renseignements personnels et les lois qui régissent les rapports de solvabilité.¹⁹⁰

Plusieurs provinces se sont dotées de lois sur les activités des coopératives de crédit et les associations coopératives. Ces lois comportent des dispositions visant à assurer la protection des renseignements personnels des consommateurs. Par exemple, la *Loi sur les coopératives de crédit et les Caisses populaires*¹⁹¹ de l'Ontario tient les directeurs, les cadres, les membres du conseil d'administration et les employés des coopératives de crédit à la plus stricte confidentialité quant aux renseignements qu'ils possèdent au sujet de leurs membres et aux transactions que ceux-ci effectuent avec l'établissement. Le *Credit Unions Act*¹⁹² (loi albertaine sur les coopératives de crédit) habilite le gouvernement de l'Alberta à adopter des règlements destinés à assurer la protection des renseignements personnels dont les coopératives de crédit disposent au sujet de leurs membres. Le *Credit Unions Act*¹⁹³ de la Saskatchewan exige, quant à lui, que les registres de membres demeurent strictement confidentiels et ne soient ouverts à personne sans l'accord du conseil d'administration. Des lois du Nouveau-Brunswick et de Terre-Neuve stipulent que les coopératives de crédit de ces provinces doivent prendre des mesures adéquates pour assurer la protection et l'exactitude des données consignées dans leurs registres.¹⁹⁴ Enfin, la Colombie-Britannique et Terre-Neuve se sont toutes deux dotées de lois régissant spécifiquement les associations coopératives.¹⁹⁵ Aux termes de ces lois, il est interdit aux associations coopératives de communiquer à qui que ce soit des renseignements personnels concernant leurs membres à moins d'une autorisation à cet effet de la part du membre en question.

¹⁹⁰ En outre, diverses lois ont également une certaine incidence sur la protection de la vie privée et des renseignements personnels. En Colombie-Britannique, le *Financial Institutions Act*, R.S.B.C. 1996, ch. 141, stipule qu'une institution financière n'est pas habilitée à communiquer des renseignements personnels au sujet de ses clients sauf aux fins d'effectuer des transactions (par. 95 et 218). En outre, l'*Insurance Licensing Regulation* de la Colombie-Britannique stipule que les agents d'assurance ne peuvent communiquer de renseignements personnels au sujet de leurs clients à qui que ce soit, sauf aux fins de s'acquitter de leurs fonctions. En Alberta, le *Financial Consumers Act*, S.A. 1990, ch. F.9.5, impose des restrictions aux fournisseurs, aux agents et aux planificateurs financiers relativement à l'utilisation des renseignements personnels à caractère financier que leur fournissent les consommateurs (art. 18).

¹⁹¹ L.O. 1994, ch. 11, art. 143.

¹⁹² S.A. 1989, ch. 31.1, art. 226.

¹⁹³ S.S. 1984-85-86, ch. 45.1, art. 27.

¹⁹⁴ *Credit Unions Act*, L.N.B. 1992, ch. C.32.2, art. 28; *Credit Unions Act*, S.N. 1997, ch. C.37.1, art. 28.

¹⁹⁵ *Cooperative Association Act*, R.S.B.C. 1996, ch. 71, art. 47; *Cooperative Societies Act*, R.S.N. 1990, ch. C-35, art. 24.

Au Canada, quatre provinces régies par la common law ont sanctionné le droit à la vie privée dans le cadre des actions en responsabilité délictuelle. Les lois de Terre-Neuve,¹⁹⁶ de la Saskatchewan,¹⁹⁷ du Manitoba,¹⁹⁸ et de la Colombie-Britannique¹⁹⁹ prévoient une responsabilité délictuelle pour atteinte à la vie privée et des recours en justice sans preuve de dommages. Aucune de ces lois ne définit l'expression « vie privée »; par conséquent, l'interprétation d'une atteinte à la vie privée relève des tribunaux. À ce jour, le système judiciaire n'a pas vraiment eu l'occasion d'invoquer ces dispositions législatives.²⁰⁰ En règle générale, les tribunaux appelés à rendre un jugement aux termes de ces lois se sont contentés d'examiner les faits pour déterminer s'il y avait vraiment eu atteinte à la vie privée. Comme nous l'avons laissé entendre ci-dessus au sujet des actions délictuelles en common law concernant l'atteinte à la vie privée, il est possible que ces dispositions s'appliquent également à l'obtention et à l'utilisation des renseignements personnels. Cependant, les poursuites intentées jusqu'ici aux termes de lois destinées à assurer la protection des renseignements personnels comportaient toutes un élément d'entrée par effraction, ce qui signifie que nous ignorons toujours si ces lois sont suffisamment souples pour s'appliquer aux renseignements personnels proprement dits.

Enfin, la plupart des provinces ont adopté des lois autorisant certains organismes à communiquer des renseignements concernant la solvabilité des consommateurs, tentant d'arriver à un juste équilibre entre l'utilité des mécanismes de protection des renseignements personnels et celle associée à l'offre de crédit aux personnes qui le méritent.²⁰¹ Les agences de renseignements sur la consommation (appelées aussi bureaux de crédit) colligent des renseignements au sujet de personnes données et les vendent à des entreprises que ce genre d'information intéresse, comme des institutions financières, lesquelles utilisent ces rapports de solvabilité pour déterminer s'il convient, ou non, d'accorder du crédit à un client.²⁰² Les rapports que produisent ces agences doivent être justes et exacts, puisque des renseignements erronés pourraient amener l'institution

¹⁹⁶ *Privacy Act*, S.N. 1981, ch. 6.

¹⁹⁷ *Privacy Act*, R.S.S. 1978, ch. P-24.

¹⁹⁸ *Privacy Act*, L.R.M. 1987, ch. P-125.

¹⁹⁹ *Privacy Act*, R.S.B.C. 1979, ch. 336.

²⁰⁰ Pour un aperçu de la jurisprudence afférente à ces lois, voir : Lawson, supra, note 116, pp. 87 à 95.

²⁰¹ *Credit Reporting Act* de la Colombie-Britannique, R.S.B.C. 1996, ch. 81; *Personal Investigations Act* du Manitoba, L.R.M. 1987, ch. P.34 modifiée; *Consumer Reporting Agencies Act* de Terre-Neuve, R.S.N. 1990, ch. C-32, modifiée; *Consumer Reporting Act* de la Nouvelle-Écosse, R.S.N.S 1989, ch. 93; *Loi sur les renseignements concernant le consommateur*, Ontario, L.R.O. 1990, ch. C-33 modifiée; *Consumer Reporting Act* de l'Île-du-Prince-Édouard, R.S.P.E.I 1988, ch. C-20 modifiée; *Credit Reporting Agencies Act* de la Saskatchewan, R.S.S. 1978, ch. C-44, modifiée; *Loi sur la protection des renseignements personnels dans le secteur privé*, Québec, L.Q. 1993, ch. P.39.1, modifiée. L'Alberta et le Nouveau-Brunswick ne se sont dotées d'aucune loi régissant les agences d'évaluation du crédit.

²⁰² Pour un aperçu général des lois régissant les agences d'évaluation du crédit, voir : Dale Gibson, « Regulating the Personal Information Industry », dans *Aspects of Privacy Law: Essays in Honour of John M. Sharp*, éd. par Dale Gibson (Toronto, Butterworths, 1980) 111, p. 113.

financière à refuser au client la marge de crédit ou les services dont il fait la demande.²⁰³ Les lois concernant les renseignements sur la consommation stipulent le genre de renseignements qu'il est possible de fournir et habilite les consommateurs à accéder à leurs propres dossiers, de manière à leur permettre d'apporter les rectifications qui s'imposent. En plus de ces lois, certains bureaux de crédit ont adopté leur propre politique de protection des renseignements personnels. Par exemple, Equifax Canada Inc., un des principaux bureaux de crédit au pays, a adopté une ligne de conduite régissant toutes ses activités liées au traitement de l'information.²⁰⁴

Bien que les lois concernant les renseignements sur la consommation régissent les agences qui exercent des activités dans ce domaine, elles contiennent également des dispositions auxquelles doivent souscrire les institutions financières. Par exemple, les institutions financières ne peuvent habituellement se procurer des renseignements au sujet de leurs clients auprès d'agences d'évaluation de crédit qu'avec l'accord écrit des clients²⁰⁵ ou en avisant le consommateur.²⁰⁶ Dans certaines provinces, les institutions financières doivent également informer le client, à la demande de ce dernier, lorsqu'il fait l'objet d'un rapport ayant un lien direct avec une transaction et, le cas échéant, en fournir une copie comportant le nom et l'adresse de l'agence de renseignements sur la consommation qui a préparé ce rapport.²⁰⁷ Règle générale, les lois stipulent que lorsqu'un client se voit refuser un service à la suite d'un rapport défavorable sur sa solvabilité, il a le droit d'être informé du nom et de l'adresse de l'agence ou de la source qui a fourni ce rapport.²⁰⁸ De même, en Ontario, une institution financière qui accorde du crédit à un consommateur ne peut transmettre une liste de noms et de critères à une agence d'évaluation de crédit, liste qui permettrait à l'agence en question de déterminer quels clients correspondraient à leurs critères, sans tout d'abord en informer les clients par écrit.²⁰⁹

²⁰³ Cependant, au moins une étude laisse entendre que les registres des agences d'évaluation de crédit contiennent un nombre relativement élevé d'erreurs. En 1991, la publication *Consumer Reports* a signalé que l'examen de 1 500 dossiers des trois principales agences d'évaluation du crédit aux États-Unis avait révélé que 43 % de leurs dossiers comportaient des erreurs. L'industrie a toutefois nié cette affirmation. Trente employés de cette publication ont alors demandé un résumé de leurs dossiers de crédit auprès de ces trois mêmes agences. Selon eux, ces documents étaient « difficiles à comprendre, incomplets et parfois inexacts » [traduction libre]. Voir : « What Price Privacy? » *Consumer Reports* (mai 1991) 356.

²⁰⁴ Pour un bref aperçu des mesures de protection des renseignements personnels adoptées par Equifax Canada Inc., voir le site Web de l'entreprise à l'adresse : <http://www.equifax.ca>.

²⁰⁵ R.S.P.E.I. 1988, ch. C-20, art. 10; L.R.O. 1990, ch. C-33, art. 8; R.S.B.C. 1996, ch. 81, art. 12; L.R.M. 1987, ch. P.34, art. 3; R.S.N. 1990, ch. C-32, art. 19; R.S.N.S. 1989, ch. 93, art. 11.

²⁰⁶ R.S.P.E.I. 1988, ch. C-20, art. 10; L.R.O. 1990, ch. C-33, art. 10; R.S.B.C. 1996, ch. 81, art. 12; L.R.M. 1987, ch. P.34, art. 3; R.S.N. 1990, ch. C-32, art. 23; R.S.N.S. 1989, ch. 93, art. 11.

²⁰⁷ R.S.S. 1978, ch. C-44, modifiée, art. 21; L.R.O. 1990, ch. C-33, art. 10; R.S.P.E.I. 1988, ch. C-20, art. 10; R.S.N. 1990, ch. C-32, art. 22; L.Q. 1993, ch. P.39.1, art. 19.

²⁰⁸ R.S.B.C. 1996, ch. 81, art. 13; L.R.M. 1987, ch. P.34, art. 6; R.S.N.S. 1989, ch. C.93, art. 11; L.R.O. 1990, ch. C-33, art. 10; R.S.P.E.I. 1988, ch. C-20, art. 10.

²⁰⁹ L.R.O. 1990, ch. C-33, art. 11.

Une des principales sources d'inquiétude en matière de protection des renseignements personnels dans le secteur des services financiers est liée aux transactions avec les bureaux de crédit. Le bureau de crédit est un établissement qui n'entretient aucun rapport personnel avec les consommateurs – il en est d'ailleurs habituellement plutôt méconnu et mal compris – mais possède de gigantesques bases de données dont les renseignements ne sont pas toujours tout à fait exacts.²¹⁰ Le bureau de crédit a la possibilité de déterminer si une personne est suffisamment solvable pour se voir accorder une marge de crédit qui lui permettrait de régler ses factures, d'acheter une maison ou de se lancer en affaires. Il constitue la quintessence de la base de données à distance. Sa taille et son pouvoir de faire du tort ne sont comparables qu'à ceux des services de perception d'impôt des gouvernements. Il va de soi que les activités liées à l'utilisation des renseignements personnels et à leur transmission aux bureaux de crédit soient réglementées. Cependant, les règlements provinciaux en la matière n'adhèrent pas tous aux mêmes normes. Il semble indispensable que le consommateur soit avisé, lorsque sa banque fait appel aux services d'un bureau de crédit, de l'adresse du bureau consulté et du nom d'une personne ressource à contacter, ainsi que de son droit d'examiner tout rapport le concernant qu'aura produit ce bureau. Puisque le gouvernement fédéral n'a pas le pouvoir de légiférer dans ce domaine, les provinces devraient être encouragées à examiner leurs lois afin de s'assurer qu'elles respectent certaines normes élémentaires. Nous n'avons pas effectué d'enquête au sujet des plaintes des clients et des pratiques des bureaux de crédit. Par conséquent, bien que l'on soit en droit de se poser certaines questions à ce sujet, nous ne sommes pas en mesure d'évaluer si les craintes théoriques sont réellement justifiées.

Une autre source de préoccupation tient aux lois provinciales en matière de partage, entre les compagnies d'assurances, de renseignements au sujet de l'état de santé de leurs clients. La réglementation de l'assurance relève des provinces, ce droit leur étant imparti par la Constitution qui stipule qu'il appartient aux provinces de réglementer les biens et les droits civils.²¹¹ D'un point de vue historique, le droit de constituer des personnes morales et de réglementer les compagnies d'assurance était acquis au gouvernement fédéral mais les provinces s'en sont largement prévaluées. Cependant, la Constitution ne comporte apparemment aucune disposition concernant les droits fédéraux en la matière comme c'est le cas pour les banques, lesquelles sont exclusivement réglementées par le gouvernement fédéral. Quoi qu'il en soit, la réglementation des transactions d'assurance et des rapports entre les assureurs et leurs clients relève clairement des compétences provinciales.

²¹⁰ *Consumer Reports*, supra, note 203.

²¹¹ Voir : Peter W. Hogg, *Constitutional Law of Canada*, format feuilles mobiles, volume 1 (Scarborough, Ont. : Carswell, mis à jour en 1997), p. 24-7 : « L'industrie de l'assurance était le champ de bataille où se sont affrontés les organismes de réglementation fédéral et provinciaux pour obtenir le contrôle d'une série de dossiers entre 1880 et 1942. Ces dossiers ont tous été résolus en faveur de l'impartition aux gouvernements provinciaux des droits de la propriété et des droits de la personne. Les compagnies d'assurance relèvent par conséquent de compétences provinciales, bien que le gouvernement fédéral joue également un rôle de premier plan dans ce dossier, rôle auquel acquiescent les provinces et l'industrie et qui s'appuie sur une question de droits constitutionnels. »

Les assureurs transmettent tous les jours des renseignements au sujet de l'état de santé de leurs clients au Bureau de renseignements médicaux Inc. (MIB), un service de documentation dont le siège social se trouve près de Boston, au Massachusetts.²¹² Mis sur pied par l'industrie de l'assurance, le MIB a pour rôle de lutter contre la fraude en servant de dépôt central où l'on peut obtenir des renseignements au sujet de l'histoire médicale des assurés. Environ six cent quatre-vingt assureurs canadiens et américains transmettent des renseignements de base au MIB. Cette démarche s'appuie sur l'autorisation à cet effet que leur confèrent leurs clients lorsqu'ils ratifient une demande d'assurance. Le MIB met ces renseignements à la disposition de ses membres, sur demande, sous forme de rapports codés. Les rapports produits par le MIB contiennent des renseignements tels que le nom de l'assuré, la date et l'endroit de sa naissance, sa profession, la région où il habite ainsi qu'une suite de codes correspondant à son état de santé et à certaines données de nature autre que médicale.²¹³ Ces rapports sont produits dans le seul but de sonner l'alerte en cas de besoin. Les assureurs qui en font la demande sont tenus d'effectuer une enquête de souscription plutôt que de se fier uniquement aux renseignements qu'on y trouve pour prendre une décision au sujet d'une demande d'assurance. À moins d'une ordonnance des tribunaux, le MIB ne fournit aucun renseignement aux compagnies d'assurance qui ne font pas partie de l'association. En outre, les membres du MIB sont tenus, aux termes des modalités de leur contrat, à la plus stricte confidentialité quant aux renseignements contenus dans ces rapports. Les résidents canadiens peuvent consulter leurs dossiers respectifs en présentant une demande à cet effet à la succursale torontoise du MIB. Ils peuvent également demander à ce que des rectifications soient apportées à leur dossier.

À ce qu'on sache, il n'existe aucune loi canadienne nous habilitant officiellement à consulter et à rectifier les renseignements qui se trouvent dans les banques de données du MIB.²¹⁴ Bien que le MIB accomplisse une tâche utile, ses activités sont de nature à soulever des inquiétudes relatives à la protection des renseignements personnels. D'aucuns font valoir, sans avoir tout à fait tort, que ce mécanisme de transmission de données au sujet de l'état de santé des assurés se compare aux rapports que les institutions financières entretiennent avec les bureaux de crédit. Le cas échéant, le MIB, ou l'assureur qui fait appel à ses services, devrait donc faire l'objet de règlements provinciaux semblables à ceux qui régissent les activités des bureaux de crédit. Par ailleurs, la nature plutôt restreinte des renseignements que l'on retrouve dans les rapports du MIB et le fait que les membres du MIB soient tenus de mener une enquête indépendante après avoir

²¹² Pour de plus amples renseignements au sujet du MIB, voir : *Medical Information Bureau: A Consumer's Guide* (non daté), publié par le MIB, ainsi que *Privacy and Data Protection: Background Paper* (Association des consommateurs du Canada, juillet 1992), pp. 68 à 70.

²¹³ Il existe environ 210 codes médicaux : « Les renseignements le plus souvent communiqués sont la taille et le poids, la tension artérielle, les résultats d'ECG et de rayons X si, et seulement si, ces renseignements sont habituellement réputés avoir un rapport avec l'état de santé et la longévité. » Il existe cinq codes correspondant à des renseignements de nature autre que médicale, dont les dossiers de conducteur défavorables, la pratique de sports dangereux et d'activités liées à l'aviation. Voir : *Medical Information Bureau: A Consumer's Guide, supra*, note 214, p. 6.

²¹⁴ Cependant, la loi du Massachusetts en matière de protection de la vie privée peut aussi s'appliquer aux activités du MIB. Voir : *Privacy and Data Protection: Background Paper* (Association des consommateurs du Canada), *supra*, note 212, p. 69.

reçu ces rapports peuvent, dans une certaine mesure, apaiser les inquiétudes. Il serait opportun de se pencher davantage sur les pratiques du MIB, ainsi que sur la façon dont les assureurs canadiens utilisent ses services, pour juger de la nécessité de formuler des règlements en la matière. Certaines provinces songent déjà à adopter des lois visant la divulgation des renseignements médicaux personnels; un projet de loi ontarien, en particulier, pourrait également s'appliquer à la transmission, par les assureurs, de renseignements médicaux au MIB ou à l'utilisation des renseignements fournis par le MIB.²¹⁵ Comme la réglementation des activités des assureurs est une question de compétence provinciale, les hauts fonctionnaires des provinces devraient être invités à se pencher sur la problématique de la transmission de renseignements de nature médicale.

La loi québécoise sur la protection des renseignements personnels dans le secteur privé

Le Québec est la seule province à s'être dotée de dispositions législatives en matière d'obtention, d'utilisation, de transmission et de conservation des renseignements personnels dans le secteur privé. La *Loi sur la protection des renseignements personnels dans le secteur privé* au Québec (aussi appelée le projet de loi 68) élargit et précise certains éléments du droit à la vie privée directement tirés du nouveau *Code civil*²¹⁶ de cette province. Cette loi est entrée en vigueur le 1^{er} janvier 1994²¹⁷ et s'applique à une vaste gamme d'entités du secteur privé, y compris les sociétés commerciales, les entreprises individuelles (ou entreprises à propriétaire unique), les sociétés en nom collectif, les organismes et les associations.²¹⁸ C'est la première loi en Amérique du Nord à imposer des principes relatifs à la protection des renseignements personnels à l'ensemble du secteur privé, ce qui n'est pas sans avoir d'importantes répercussions pour les autres provinces canadiennes. Comme le disait le professeur Colin J. Bennett : « Le Canada est le seul pays dont l'une des composantes s'est dotée d'une politique de protection des renseignements personnels plus exhaustive que celle du gouvernement fédéral. »²¹⁹

À la lecture du libellé de la Loi, on constate qu'elle s'applique autant aux banques qu'aux autres institutions financières. Cependant, il convient de se demander si les banques, qui relèvent essentiellement du fédéral aux termes de la *Loi constitutionnelle* de 1867²²⁰, sont tenues d'adhérer à des politiques provinciales. Dans un article publié en 1994, M^e Étienne DuBreuil

²¹⁵ Voir les notes de bas de page 64 à 67 à la Partie I de la présente étude, de même que le texte qui les accompagne.

²¹⁶ L.R.Q. ch. P-39.1. La Loi étoffe et précise certaines des dispositions sur le droit à la vie privée et l'accès à l'information qui sont énoncés dans les articles 35 à 41 du *Code civil du Québec*.

²¹⁷ Soulignons cependant que certaines de ces dispositions ne sont entrées en vigueur que six mois ou un an après le 1^{er} janvier 1994. Voir la promulgation originale de la loi : L.Q. 1993, ch. 17, art. 114 et 115.

²¹⁸ La définition des organismes visés par la Loi se trouve aux articles 1, 96 et 97 de la Loi et à l'article 1525 du *Code civil du Québec*.

²¹⁹ Colin J. Bennett, *Implementing Privacy Codes of Practice*, PLUS 8830 (Etobicoke, Ontario, ACNOR, 1995), p. 10.

²²⁰ L.R.C. 1985, Annexe II, N° 5.

faisait valoir que les banques pourraient invoquer l'inconstitutionnalité de cette loi tout en précisant que si cela arrivait, il était probable qu'elles finiraient par devoir se soumettre aux dispositions de la loi québécoise.²²¹ Il a également fait remarquer qu'en l'absence de lois fédérales en la matière, une loi adoptée par un gouvernement provincial pourrait s'appliquer à un domaine de compétence fédérale à moins qu'elle n'empêche le gouvernement fédéral d'accomplir les devoirs qui lui incombent habituellement. Voici ce qu'a écrit M^e Dubreuil après avoir examiné le texte de cette loi :

Compte tenu des circonstances, nous pouvons tout d'abord conclure que le gouvernement fédéral n'a encore adopté aucune loi en matière de protection des renseignements personnels dans le secteur privé. Cela étant, il appert que la loi dont s'est doté le gouvernement du Québec s'applique aux sociétés de compétence fédérale. Le projet de loi 68 s'appliquera par conséquent à toutes les entreprises qui exercent des activités commerciales dans la province de Québec. Le seul obstacle à ladite application serait une décision par les tribunaux à l'effet que cette loi nuit au gouvernement fédéral dans l'exercice de ses fonctions. En d'autres mots, les tribunaux devraient être convaincus que le projet de loi 68 empêcherait la législation fédérale de jouer le rôle qui lui incombe et pour lequel elle a été mise en place.²²²

Bien que cette étude ne veuille aucunement se prononcer quant à la constitutionnalité du projet de loi 68, les auteurs remarquent qu'il est possible que les projets de règlements stipulant que les banques doivent adopter un modèle de code relativement à la protection des renseignements personnels auraient une incidence sur l'analyse de M^e DuBreuil. On ne peut passer outre au fait que toute réglementation fédérale en la matière, fût-elle adoptée ultérieurement, aurait préséance sur les lois provinciales.

La loi québécoise comporte des dispositions qui régissent l'obtention de « renseignements personnels », lesquels sont définis comme des renseignements qui concernent une personne et qui permettent d'identifier cette dernière.²²³ Par exemple, une entreprise ouvrant un dossier contenant des renseignements personnels à propos d'un client doit indiquer la raison de cette démarche. De plus, si elle s'adresse directement au client pour obtenir les renseignements qui seront versés à ce dossier, l'entreprise doit informer le client de l'existence d'un tel dossier. Elle

²²¹ Étienne DuBreuil, « Quebec Bill 68: Is it Sufficient for the Federal Canadian Financial Institutions Sector? » in *Privacy in Financial Services: Striking a Balance between Privacy Rights and Profits* (Toronto, Canadian Institute, 27 avril 1994).

²²² *Ibid.*, pp. 6-7. Toutefois, DuBreuil précise également que cet article ne doit pas être interprété comme un énoncé d'opinion sur la constitutionnalité du projet de loi 68. Par la suite, le professeur Colin J. Bennett a souligné que bien que les questions de compétences liées au projet de loi 68 n'avaient pas été résolues, les organismes à charte fédérale du secteur privé, comme les banques et les sociétés de transport aérien, s'étaient déclarées prêtes à se conformer aux conditions imposées par la loi. Voir : Bennett, *supra*, note 219, p. 10.

²²³ L.R.Q. ch. P-39.1, art. 1, 2 et 4 à 9. Soulignons que l'article 1 stipule que la *Loi* ne s'applique pas aux documents journalistiques recueillis et utilisés aux fins de renseigner le public.

ne peut se procurer que les renseignements pertinents.²²⁴ En outre, le règlement stipule qu'à moins qu'il ne s'agisse d'une situation exceptionnelle, les entreprises doivent obtenir directement du client les renseignements dont elles ont besoin et ce, uniquement par des moyens légaux.

L'utilisation et la transmission des renseignements personnels font également l'objet d'autres dispositions.²²⁵ Les entreprises doivent veiller à ce que les renseignements personnels sur lesquels elles s'appuient pour prendre des décisions au sujet de leurs clients soient exacts et aussi récents que possible. En règle générale, il est interdit aux entreprises de divulguer, de transmettre ou d'utiliser des renseignements personnels à des fins autres que celles auxquelles lesdits renseignements étaient destinés lorsqu'ils ont été versés au dossier du client. On peut toutefois les transmettre, les divulguer et les utiliser à d'autres fins avec le consentement de la personne concernée ou dans des circonstances prévues par la Loi.²²⁶ La Loi n'offre qu'une bien mince définition du concept de consentement, qui s'entend essentiellement du consentement manifeste, libre et éclairé de transmettre ou d'utiliser des renseignements personnels à des fins précises. Le consentement n'est valable que pour la période nécessaire à la réalisation des objectifs pour lesquels il a été demandé.²²⁷ La Loi interdit également aux entreprises établies au Québec de transmettre des renseignements personnels à l'extérieur de cette province sans avoir pris des mesures raisonnables pour s'assurer que ces renseignements seront protégés de façon adéquate par les lois auxquelles le destinataire est assujéti.²²⁸

Les « listes nominatives », ou listes de noms, d'adresses et de numéros de téléphone d'individus, font l'objet de dispositions particulières.²²⁹ La Loi stipule qu'une entreprise qui désire utiliser la liste nominative de ses clients à des fins commerciales ou de bienfaisance, doit offrir à ces derniers la possibilité de faire rayer leur nom de cette liste. Quelle que soit la décision du client, l'organisme chargé de l'application de cette loi estime qu'il incombe aux entreprises d'envoyer une lettre à tous les clients dont le nom apparaît dans la liste afin de leur expliquer comment procéder pour en faire rayer leur nom.²³⁰ Enfin, les gens dont le travail consiste à communiquer, au téléphone ou par le courrier, avec des personnes dont le nom provient d'une liste nominative doivent informer celles-ci de leur droit de faire rayer leur nom de cette liste.

²²⁴ Alors que la *Loi* stipule qu'une entreprise ne peut recueillir que les renseignements « nécessaires » à la réalisation des objectifs aux fins desquels un dossier est constitué, le *Code civil* précise qu'une entreprise ne peut recueillir que les renseignements « opportuns » aux objectifs à atteindre. Voir : L.R.Q. ch. P-39.1, art. 5, et *Code civil du Québec*, article 37.

²²⁵ L.R.Q. ch. P-39.1, art. 10 à 26.

²²⁶ La *Loi* énonce plus d'une douzaine de conditions ouvrant droit à une exonération. Voir : L.R.Q. ch. P-39.1, art. 18 et 21.

²²⁷ L.R.Q., ch. P-39, art. 14.

²²⁸ *Ibid.*, art. 17.

²²⁹ *Ibid.*, art. 22 à 26.

²³⁰ Commission d'accès à l'information du Québec, Info-conseils sur la confidentialité des renseignements personnels : le marketing direct (janvier 1995).

La Loi étoffe également le droit à la consultation et à la correction des renseignements personnels garanti par le *Code civil du Québec*.²³¹ Selon la Loi, une entreprise doit confirmer ou infirmer l'existence de dossiers contenant des renseignements personnels et permettre aux personnes qui le désirent de consulter leur dossier personnel au plus tard trente jours après la demande. Cette consultation doit être gratuite, à l'exception des frais qu'il serait raisonnable d'exiger pour un service de transcription, de reproduction ou de transmission de l'information. En plus des dispositions du *Code civil* habilitant les personnes à corriger les renseignements personnels qui se trouvent dans leur dossier, les intéressés peuvent exiger de l'entreprise qu'elle efface tout renseignement recueilli par des moyens « autres que ceux prévus par la loi ». Soulignons cependant que la Loi prévoit des circonstances dans lesquelles les entreprises ne sont pas tenues d'autoriser la consultation des dossiers personnels et fixe aussi parfois des limites quant à la nature des renseignements qui peuvent être consultés.²³²

La Loi québécoise devrait avoir d'importantes conséquences sur la collecte et l'utilisation de tous les genres de renseignements personnels par les institutions financières. Une institution financière qui entend recueillir des renseignements de cette nature doit en prévenir l'intéressé et ouvrir un dossier à des fins précises formulées en toutes lettres. Les renseignements obtenus ne devront servir qu'aux fins pour lesquelles le dossier a été constitué, sauf pour les exceptions prévues dans la Loi. L'établissement doit formuler une marche à suivre permettant à la personne de consulter les renseignements qui la concernent. Si l'institution entend utiliser cette liste à des fins de sollicitation commerciale ou dans le cadre d'une campagne de bienfaisance, elle doit observer les dispositions de la Loi en matière d'utilisation des listes nominatives. Par conséquent, une institution ne peut constituer une liste de ses clients dans le but de la vendre à une autre entreprise sans offrir aux intéressés la possibilité de faire rayer leur nom de cette liste. En outre, cette Loi a des conséquences qui ne se limitent pas qu'au territoire québécois. Les institutions nationales établies un peu partout au pays devront composer avec ses dispositions en matière de transmission de renseignements personnels à l'extérieur du Québec. En termes pratiques, cela signifie qu'elles pourront être tenues d'éviter de transmettre des renseignements personnels au sujet de personnes qui habitent au Québec, à moins de mettre en œuvre des mesures qui satisferont aux exigences de la Loi partout au Canada.

²³¹ Voir : *Code civil du Québec*, articles 37 à 40, et L.R.Q. ch. P-39.1, art. 27 à 41.

²³² La Loi impose des restrictions relatives au droit à l'accès à l'information de certaines personnes mineures en stipulant que les personnes de moins de quatorze ans ne sont pas autorisées à consulter des renseignements à caractère médical ou social. La Loi prévoit aussi quelques exceptions au droit à l'accès à l'information. La principale exception prévue par règlement stipule qu'une entreprise doit refuser de permettre l'accès à des renseignements concernant une personne autre que le demandeur lorsque la divulgation de tels renseignements risque de nuire gravement à la personne en question. La Loi prévoit trois catégories de renseignements que l'on peut refuser de divulguer, soit : 1) les renseignements médicaux dont la divulgation pourrait nuire sérieusement à la personne intéressée; 2) les renseignements dont la divulgation pourrait entraver le travail d'un service de sécurité, d'une agence de sécurité ou d'une agence de détectives; 3) les renseignements dont la divulgation serait susceptible d'avoir une incidence sur des procédures judiciaires qui ont un lien avec l'entreprise ou l'intéressé.

Codes des associations industrielles

Depuis le début des années quatre-vingt, nous avons assisté à une prolifération des codes et politiques d'entreprise en matière de protection des renseignements personnels des clients des institutions financières.²³³ Au cours des années quatre-vingt et quatre-vingt-dix, les associations de banques et de sociétés de fiducie ont adopté des modèles de code à l'intention de leurs membres.²³⁴ À la demande pressante du gouvernement et d'associations industrielles, nombre d'institutions financières se sont dotées de codes inspirés des modèles fournis par les associations dont elles sont membres. Bien que ces codes visant la protection des renseignements personnels n'aient pas force de loi, ils témoignent d'un engagement concret en la matière. Un client préoccupé par l'obtention et l'utilisation de renseignements le concernant peut loger une plainte ou demander de consulter son dossier aux termes du code de protection des renseignements personnels de l'établissement. Nous allons maintenant nous pencher sur les principaux modèles de code que l'on retrouve dans l'industrie.

Soulignons que nous avons tenté, sans succès, d'obtenir des renseignements auprès de l'Association canadienne des courtiers en valeurs mobilières (IDA) et de trois courtiers indépendants dans le but de cerner leur politique en matière de protection des renseignements personnels.²³⁵

Association des banquiers canadiens

En 1990, l'Association des banquiers canadiens (ABC) a adopté un *Modèle de code pour la protection des renseignements personnels des consommateurs*, après avoir consulté les gouvernements fédéral et provinciaux, ainsi que l'Association des consommateurs du Canada.²³⁶ Ce code s'inspirait essentiellement des principes formulés dans les lignes directrices de

²³³ Pour de plus amples renseignements au sujet des codes des institutions financières en matière de protection des renseignements personnels, voir : Richard C. Owens, Thomas S. Onyshko, et Peter C. Goode, « Reform Proposals Relating to Customer Privacy and Tied Selling in the Federally-Regulated Financial Services Sector » dans *The Regulation of Financial Institutions: Issues and Perspectives* (Scarborough, Carswell, 1997) 143, p. 153ff.

²³⁴ En 1990, la législation fédérale visant les institutions financières, les banques, les compagnies d'assurance et les sociétés de fiducie a été modifiée de manière à restreindre l'utilisation des renseignements personnels. Plus récemment, cette même législation a fait l'objet d'autres modifications pour permettre au gouvernement d'adopter des règlements obligeant les banques, les sociétés de prêt et de fiducie ainsi que les compagnies d'assurance à se doter d'un code en matière de protection des renseignements personnels. Pour de plus amples renseignements à ce sujet, voir la rubrique « Dispositions législatives visant les institutions financières et la protection des renseignements personnels » dans la présente Partie.

²³⁵ L'Association canadienne des courtiers en valeurs mobilières (IDA) n'a fourni aucun document aux auteurs de la présente étude en précisant qu'elle ne désirait pas participer à cette étude. L'étudiant chargé d'obtenir un exemplaire des codes de trois grandes agences canadiennes de courtage en valeurs mobilières n'est pas parvenu à s'acquitter de cette tâche. Dans un cas, on lui a répondu que ces renseignements n'étaient pas disponibles. Dans les deux autres cas, les agents n'ont pas retourné ses appels.

²³⁶ *Modèle de code; confidentialité* (1990) de l'Association des banquiers canadiens. Soulignons que l'ABC a présenté un modèle de code sur la protection des renseignements personnels à ses membres en 1986, mais ces derniers ont refusé d'y adhérer. Voir Bennett, *supra*, note 221, p. 26. Pour de plus amples renseignements au sujet de la version de 1990 du code de l'ABC, voir Edward K. Rowan-Legg, « Confidential Information » dans *I've Got A Secret: The Duty of Confidentiality in the Private Sector* (Toronto, Association du Barreau canadien - Ontario, mars 1994).

l'OCDE.²³⁷ Il énonçait des principes relatifs à la collecte de renseignements personnels, à la qualité de ces renseignements, à leurs objectifs, aux limites applicables à leur utilisation, aux mesures de protection, à la participation des intéressés, à la responsabilité des banques et à la transparence du processus.

Le code contenait diverses dispositions concernant l'obtention des renseignements. Ainsi, les banques étaient tenues d'obtenir les renseignements dont elles avaient besoin « essentiellement » auprès de leurs clients, mais jouissaient également d'une certaine marge de manœuvre les habilitant à consulter d'autres sources comme les octroyeurs de crédit, les bureaux de crédit, les sources de revenus et les connaissances personnelles du client. En vertu de l'article 5a), les banques étaient autorisées à recueillir des renseignements personnels à plusieurs fins, notamment celles d'établir et d'entretenir des rapports avec les clients, de leur offrir des produits et des services autorisés par la loi, d'observer la loi et d'assurer la protection des intérêts des clients et de la banque. Les banques étaient aussi tenues d'informer les clients, lorsqu'elles leur demandaient de fournir des renseignements personnels, des fins auxquelles étaient destinés ces renseignements et d'obtenir leur consentement avant de faire appel à d'autres sources pour se procurer des renseignements supplémentaires.

D'autres dispositions portaient sur l'utilisation de ces renseignements. Lorsque des renseignements devaient être utilisés à des fins autres que celles pour lesquelles ils avaient été recueillis (même si elles étaient compatibles), la banque était tenue d'obtenir le consentement du client avant de procéder. Les banques n'étaient autorisées à divulguer des renseignements personnels au sujet de leurs clients à des tiers que dans quatre circonstances bien précises, lesquelles s'inspiraient directement des quatre conditions énoncées dans le jugement rendu au terme de l'affaire *Tournier* : avec le consentement du client, pour se plier à une loi, pour protéger les intérêts de la banque ou lorsque l'intérêt public réclame que ces renseignements soient divulgués. Cependant, la définition de ce qui constituait les « intérêts de la banque » était plutôt floue, n'offrant pour seul exemple le fait qu'une banque pouvait être appelée à respecter « divers décrets des tribunaux exigeant qu'elle divulgue des renseignements personnels au sujet des comptes de ses clients en tant qu'élément de preuve ».²³⁸ Les banques étaient tenues de conserver des renseignements aux seules fins énoncées dans l'article 5a) et de veiller à ce que ceux-ci demeurent aussi exacts et complets que l'exigent les fins pour lesquelles ils avaient été recueillis.

Le code traitait aussi du droit d'accès aux renseignements personnels dont jouissent les clients.²³⁹ Toutefois, ce droit ne donnait accès qu'aux renseignements factuels et non aux « opinions et aux décisions », lesquelles étaient gardées confidentielles par la banque. Le code autorisait la banque

²³⁷ Il est question des lignes directrices de l'OCDE à la Partie I de la présente étude, sous la rubrique « Droit à la vie privée et questions liées à la protection des renseignements personnels », sous-rubrique c) « L'informatisation des renseignements personnels ».

²³⁸ Association des banquiers canadiens, *Modèle de code 1990*, *supra*, note 236, art. 6(c).

²³⁹ *Ibid.*, art. 8.

à prendre un délai raisonnable et à exiger des frais raisonnables pour l'accès aux renseignements personnels. En cas de refus, la banque devait préciser au client pourquoi elle ne pouvait l'autoriser à consulter son dossier personnel. Les clients qui se voyaient accorder l'accès à leur dossier personnel avaient également le droit d'en appeler de l'exactitude des renseignements qui s'y trouvaient. Le cas échéant, la banque devait prendre note des erreurs qui se trouvaient dans le dossier. La banque avait également le devoir de communiquer à des tiers toutes les corrections apportées lorsque les renseignements erronés étaient susceptibles de nuire aux intérêts du client. Les banques devaient conserver un registre de toutes les circonstances dans lesquelles elles divulguaient des renseignements personnels au sujet des comptes de leurs clients, sauf dans le cadre de divulgations de routine, qu'il n'était pas nécessaire de consigner nulle part.

D'autres dispositions du code exigeaient que les banques mettent en œuvre de mesures destinées à assurer la protection des renseignements personnels, chargent un cadre supérieur de prendre ce dossier en main et communiquent à tous leurs clients leurs politiques en matière de protection des renseignements personnels, y compris la marche à suivre pour porter plainte. Les clients insatisfaits de la façon dont leurs plaintes avaient été traitées pouvaient s'adresser au Bureau du Surintendant des institutions financières.

La version de 1990 du Code de l'ABC a fait l'objet de certaines critiques de la part de l'Association des consommateurs du Canada²⁴⁰ et du Commissaire à la protection de la vie privée. Ce dernier a d'ailleurs souligné que le Code limitait indûment l'accès aux renseignements et ne définissait pas assez précisément les circonstances dans lesquelles les institutions étaient habilitées à dévoiler des renseignements personnels. En 1994, le commissaire Phillips a entre autres écrit ce qui suit à ce sujet :

Le Code de l'Association des banquiers canadiens, de même que ceux des banques individuelles, ne traite pas des renseignements subjectifs concernant leurs clients et ne prévoit aucune mesure de protection des employés des banques. Il autorise la divulgation à grande échelle de renseignements personnels dans le but de servir les intérêts commerciaux de l'établissement (comme peut en témoigner toute personne qui s'est déjà donnée la peine de lire le texte en caractères fins au verso des demandes d'adhésion aux cartes bancaires). En outre, les codes ne prévoient pas non plus de mesures pour empêcher les banques de transmettre des renseignements personnels au sujet de leurs clients à des compagnies d'assurance et à des sociétés de courtage dont elles pourraient, aujourd'hui, fort bien être propriétaires suite aux récentes modifications apportées aux lois régissant le secteur financier.²⁴¹

²⁴⁰ Bennett, *supra*, note 219 p. 26.

²⁴¹ *Commissaire à la protection de la vie privée au Canada, Rapport annuel 1993-1994* (Ottawa : Canada Groupe des communications, 1994) p. 6. Voir aussi *Commissaire à la protection de la vie privée au Canada, Rapport annuel 1990-1991* (Ottawa : Approvisionnement et Services Canada, 1991) p. 16.

En 1996, l'ABC a émis une nouvelle version de son code intitulée *Confidentialité; modèle de code – Pour protéger les renseignements personnels des clients des banques* et reflétant essentiellement les articles du code type de l'ACNOR.²⁴² Le nouveau code de l'ABC est plus détaillé, met davantage l'accent sur la nécessité d'obtenir le consentement du client, aborde la question du marketing ciblé auquel se livrent les banques et se penche sur la nécessité d'étoffer les droits des clients en matière d'accès aux renseignements personnels. Le nouveau code s'articule autour de dix principes : la responsabilité de la banque, la détermination des fins de la collecte des renseignements personnels, le consentement du client, les limites applicables à la collecte des renseignements personnels, les limites applicables à l'utilisation, à la divulgation et à la conservation des renseignements personnels, la mise à jour des renseignements personnels, les mesures de sécurité, l'accessibilité du client aux normes et aux méthodes, l'accessibilité du client aux renseignements personnels le concernant, le règlement des plaintes et le traitement des demandes de renseignements. Le cabinet d'experts-comptables Price Waterhouse a produit un rapport affirmant que le nouveau code de l'ABC est conforme au code type de l'ACNOR.²⁴³

Le code offre une nouvelle liste (enrichie) des fins auxquelles peuvent servir les renseignements personnels, c'est-à-dire : comprendre les besoins du client, s'assurer de la pertinence des produits et des services qu'on désire lui offrir, élaborer et offrir des produits et des services qui correspondent à ses besoins, lui offrir des services continus et satisfaire aux exigences légales et réglementaires.²⁴⁴ Lors de la collecte des renseignements, la banque doit maintenant informer le client des fins de l'exercice, du fait que ces renseignements pourront être utilisés, avec son consentement, à des fins autres que celles prévues à l'origine et du fait qu'il peut refuser que ces renseignements soient utilisés à d'autres fins. Le nouveau code conserve cependant la même approche en ce qui concerne la provenance des renseignements personnels, stipulant que les employés de la banque doivent « essentiellement » recueillir ces renseignements auprès des clients, mais qu'ils peuvent aussi s'adresser à d'autres sources comme les bureaux de crédit, les employeurs et d'autres prêteurs.

En ce qui a trait au consentement, le code oblige la banque à faire un « effort raisonnable » pour s'assurer que le client aura compris à quelles fins ses renseignements personnels pourront être utilisés et divulgués. Il incombe à la banque d'obtenir le consentement du client au moment de la collecte pour utiliser et divulguer ces renseignements.²⁴⁵ Ce consentement peut être exprès ou implicite, bien que l'on « préfère » le consentement exprès (comparativement au projet de loi 68 du Québec, qui stipule que le consentement doit être « manifeste, libre, éclairé et accordé à

²⁴² Pour de plus amples renseignements au sujet du modèle de code de l'Association canadienne de normalisation (CSA), voir les notes de bas de page 53 à 55 sous la rubrique « Évolution de la perception du droit à la vie privée dans le secteur des services financiers au Canada » à la Partie I de la présente étude, ainsi que le texte qui les accompagne.

²⁴³ Le court rapport de la société Price Waterhouse est repris dans la version de novembre 1996 du code de l'Association des banquiers canadiens.

²⁴⁴ *Modèle de code; confidentialité : Pour protéger les renseignements personnels de clients des banques*, Association des banquiers canadiens (1996), art. 2.2.

²⁴⁵ *Ibid.*, Principe 3.

des fins précises ».²⁴⁶) On parlera de consentement implicite lorsqu'un client utilise un produit ou un service bancaire ou omet de répondre à une lettre lui offrant de faire rayer son nom d'une liste nominative qui sera utilisée à des fins de marketing. Une banque peut utiliser des renseignements sans le consentement du client pour repérer les fraudes, percevoir des comptes en souffrance, obéir à la loi ou fournir de l'information à des mandataires de la banque qui en ont besoin pour faire leur travail (comme imprimer des chèques). Le client peut, à tout moment, retirer son consentement sous réserve de restrictions juridiques ou contractuelles. Mais un tel retrait de consentement risque de se traduire par l'impossibilité pour la banque d'offrir certains genres de produits et services.²⁴⁷ Par exemple, une banque peut refuser de prêter de l'argent à un de ses clients qui refuse qu'on demande un rapport de solvabilité à son sujet à un bureau de crédit.

D'autres dispositions stipulent que la banque doit obtenir le consentement du client avant d'utiliser ses renseignements personnels à des fins de marketing.²⁴⁸ Lorsqu'une banque désire utiliser les renseignements personnels de ses clients pour mettre en marché un nouveau produit ou un nouveau service, que ce soit directement ou par l'entremise d'une société affiliée, elle doit obtenir le consentement du client à cet effet lors de la collecte des renseignements. Lorsqu'un client demande un service ou un produit, il fournit des renseignements personnels. Le préposé doit alors le prévenir que ces renseignements pourront être utilisés par la banque ou ses sociétés affiliées pour mettre en marché de nouveaux produits et services et lui demander s'il y consent en précisant que cette utilisation des renseignements personnels est facultative.²⁴⁹

Les sociétés affiliées qui offrent des services aux clients de la banque sont également tenues de s'acquitter d'une tâche complémentaire. La première fois qu'une société affiliée discute d'un produit ou d'un service avec le consommateur, elle doit lui préciser comment les renseignements personnels le concernant seront utilisés et lui offrir la possibilité de retirer son consentement, de manière à ce que ces renseignements ne soient dorénavant plus utilisés à des fins autres que celles prévues initialement.

²⁴⁶ Voir : *Loi sur la protection des renseignements personnels dans le secteur privé*, L.R.Q. ch. P-39.1, art. 14.

²⁴⁷ La disposition portant sur le retrait du consentement mentionne, entre autres, que : « Sous réserve d'obligations légales ou contractuelles, le client peut refuser de donner son consentement à la banque ou le lui retirer à n'importe quel moment, dans la mesure où : la banque en est avisée dans un délai raisonnable [et où] le consentement ne s'applique pas à un produit de crédit à l'égard duquel la banque doit obtenir et divulguer de l'information après avoir octroyé un crédit. Cette mesure vise à préserver l'intégrité du système de crédit. [...] La banque doit informer le client qui s'apprête à refuser ou à retirer son consentement des conséquences que son geste peut avoir. Par exemple, si le client refuse de donner son consentement ou le retire après l'avoir donné, certains produits, services ou renseignements importants pourraient lui être refusés. » Cette disposition du code de l'ABC sur le retrait du consentement s'inspire d'une disposition semblable que l'on retrouve dans le code type de l'Association canadienne de normalisation (CSA). Voir le modèle de code de l'ABC, version 1996, *supra*, note 244, art. 3.5.

²⁴⁸ *Ibid.*, art. 5.3.

²⁴⁹ *Ibid.*, art. 5.3.

L'utilisation et la divulgation de l'information font également l'objet d'un principe dans le nouveau code, lequel stipule que la banque ne doit utiliser les renseignements personnels qu'aux fins pour lesquelles ils ont été recueillis, à moins que le consommateur ne consente à ce qu'ils soient utilisés à d'autres fins. Toutefois, le nouveau code est moins précis en ce qui a trait à la capacité de la banque de divulguer des renseignements personnels sans le consentement du client. On peut y lire que « dans certaines circonstances exceptionnelles, la banque a le devoir public ou le droit de divulguer des renseignements personnels sans le consentement du client pour protéger son propre intérêt ou l'intérêt public. »²⁵⁰ On y précise aussi que la banque peut divulguer des renseignements lorsque la loi l'exige comme, par exemple, dans le cadre de citations à comparaître, de mandats de perquisition, d'autres ordonnances de la Cour et du gouvernement ou de demandes formulées par des tiers qui ont légalement le droit d'accéder aux renseignements personnels. Lorsqu'une banque doit divulguer des renseignements personnels pour obéir à la loi, elle devrait protéger les intérêts de ses clients en s'assurant que l'ordonnance est conforme à la loi aux termes de laquelle elle semble avoir été émise, en ne fournissant que les renseignements visés par l'ordonnance et en refusant de répondre aux demandes « officieuses » de renseignements que lui adressent la police ou le gouvernement.

Les renseignements personnels concernant la santé du client sont quant à eux visés par des dispositions particulières. Ces dispositions semblent vouloir apaiser les inquiétudes à l'effet que les banques utiliseraient ce genre de renseignements à des fins autres que celles pour lesquelles elles ont été obtenues.²⁵¹ Selon le code, une banque ne peut se procurer des renseignements personnels au sujet de l'état de santé de ses clients qu'à des fins précises et ne peut les divulguer à aucune société affiliée, pas plus qu'une société affiliée ne peut lui divulguer de tels renseignements. Par conséquent, les banques n'ont pas accès aux renseignements sur l'état de santé des clients de leurs sociétés affiliées pour évaluer une demande de prêt.

Le nouveau code est plus précis que l'ancien en ce qui a trait au droit d'accès d'un client à ses renseignements personnels et à ce qu'il doit faire pour faire corriger les erreurs. Une des nouveautés les plus importantes tient au fait que le droit d'accès ne se limite plus désormais aux renseignements factuels. En outre, le code énonce en toutes lettres certaines des raisons qui peuvent être invoquées pour refuser l'accès aux renseignements personnels. L'article 9.3 du code traite en ces termes du droit d'accès aux renseignements personnels :

La banque identifie où elle a recueilli les renseignements personnels, à qui et comment elle les a divulgués ainsi que le moment où elle les a divulgués. La banque extrait cette information de ses dossiers et la fournit au client sous une forme facile à comprendre, en lui expliquant les abréviations et les codes, s'il y en a. La banque fournit les renseignements personnels au client dans un délai raisonnable et à un coût minime ou nul.

²⁵⁰ *Ibid.*, Principe 5.

²⁵¹ *Ibid.*, art. 5.4. Pour un aperçu des inquiétudes que soulève l'utilisation des renseignements personnels, voir le document *Reform of Financial Services: Retailing of Insurance by Deposit-Taking Institutions* que l'Association des consommateurs du Canada a présenté au ministère fédéral des Finances (août 1995), p. 16ff.

Le code stipule qu'il arrive que la banque doive refuser à un client le droit de consulter les renseignements personnels le concernant, mais uniquement pour des raisons précises qui doivent être énoncées dans la politique de l'établissement. Certains renseignements personnels peuvent, par exemple, se révéler trop coûteux à extraire, faire allusion à d'autres personnes, être assujettis au secret professionnel ou à une procédure judiciaire, contenir des « renseignements exclusifs » de la banque ou ne pouvoir être divulgués pour des raisons d'ordre juridique.²⁵²

La grandes banques canadiennes se sont toutes dotées d'un code type ou d'une politique en matière de protection des renseignements personnels après que l'ABC ait adopté son premier code type en 1990. Plus récemment, les banques ont entrepris une révision de leurs codes et de leurs politiques pour les harmoniser avec la nouvelle version du code de l'ABC. Certaines banques offrent à leurs clients, sur demande, un exemplaire de leur code type ou de leurs politiques en matière de protection des renseignements personnels. Ainsi, les clients de la Banque Canadienne Impériale de Commerce peuvent se procurer : *La CIBC s'engage à protéger vos renseignements personnels*; la Banque Scotia, *À la Banque Scotia, vos renseignements personnels sont bien protégés*²⁵³; la Banque Toronto-Dominion, *Respect de la confidentialité – Code de protection de la vie privée TD*; la Banque Royale, *L'essentiel sur la protection de la vie privée des clients*; la Banque de Montréal, le Guide-conseil, et la Banque Nationale du Canada, *La protection des renseignements personnels des clients*. (D'autres banques exerçant des activités commerciales au Canada, dont la Banque American Express, Citibank Canada, la Banque Hongkong du Canada et ING Bank of Canada ont publié de la documentation au sujet de leurs mesures de protection des renseignements personnels.²⁵⁴) En règle générale, ces publications énoncent les grandes lignes de leurs politiques en la matière, lesquelles s'inspirent de la nouvelle version du code de l'ABC. Soulignons que l'étudiant que nous avons chargé d'obtenir un exemplaire de ces codes n'a pas réussi à obtenir ceux de deux des banques moins importantes. Les personnes auxquelles cet étudiant s'est adressé n'ont pu lui fournir un exemplaire du code ou de la politique de la banque en matière de protection des renseignements personnels. En outre, étant donné que nombre de petites institutions bancaires (mais non celles avec lesquelles nous avons communiqué) ne contribuent pas de façon suffisamment importante au marché de la consommation des services financiers, il n'est pas nécessairement opportun, dans leur cas, de se doter d'une politique ou d'un code en la matière.

²⁵² « Par exemple, une banque pourrait faire emploi d'une formule de pointage ou émettre une recommandation dont elle désire garder le secret. » Modèle de code de l'ABC, 1996, *supra*, note 244, art. 9.4.

²⁵³ Le site Web de la Banque Scotia offre la version intégrale du code dont s'est dotée cette institution bancaire en matière de protection des renseignements personnels. Voir : <http://www.scotiabank.ca/privcode.html>.

²⁵⁴ Voir : *American Express Privacy Code*, de la Banque Amex; *Your Privacy*, de la Citibank of Canada; *Strictly Between Us: Protecting your privacy and resolving your complaints* de la Banque HongKong du Canada, et *ING DIRECT: Personal Account Terms*, de la Banque ING of Canada. Voir aussi Bennett, *supra*, note 219, p. 26.

Association des compagnies de fiducie du Canada

En 1993, l'Association des compagnies de fiducie du Canada (ACFC) s'est également dotée d'un code type en matière de protection des renseignements personnels : *La vie privée des clients : une responsabilité de confiance*. À toutes fins utiles, ce document est pratiquement identique à la version de 1990 du code de l'ABC. On y retrouve huit principes portant sur la collecte des renseignements personnels, la qualité des renseignements personnels, les fins de la collecte des renseignements personnels, l'utilisation des renseignements personnels, les mesures de protection des renseignements personnels, les droits des clients en matière de consultation et de correction de leurs renseignements personnels, ainsi qu'un mécanisme de résolution des différends. Tout comme la première version du code de l'ABC, le code de l'ACFC ne permet aux clients que de consulter les renseignements factuels qui se trouvent dans leurs dossiers. Les plaintes doivent être réglées selon le mécanisme de résolution de la société de fiducie à laquelle elles sont adressées.

Il semble que les sociétés des fiducie aient adopté leurs propres politiques en matière de protection des renseignements personnels ou utilisent le code de la banque à laquelle elles sont affiliées. La société Canada Trust offre à ses clients sa propre brochure en la matière, et ses politiques s'inspirent directement des principes que l'on retrouve dans le modèle type de l'ACNOR, alors que la National Trust et la Montreal Trust utilisent la brochure et le code de leur banque mère.²⁵⁵ L'étudiant que nous avons chargé d'obtenir les codes de nombre d'autres sociétés de fiducie n'a pas réussi à se les procurer. Les sociétés avec lesquelles il a communiqué n'ont pas retourné son appel ou ne lui ont pas fourni les renseignements demandés.

Associations de l'industrie de l'assurance

L'industrie de l'assurance compte deux associations distinctes : l'Association canadienne des compagnies d'assurances de personnes inc. (ACCAP), qui représente les compagnies d'assurance vie et d'assurance maladie, et le Bureau d'assurance du Canada (BAC), qui représente les compagnies d'assurance automobile et d'assurance risques divers.²⁵⁶ Toutes deux ont joué une part active dans l'élaboration des codes de déontologie de l'industrie de l'assurance en matière de protection des renseignements personnels.

Notons que l'ACCAP avait commencé des démarches avant même la publication officielle des principes de l'OCDE. En 1980, l'Association a adopté un ensemble de lignes directrices à l'intention de ses membres. Ces lignes directrices s'inspiraient de celles qui étaient énoncées dans la version préliminaire du document de l'OCDE. Le professeur Colin J. Bennett a cerné de nombreux facteurs susceptibles d'expliquer l'intérêt que cette association porte à la question de

²⁵⁵ Le code sur la protection des renseignements personnels de la société Canada Trust s'intitule : *Protecting Your Privacy*. (novembre 1997). Les renseignements afférents à l'approche des sociétés National Trust et Montreal Trust sont tirés d'entretiens que N. Djordjevic a eus avec des agents de ces sociétés en février 1998.

²⁵⁶ Voir Bennett, *supra*, note 219, p. 28. Mentionnons que le Bureau d'assurance du Canada s'est récemment joint à un autre groupe appelé Conseil d'assurance du Canada.

la protection des renseignements personnels, dont le fait que les assureurs dont le siège social se trouvait aux États-Unis avaient déjà élaboré des codes à ce sujet pendant les années soixante-dix et que les organismes provinciaux de réglementation de l'industrie de l'assurance avaient manifesté de l'intérêt à l'égard de ce dossier.²⁵⁷ Par la suite, l'Association s'est dotée de lignes directrices précises en matière de traitement des renseignements personnels sur le VIH.²⁵⁸

En 1990, l'ACCAP prit des mesures pour mettre à jour ses lignes directrices en matière de renseignements personnels et le résultat de cet exercice fut publié en 1993. La version actuelle de ce document énonce une série de principes visant la collecte et la qualité des renseignements personnels, les fins de la collecte, l'utilisation et la divulgation de ce genre de renseignements, le droit d'accès imparti aux clients, les mesures de résolution des différends et les mécanismes de protection des renseignements personnels. Le libellé et l'esprit de ces lignes directrices s'inspirent également des principes formulés par l'OCDE. Elles ne comportent cependant aucune disposition relative à la correction des erreurs et les plaintes doivent être réglées par les sociétés elles-mêmes. Les lignes directrices s'accompagnent de notes explicatives qui traitent de façon plus étoffée de la signification des principes énoncés dans la brochure.²⁵⁹

En 1992, le BAC s'est doté du *Code modèle de protection des renseignements privés de clients*, lequel s'inspirait, lui aussi, des directives de l'OCDE et qui était semblable, à bien des égards, au code de 1990 de l'Association des banquiers canadiens. La version de 1992 de ce code énonçait une série de principes sur les objectifs des renseignements personnels, la qualité des renseignements personnels, la collecte des renseignements personnels, les limites relatives à

²⁵⁷ *Ibid.*, p. 29.

²⁵⁸ Association canadienne des compagnies d'assurances de personnes inc., *Lignes directrices concernant le sida – Sélection des risques et souscription d'assurance vie et d'assurance maladie* (1987).

²⁵⁹ Certains éléments des nouvelles lignes directrices de l'ACAAP méritent qu'on s'y attarde. Le principe relatif aux limites applicables à la collecte de renseignements suggère que l'on doit tout d'abord tenter d'obtenir les renseignements « appropriés » auprès de la personne intéressée, après quoi l'on pourra s'adresser à une autre source, mais non sans en avoir tout d'abord prévenu le client. Ce principe ne s'applique toutefois pas aux associations de compagnies d'assurance, puisqu'elles n'ont aucun droit de regard sur les méthodes qu'emploient les employeurs pour recueillir des renseignements au sujet de leurs employés. Le principe relatif à l'utilisation et à divulgation des renseignements personnels stipule que ces renseignements doivent être utilisés aux fins précisées à l'intéressé au moment où ils ont été recueillis, ou dans l'une des quatre circonstances prévues par le code. Le principe relatif à l'accès à l'information s'applique à tous les renseignements qui se trouvent dans les dossiers de la compagnie d'assurance, sans établir de distinctions entre les renseignements factuels et les dossiers d'opinion, comme le faisait la première version du code de l'ABC. Le code permet à une compagnie d'assurance d'exiger une redevance raisonnable des personnes qui désirent consulter leur dossier personnel et stipule que les renseignements à caractère médical ne peuvent être divulgués que par l'entremise d'un médecin.

l'utilisation des renseignements personnels, les mesures de protection, le droit du client à consulter son dossier, la responsabilité de l'assureur et la transparence dont il devait faire preuve. Les assureurs devaient eux-mêmes régler les plaintes selon leur propre marche à suivre.²⁶⁰

Quelques années plus tard, soit en 1997, le BAC entreprit de mettre à jour son code type à la lumière des dix principes énoncés dans le code de l'ACNOR. Le nouveau code du BAC a reçu l'approbation du Quality Management Institute of Canada, ce qui signifiait qu'il était conforme à celui de l'ACNOR.²⁶¹ Cette nouvelle version contient nombre de dispositions remarquables en matière d'énoncé de consentement, de limite de l'utilisation et de droit d'accès à l'information. Le principe du consentement prévoit qu'une personne peut, dans un délai raisonnable, retirer son consentement à l'utilisation des renseignements personnels la concernant, sous réserve de restrictions juridiques ou contractuelles, et exige que les assureurs de dommages s'assurent de l'exactitude des statistiques et des données dont ils ont besoin pour mener leurs activités.²⁶² Le

²⁶⁰ Nombre d'autres dispositions du code du BAC, version 1992, méritent d'être soulignées. Le principe relatif aux limites applicables à la collecte des renseignements personnels contenait une liste de fins à l'égard desquelles les compagnies d'assurance pouvaient recueillir de tels renseignements. Ces fins avaient été spécifiquement formulées à l'intention des compagnies d'assurance. Il y était question de risques de souscription témoignant de prudence, de l'étude et du règlement de demandes d'indemnité, et de l'établissement de statistiques. Les renseignements personnels devaient être principalement recueillis auprès de la personne intéressée, mais il était aussi possible de s'adresser à nombre d'autres sources opportunes dans les circonstances (comme des courtiers, le Service anti-crime des assureurs et les réseaux de renseignements sur la souscription). Le client devait consentir à ce que l'assureur demande des renseignements personnels à son sujet, sauf dans des « circonstances exceptionnelles où l'on pouvait raisonnablement soupçonner une fraude ». En ce qui a trait au principe sur les limites d'utilisation, le code du BAC prévoyait, comparativement à la version 1990 du code de l'ABC, une liste encore plus longue de circonstances dans lesquelles il était possible de divulguer des renseignements personnels sans le consentement du client. Ces circonstances comprenaient la transmission de renseignements à une société qui prenait part au risque, la transmission à des fins de souscription ou d'étude d'une demande d'indemnité, ainsi que la transmission à des mandataires de compagnies d'assurance. En ce qui a trait au principe d'accès à l'information, le code du BAC adhérait aux modalités énoncées dans le code de l'ABC, version 1990, en n'autorisant l'accès qu'aux renseignements factuels concernant la personne elle-même. Enfin, le code du BAC prévoyait un mécanisme de résolution des différends lorsque l'assureur refusait de permettre à son client de consulter son dossier. On y précisait qu'un client qui désirait contester la décision de son assureur de lui interdire l'accès à son propre dossier devait envoyer une lettre à cet effet au président de la compagnie, lequel avait alors pour mission « d'entamer le dialogue avec le client dans les meilleurs délais » [traduction libre]. Les deux parties devaient également convenir d'une façon d'en arriver à une solution satisfaisante en cas d'échec de ce dialogue.

²⁶¹ « Le code du BAC est le premier à avoir reçu la sanction de l'Association canadienne de normalisation. »

Observation tirée d'une publication du *Bureau d'assurance du Canada*, (mars 1997), p. 1.

²⁶² Bureau d'assurance du Canada, *Modèle de code sur les renseignements personnels du Bureau d'assurance du Canada* (1996), art. 4.3.10. La disposition relative au consentement du client contient nombre de modalités dignes d'intérêt. On y fait état de certaines caractéristiques propres aux activités des assureurs de dommages qui font en sorte qu'il est parfois impossible d'obtenir le consentement explicite ou écrit du client, comme le fait que ces assureurs transigent par l'entremise d'agents et de courtiers indépendants. On y précise que l'assureur peut refuser d'assurer les clients qui ne consentent pas à fournir des renseignements au sujet de leur date de naissance, leur adresse et les demandes d'indemnité qu'ils ont présentées dans le passé parce qu'il serait alors impossible à l'assureur d'établir une prime au taux adéquat. On y précise également qu'une personne peut consentir à la collecte et à l'utilisation de renseignements personnels au nom de plusieurs personnes, comme, par exemple, dans le cas des personnes qui désirent obtenir une assurance automobile pour leur famille. Enfin, on y stipule que certaines catégories de renseignements personnels de nature délicate, comme les renseignements provenant de dossiers médicaux ou d'établissements hospitaliers, de dossiers d'emploi ou de déclarations d'impôt, ne peuvent être obtenus sans le consentement explicite et écrit du client. Voir respectivement les articles 4.3.1, 4.3.5, 4.3.8, et 4.3.6.

principe portant sur la limite de l'utilisation prévoit plusieurs circonstances précises dans lesquelles un assureur de dommages peut divulguer à des tiers des renseignements personnels au sujet de ses clients « par mesure de prudence ». ²⁶³ Le principe relatif au droit d'accès à l'information offre aux clients la possibilité de faire appel à un médiateur lorsque l'assureur refuse d'ouvrir ses dossiers. ²⁶⁴

Les politiques des compagnies d'assurance vie en matière de protection des renseignements personnels sont tirées à la fois des lignes directrices de l'ACCAP et du code type du BAC. ²⁶⁵ Celles de la London Life suivent le modèle de l'ACCAP alors que la Mutuelle du Canada, Compagnie d'assurance sur la vie, a préféré insérer des dispositions à cet égard dans un document à portée plus générale traitant des rapports avec les clients. L'étudiant que nous avons chargé d'obtenir des exemplaires de ces codes et brochures auprès de nombreuses autres compagnies d'assurance n'y est pas parvenu. Un agent de l'Aetna Life Insurance Company l'a informé que leurs politiques en la matière s'appuient sur les lignes directrices de l'ACCAP, mais qu'elles n'étaient pas diffusées à l'intention du grand public. Les autres compagnies d'assurance n'ont pas retourné ses appels, lui ont répondu qu'elles n'avaient aucune politique en la matière ou n'ont pas fourni les documents en question.

Plus de quatre-vingts assureurs ou groupes d'assureurs de dommages, représentant près de 75 p. 100 du marché (en termes de primes) ont adhéré à la version 1992 du code type du BAC. ²⁶⁶ Puisque cette version était destinée à être adoptée telle quelle, ces compagnies d'assurances se sont engagées à l'utiliser sans publier leurs propres brochures ou politiques. ²⁶⁷ On s'attend à ce que les membres du BAC adoptent bientôt la version 1997 de ce code.

²⁶³ Cela comprend : la divulgation de renseignements personnels à des compagnies de réassurance qui prennent part au risque, la divulgation de renseignements personnels à des fins de souscription, d'examen d'une demande d'indemnité, de classification ou de pointage, de même que la divulgation de renseignements personnels à des mandataires de compagnies d'assurance comme les agents et les courtiers. Voir le modèle de code du BAC, *supra*, note 262, art. 4.5.1.

²⁶⁴ Le principe relatif à l'accès à l'information stipule que si une demande d'accès est refusée, le client a le droit de connaître le motif du refus et d'être informé de la façon de contester ce refus. Il a notamment le droit « a) d'être invité à transmettre au président de l'assureur I.A.R.D. une lettre dans laquelle il prie l'assureur I.A.R.D. de revenir sur sa décision; b) d'obtenir un engagement de la part de l'assureur I.A.R.D. d'établir sans retard un dialogue avec le client; et c) d'obtenir l'engagement de la part de l'assureur I.A.R.D. de participer à un processus de médiation indépendante si les parties ne parviennent pas à prendre des dispositions en vue de ce processus de médiation indépendante. » Voir le Modèle de code du Bureau d'assurance du Canada, 1996, *supra*, note 262, art. 4.9.1.

²⁶⁵ Un observateur a fait remarquer que les grandes compagnies d'assurance de personnes ont commencé à publier des lignes directrices et des codes sur la protection des renseignements personnels pendant les années quatre-vingt. Voir Bennett, *supra*, note 219, p. 29.

²⁶⁶ Télécopie adressée par Steven Lingard, du Bureau d'assurance du Canada, à T.S. Onyshko, le 22 mai 1998.

²⁶⁷ Entrevue réalisée par T.S. Onyshko auprès de Steven Lingard, du Bureau d'assurance du Canada, le 20 février 1998.

Centrale des caisses de crédit du Canada

La Centrale des caisses de crédit du Canada (CCCC) est en voie d'élaborer un modèle de code sur la protection des renseignements personnels à l'intention de ses membres. Les lignes directrices qu'il contient devraient être mises en œuvre vers la fin de 1998.²⁶⁸ La version préliminaire du modèle de code de la CCCC s'inspire du code type de l'ACNOR en ce qu'on y retrouve essentiellement les mêmes principes généraux.²⁶⁹ Toutefois, elle comporte nombre de dispositions dignes d'intérêt. Ainsi, le principe stipulant que la caisse de crédit doit préciser les fins auxquelles sont destinés les renseignements personnels au moment où elle les demande au client exige également que ces fins doivent être propres à la personne concernée.²⁷⁰ Le principe selon lequel il est nécessaire d'obtenir le consentement du client contient certaines modalités relatives à ce que ce dernier serait raisonnablement en droit de s'attendre dans des circonstances précises;²⁷¹ en outre, le principe qui traite du consentement offre au client la possibilité de retirer son consentement en tout temps, sous réserve d'impératifs juridiques ou contractuels.²⁷² Le principe qui porte sur l'utilisation, la divulgation et la conservation des renseignements personnels contient une disposition particulière visant le traitement des renseignements de nature médicale, laissant entendre que ces renseignements peuvent être utilisés dans le cadre des évaluations de demande de crédit ainsi qu'à d'autres fins liées à l'assurance.²⁷³ Enfin, le principe

²⁶⁸ Lettre adressée par Susan Murray, Directrice des affaires gouvernementales, Centrale des caisses de crédit du Canada, à Richard C. Owens, le 28 novembre 1997.

²⁶⁹ Centrale des caisses de crédit du Canada, *Credit Union Code for the Protection of Personal Information* (version préliminaire) (juin 1996).

²⁷⁰ *Ibid.*, s. 2.3. On peut supposer que cela signifie que l'explication écrite ou verbale que l'on fournit au client doit tenir compte, dans une certaine mesure, des circonstances particulières. La version préliminaire du code laisse entendre, par exemple, qu'une demande de services ou d'adhésion précisant les fins à l'égard desquelles les renseignements sont demandés pourrait satisfaire à cette exigence.

²⁷¹ « Dans le processus visant à obtenir le consentement, il faut également tenir compte des attentes raisonnables du membre. Par exemple, un membre qui présente une demande de carte de débit doit s'attendre à ce que la caisse de crédit, en plus d'utiliser le nom et l'adresse du membre aux fins de lui faire parvenir ses relevés par la poste, doive également utiliser ses coordonnées pour renouveler sa carte. De même, il n'est pas nécessaire d'obtenir le consentement du membre pour communiquer des renseignements aux mandataires de la caisse de crédit aux fins de leur permettre de s'acquitter des tâches qui leur sont imparties, comme le traitement des données et l'impression de chèques personnalisés. Le cas échéant, la caisse peut présumer que la demande que présente le membre équivaut à un consentement tacite à des fins précises. Par ailleurs, on ne peut raisonnablement s'attendre à ce que ce consentement tacite s'applique également à la transmission de ces renseignements à une compagnie qui vend des produits d'assurance. La caisse de crédit ne saurait donc poser un tel geste sans le consentement explicite du membre. » Version préliminaire du code de la CCCC, traduction libre, *supra*, note 269, art. 3.5.

²⁷² Dans une disposition de même nature que l'on retrouve dans la version préliminaire des modèles de code de l'ABC et du BAC, il est stipulé que : « Un membre peut retirer son consentement en tout temps, sous réserve d'obligations légales ou contractuelles, dans la mesure où : (a) la caisse de crédit en est avisée dans un délai raisonnable; et (b) le consentement ne s'applique pas à un produit de crédit à l'égard duquel la caisse de crédit doit obtenir ou divulguer de l'information après avoir octroyé un crédit. » [traduction libre] Voir le code de la CCCC, *supra*, note 269, art. 3.7.

²⁷³ « Les renseignements provenant des dossiers médicaux détenus par la caisse de crédit peuvent être utilisés pour l'étude de demandes de crédit et à d'autres fins liées à l'assurance. La caisse de crédit ne peut ni recueillir, ni divulguer des renseignements médicaux auprès d'un autre organisme. » Voir la version préliminaire du code de la CCCC, *supra*, note 269, art. 5.4.

de l'observation des règles susmentionnées offre aux clients insatisfaits du traitement de leurs plaintes la possibilité d'obtenir une audience auprès d'un médiateur ou d'un arbitre indépendant.²⁷⁴

Observations concernant les codes des associations

Nombre d'observations peuvent être formulées quant aux améliorations qu'il serait possible d'apporter à l'ensemble des codes dont nous venons de parler dans le but de les rendre plus conformes aux principes formulés par l'OCDE et à la théorie sur la protection des renseignements personnels. En premier lieu, ces codes autorisent tous le consentement implicite, soit en définissant le consentement de manière à en prévoir la qualité implicite, soit en omettant tout simplement de l'exclure des mesures de consentement. Les données théoriques sur la protection des renseignements personnels laissent entendre qu'il faut accorder la préférence au consentement exprès, particulièrement lorsqu'il est question de renseignements de nature délicate. Certains de ces codes accordent la préférence au consentement exprès et stipulent même que dans certaines circonstances, cette forme de consentement devrait être incontournable.²⁷⁵ Toutefois, les codes devraient plutôt restreindre l'utilisation du consentement implicite au traitement des renseignements de nature autre que délicate et fournir des consignes précises quant aux circonstances dans lesquelles il serait opportun d'y faire appel.

Deuxièmement, aucun de ces codes ne traite de façon précise de l'exploration de données et de l'utilisation des renseignements personnels à des fins de marketing. Afin de permettre aux gens de conserver un certain contrôle de leurs renseignements personnels, il serait souhaitable de leur permettre d'interdire l'exploration de données provenant de leurs dossiers personnels à des fins de ciblage et de marketing. Les codes types contiennent des dispositions qui pourraient être interprétées comme visant l'extraction des données et les activités de marketing. Ainsi, on y exige généralement que, sous réserve d'obtenir le consentement du client à l'effet contraire, les renseignements ne soient utilisés qu'aux fins pour lesquelles ils ont été recueillis en premier lieu. De plus, certains codes stipulent que le client peut retirer son consentement en tout temps, à certaines conditions.²⁷⁶ Le code de l'ABC exige des banques qu'elles obtiennent le

²⁷⁴ *Ibid.*, art. 10.3. La version préliminaire du code stipule que les plaintes que les mandataires autorisés de la caisse de crédit ne parviennent pas à résoudre peuvent être confiées au conseil d'administration de la caisse. Lorsque le conseil d'administration ne parvient pas à les résoudre, les plaintes doivent être confiées à la Centrale des caisses de crédit, à un organisme de réglementation ou à un arbitre ou un médiateur indépendant, selon les circonstances."

²⁷⁵ Le code de la CCCC précise qu'il est préférable d'obtenir le consentement explicite du client, alors que celui du BAC stipule qu'il est nécessaire de l'obtenir avant de recueillir des renseignements à caractère médical, des renseignements provenant d'un établissement hospitalier, des renseignements sur l'emploi et des renseignements sur les déclarations d'impôt sur le revenu du client. Voir le modèle de code de l'ABC, 1996, *supra*, note 244, art. 3.3 et le modèle de code du BAC, 1996, *supra*, note 262, art. 4.3.6.

²⁷⁶ Le code de l'ABC, le code du BAC et la version préliminaire du code de la CCCC précisent qu'un client peut retirer son consentement après l'avoir exprimé, sous réserve de conditions précises,. Voir le modèle de code de l'ABC, 1996, *supra*, note 244, art. 3.5; le modèle de code du BAC, 1996, *supra*, note 262, art. 4.3.10; et la version préliminaire du code de la CCCC, *supra*, note 269, art. 3.7.

consentement du client avant d'utiliser les renseignements personnels qui se trouvent dans son dossier à des fins de marketing.²⁷⁷ Il serait toutefois préférable que les codes précisent en toutes lettres que les clients peuvent demander aux institutions financières de ne pas utiliser leurs renseignements personnels à des fins d'exploration de données et de marketing. Certaines institutions financières ne possèdent peut-être pas encore l'infrastructure informatique nécessaire à la radiation du nom de clients précis de leurs listes établies à des fins de marketing. Afin de ne pas leur imposer de trop lourdes dépenses, les codes pourraient exiger qu'elle prennent des mesures raisonnables afin de satisfaire aux souhaits de leurs clients en la matière.

Troisièmement, les codes traitent tous de la détermination des fins de la collecte des renseignements personnels, bien que leurs dispositions à cet effet ne soient pas toutes libellées de la même manière. Certains d'entre eux spécifient que les renseignements ne peuvent être obtenus que s'ils ont un lien direct avec les objectifs énoncés dans le code, d'autres stipulent que les renseignements doivent être « opportuns » aux activités de l'institution, ou encore « nécessaires à la réalisation des fins » qui ont été établies par l'institution. Afin de mieux correspondre au principe de l'OCDE en matière de limites applicables à la collecte des renseignements personnels, les codes devraient offrir une description plus précise des genres de renseignements qu'il est possible de recueillir, voire même de ceux qui ne devraient pas être recueillis. Il y a également la question de la collecte de renseignements personnels auprès de tiers plutôt que de l'intéressé lui-même. Les codes devraient détailler les circonstances dans lesquelles il est opportun de s'adresser à des tiers pour obtenir des renseignements personnels à propos d'un client. Ils pourraient aussi exiger de l'institution qu'elle avise ses clients lorsqu'elle demande un rapport de solvabilité à leur sujet.

Quatrièmement, les codes offrent généralement une liste ouverte de raisons pour lesquelles il est possible de refuser à une personne le droit de consulter son dossier personnel. On reconnaît ainsi le droit de refuser l'accès (certains codes ajoutent : pour des motifs « valables » ou « précis ») sans toutefois énoncer de circonstances précises. Les lois sur l'accès à l'information et la protection des renseignements personnels visant les gouvernements fédéral et provinciaux énoncent justement les circonstances dans lesquelles on peut contourner ce droit. Il serait préférable que les codes en fassent autant plutôt que de laisser la question en suspens, ne fournissant qu'une liste ouverte prêtant à interprétation, bien que d'aucuns pourront alléguer que cette façon de faire confère une certaine souplesse à la marche à suivre.

Pour terminer, nous allons nous pencher sur deux autres questions liées à la mise en œuvre des modèles de code. Premièrement, il faut se demander dans quelle mesure les institutions financières fournissent des exemplaires de leurs codes au public. Comme nous l'avons souligné un peu plus tôt, les étudiants chargés d'obtenir des exemplaires de ces documents n'ont pas toujours eu la tâche facile, particulièrement lorsqu'ils se sont adressés à de petits établissements, qu'il s'agisse d'institutions bancaires, de sociétés de fiducie ou de compagnies d'assurance. Pour fonctionner adéquatement, un système fondé sur de tels codes doit comporter un mécanisme efficace de diffusion. Les institutions, les associations dont elles sont membres et, au besoin, les

²⁷⁷ Modèle de code de l'ABC, 1996, *supra*, note 244, art. 5.3.

organismes de réglementation, devraient prendre des mesures concrètes pour veiller à ce que le public ait facilement accès aux codes de tous les fournisseurs de services financiers. Nous croyons savoir qu'un projet de règlement à cet effet est présentement à l'étude dans le cadre de la loi fédérale, lequel exigera des institutions financières qu'elles fournissent des renseignements à leurs clients au sujet de leurs politiques en matière de protection des renseignements personnels.

Vient ensuite la question du traitement, aux termes des dispositions des codes, des plaintes formulées par les clients. Le modèle de code de l'ABC mérite des éloges à cet égard puisqu'il offre aux clients la possibilité d'en appeler d'un règlement insatisfaisant auprès de l'Ombudsman bancaire canadien. D'autres codes proposent de faire appel à un tiers (comme un médiateur) pour régler les plaintes complexes. Du point de vue de la protection des renseignements personnels, il serait préférable que toutes les associations de l'industrie prévoient un mécanisme précis de résolution des différends, comme faire appel à l'Ombudsman bancaire canadien ou à quelque autre méthode de médiation. On ne saurait cependant faire abstraction des coûts liés à un tel système. Les dépenses qu'il faudrait engager pour le mettre sur pied pourraient être supérieures à ses retombées. Nous aborderons cette question de façon plus détaillée dans les conclusions de ce document (Parties VI et VII).

Ces observations ne visent pas à signaler des lacunes que nous avons jugées importantes, mais plutôt à cerner les éléments pouvant faire l'objet d'améliorations dans une conception sans faille de la protection des renseignements personnels. Il faut souligner que ces codes témoignent d'un engagement sérieux envers la protection des renseignements personnels. Chacun d'entre eux répond aux préoccupations qui ont amené l'OCDE à formuler des principes afférents au droit à la vie privée et à la protection des renseignements personnels. Chacun d'entre eux énonce une série de principes raisonnables et stipule, dans une certaine mesure, le droit des particuliers de consulter les renseignements qui se trouvent dans leurs dossiers personnels et d'y apporter des corrections au besoin. Ces codes constituent la pierre d'assise du système d'autoréglementation raisonnable qu'avaient envisagé les principales associations de l'industrie du secteur des services financiers.

III. Problèmes relatifs à la protection de la vie privée

Introduction

La Partie III porte sur les menaces à la protection des renseignements personnels. Elle commence par un examen des principales préoccupations des associations de consommateurs et des spécialistes en la matière, lesquelles ont essentiellement trait à la diffusion et à la consultation des renseignements personnels, au recours au consentement implicite (par opposition à explicite), aux mécanismes de résolution des différends, à la transparence des institutions et au fait que nombre de fournisseurs de services financiers ne sont assujettis à aucune loi fédérale. Nous poursuivons avec l'étude des technologies et des tendances commerciales ayant une incidence sur la protection des renseignements personnels, comme le recoupement des données, le marketing ciblé et l'exploration de données, les cartes à puce, les opérations bancaires sur Internet et les logiciels de gestion de fonds, de même que l'échange de renseignements et la prestation de services financiers à l'échelle internationale.

Inquiétudes des consommateurs²⁷⁸

Le partage et l'utilisation des renseignements personnels

Comme les institutions financières offrent un éventail de plus en plus large de produits et services et qu'elles continuent à améliorer leurs programmes de vente directe, il faut s'attendre à ce qu'elles cherchent à exploiter davantage les renseignements personnels dont elles disposent. L'utilisation des renseignements personnels pour « cibler le marché » ou « la mise en marché sur mesure » est une des grandes orientations dans le commerce au détail, et nous devons prévoir que les services financiers s'y adonneront de plus en plus, de la même façon que tout autre détaillant

²⁷⁸ Pour en savoir davantage sur les préoccupations des consommateurs, voir, par exemple : Association des consommateurs du Canada, *Privacy and Data Protection: Background Paper* (La vie privée et la protection des renseignements : document de base) (Ottawa, Association des consommateurs du Canada Consumers, juillet 1992); Association des consommateurs du Canada, *Consumer Data Protection* (Protection des renseignements sur les clients) (Ottawa, Association des consommateurs du Canada, mars 1993); Association des consommateurs du Canada, *Privacy in the Age of the Information Highway* (La vie privée à l'âge de l'information) (Ottawa, Association des consommateurs du Canada, mars 1995); Ed Pawlusiak, *Codes, standards and practices: Do they protect consumer interests ?* (Codes, normes et pratiques : Protègent-ils les intérêts des consommateurs?) (Ottawa, Association des consommateurs du Canada, avril 1996); Option consommateurs, *Les Canadiens et la protection des renseignements personnels détenus par les entreprises : éléments d'une législation (sommaire d'une étude à paraître)* (Montréal, Fédération nationale des associations de consommateurs du Québec et Option consommateurs, février 1998); Association coopérative d'économie familiale du Centre de Montréal, *Les consommateurs et l'examen de 1997 de la législation régissant les institutions financières : Observations présentées au ministère des Finances du Canada* (Montréal, Association coopérative d'économie familiale du Centre de Montréal, 1996). Voir aussi les propositions contenues dans la lettre de Richard D. Speers (Toronto) adressée au Groupe de travail sur l'avenir du secteur des services financiers au Canada et datée du 23 septembre 1997, dans laquelle M. Speers aborde certaines préoccupations liées aux pratiques bancaires et aux codes de protection des renseignements personnels.

le ferait. Les institutions financières, en tant qu'utilisatrices intensives des technologies d'information, sont peut-être dans le peloton de tête de cette tendance. On peut y voir un côté positif en constatant que les banques se dotent de meilleurs outils pour fournir un service personnalisé. Cependant, des groupes de consommateurs et quelques experts en matière de protection de la vie privée prétendent que l'utilisation et la manipulation continue des renseignements personnels soulèvent des inquiétudes importantes relatives à la protection de la vie privée et des libertés individuelles. À l'extrême, on postule que les renseignements pourraient être utilisés pour manipuler et intimider les consommateurs. Par exemple, l'Association des consommateurs du Canada a évoqué la possibilité que des personnes puissent subir des pressions implicites pour accepter de nouveaux services offerts par une banque les ayant sollicitées par le biais de d'une campagne de marketing ciblé.²⁷⁹ L'argument se fonde sur le fait qu'une personne va se sentir obligée d'accepter les nouveaux produits qui lui sont offerts si elle veut garder de bonnes relations avec la banque et pour s'assurer un accès aux services essentiels qui pourraient lui être offerts dans le futur, les facilités de crédit par exemple.

Parallèlement aux inquiétudes générales sur l'utilisation croissante des renseignements personnels, les défenseurs des intérêts des consommateurs ont exprimé une inquiétude particulière, relative à l'utilisation par les banques des renseignements personnels fournis à des fins d'assurance. Comme la capacité des banques à offrir des produits d'assurance s'est accrue par l'intermédiaire de filiales, de nouvelles perspectives d'utilisation des renseignements personnels acquis grâce au secteur des assurances pourraient se matérialiser. L'Association des consommateurs du Canada a soutenu que les renseignements personnels fournis à des fins d'assurance ne devraient pas être utilisés dans le cas de prises de décision relatives aux services bancaires offerts aux particuliers.²⁸⁰ Par exemple, la décision de refuser une couverture d'assurance à une personne ne devrait pas être utilisée pour réduire sa cote de crédit. De plus, des renseignements personnels sur un problème de santé potentiel révélés par une personne à un assureur dans le cas d'une obligation de divulgation à l'assureur, ne devraient pas être utilisés contre cette personne lorsqu'elle fera ultérieurement une demande d'emprunt.

Ces préoccupations méritent d'être examinées plus sérieusement. Les programmes de marketing peuvent entraîner des atteintes à la vie privée par des appels téléphoniques ou du courrier non sollicités.²⁸¹ Cependant, ces programmes peuvent aussi avoir l'avantage de porter à l'attention des consommateurs des produits ou des services qui pourraient leur être utiles ou correspondre à des besoins particuliers. Quoique « l'exploration des données » et le marketing ciblé se soient sans contredit avérés utiles pour les spécialistes du marketing, il est faux de prétendre que ces

²⁷⁹ Voir, par exemple : Association des consommateurs du Canada, *Reform of Financial Services: Retailing of Insurance by Deposit-Taking Institutions* (Réforme des services financiers, vente au détail d'assurances par des institutions de dépôt) (août 1995).

²⁸⁰ *Ibid.*

²⁸¹ Certaines catégories de sollicitations téléphoniques sont réglementées par le CRTC en vertu de dispositions de protection de la vie privée, cette notion faisant l'objet d'une politique explicite devant être mise en œuvre dans le cadre de l'interprétation de la nouvelle loi sur les télécommunications. Le code de l'Association canadienne de marketing direct, dont l'observance est volontaire, impose des limites aux envois de courrier non sollicité par les membres de l'Association.

stratégies ont la capacité d'influencer indûment les gens ou qu'elles ont été créées dans cette intention. Par ailleurs, selon les codes de protection de la vie privée, les banques et les assureurs se sont eux-mêmes engagés à respecter le principe selon lequel une personne peut retirer ultérieurement son consentement relatif à l'utilisation des renseignements personnels la concernant à des fins particulières.²⁸² La sophistication croissante des réseaux de services financiers pourrait même faire en sorte qu'un tel consentement puisse être refusé ou retiré pour des catégories spécifiques de services.

On allègue pertinemment que les renseignements médicaux recueillis à des fins d'assurance ne devraient pas être utilisés pour prendre des décisions au sujet de services bancaires, d'autant plus que le personnel affecté à ces services n'a pas l'habitude de vérifier de tels renseignements. Les données financières et les renseignements médicaux sont considérés par le public comme étant de nature très délicate et il est possible qu'il y ait des objectifs politiques légitimes sous-jacents au cloisonnement de ces deux catégories de renseignements.²⁸³ Le modèle de code de l'ABC traite directement de cette question en déclarant que les dossiers médicaux ne seront recueillis qu'à des fins précises et que les banques et leurs filiales ne devront pas se transmettre les dossiers médicaux entre elles.²⁸⁴ En général, l'institution est mieux servie en recueillant seulement les informations nécessaires à sa prise de décision concernant le crédit. Les institutions sont obligées d'avoir et de suivre des politiques internes de crédit pour régler l'enquête de crédit et la procédure d'approbation. De telles politiques seraient mal utilisées si elles s'appliquaient à des renseignements n'ayant aucun rapport et d'un intérêt douteux hors contexte. D'ailleurs, les assureurs, incluant les compagnies d'assurance qui appartiennent à d'autres fournisseurs de services financiers, ont un intérêt essentiel à communiquer des renseignements exacts sur leurs assurés.²⁸⁵ En particulier, les assureurs se fient sur la doctrine *uberrimae fides*, ou sur le devoir de la plus grande franchise, qui stipule qu'un assuré a le devoir de communiquer à l'assureur tous les renseignements utiles demandés par ce dernier en ce qui a trait à une police d'assurance. À l'intérieur de cette obligation, il est implicite que l'assureur doit se porter garant de ces renseignements. L'assureur ne voudrait certainement pas nuire à la communication de

²⁸² Les modèles de code de l'Association des banquiers canadiens et du Bureau d'assurance du Canada permettent aux personnes de retirer leur consentement à certaines conditions. De plus, le code de l'Association oblige les banques à obtenir le consentement des individus avant d'utiliser des renseignements personnels à des fins de marketing. Voir les notes 276 et 277 de la Partie II ainsi que le texte de cette section.

²⁸³ Les Associés de recherche Ekos inc., *Privacy Revealed: The Canadian Privacy Survey* (Vie privée exposée : Sondage canadien sur la vie privée) (Ottawa, Les Associés de recherche Ekos inc., 1993), p. 20. Cette étude est abordée plus en profondeur à la Partie I dans la section intitulée « Préoccupations du grand public à l'égard de la protection des renseignements personnels et plaintes afférentes ».

²⁸⁴ Association des banquiers canadiens, *Modèle de code; confidentialité – pour protéger les renseignements personnels des clients des banques* (1996), Principe 5.

²⁸⁵ Paradoxalement, les entreprises n'ont pas intérêt à tout savoir. Comme Trevor Hoffman l'a démontré éloquemment dans une analyse économique contenue dans un document qui n'a pas été publié et qui s'intitule *The Economics of Privacy: an analysis of information access in the insurance context* (1997) (Les aspects économiques de la protection de la vie privée : une analyse de l'accès à l'information dans le contexte de l'assurance), dans un monde où l'on saurait tout, l'industrie de l'assurance ne survivrait pas car les primes équivaldraient aux coûts marginaux du moindre risque. Seule la capacité de répartir les risques actuariels sur un grand nombre permet au secteur de l'assurance d'aller de l'avant.

renseignements en passant pour une personne (morale) qui utilise les renseignements fournis à des fins d'assurance de façon inappropriée. Après tout, il n'y a généralement aucune restriction sur ce qui peut être demandé dans le cas d'une demande de crédit à condition que les renseignements soient pertinents. Il est préférable pour un organisme de crédit de redemander des renseignements, même si cela ne fait que reproduire des renseignements déjà obtenus dans le contexte de l'assurance, plutôt que de compter sur d'autres dossiers de renseignements, peut-être anciens, obtenus dans un autre contexte et sous d'autres conditions.

La transmission et l'utilisation de renseignements personnels en dehors des organismes qui ont recueilli ces renseignements sont des préoccupations souvent évoquées lors de discussions sur la protection des renseignements personnels. Cependant, la question semble moins pertinente dans le cadre des institutions financières réglementées. De telles institutions sont soumises à une obligation législative de protéger les renseignements liés à leurs clients et possèdent une longue tradition de confidentialité à l'égard de ces derniers.²⁸⁶ De plus, de telles institutions sont probablement assujetties à l'obligation implicite, reconnue dans la décision *Tournier*, de garder le secret.²⁸⁷ Bien que cette décision s'applique aux banques, il n'y a aucun fondement permettant de distinguer d'autres fournisseurs de services financiers qui y seraient assujettis. Des transmissions ou des communications de renseignements non autorisées à l'extérieur des institutions financières réglementées sont illégales et seraient certainement nuisibles pour les affaires de ces institutions si ces faits étaient révélés au public. En général, des transmissions ou des communications de renseignements à l'extérieur des institutions financières se produiront seulement avec le consentement explicite ou implicite du client. Par exemple, les banques fournissent couramment des renseignements sur le crédit de leurs clients à des bureaux de crédit, mais le consentement à de telles communications sera donné sur des formulaires que le client doit remplir pour obtenir les services d'une banque.²⁸⁸ D'ailleurs, il existe une contrainte sociale pour s'assurer que cette communication se fasse de manière à ce que les entreprises de crédit puissent évaluer les antécédents de tout demandeur en matière de crédit. Il arrive, *occasionnellement*, que des transmissions ou des communications de renseignements personnels non autorisées se produisent, comme semblent le suggérer des plaintes adressées à l'Ombudsman

²⁸⁶ Les dispositions relatives à la protection des renseignements personnels et des renseignements liés à la clientèle dans les lois et règlements fédéraux sont commentées à la Partie II dans la section intitulée « Dispositions législatives visant les institutions financières et la protection des renseignements personnels ».

²⁸⁷ Le jugement *Tournier* fait l'objet de remarques à la Partie II sous la rubrique intitulée « L'exigence contractuelle implicite de confidentialité ». La cause *Tournier* impliquait une banque et des cas semblables faisant ressortir l'exigence implicite de confidentialité impliquent aussi des banques, car on fait très souvent appel à celles-ci, semble-t-il, pour obtenir des renseignements sur le crédit de quelqu'un ou sur des sujets connexes le concernant. Il semble cependant qu'il n'y a aucun motif pour que ce jugement ne puisse s'appliquer à d'autres institutions financières détenant des renseignements confidentiels. De fait, nous souhaiterions que l'exigence implicite de confidentialité puisse être également applicable à des institutions non réglementées, telles que les entreprises de crédit à la consommation.

²⁸⁸ Veuillez consulter les remarques contenues à la Partie II dans les notes de bas de page 136-140 et dans les autres textes à propos des formulaires d'ouverture de compte dans les banques.

bancaire canadien ainsi qu'à la Commission québécoise d'accès à l'information.²⁸⁹ Mais ces situations sont le résultat d'erreurs ou de malentendus de la part d'employés de banques et ne sont pas représentatives des pratiques normales dans les banques.

Consentement implicite par opposition à consentement explicite

Un autre enjeu concerne la question du consentement implicite par rapport au consentement explicite. Des groupes de consommateurs et certains experts en matière de protection de la vie privée jugent qu'une institution ne devrait pas utiliser des renseignements personnels sans avoir obtenu au préalable le consentement explicite de la personne concernée.²⁹⁰ En outre, lorsqu'une institution obtient le consentement d'une personne, elle devrait lui demander qu'elle « exerce son option de consentement » par un acte manifeste (par exemple, en cochant une case décrivant l'utilisation des renseignements proposée par l'institution). Des groupes de consommateurs et certains experts prétendent que l'alternative à ce geste – soit celle de donner la possibilité à toute personne d'« exercer son option de refus » avant que l'institution ne s'abstienne d'utiliser les renseignements, tel que proposé – ne procure pas un degré suffisant de protection des renseignements personnels. Autrement dit, ils soutiennent que la protection des renseignements personnels devrait être la règle et que toute proposition d'utilisation des renseignements personnels devrait être traitée comme une exception exigeant le consentement de la personne concernée par un acte manifeste.

Par opposition, les codes de protection de la vie privée dans l'industrie stipulent que le consentement à l'utilisation des renseignements personnels peut être implicite. Par exemple, le code de l'ABC de 1996 dit que : « Le consentement d'un client peut être explicite, implicite ou fourni par un mandataire autorisé. »²⁹¹ Le modèle de code de l'ABC mentionne que bien que le consentement de manière expresse soit « la formule de prédilection », une banque peut obtenir un consentement implicite à partir de l'utilisation par un client d'un produit ou d'un service bancaire, ou à partir de l'absence de réponse du client suite à une offre faite par la banque de retirer d'une liste de prospection commerciale les informations personnelles le ou la concernant. Mais le code de l'ABC ajoute qu'avant de décider quel type de consentement est approprié (c'est-à-dire, oralement ou par écrit, de manière expresse ou implicite), la banque devra tenir compte du genre de renseignements personnels en jeu, des raisons de leur utilisation, et du genre de communications requises avec le client. Le modèle de code de l'ACNOR reconnaît également

²⁸⁹ Veuillez consulter les commentaires sur les plaintes déposées au bureau de l'Ombudsman bancaire canadien et à la Commission d'accès à l'information du Québec à la Partie I sous la rubrique intitulée « Préoccupations du grand public à l'égard de la protection de la vie privée et plaintes afférentes ».

²⁹⁰ Veuillez consulter, p. ex., les documents suivants : Association des consommateurs du Canada, *Privacy, Data Protection and Financial Institutions* (Vie privée, protection des renseignements et institutions financières) : *Mémoire présenté par l'Association des consommateurs du Canada au Comité permanent du Sénat sur les banques, l'industrie et le commerce* (Ottawa, Association des consommateurs du Canada, 1992) p. 3 : « Les consommateurs ont le droit fondamental à l'autodétermination quant à leurs renseignements personnels. Ce sont à eux de décider s'ils veulent que ces renseignements soient utilisés. L'association endosse entièrement ce concept désigné simplement par l'expression 'consentement positif'. » [traduction libre]

²⁹¹ Modèle de code de l'Association des banquiers canadiens, 1996, *supra*, note 284, Principe 3.

la possibilité du consentement implicite, en mentionnant que la forme du consentement devrait varier selon les circonstances et le type de renseignements.²⁹² Bien que l'on ne nie pas la valeur d'un consentement implicite, un consentement explicite est parfois plus important que les autres. Il peut être difficile de prévoir à l'avance toutes les utilisations potentielles et nécessaires de renseignements personnels lors d'une demande de consentement. Le besoin de recourir à des utilisations différentes peut survenir ultérieurement sans que des intérêts importants soient mis en cause et que cela vaille la peine d'obtenir à nouveau un consentement explicite. Cependant, si c'est le cas et que les institutions feignent d'ignorer ces intérêts, le marché leur fournira bientôt les incitatifs pour qu'elles modifient leur comportement.

Étant donné qu'au moins certains types de renseignements personnels ne suscitent pas vraiment d'inquiétudes importantes relativement à la protection de la vie privée, il semble raisonnable de privilégier une approche souple en ce qui a trait au consentement. Un jugement sûr permettant de déterminer quand un consentement implicite est approprié constitue le facteur clé. Si les choix faits par les institutions ne s'accordent pas avec les attentes de la plupart des gens, on peut s'attendre à un tollé général qui incitera les législateurs à intervenir. Par ailleurs, la manière précise dont un consentement est obtenu peut s'avérer de moindre importance si on permet aux clients de retirer leur consentement en tout temps. Comme cela a été mentionné auparavant, plusieurs institutions financières se sont engagées à respecter le principe selon lequel une personne devrait, avec certaines exceptions, bénéficier de la possibilité de retirer son consentement à l'utilisation des renseignements personnels la concernant. Finalement, la stratégie visant à obtenir le consentement du client en lui offrant le loisir « d'exercer son option de refus » peut être justifiée si on s'attend à une majorité de consentements. La proportion très modeste des plaintes relatives à la protection de la vie privée déposées par la clientèle des institutions financières confirme la pertinence de cet énoncé.

Méthodes de règlement des différends et transparence

Un autre enjeu soulevé par des groupes de consommateurs et par certains experts en matière de protection de la vie privée concerne les mécanismes de résolution des plaintes qui sont présentées en rapport avec les codes des institutions financières sur la protection des renseignements personnels. Ces codes font généralement appel à des procédures de résolution des différends adoptées par les institutions financières elles-mêmes. Des groupes de consommateurs et certains experts se demandent si ces mécanismes fournissent des outils efficaces et appropriés pour évaluer les plaintes reçues. Par conséquent, ils proposent que les consommateurs puissent

²⁹² Le modèle de code de l'Association canadienne de normalisation précise que lorsque les renseignements sont vraisemblablement de nature délicate, un consentement exprès devrait être sollicité, tandis que lorsqu'il s'agit de renseignements moins « délicats », un consentement implicite peut suffire. En outre, lorsque l'on obtient un consentement, il vaut la peine de sonder les attentes (raisonnables) du client. Par ailleurs, si les attentes raisonnables de l'individu ne recouvrent pas une utilisation particulière de renseignements personnels, le consentement exprès serait préférable. Veuillez consulter le *Code type sur la protection des renseignements personnels : Norme nationale du Canada*, CAN/CSA-Q830-96 (Etobicoke, Ontario, ACNOR, 1996), Cinquième principe, publié par l'Association canadienne de normalisation.

déposer leurs plaintes auprès d'une agence gouvernementale indépendante chargée d'examiner celles-ci et dotée d'un pouvoir exécutoire à l'égard des institutions financières.²⁹³

Des questions de partialité se posent quant à savoir si on peut se fier aux mécanismes internes d'une institution pour résoudre les plaintes. Un responsable interne, même s'il jouit d'une grande autonomie, partage néanmoins le point de vue général de l'institution ou fait face à des pressions implicites l'amenant à juger certaines affaires selon certaines perspectives. Cependant, l'inquiétude semble moins grande lorsqu'il est également possible de faire appel à un processus d'examen se déroulant à l'extérieur de l'institution. Certains codes de l'industrie prévoient cette possibilité dans une certaine mesure. Le code du BAC, par exemple, propose une médiation devant un médiateur indépendant dans le cas où un client se verrait refuser l'accès à ses propres renseignements.²⁹⁴ Le code type de l'ABC stipule quant à lui que les clients insatisfaits de la manière dont une banque traite une plainte peuvent s'adresser à l'Ombudsman bancaire canadien.²⁹⁵ L'industrie des banques semble avoir mis sur pied le processus de traitement des plaintes le plus complet en permettant, dans un premier temps, un examen des plaintes par les ombudsmans des banques respectives ou par des agents affectés aux plaintes et, dans un deuxième temps, le dépôt des plaintes auprès de l'Ombudsman bancaire canadien.

Le degré exact d'impartialité et d'indépendance de l'Ombudsman bancaire canadien peut être sujet à discussion.²⁹⁶ D'une part, le bureau de l'Ombudsman a été créé par l'industrie des banques; celui-ci doit se rapporter à un conseil composé en partie de représentants des banques; et il n'a pas le pouvoir d'obliger une banque à suivre ses recommandations. D'autre part, l'Ombudsman n'est redevable envers aucune banque en particulier, a le mandat d'agir comme enquêteur indépendant et médiateur de différends et peut s'assurer que ses recommandations

²⁹³ Veuillez consulter, p. ex., le document suivant : *Privacy, Data Protection and Financial Institutions* (Vie privée, protection des renseignements et institutions financières) : Mémoire présenté par l'Association des consommateurs du Canada au *Comité permanent du Sénat sur les banques, l'industrie et le commerce*, supra, note 294, p. 5 : « Même si les codes de protection de la vie privée devenaient une caractéristique du marché canadien, leur efficacité à protéger les renseignements personnels des consommateurs resterait douteuse. L'Association affirme depuis un certain temps et continue d'affirmer que les consommateurs ne peuvent protéger leur vie privée sans l'aide d'organismes de réglementation. Cette assistance inclut aussi la nécessité d'élaborer un mécanisme efficace de vérification de l'observance des règles. »

²⁹⁴ Bureau d'assurance du Canada, *Model Personal Information Code* (Modèle de code de protection des renseignements personnels) (1996), s. 4.9.1.

²⁹⁵ Modèle de code de l'Association des banquiers canadiens, 1996, supra, note 284, Principe 10. De plus, le modèle de code du Bureau d'assurance du Canada évoque la possibilité d'une médiation indépendante dans le cas où une personne se verrait refuser l'accès aux renseignements personnels qui la concernent, et la version préliminaire du code envisagé par la Credit Union Central of Canada laisse entendre que les plaintes qui n'auraient pu être réglées dans le cadre des procédures internes d'une coopérative de crédit devraient être soumises à la « centrale » ou encore, à un médiateur ou à un arbitre indépendant. Voir le modèle de code du BAC, supra, note 294, s. 4.9.1; Credit Union Central of Canada, *Credit Union Code for the Protection of Personal Information* (code de protection des renseignements personnels pour les coopératives de crédit – version préliminaire) (1996), Principe 10

²⁹⁶ Pour obtenir de plus amples renseignements sur le bureau de l'Ombudsman bancaire canadien, veuillez consulter les documents suivants : Ombudsman bancaire canadien, *Rapport annuel, 1996*, et Ombudsman bancaire canadien, *Rapport des neuf mois terminés le 31 juillet 1997*.

soient suivies en appliquant une pression morale et en faisant peser la menace d'une publicité moins que flatteuse. Les quelques expériences connues à ce jour laissent présager que l'Ombudsman fera des recommandations en faveur des plaignants.²⁹⁷ Cependant, comme le bureau de l'Ombudsman n'en est qu'à ses premiers balbutiements, il n'est pas encore possible d'évaluer précisément son efficacité. Enfin, nous pouvons dire qu'il y a peut-être plus de volonté de collaboration au sein des milieux bancaires de se plier aux recommandations d'un Ombudsman choisi par l'industrie, plutôt qu'aux ordonnances imposées par un organisme gouvernemental d'examen des plaintes. Il est utile de noter, également, que même si l'on peut soupçonner l'Ombudsman de partialité, il représente les intérêts de toutes les grandes banques et que, dans chacun des dossiers, tous les membres de son conseil, sauf un, ont un intérêt concurrentiel à mettre l'institution impliquée dans l'embarras.

En plus de la préoccupation particulière se rapportant à l'impartialité des mécanismes de résolution des plaintes, il existe une préoccupation plus générale qui touche la transparence des institutions quant à leurs politiques de protection de la vie privée et à leurs méthodes de traitement des renseignements. Les codes de l'industrie incluent le principe selon lequel les institutions devraient être transparentes sur ces questions et exigent aussi, en général, que les institutions fournissent des informations spécifiques sur leurs politiques à l'égard de la protection de la vie privée et sur les mécanismes qu'elles ont mis en oeuvre pour traiter les plaintes. Manifestement, une telle transparence concernant les avantages dont bénéficient les consommateurs est dans l'intérêt des institutions. Cependant, une inquiétude légitime se manifesterait s'il s'avère que, dans la pratique, les informations réclamées sont difficilement accessibles. Certains domaines du secteur des services financiers pourraient bien connaître des problèmes de cette nature. En effet, un stagiaire qui travaillait comme assistant dans le cadre de la présente étude et qui avait pour mission de recueillir codes et politiques concernant la protection de la vie privée a eu beaucoup de difficulté à s'acquitter de cette tâche auprès de certaines banques d'envergure modeste, de quelques sociétés de fiducie ainsi que de certains assureurs.²⁹⁸ Dans plusieurs cas, les personnes à qui il avait laissé des messages téléphoniques n'ont pas rappelé et ses questions n'ont pas trouvé réponse. Dans d'autres cas, certaines institutions ont affirmé ne pas avoir de code relatif à la protection de la vie privée ou alors, leur représentant n'était pas au courant de l'existence d'un tel code. Situation assez cocasse, une compagnie d'assurance a soutenu qu'elle possédait bel et bien un code de ce type mais que celui-ci n'était pas disponible pour les représentants du public.

²⁹⁷ Voir : Ombudsman bancaire canadien « Privacy Case Summary » (résumé de cas d'atteintes à la vie privée, 17 novembre 1997); il s'agit d'un bref document transmis par l'Ombudsman aux auteurs de la présente étude. Dans le cas de deux plaintes résolues par le bureau de l'Ombudsman, les banques concernées ont versé des sommes de 4 000 \$ et de 500 \$ pour dédommager les plaignants, conformément aux recommandations de l'Ombudsman.

²⁹⁸ Pour en savoir davantage, veuillez consulter la rubrique intitulée « Codes des associations industrielles » à la Partie II.

Établissements non réglementés par la loi fédérale

Une des dernières inquiétudes exprimées par les consommateurs a trait au fait que plusieurs établissements offrant des services financiers ne sont pas assujettis aux mêmes obligations légales et ne font pas l'objet d'une surveillance aussi étroite que les institutions réglementées par le gouvernement fédéral. Les banques, les compagnies d'assurance et les sociétés de fiducie qui sont réglementées font face à des pressions de la part de responsables fédéraux pour qu'elles adoptent des codes relatifs à la protection de la vie privée; par surcroît, de nouveaux règlements pour obliger ces institutions financières à aller de l'avant sont attendus pour bientôt. Les dispositions des lois fédérales et des règlements afférents exigent aussi l'implantation de politiques relatives à la confidentialité des renseignements sur la clientèle.²⁹⁹ Cependant, plusieurs établissements offrant des services financiers et faisant concurrence aux banques, aux compagnies d'assurance et aux sociétés de fiducie, sont à peine réglementés. Pensons par exemple aux firmes de crédit qui ne tombent pas sous le coup de la loi fédérale sur les institutions financières et qui peuvent offrir des facilités de crédit au public. Quoiqu'elles doivent se soumettre à la législation provinciale en matière de crédit, de telles compagnies ne sont pas assujetties aux dispositions de la loi fédérale concernant la protection de la vie privée ni à la surveillance étroite des organismes fédéraux. Ainsi, certaines entreprises offrant des services similaires à ceux des institutions réglementées par le gouvernement fédéral peuvent se soustraire aux exigences relatives à la protection des renseignements personnels ou du moins « s'en tirer à bon compte ». Le consommateur moyen n'est peut-être pas au courant de cette disparité au chapitre de la protection de la vie privée. Cependant, il faut noter que les institutions moins réglementées détiennent habituellement des renseignements qui sont moins délicats que ceux qui sont confiés, par exemple, à une banque ou à un assureur. Bien sûr, certains représentants de l'industrie du crédit disposent de politiques relatives à la protection de la vie privée, mais nous ne savons pas dans quelle mesure l'application de celles-ci est répandue en-dehors de la juridiction du gouvernement fédéral. Quoi qu'il en soit, nous ne disposons d'aucune preuve empirique témoignant de problèmes relatifs à la protection de la vie privée d'une quelconque ampleur dans ce secteur. Il n'est donc pas question d'y recommander une réglementation plus poussée.

Tendances et technologies nouvelles

Recoupement des données

Au fur et à mesure que les institutions financières grandissent et diversifient leurs produits et services, elles évoluent dans leur façon d'emmagasiner et d'évaluer l'information. Normalement, l'information relative au client était stockée dans des « réserves de données » – ce qui produisait

²⁹⁹ Vous trouverez des textes portant sur les dispositions législatives fédérales relatives à la protection de la vie privée et des renseignements des clients sous la rubrique intitulée « Dispositions législatives visant les institutions financières et la protection des renseignements personnels », à la Partie II.

des accumulations de données pertinentes pour une subdivision ou l'autre de l'institution ou pour un ensemble particulier de produits et services, sans pour autant être accessibles partout dans l'institution. Ainsi, l'information sur un compte de dépôts pouvait se trouver dans une réserve de données, alors que les relevés de placement étaient stockés dans une autre réserve. Comme les institutions financières se sont dotées de diverses subdivisions et qu'elles voudraient voir celles-ci travailler de manière plus concertée, le concept « entrepôt de données » (centralisation de données) s'est substitué à celui de la réserve de données.³⁰⁰ Idéalement, les institutions souhaitent emmagasiner les données dans un format type qui puisse être accessible à toutes les unités, avec polyvalence et convivialité. Dans certains cas, cela présuppose l'acquisition de nouveaux systèmes informatiques qui permettent un meilleur échange de données, ainsi que de nouveaux logiciels grâce auxquels le personnel de différentes unités pourra se faire une idée assez représentative quant à la personne traitant avec l'institution. L'entrepôt de données de l'institution peut avoir plusieurs applications. Ainsi, il peut permettre à l'institution de mettre à jour l'adresse du client une seule fois plutôt qu'à chaque point d'accès entre le particulier et l'institution, ou encore offrir un meilleur service aux clients qui se déplacent d'une ville à l'autre. En outre, l'institution pourra mettre en œuvre des techniques d'« exploration de données » pour analyser l'information recueillie sur le client et, par voie de conséquence, savoir comment optimiser la conception des produits destinés à ce dernier.

Même si les renseignements personnels restent dans les murs des institutions financières, la vie privée risque d'être de moins en moins protégée au fur et à mesure qu'augmentent les usages de l'information. Ce qui pose la question de la confidentialité des données dans les rapports établis entre l'institution et le particulier, de manière similaire à ce qui a été abordé plus haut.³⁰¹ Cependant, une fois qu'on a pris la décision politique de permettre à une même institution d'offrir une vaste gamme de produits et de services par le biais de ses subdivisions, il serait illogique d'imposer des mesures visant un cloisonnement étanche de ces subdivisions. Il est naturel que les institutions visent à optimiser leur efficacité, leur souplesse et l'intégration de leurs systèmes d'information. Cela leur permet, entre autres, de concevoir et de commercialiser leurs produits de manière plus ciblée. Les préoccupations concernant la protection de la vie privée face à l'usage de plus en plus marqué de l'information à caractère personnel sont bel et bien justifiées, mais doivent être évaluées en fonction des avantages pratiques que la formule permet, tant pour les institutions que pour les clients.³⁰²

³⁰⁰ « La centralisation des données est une stratégie qui vise à garantir en tout temps l'accessibilité de données précises, quel que soit le point de consultation. Cela présuppose souvent une duplication du contenu existant dans les ordinateurs de chaque service afin de les intégrer en un lieu de consultation centralisée, où l'on pourra s'assurer qu'on a les mêmes définitions de données... », Michael Bell, A Data Mining FAQ, <http://www.qwhy.com/dmfaq.htm>.

³⁰¹ Voir, dans la présente Partie III, à la rubrique « Inquiétudes des consommateurs », sous-rubrique « Le partage et l'utilisation des renseignements personnels ».

³⁰² Quoi qu'il en soit, il faut garder à l'esprit le fait que la centralisation des données n'est pas encore pour demain. Dans la réalité, la plupart des institutions ont devant elles une multitude de systèmes incompatibles, issus d'initiatives commerciales distinctes et de dépenses discrétionnaires hétéroclites en matière de technologie, et ce d'année en année. S'il est vrai qu'on recherche aujourd'hui LA donnée idéale, celle à laquelle on peut accéder à partir de n'importe quel nœud dans un réseau de longue portée, il faudra sans doute attendre bien des années avant que l'objectif ne soit atteint.

Marketing ciblé et exploration de données

À l'avenir, le marketing ciblé et l'exploration de données joueront un rôle crucial dans les activités des institutions financières. Par *marketing ciblé*, on entend le principe voulant qu'une institution axe sa démarche de commercialisation sur les personnes physiques ou morales le plus susceptibles d'accepter un produit ou un service particulier.³⁰³ Plutôt que de lancer un programme de commercialisation de masse visant toute la clientèle de l'institution, cette dernière devrait circonscrire un plus petit segment qui présenterait les attentes ou tendances pertinentes à un produit ou service. Les transactions antérieures d'un particulier avec l'institution, de même que son actif et son revenu, peuvent permettre de bien évaluer ses besoins ou ses intérêts. En effet, un client dont le compte d'épargne est bien garni pourrait être intéressé par les services d'un courtier en valeurs mobilières, tandis que le client ayant souscrit une hypothèque recherchera plutôt une assurance pour sa propriété. À l'aide d'un marketing bien ciblé, l'institution pourra axer sa démarche de commercialisation de manière plus efficace. De la sorte, les personnes qui semblent les moins intéressées par de nouveaux produits ne feront pas l'objet de démarches pressantes, tandis que celles qui sont susceptibles d'accrocher seront sollicitées de manière plus intense, et plus personnalisée. C'est, en fait, l'information à caractère personnel qui décidera de la manière dont on doit classer telle ou telle personne.

Le concept de l'exploration de données s'est fait connaître au cours des quelques dernières années; et il a de fortes chances de marquer de nouveaux points dans les années à venir. Il s'agit là d'un ensemble de techniques destinées à révéler de nouveaux rapports, de nouveaux modèles ou associations entre divers éléments d'information réunis. Selon une étude menée plus tôt :

L'exploration de données est un ensemble de techniques automatisées qui visent à extraire des fragments d'information personnelle qui étaient jusque-là méconnus ou bien cachés au fond de grandes bases de données. Lorsque cette exploration est réussie, elle permet de détecter des modèles et des rapports, utiles, puis d'exploiter cette « nouvelle » information de manière à prendre des décisions commerciales anticipatoires (proactives), axées sur les connaissances. Le couplage ou comparaison des données, quant à lui, « met l'accent sur la découverte automatique de faits et de rapports nouveaux dans les données. La matière première est constituée des données commerciales, tandis que l'algorithme d'exploration serait une espèce d'excavatrice qui sonde d'énormes masses de données brutes, en quête des précieuses pépites d'information. »³⁰⁴

À la différence des modalités d'analyse traditionnelles, l'exploration de données ne cherche pas à régler une problématique particulière au moyen d'une information pertinente extraite d'une base de données. Il s'agit plutôt de repérer un certain nombre de rapports pertinents qui pourraient passer inaperçus pour l'institution comme pour le particulier. « Les données sont passées au crible, en quête de modèles, de tendances et de généralisations, sans la moindre intervention ou orientation de la part de l'utilisateur. La recherche se fait alors sans aucune idée préconçue autre que

³⁰³ Pour de plus amples renseignements sur le marketing ciblé, voir notamment : Garth Hallberg, *All Consumers Are Not Created Equal: The Differential Marketing Strategy for Brand Loyalty and Profits* (New York: Wiley & Sons, 1995).

³⁰⁴ Ann Cavoukian, *Data Mining: Staking A Claim on Your Privacy* (Commissaire à l'information et à la protection de la vie privée/Ontario, janvier 1998) p. 3, www.ipc.on.ca.

le regroupement des clients en fonction des caractéristiques communes relevées. »³⁰⁵ Au moyen des techniques d'exploration de données, l'institution peut ainsi découvrir que l'individu présentant les caractéristiques A, B et C mais non D risque davantage de s'intéresser à un produit ou service X.

Avantage de la technique d'exploration de données : on libère les mercaticiens (spécialistes en mercatique, alias marketing) de toute forme d'approche préconçue à l'endroit de la clientèle. En outre, cette exploration a déjà produit des résultats positifs dans le cadre de la répression des fraudes (ex. : elle a permis de mettre au point des techniques pouvant identifier les transactions anormales par carte de crédit). Il faut cependant noter qu'une bonne exploration de données est difficile à réaliser, et qu'elle dépend autant de la qualité des outils sur logiciel que de celle des données accumulées sur la clientèle. Bien souvent, cette exploration produit des résultats plutôt quelconques, superflus ou erronés.³⁰⁶

Avec la démocratisation des coûts associés à des ordinateurs puissants et à des logiciels de plus en plus performants, à laquelle s'ajoute le volume croissant des données recueillies par les institutions, l'exploration de données est devenue une réalité. En outre, cette activité est facilitée du fait du regroupement des fonds de renseignements dans des entrepôts centraux où l'on stocke des données personnelles dans un format normalisé et convivial. De telles techniques sont couramment utilisées par de grandes entreprises comme Blockbuster Entertainment, MasterCard International, American Express et WalMart.³⁰⁷ Au fur et à mesure que les institutions financières du Canada adoptent des programmes de marketing ciblé, les techniques d'exploration de données se généraliseront dans le secteur des services financiers. Il est cependant probable que ces techniques demeureront méconnues du grand public, à moins que certaines mesures concrètes ne soient prises pour renseigner la clientèle sur la manière dont l'information est utilisée.

Le marketing ciblé et l'exploration de données constituent des tendances qui soulèvent un certain nombre de questions intéressantes pour ce qui est du respect de la vie privée. Dans les deux cas, il y a intensification de l'usage des renseignements à caractère personnel dans la prise de décisions commerciales sur les particuliers, avec, à la clé, un certain nombre d'activités que les particuliers n'avaient peut-être pas prévues au moment où ils avaient donné les renseignements. Dans une analyse récente sur les implications de l'exploration des données, le Commissaire à l'information et à la protection de la vie privée en Ontario a soulevé un certain nombre de préoccupations importantes.³⁰⁸ Ainsi, l'exploration de données fait nécessairement appel à d'importantes sommes d'informations. Par conséquent, à moins que l'institution ne prenne des dispositions précises à cet effet, les données pourraient contenir des événements intéressants, certes, sur le plan historique mais néanmoins dépassés. De plus, la protection des données

³⁰⁵ Queen's University de Belfast, What is Data Mining, http://www.pcc.qub.ac.uk/tec/courses/datamining/stu_notes/dm_book_2.html#HEADING2, cité par Cavoukian, *supra*, note 304.

³⁰⁶ Craig Stedman, « Data Mining for Fool's Gold », *Computerworld*, 1^{er} décembre 1997, pp. 1 et 28.

³⁰⁷ Cavoukian, *supra*, note 304, pp. 6-7.

³⁰⁸ *Ibid.*, p. 8-11.

pourrait présupposer que les institutions révèlent, au moment où elles obtiennent l'information de l'individu, qu'elles procéderont à des explorations de données. Autrement, ce genre d'opérations pourrait ne pas répondre aux attentes du particulier et donc être perçu comme incompatible, *a priori*, avec la raison d'être de la collecte de données (savoir la vente d'un produit ou la prestation d'un service particulier). Toutefois, indiquer simplement que l'exploration de données pourrait constituer l'une des applications potentielles de l'information fournie risque de ne pas représenter en soi une déclaration d'intentions assez claire par l'institution, pas plus qu'un consentement réel par l'individu. D'un autre côté, il est possible que l'institution ne connaisse pas la véritable finalité des données utilisées vu que cette finalité dépendra des associations qui se feront seulement une fois le processus d'exploration mené à terme.

On notera ici que le degré d'interdépendance entre l'exploration de données et la protection de la vie privée fait toujours l'objet de débats. L'exploration entraîne la découverte de relations entre de vastes quantités de données recoupées, relations qui ne sont pas ramenées à des personnes identifiables. De même, l'action de réunir d'importantes sommes d'informations personnelles sous forme de statistiques démographiques générales ne révèle rien sur des particuliers identifiables. On pourrait en conclure que la protection de la vie privée n'est mise en danger ni par l'exploration de données ni par la compilation de statistiques générales. Par contre, il est bien connu que l'étape qui suit l'exploration consiste généralement à appliquer à certains individus les relations qu'on aura pu dégager, dans le but de faire une prospection bien ciblée ou de prendre certaines décisions à l'endroit de ces personnes. Ce qui revient à dire que l'exploration de données peut avoir des répercussions indirectes sur la protection de la vie privée puisqu'elle offre aux institutions les outils qui seront appliqués à l'endroit de certaines personnes en particulier, en fonction des caractéristiques spécifiques connues qui permettront de structurer les relations établies entre l'institution et l'individu.

Cartes de valeur

La première application grand public de la technologie de la carte à puce (« carte intelligente ») dans le secteur des services financiers sera la carte de valeur.³⁰⁹ La carte intelligente présente essentiellement les mêmes dimensions et formes qu'une carte de crédit, et possède des circuits logiques intégrés, de même qu'une mémoire numérique. Ce genre de carte peut recevoir une bien plus grande quantité d'informations que la carte à bande magnétique conventionnelle; de plus, il est possible de modifier et de tenir à jour les données qui y figurent chaque fois que le

³⁰⁹ En plus des cartes de valeur, dont il sera fait état plus loin, la technologie des cartes intelligentes pose, à terme, certains problèmes. Les observateurs spécialistes ont en effet noté qu'une même carte intelligente pourrait offrir toute une série de services non reliés les uns aux autres. Par exemple, une seule et même carte pourrait donner des renseignements sur un traitement médical, ouvrir l'accès à des secteurs réglementés dans une entreprise, et renseigner sur des opérations financières effectuées par le consommateur. Or, une carte de valeur dont on se servirait à diverses fins n'ayant aucun caractère économique finirait par poser la question de l'accès aux données privées n'ayant aucun rapport avec la transaction entre l'entité et l'individu. Pour de plus amples renseignements sur ce genre de carte, consulter T.S. Onyshko et R.C. Owens, « *Debit Cards and Stored Value Cards: Legal Regulation and Privacy Concerns* », (1997) 16 *National Banking Law Review*, p. 65.

porteur l'utilise pour une quelconque transaction. On s'attend à ce que, au cours des quelques prochaines années, la technologie des cartes intelligentes se substitue graduellement à celle des cartes à bande magnétique conventionnelles, et ce dans toute une gamme d'applications.

La carte de valeur (également dite *porte-monnaie électronique*) constituera une bonne solution de remplacement au numéraire, pour tous genres d'achats à la consommation. Théoriquement, le consommateur se procure sa carte auprès d'un organisme émetteur et y charge une certaine valeur. Par la suite, il fait des achats auprès de commerçants équipés de machines pouvant déduire des fonds à même la valeur figurant sur la carte;³¹⁰ dans certains systèmes, le consommateur a également la possibilité de virer des fonds d'une carte à une autre. Le degré de protection varie selon la conception de la carte. Dans les systèmes permettant une protection supérieure, le bilan n'est donné que sur la carte elle-même et sur le lecteur du commerçant; dans d'autres systèmes, l'émetteur de la carte tient un bilan détaillé.

La plupart des grandes institutions de dépôt participent à l'introduction au Canada du système de valeur Mondex. Ce système a été mis en œuvre à Guelph (Ontario) et devrait sous peu se généraliser dans le pays.³¹¹ À la différence des autres systèmes, le Mondex ne s'appuie pas sur une base de données centrale pour la comptabilité ou l'archivage des données. Les relevés des dix dernières transactions se trouvent sur la carte elle-même; ceux des 300 dernières transactions (correspondant uniquement à un numéro de carte et non à l'identité du titulaire) se trouvent sur les lecteurs des commerçants.³¹² Les commerçants peuvent sortir des copies papier de ces données pour se protéger advenant litige. Toutefois, ils ne connaîtront l'identité de l'acheteur que si celui-ci leur fournit l'information. Les organismes émetteurs de cartes ne donneront aucune information permettant d'identifier le titulaire à moins d'y être contraints de par la loi ou à moins que le titulaire n'ait accepté de participer à une démarche de fidélisation de la clientèle mise en place par le commerçant.³¹³ Le système Mondex assure une protection optimale du consommateur, bien que le commerçant et l'organisme émetteur pourront, avec l'assentiment du titulaire, coopérer pour créer des bases de données électroniques sur les transactions qui concernent notamment la carte Mondex.³¹⁴

³¹⁰ Outre les lecteurs de cartes qui se trouvent chez les commerçants, il existe un certain nombre de prototypes d'appareils qui permettront un jour aux consommateurs de faire des achats au moyen d'une carte de valeur en passant par un ordinateur personnel équipé d'un modem.

³¹¹ On peut visiter le site Web de Mondex International à l'adresse <http://www.mondex.com> et celui de Mondex Canada à <http://www.mondex.ca>. À l'heure actuelle, les institutions suivantes (entre autres) participent au système mis en place par Mondex Canada : Banque de commerce canadienne impériale (CIBC), Banque Royale, Banque de Hongkong du Canada, Centrale des caisses de crédit du Canada (CCCC), Banque de Montréal, Canada Trust, Mouvement des caisses Desjardins, Banque Nationale du Canada, Banque Toronto Dominion et Banque Scotia.

³¹² Consulter la présentation « How private is a Mondex transaction? » sur le site Web de Mondex International, à l'adresse <http://mondex.com>, sous la rubrique « About » et « Mondex FAQ », ainsi que sur le site Web de Mondex Canada à l'adresse <http://mondex.ca/faq5.html>.

³¹³ *Ibid.*

³¹⁴ Entrevue réalisée par T.S. Onyshko auprès du porte-parole de Mondex Canada, Joe Clark, le 8 septembre 1997.

Selon des experts en la matière, le respect de la vie privée fait partie intégrante du système de carte de valeur. Car si un pareil système venait à se substituer au numéraire sans en préserver le caractère anonyme, il provoquerait une explosion d'informations au sujet des mouvements du consommateur et de ses habitudes d'achat. On pourrait d'ailleurs reprendre à ce sujet l'observation que quelqu'un avait faite à propos de la protection des renseignements personnels lors des transactions par Internet : « Sans cette protection, une tierce partie pourrait facilement traquer le consommateur, créer, à des fins commerciales, un profil personnel de ce dernier, ou prendre connaissance des détails les plus intimes de sa vie privée, tout simplement en suivant de près ses transactions financières... »³¹⁵ Toutefois, cet argument ne justifie pas vraiment la réglementation d'un système de carte de valeur, étant donné qu'on ne dispose d'aucune preuve du problème lui-même. D'abord, le système Mondex est un système privé. Selon les déclarations faites par la société Mondex, le système ne permettra la constitution d'une base de données sur le consommateur que si ce dernier décide d'adhérer à une démarche de fidélisation de la clientèle. Par conséquent, la protection de la vie privée sera la règle plutôt que l'exception, à moins que le consommateur n'ait autorisé un usage particulier des données afférentes à ses achats. Deuxièmement, le système Mondex revêt un caractère privé plus marqué que celui des systèmes de règlement concurrents, comme les cartes de crédit ou cartes de débit, systèmes qui justement utilisent des relevés détaillés sur les achats faits par le consommateur. De même qu'il n'existe pas de réglementation particulière pour protéger la vie privée dans le cadre des transactions effectuées par carte de crédit ou carte de débit, il n'apparaît pas nécessaire de mettre en place un tel système dans le cas des archives qui seront tenues pour la carte Mondex. Finalement, il n'est pas évident que la montagne d'informations provenant d'achats au jour le jour pourra servir à quelque chose dans un système centralisé de cartes de valeur (système différent donc de celui de Mondex). En effet, le coût de stockage, de tri et d'analyse des millions et millions de transactions courantes pourrait bien invalider tout avantage découlant d'une pareille accumulation de données.

Opérations bancaires sur Internet et logiciels de gestion de fonds au Canada

Dans le but d'offrir de nouveaux circuits de distribution, les banques et sociétés de fiducie canadiennes proposent des services bancaires sur ordinateur personnel et sur Internet.³¹⁶ Ces services permettent aux consommateurs d'effectuer des opérations bancaires de chez eux, au moyen d'un modem, plutôt que de se rendre dans une succursale bancaire ou un guichet automatique. De la sorte, les consommateurs seraient en mesure de virer des fonds d'un compte à l'autre, de régler des factures ou de faire des demandes de prêts personnels. À l'avenir, on s'attend à ce que les institutions offrent des services sur ordinateur personnel et sur Internet qui soient compatibles avec les logiciels de comptabilité personnelle les plus courants, comme

³¹⁵ Catherine M. Downey, « *The high price of a cashless society: exchanging privacy rights for digital cash?* » (1996) 14 *John Marshall Journal of Computer & Information Law* 303, p. 315.

³¹⁶ Voir notamment Michael Smith, *The Internet has landed*, *Canadian Banker* (septembre-octobre 1997), vol. 34; et Michael Smith, *Technology and Trust*, *Canadian Banker* (novembre-décembre 1997), vol. 35.

Money de Microsoft ou *Quicken* de Intuit.³¹⁷ Les clients pourraient alors se servir de leur logiciel de comptabilité pour retirer ou déposer des fonds, ou pour d'autres transactions au moyen d'un ordinateur personnel et d'un serveur Internet. Les institutions pourraient alors documenter ce genre de transactions de façon à les rendre compatibles avec les logiciels de comptabilité personnelle.

Les nouveaux services bancaires axés sur l'ordinateur personnel et sur Internet posent bien sûr un certain nombre de questions quant à la protection de la vie privée. On croit notamment que de tels services seraient vulnérables à des *raids* de l'extérieur, susceptibles d'en modifier ou d'en effacer la teneur. L'étude du facteur sécurité pour les services bancaires axés sur un ordinateur personnel ou sur l'Internet déborde du cadre de la présente étude. Toutefois, il ne faut pas oublier que les infractions font aussi partie du monde matériel; le but deviendrait donc de ramener à un niveau acceptable les accès non autorisés, plutôt que de les supprimer complètement. Autre préoccupation : les données relatives aux transactions effectuées par ordinateur personnel et sur Internet pourraient être conservées sur les machines des particuliers; à défaut de cryptage ou d'archivage dans des fichiers verrouillés, cette information pourrait alors être connue de quiconque accède à la machine, notamment les amis ou les membres de la famille. À cet égard, on rappellera que le particulier doit protéger le caractère confidentiel des données bancaires électroniques de la même manière qu'il le fait pour les données sur papier. C'est donc à lui qu'il incombe de prendre les mesures nécessaires pour assurer cette protection. C'est dire qu'une carence en matière de sécurité semble plus probable sur l'ordinateur du consommateur (faisant ici office de terminal bancaire) que dans le système informatique de la banque à proprement parler.

Échange de renseignements et prestation de services à l'échelle internationale

Un dernier ensemble de tendances concerne la globalisation de plus en plus marquée du marché des services financiers. En général, s'il est vrai que ces tendances augmentent les échanges de renseignements et le maniement de données hors du Canada, il est improbable que cela constitue un risque sérieux pour la sécurité.

Dans les années à venir, il est probable que les institutions financières du Canada collaboreront plus étroitement avec les institutions étrangères. Ainsi, elles pourraient participer à des coentreprises ou à d'autres mécanismes commerciaux menant à la mise en œuvre de systèmes et de technologies Nouvelle Génération. Parmi ces nouveaux mécanismes, l'échange d'informations sur les clients. À notre connaissance, ce genre d'échange ne devrait pas toutefois dépasser ce que nous connaissons aujourd'hui dans le domaine des cartes de crédit : c'est-à-dire le strict minimum d'informations nécessaires à l'usage d'une carte de crédit à l'extérieur du cadre où évolue normalement le titulaire. (Ainsi, le système de carte de valeur Mondex présuppose l'échange d'informations à l'échelle internationale en ce qui a trait aux achats

³¹⁷ Voir notamment Kevin Marron, Bankers edgy over software middlemen, *The Globe and Mail*, 25 novembre 1997, p. C-1.

effectués à l'étranger.) Il apparaît certain que les contrats liant les institutions qui participent de ces mécanismes incluront des clauses protégeant la confidentialité des données réunies sur les consommateurs canadiens. Toutefois, il n'en reste pas moins que de tels mécanismes favoriseront une plus grande dissémination de l'information, au sein d'institutions et de pays de plus en plus nombreux.

Il est également possible que les institutions financières canadiennes fassent traiter les données à l'extérieur du pays, quelque part dans leurs empires tentaculaires, ou encore qu'elles confient ce travail à un fournisseur de services à rabais dans un autre ressort territorial. À l'heure actuelle, ce genre d'activités pour une institution fédérale ne peut se faire que moyennant autorisation par le Bureau du surintendant des institutions financières, conformément à la loi pertinente. L'objet de cette autorisation est d'assurer de manière manifeste la sécurité des données et leur disponibilité s'il y a lieu dans le cadre de la réglementation; quoi qu'il en soit, ce contrôle contribue de manière significative à protéger le caractère confidentiel des données. Les facteurs qui déterminent le lieu de traitement, surtout avec la diversification des services de télécommunications et l'allègement des coûts y afférents, pourraient de plus en plus favoriser des ressorts territoriaux permettant une réduction des coûts (ce qui pourrait bien vouloir dire le Canada). Les fournisseurs de services non réglementés appartenant à des intérêts étrangers sont plus susceptibles de faire le traitement des données à l'extérieur du Canada, compte tenu des modalités de traitement plus souples qui s'appliquent à leurs territoires. Il est plus probable que ces institutions traitent les données à caractère personnel à l'extérieur du pays, auquel cas elles pourraient ou non être soumises à certains critères de confidentialité contenus dans la *Loi sur les banques* ou dans tout autre texte de loi fédérale. À nouveau, il faut souligner que nous ne disposons d'aucune donnée empirique qui établisse la présence de difficultés dans ce secteur.

Un dernier problème qui pourrait survenir : une entreprise étrangère offre des services financiers à des Canadiens par le biais d'Internet puis exploite cette information sans tenir compte des critères régissant le respect de la vie privée. Une telle situation poserait de sérieux problèmes mais serait difficile, voire impossible, à gérer étant donné les limites de juridiction qui s'appliquent aux agents de réglementation canadiens. De manière générale, la réglementation portant sur les prestataires de services financiers étrangers ont été couverts dans le récent document de consultation sur les banques étrangères, produit par le ministère des Finances.³¹⁸ Exception faite des cas où les agents de réglementation étrangers sont prêts à collaborer pour régler un problème identifié par leurs homologues canadiens, les options de réglementation seraient si limitées que, règle générale, l'acheteur devra continuer à prendre garde (*caveat emptor*).

³¹⁸ Gouvernement du Canada, ministère des Finances, *Document de consultation sur la politique d'accès des banques étrangères* (26 septembre 1997), www.fin.gc.ca/toce/1997/foreignoc-e.html.

IV. Conventions internationales, directive UE et textes de loi à l'étranger comme au pays

Introduction

La Partie IV traite des ententes et des lois internationales qui protègent la vie privée dans certains ressorts territoriaux, à l'étranger comme au pays. Elle commence par une description sommaire des ententes et conventions internationales touchant le Canada et portant sur la protection de la vie privée. Elle présente ensuite une étude détaillée de la directive de protection émise par l'Union européenne; en particulier, les restrictions que la directive place à l'endroit des transferts internationaux de données à caractère personnel. Le reste de cette partie traite des lois concernant la protection de la vie privée dans trois territoires distincts, ainsi que de l'expérience dans un quatrième territoire qui a choisi de ne pas se doter d'une pareille loi. Le *Data Protection Act* promulgué en 1994 par le Royaume-Uni constitue un exemple de loi qui contraint les utilisateurs de données à s'enregistrer auprès d'une autorité centrale. Au Québec, la *Loi sur la protection des renseignements personnels* dans le secteur privé est un exemple de système dépourvu de mécanisme d'enregistrement mais qui inclut des responsabilités circonstanciées en matière de protection de la vie privée. En Nouvelle-Zélande, le *Privacy Act* de 1993 constitue un exemple de loi combinant les obligations d'origine législative à des codes approuvés dans le secteur public. Finalement, l'Australie constitue un exemple de pays ayant envisagé puis rejeté l'élargissement au secteur privé du cadre juridique de la protection des données.

Ententes et conventions internationales touchant le Canada

Le Canada a démontré son engagement à protéger la vie privée de ses citoyens en adhérant à un certain nombre de conventions internationales. À preuve, il est signataire de la *Déclaration universelle des droits de l'homme*, adoptée et proclamée le 10 décembre 1948 par l'Assemblée générale des Nations Unies. Or, l'article 12 de cette déclaration traite expressément de la question de la vie privée.

Nul ne sera l'objet d'immixtions arbitraires dans sa vie privée, sa famille, son domicile ou sa correspondance, ni d'atteintes à son honneur et à sa réputation. Toute personne a droit à la protection de la loi contre de telles immixtions ou de telles atteintes.³¹⁹

La *Déclaration universelle des droits de l'homme* traite notamment du droit à la vie, à la liberté et à la sûreté de la personne, du droit de ne pas être arbitrairement arrêté, soumis à des traitements cruels ou à une discrimination, et du droit à la liberté de pensée et de religion. Le fait que soit invoqué le droit à la vie privée constitue une indication claire de l'importance que la communauté internationale accorde à cet élément. Il faut noter toutefois que la vie privée,

³¹⁹ Rés. 217 (III) de l'U.N.G.A. (Assemblée générale des Nations Unies), 3 ONU GAOR suppl. (n° 3) p. 71, doc. ONU A/810 (1948).

envisagée dans un contexte pré-informatique, ne portait pas réellement sur les questions relatives à l'information que nous abordons dans le présent document. On sait que le Canada est également signataire du *Pacte international relatif aux droits civils et politiques*,³²⁰ dont l'article 17 présente un libellé semblable à celui de l'article 12 de la Déclaration universelle.

Les *Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel*³²¹, établies par l'OCDE, représentent un développement plus significatif dans le dossier de la protection de la vie privée à l'échelle internationale. En 1984, le Canada exprimait son adhésion officielle aux lignes directrices de l'OCDE, ce qui engageait le gouvernement fédéral dans la voie de la protection des droits de la personne, dans les secteurs public et privé.³²² Les directives, dont l'application est volontaire et qui n'ont donc pas force de loi, sont axées sur huit principes concernant les pratiques équitables de traitement de l'information, qui portent notamment sur la collecte et la divulgation de données personnelles, et sur l'accès de l'individu à l'information le concernant.³²³ Les États membres de l'OCDE devront se doter de lois protégeant les particuliers, avec des sanctions et des recours adéquats advenant le non-respect, par les utilisateurs de données, des principes énoncés.³²⁴

Directive de l'Union européenne

La démarche européenne en matière de lois sur la protection des renseignements personnels

La Directive de l'Union européenne³²⁵ constitue une évolution significative dans le domaine de la protection de la vie privée et des renseignements personnels. En plus de constituer un certain modèle pour ce genre de protection, elle présente diverses implications pour la protection des données à l'intérieur même du Canada.

Avant d'aller plus loin, il conviendrait de traiter de la démarche générale empruntée par les Européens pour assurer la protection des données, avant de faire le parallèle avec les démarches canadienne et américaine. La législation européenne en matière de protection des données est fortement réglementée et présente une certaine exhaustivité. Cette démarche participe du style de

³²⁰ Pacte signé en 1966, annexé à la résolution 2200A de l'Assemblée générale, 21 ONU GAOR, suppl. (n° 16) p. 52, doc. ONU A/6316 (1966). Au Canada, ce pacte est entré en vigueur le 19 août 1976.

³²¹ Pour le texte intégral des lignes directrices de l'OCDE, se reporter notamment à James Michael, *Protection de la vie privée et droits de la personne* (Paris, Édition de l'UNESCO, 1994), p. 39ff.

³²² *Commissariat à la protection de la vie privée du Canada, Rapport annuel 1984-1985* (Ottawa, Approvisionnement et Services Canada, 1985), p. 11.

³²³ Pour une étude plus approfondie des lignes directrices de l'OCDE, se reporter à la Partie I de la présente étude, sous la rubrique « Droit à la vie privée et questions liées à la protection des renseignements ».

³²⁴ Voir art. 19 des lignes directrices de l'OCDE.

³²⁵ *Directive 95/46/CE relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données*, JO des Communautés européennes du 23 novembre 1995, n° L. 281 p. 31.

droit public pratiqué par les Européens, en vertu duquel les États tentent d'inscrire les droits fondamentaux (y compris le droit à la protection de la vie privée) dans les textes de loi assez englobants.³²⁶ En général, les pays européens ont adopté soit un système d'enregistrement soit un système d'octroi de permis pour la protection des données, tant dans le secteur public que dans le secteur privé. Sous un régime d'enregistrement, une institution du secteur public ou du secteur privé qui réunit ou utilise des informations personnelles doit s'inscrire dans un registre central de protection des données. L'autre système est semblable mais plus réglementé. Il impose à l'institution d'obtenir un permis de l'autorité centrale *avant* d'entreprendre le traitement des données personnelles. La première vague d'États européens à se doter de lois en la matière ont adopté des systèmes d'octroi de permis; par contre, les pays qui ont adopté des lois plus récemment ont choisi le système d'enregistrement. En France, la *Loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés* illustre bien le système d'octroi de permis, tandis que le *Data Protection Act* promulgué en 1984 par le Royaume-Uni est représentatif du système d'enregistrement.³²⁷

À la différence de ce qui se passe en Europe, de nombreux autres pays ont adopté une approche sectorielle pour la protection des renseignements personnels dans le secteur privé, dont les États-Unis et le Canada. À l'échelon fédéral comme à celui des cinquante États américains, il existe des lois qui protègent les renseignements personnels dans certains secteurs comme l'évaluation du crédit, les téléversements, et la protection des données relatives à l'abonnement à la câblodiffusion ou à la location de films vidéo.³²⁸ Toutefois, il n'existe aux États-Unis aucun texte de loi qui assure de manière exhaustive la protection des renseignements personnels dans le secteur privé, pas plus qu'il n'existe d'organisme indépendant pour contrôler et surveiller l'application des droits relatifs au respect de la vie privée et à la protection des données personnelles.³²⁹ Les observateurs ont souvent noté que la démarche des Américains dans le domaine de la protection de la vie privée semble découler du droit privé et de la conduite du libéralisme que certains qualifient d'ultralibéralisme.³³⁰ Le législateur américain répugne à réglementer le secteur privé tant qu'on n'a pu démontrer le besoin d'une telle opération, choisissant plutôt de se concentrer sur les excès commis par les services publics plutôt que par

³²⁶ James Maxeiner, *Business Information and Personal Data: Some Common-Law Observations About the EU Draft Data Protection Directive* (1995), vol. 80, *Iowa Law Review*, p. 619 (p. 627).

³²⁷ Pour une étude des textes de loi français, se reporter notamment à David H. Flaherty, *Protecting Privacy in Surveillance Societies* (Chapel Hill: University of North Carolina Press, 1989), p. 165ff.

³²⁸ Ian Lawson, *Protection de la vie privée et autoroute de l'information : options canadiennes en matière de réglementation* (Industrie Canada, 1996), <http://strategis.ic.gc.ca/SSG/ca00265f.html>.

³²⁹ En 1977, la U.S. Privacy Protection Study Commission s'est clairement prononcée contre la promulgation d'une loi d'ensemble (loi omnibus) pour réglementer la circulation de renseignements personnels dans diverses circonstances. La Commission a souligné l'importance de la libre circulation des données, ainsi que la difficulté d'établir un projet de loi qui puisse couvrir toutes les facettes de la collecte des données et de leur utilisation. Voir Joseph Rosenbaum, *The European Commission's Draft Directive on Data Protection* (1992), vol. 33, *Jurimetrics Journal of Law, Science and Technology*, p. 1 (pp. 3-4).

³³⁰ Joel Reidenberg, *Rules of the Road for Global Electronic Highways: Merging the Trade and Technical Paradigms* (1993), vol. 6, *Harvard Journal of Law & Technology*, p. 287 (p. 302).

des représentants du secteur privé.³³¹ C'est notamment pourquoi l'administration Clinton a refusé de se doter d'une loi protégeant la vie privée sur Internet, demandant plutôt au secteur privé de mettre en œuvre des codes de conduite à cet effet.³³²

Mise au point de la directive de l'Union européenne

Convention du Conseil de l'Europe

Un an après la publication des lignes directrices de l'OCDE, le Conseil de l'Europe promulguait sa *Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel*³³³ (« **Convention** »), qui entrerait en vigueur en 1985. Cette Convention exige des signataires qu'ils mettent en œuvre des lois nationales concrétisant les principes de protection inclus dans la Convention. Le Préambule de la Convention reconnaît l'accroissement des flux transfrontières de données informatisées de caractère personnel, l'utilité de sauvegarder le droit à la vie privée, et la nécessité de réconcilier les valeurs fondamentales du respect de la vie privée et de la libre circulation de l'information entre les peuples.

La Convention rejoint, dans le fond, les lignes directrices de l'OCDE; toutefois, alors que celles-ci mettent l'accent sur la libre circulation de l'information, la Convention souligne plutôt la protection du droit à la vie privée. L'objet de la Convention, décrit dans l'article 1, consiste à préserver pour chaque personne « le respect de ses droits et de ses libertés fondamentales, et notamment de son droit à la vie privée, à l'égard du traitement automatisé des données à caractère personnel la concernant ». Comme dans le cas des lignes directrices, la Convention s'applique au traitement automatisé des données personnelles, dans le secteur public comme dans le secteur privé. « Les données à caractère personnel faisant l'objet d'un traitement automatisé sont :

- a) obtenues et traitées loyalement et licitement;
- b) enregistrées pour des finalités déterminées et légitimes et ne sont pas utilisées de manière incompatible avec ces finalités;
- c) adéquates, pertinentes et non excessives par rapport aux finalités pour lesquelles elles sont enregistrées;
- d) exactes et, si nécessaires, mises à jour;

³³¹ Barbara Wellbery, *An Overview of Information Privacy in the United States and European Union in Privacy in Electronic Commerce: A Compendium of Essays on the Use of Information*, éd. par L. Fischer et R. Bennett (Washington: American Bankers Association, 1997), 69 à 75.

³³² Les observateurs américains ont indiqué que, vu l'évolution constante de l'Internet, du commerce électronique et des autres médias, toute loi sur la protection des données est condamnée à une rapide désuétude et pourrait même ralentir le développement de ces médias. Voir Wellbery, *supra*, note 331.

³³³ STE n° 108 europ., 28 janvier 1981.

e) conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire aux finalités pour lesquelles elles sont enregistrées.³³⁴

La Convention contient également des dispositions qui traitent de la sécurité des données, des sanctions et recours, et des données personnelles de nature délicate. L'article 12 revêt un intérêt particulier, lui qui autorise toute partie à la Convention de se déroger aux dispositions de l'entente lorsque la réglementation de l'autre partie n'apporte pas une protection *équivalente*.

Avant-projet de directive UE

Même si la Convention lie les membres et exige des signataires qu'ils mettent en œuvre des lois nationales qui y sont conformes, ce ne sont pas tous les pays européens qui l'ont ratifiée. De plus, tout comme les lignes directrices, elle permet de larges écarts entre les divers régimes d'assurance, ce qui se traduit par une application hétérogène. Ainsi, certains États se sont dotés d'un mécanisme de protection spéciale pour des catégories particulières de données délicates tombant sous le coup de l'article 6, tandis que d'autres ne l'ont pas fait.³³⁵ La Commission européenne craignait que le flux transfrontières de données soit entravé par le manque d'uniformité dans les lois nationales, ce qui ne manquerait pas d'avoir un effet sur la santé économique du Marché commun et sur la mise en place de structures appropriées pour le transfert des données.³³⁶ Par conséquent, la directive UE reflète le principe directeur visant l'uniformité parmi les États membres de l'Union européenne. Il arrivera souvent à l'Union de pécher par abus de réglementation, en visant l'uniformité aux dépens de l'efficacité. À cet égard, on peut dire que l'Union n'est pas nécessairement un modèle de fédéralisme irréprochable.

En juillet 1990, la Commission publiait un avant-projet de *Directive du Conseil relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données* (« **avant-projet** »)³³⁷ avec, comme objectif, l'harmonisation des lois sur la protection de la vie privée dans les États membres afin de faciliter la libre circulation de renseignements personnels au sein de l'Union européenne. L'avant-projet de directive était plus détaillé et avait une plus grande portée que la Convention. Selon des auteurs, ce document s'inscrivait dans un programme établi par les pays membres de l'Union européenne pour aller au-delà de l'union économique et monétaire, afin de former une union politique conforme au libellé du Traité sur l'Union européenne.³³⁸ L'avant-projet promettait une meilleure harmonisation des lois européennes sur la protection des données puisque, à la différence de la Convention (ne liant les États membres que dans la mesure où ceux-ci l'avaient

³³⁴ *Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel*, STE n° 108 europ., 28 janvier 1981.

³³⁵ Paul Schwartz, *European Data Protection Law and Restrictions on International Data Flows* (1995), vol. 80, *Iowa Law Review*, p. 471 (p. 478).

³³⁶ Lawson, *supra*, note 328.

³³⁷ COM (92), vol. 314, final-SYN 287 Bruxelles, 13 septembre 1990 : (1990) JO C277/3.

³³⁸ Fred Cate, *The EU Data Protection Directive, Information Privacy, and the Public Interest* (1995), vol. 80, *Iowa Law Review*, p. 431 (p. 432).

incorporée à leurs lois nationales), une directive constituerait un outil fiable, tant pour le simple citoyen que pour les commissaires à la protection de la vie privée, si un État membre dépasse l'échéance prévue pour la mise en œuvre de lois nationales, ou lorsque cet État ne met pas en application la totalité de la directive³³⁹

Les États membres devaient promulguer le 1^{er} janvier 1993 une loi mettant en vigueur l'avant-projet de directive; toutefois, devant les nombreuses critiques, la Commission fut contrainte de modifier l'avant-projet. Principale pomme de discorde : une clause interdisant, en l'absence d'un niveau de protection « adéquat », le transfert de données vers des pays tiers. On avait alors espéré que l'avant-projet lève l'ambiguïté figurant dans la clause de la Convention faisant état de lois « équivalentes » pour assurer la protection des données dans les pays bénéficiaires. Or, non seulement cette directive n'a pas eu l'effet escompté, elle a même compliqué la situation en introduisant un double critère de protection : désormais, on imposait un niveau de protection « équivalent » pour les échanges de données personnelles entre États membres, tandis que les échanges à destination de pays non membres nécessitait un niveau « adéquat ».³⁴⁰

De plus, l'avant-projet de directive a été critiqué par le Royaume-Uni, qui y voyait un net recul par rapport à ses propres lois en la matière, ainsi qu'une entrave superflue à la bonne marche des affaires. Pour Londres, la Convention était assez claire sur le plan juridique.³⁴¹ D'autres pays, l'Allemagne notamment, craignaient que l'avant-projet de directive soit moins complet que leurs propres dispositifs de protection, et que cela n'entraîne un affaiblissement du mécanisme de protection à l'échelle nationale.³⁴² Autres critiques à l'endroit de l'avant-projet de directive : la crainte d'une augmentation inévitable du publipostage direct, étant donné que la directive compliquait le ciblage d'une clientèle potentielle. De surcroît, l'avant-projet de directive semblait entraîner dans son sillage des critères de sécurité irréalistes qui auraient nui aux systèmes automatisés de prise de décision.³⁴³ Ce document était également perçu par certains critiques comme une barrière non tarifaire au commerce ou, en des termes plus brutaux, comme une attaque européenne à l'endroit des industries de l'information et de la programmation particulièrement rentables aux États-Unis. D'un autre côté, les spécialistes en la matière estimaient que l'avant-projet forcerait tôt ou tard les États-Unis à optimiser leur propre dispositif de protection.³⁴⁴

³³⁹ Schwartz, *supra*, note 335, pp. 481-482.

³⁴⁰ Voir Olga Estadella-Yuste, The Draft Directive of the European Community Regarding the Protection of Personal Data (1992), vol. 41, *International and Comparative Law Quarterly*, p. 170 (pp. 174-179).

³⁴¹ Fiona Carlin, *The Data Protection Directive: The Introduction of Common Privacy Standards* (1996), vol. 21, *European Law Review*, p. 65 (p. 65).

³⁴² Voir Ian Lloyd, An Outline of the European Data Protection Directive (1996), vol. 1, *Journal of Information, Law and Technology*, <http://eli.warwick.ac.uk/elj/jilt/dp/intros/>.

³⁴³ Rosenbaum, *supra*, note 329, p. 5.

³⁴⁴ Estadella-Yuste, *supra*, note 340, pp. 440-441.

Harmonisation des lois sur la protection des données dans l'Union européenne

Un certain nombre d'obstacles faisaient entrave à l'adoption de la directive par les États membres. En effet, même si la plupart des États étaient déjà dotés de leurs propres lois en matière de protection de la vie privée, cela allait compliquer les choses plutôt que de les faciliter puisque chacun s'efforçait de préserver son propre système judiciaire, déjà bien rodé. Par conséquent, l'élaboration de la directive allait constituer un exercice d'adaptation, combinant les textes de loi des divers États membres, ce qui influa forcément sur la portée et la teneur de la directive. Un certain nombre de compromis allaient s'avérer nécessaires, compte tenu de différences importantes dans les divers systèmes nationaux. Ainsi, les lois sur la protection des données en Grande-Bretagne et aux Pays-Bas incitaient le secteur privé à établir son propre code de conduite, démarche totalement absente des lois allemandes et françaises.³⁴⁵ L'approche nationale pour ce qui est du traitement de certaines catégories de données particulièrement sensibles, et le statut particulier accordé aux médias à cet égard variaient également. La quête d'un compromis combinant les prescriptions des diverses lois nationales préexistantes risquait de réduire le niveau de protection visé.³⁴⁶ C'est, à titre d'exemple, la raison pour laquelle on allait inclure une disposition particulière dans la directive modifiée, concédant au Royaume-Uni un délai de grâce de douze ans pour la mise en conformité des données manuelles déjà réunies, données manuelles qui n'étaient pas touchées par les lois britanniques.³⁴⁷ L'objectif visé par la Commission européenne, c.-à-d. la réglementation du traitement des données personnelles partout dans l'Union européenne, a lui aussi rencontré certains obstacles, plus précisément dans le cas des dispositions que certains pays jugent exclusives à leur système judiciaire. Cela explique l'insistance des gouvernements français et britannique à l'effet que le traitement policier des données personnelles soit exempté des prescriptions de la directive. Résultat pratique, l'article 13 des *Considérants* reconnaît que la sécurité publique, la défense, la sûreté de l'État et les activités de l'État dans le secteur du droit pénal (ou droit criminel) débordent du cadre législatif de la Communauté européenne. La Commission a aussi dû faire un autre compromis, en incluant une clause dans les *Considérants* non exécutoires, voulant que la directive puisse s'appliquer *en principe* au traitement des données audiovisuelles. On sait que, dans certains États membres, toute réglementation de données personnelles réunies par des moyens audiovisuels est perçue comme une entrave aux activités policières.³⁴⁸

³⁴⁵ Pour un examen plus poussé de la question, voir Spiros Simitis, *From the Market to the Polis: The EU Directive on the Protection of Personal Data* (1995), vol. 80, *Iowa Law Review*, p. 445 (pp. 449-450).

³⁴⁶ Dans le cadre de la conférence tenue en juillet 1996, bien après l'adoption de la directive UE par les États membres, des intellectuels et universitaires d'Allemagne, d'Autriche, de Norvège et des Pays-Bas se sont montrés inquiets du risque d'interférence de la directive avec le niveau de protection des données déjà assuré par leurs lois nationales respectives. Voir : A. Wiebe, *Harmonization of Data Protection Law in Europe* (rapport de conférence) (1996), vol. 3, *The Journal of Information, Law and Technology*, <http://lrc.law.warwick.ac.uk/jilt/confs/3dp/default.htm>.

³⁴⁷ Carlin, *supra*, note 346, p. 65. On notera toutefois que le gouvernement britannique est en train d'amender la loi sur la protection des données, dont il envisage d'élargir le champ d'application de manière à englober également certains fichiers manuels.

³⁴⁸ Simitis, *supra*, note 345, p. 454.

Aperçu de la directive UE

La version définitive de la directive UE a été adoptée le 24 octobre 1995. Les États membres de l'Union européenne sont censés mettre en application les dispositions de la direction UE d'ici le 24 octobre 1998. Le double objectif de cette directive est de protéger les droits des individus face à la circulation des données qui les concernent, tout en assurant la libre circulation des données personnelles entre États membres, grâce à l'harmonisation des lois nationales pertinentes. La directive UE s'applique à l'ensemble du traitement automatisé des données personnelles, de même qu'à certains fichiers établis manuellement.³⁴⁹

La directive UE énonce un certain nombre de principes qualitatifs sur les données. Les États membres doivent s'assurer que les données à caractère personnel sont : traitées loyalement et licitement; collectées pour des finalités déterminées, explicites et légitimes; adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées; exactes et mises à jour; gardées uniquement le temps nécessaire.³⁵⁰ En outre, les données ne pourront être utilisées que si la personne concernée a donné son consentement de manière inéquivoque, à quelques exceptions près. Ces exceptions incluent le respect de certaines obligations légales ou précontractuelles, ainsi que la sauvegarde de l'intérêt vital ou public de la personne concernée ou du responsable du traitement.³⁵¹ Hormis certains cas d'exception, les États interdisent le traitement des données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ainsi que le traitement des données relatives à la santé et à la vie sexuelle.³⁵²

Le transfert des données à caractère personnel bénéficie de plusieurs protections en vertu de la directive UE. Ainsi, advenant collecte auprès de la personne concernée, celle-ci doit être informée de l'identité du responsable du traitement, des finalités du traitement auquel les données sont destinées, et des destinataires des données. En outre, le responsable du traitement doit aviser la personne concernée de son droit à l'accès et à la rectification des données le concernant. Lorsque les données n'ont pas été collectées directement auprès de la personne concernée, le responsable du traitement reste dans l'obligation de fournir à la personne concernée les mêmes informations, à moins que cela se révèle impossible ou implique des efforts démesurés. Dans ce cas, les États membres prévoient des garanties appropriées.³⁵³ La personne a le droit de s'opposer à ce que des données la concernant fassent l'objet d'un traitement à des fins de prospection,³⁵⁴ et de ne pas être soumise à une décision produisant des effets néfastes à son égard ou l'affectant de manière significative, décision strictement fondée sur un traitement automatisé des données.³⁵⁵ La directive prévoit en outre que chacun dispose d'un recours

³⁴⁹ Directive UE, *supra*, note 325, art. 1.

³⁵⁰ *Ibid.*, art. 6.

³⁵¹ *Ibid.*, art. 7.

³⁵² *Ibid.*, art. 8.

³⁵³ *Ibid.*, art. 10 et 11.

³⁵⁴ *Ibid.*, art. 14.

³⁵⁵ *Ibid.*, art. 15. Il est possible cependant d'arrêter des décisions individuelles automatisées, à condition qu'on ait pris des mesures adéquates pour sauvegarder les intérêts légitimes de la personne concernée.

juridictionnel en cas de violation des droits qui sont garantis par les dispositions nationales applicables au traitement des données personnelles. Toute personne ayant subi un dommage du fait d'un traitement illicite ou de toute action incompatible avec les dispositions nationales a le droit d'obtenir réparation du préjudice subi.³⁵⁶

Chaque État membre prévoit qu'une ou plusieurs autorités publiques sont chargées de surveiller l'application, sur son territoire, des dispositions adoptées par les États membres en application de la directive UE. Chaque autorité de contrôle dispose notamment de pouvoirs d'investigation, de pouvoirs effectifs d'intervention et du pouvoir d'ester en justice en cas de violation des dispositions nationales prises en application de la directive UE.³⁵⁷ Les responsables du traitement doivent adresser une notification à l'autorité de contrôle préalablement à la mise en œuvre d'un traitement automatisé. Les informations qui doivent figurer dans la notification comprennent la ou les finalités du traitement, les destinataires auxquels les données sont susceptibles d'être communiquées, et les transferts de données envisagés à destination de pays tiers. Les États membres peuvent prévoir une simplification de la notification ou une dérogation à cette obligation, lorsque les données à traiter ne sont pas susceptibles de porter atteinte aux droits et libertés des personnes concernées.³⁵⁸ L'autorité de contrôle nationale est également chargée d'encourager les associations professionnelles et les autres organisations visées à élaborer des projets de codes nationaux pour les soumettre à l'examen de l'autorité nationale.³⁵⁹

La directive UE prévoit la libre circulation des données entre les États membres. Elle prévoit également que le transfert de données à caractère personnel vers un pays tiers ne peut avoir lieu que si ce pays assure un niveau de protection adéquat. Le caractère adéquat du niveau de protection offert par le pays tiers s'apprécie au regard de toutes les circonstances relatives à un transfert; en particulier, sont prises en considération la nature des données, la finalité et la durée du ou des traitements envisagés, les pays d'origine et de destination finale, les règles de droit, générales ou sectorielles, en vigueur dans le pays tiers en cause, ainsi que les règles professionnelles et les mesures de sécurité qui y sont respectées.³⁶⁰ Par dérogation à ce qui précède, le transfert de données à caractère personnel vers un pays tiers n'assurant pas un niveau de protection adéquat peut être effectué, à condition que :

- la personne concernée ait indubitablement donné son consentement au transfert envisagé;
- le transfert soit nécessaire à l'exécution d'un contrat entre la personne concernée et le responsable du traitement, ou à l'exécution de mesures précontractuelles prises à la demande de la personne concernée;
- le transfert soit nécessaire pour la sauvegarde d'un intérêt public important ou pour la sauvegarde de l'intérêt vital de la personne concernée;

³⁵⁶ Directive UE, *supra*, note 325, art. 22 et 23.

³⁵⁷ *Ibid.*, art. 28.

³⁵⁸ *Ibid.*, art. 18 et 19.

³⁵⁹ *Ibid.*, art. 27.

³⁶⁰ *Ibid.*, art. 25.

- le transfert intervienne au départ d'un registre public qui est destiné à l'information du public et est ouvert à toute personne justifiant d'un intérêt légitime.³⁶¹

Protection « adéquate » et transfert de données vers des pays tiers en vertu de la directive UE

Protection « adéquate » et lois en vigueur dans les pays tiers

Les restrictions qu'apporte la directive UE en matière de transfert transfrontières des données à caractère personnel vers des pays n'offrant pas un niveau de protection adéquat ont été à l'origine de débats considérables sur ce que constitue justement une protection « adéquate ». Certaines personnes ont indiqué que les lois sur la protection de la vie privée au Canada et aux États-Unis ne répondraient sans doute pas aux critères d'adéquation contenus dans la directive vu que ces deux pays présentent des carences dans les procédures de notification et de recours. En outre, les systèmes d'enregistrement et de permis sont tout à fait étrangers aux réalités canadienne et américaine.³⁶² D'un autre côté, le Home Office du Royaume-Uni a publié en 1996 un document selon lequel « les nombres seront probablement négligeables pour ce qui est des cas pouvant nécessiter l'interdiction de transfert devant l'inadéquation de la protection dans des pays tiers ».³⁶³

En outre, l'utilité des exceptions prévues à l'article 26, qui autorisent les transferts vers des pays tiers en dépit d'une protection inadéquate, a été également remise en question. De nombreux spécialistes croient que seul un texte de loi garantit aux personnes concernées une protection suffisante en ce qui a trait au transfert de données vers des pays tiers, et que la protection de type contractuel pourrait s'avérer inefficace.³⁶⁴ (Pour un point de vue diamétralement opposé, se reporter au passage suivant qui traite de la protection contractuelle.³⁶⁵) On notera également que les prescriptions contractuelles liant le responsable du traitement à une tierce partie pourrait s'avérer de peu d'utilité dans les pays qui pratiquent la common law étant donné le principe de connexité contractuelle qui caractérise ce droit. De plus, il serait difficile d'évaluer les pertes de données que la personne concernée pourrait subir pour justifier une action en dommages-intérêts.

³⁶¹ *Ibid.*, art. 26.

³⁶² A. Perey et H. Janisch, *International Restrictions on the Exchange of Information: Privacy, Transborder Data Flows and Trade in Services*, extrait de *Privacy in Financial Services: Striking a Balance between Privacy Rights and Profits* (Toronto: The Canadian Institute, 1994).

³⁶³ Home Office du Royaume-Uni, *Consultation Paper on the EC Data Protection Directive (95/46/EC)* (mars 1996), chap. 7.1, http://www.open.gov.uk.home_off/ccpd/dataprot.htm.

³⁶⁴ Schwartz, *supra*, note 335, p. 486.

³⁶⁵ Voir le passage ci-dessous, à la rubrique Protection « adéquate » et dispositions contractuelles.

Le Groupe de protection des personnes à l'égard du transfert de données à caractère personnel (le « **Groupe** »), établi en vertu de l'article 29 de la directive UE, a publié en juin 1997 un document traitant du problème de la protection « adéquate ».³⁶⁶ Même si ce document n'apporte pas une démarche définitive à ce dossier, il permet de mieux comprendre les perceptions initiales au sein de la Commission. On y indique notamment que, s'il est vrai que l'article 25 prévoit une démarche au cas par cas, il ne serait pas réaliste d'étudier chaque dossier dans le détail compte tenu de la masse de transferts qui s'effectuent quotidiennement. On présente donc deux mécanismes pour rationaliser le processus décisionnel.

D'abord, le document indique que les responsables pourraient élaborer une « liste blanche » des pays tiers supposés offrir une protection « adéquate ». Par souci de conformité avec les prescriptions de l'article 25, il serait nécessaire d'étayer au cas par cas la décision d'inclure un pays sur ladite liste. Une fois qu'on a évalué plusieurs cas représentatifs de transferts vers un pays particulier, et qu'on arrive à la conclusion qu'il y existe une protection « adéquate », ce pays sera ajouté à la « liste blanche ». Variante sur ce thème : l'établissement d'un « listage partiel ». En effet, un pays pourrait faire l'objet d'un « listage partiel » si la protection qui y est accordée n'est pas uniforme dans tous les secteurs d'activités (ex. : la protection existe dans le secteur public mais non dans le secteur privé); s'il s'est doté de lois particulières pour certaines industries et non pas d'autres; ou encore si les provinces ou États qu'il réunit au sein d'un système de type fédéral offrent des niveaux de protection différents. On notera en particulier que si les codes de conduite de l'industrie sont dictés par des textes de loi, il est improbable qu'ils ne satisfassent pas aux critères de l'Union européenne.

Ensuite les transferts d'informations à destination de pays tiers ne figurant pas sur la « liste blanche » pourraient être permis, selon la catégorie d'information en question. Ainsi, le transfert de données « délicates », susceptibles d'entraîner des pertes financières ou de mettre en danger la sécurité des personnes, nécessiterait, en pays tiers, un niveau de protection plus élevé que celui qu'on attendrait d'autres types de données.

Selon ce document, l'analyse de ce qui constitue une protection « adéquate » dans un pays donné doit tenir compte de deux grands facteurs : la teneur de la réglementation pertinente et les moyens dont on dispose pour mettre celle-ci en application. Pour ce qui est de la teneur de la réglementation, il faudra inclure ce qui suit dans tout dispositif de protection de la vie privée : le principe de la finalité; le principe de la nature des données et de la proportionnalité; le principe de la transparence; le principe de la sécurité; les droits d'accès, de rectification et d'opposition; et les restrictions quant au transfert vers d'autres pays. Au sujet des moyens permettant d'assurer la mise en œuvre de la réglementation, le document indique que, même si l'on constate en Europe une forte volonté d'incorporer ces principes dans un cadre législatif, ce qui importe c'est que le

³⁶⁶ Direction générale de la Commission européenne, *First Orientations on Transfers of Personal Data to Third Countries – Possible Ways Forward in Assessing Adequacy: Discussion Document Adopted by the Working Party on June 26, 1997*, <http://www.open.gov.uk/dpr/d5020en2.htm>.

système de protection aboutisse au résultat suivant : permettre un niveau acceptable de conformité à la réglementation; offrir le soutien et l'aide voulus aux personnes concernées; et, le cas échéant, garantir des recours aux personnes lésées.

Dans un certain nombre de cas, des pays européens ont agi, conformément à leur législation nationale pour restreindre le flux transfrontières des données. En 1990 par exemple, le British Data Protection Registrar a interdit la vente d'une liste d'adresses britanniques à une entreprise de publipostage américaine.³⁶⁷ Dans un autre cas, la France a défendu à la filiale d'une société italienne établie sur son territoire de transférer des données vers l'Italie étant donné que ce pays ne dispose pas d'une législation suffisante en matière de protection de la vie privée.³⁶⁸ Bien que ces cas remontent à quelques années déjà, ils indiquent clairement que les États et les entreprises ne peuvent se permettre de prendre à la légère les éventuelles restrictions portant sur le transfert de données. D'un autre côté, le critère de l'« adéquation » figurant dans la directive de l'Union européenne ne constitue pas réellement un fardeau nouveau pour les pays tiers, vu que de nombreux États européens disposent depuis quelque temps déjà de lois nationales pour réglementer le transfert de données au-delà des frontières; or, ces lois incorporent, dans la plupart des cas, le critère de la protection « équivalente ».³⁶⁹

Reste à voir si les mécanismes en place au Canada et aux États-Unis pourront satisfaire ces deux critères. Ce qui est sûr, c'est que des restrictions sur le transfert de données vers ces deux pays auraient un impact négatif sur les économies des États-Unis, du Canada et de l'ensemble de la planète. On dit que les produits et services de l'information constituent, en importance, le premier ou le deuxième secteur de l'économie américaine, comptant pour 10 à 12 p. 100 du produit national brut. Au Canada, il en va probablement de même; à défaut, il faudrait tendre vers un tel résultat. On estime à la moitié ou aux deux tiers de la main-d'œuvre nationale américaine le nombre de travailleurs affectés à des emplois liés à l'information.³⁷⁰ La Information Infrastructure Task Force de l'administration Clinton a souligné l'importance de l'information : « L'information est l'une des ressources économiques les plus critiques du pays. À l'âge de la globalisation des marchés et de la concurrence, les technologies permettant de créer, de manier, de gérer et d'exploiter l'information revêtent une importance capitale pour les États-Unis. »³⁷¹

³⁶⁷ U.K. Office of the Data Protection Registrar, *Seventh Annual Report* (1990), pp. 33-34, cité dans Cate, *supra*, note 338, p. 438.

³⁶⁸ Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, cité dans Cate, *supra*, note 338, p. 438.

³⁶⁹ Voir Schwartz, *supra*, note 335, pp. 474-476.

³⁷⁰ Cate, *supra*, note 338, p. 439-440.

³⁷¹ *Ibid.*, pp. 439-440, cité de *Information Infrastructure Task Force, National Information Infrastructure Agenda for Action 5* (1990).

Protection « adéquate » et dispositions contractuelles

Lorsque les lois nationales du pays destinataire ne satisfont pas les critères de protection « adéquate » énoncés à l'article 25 de la directive UE, il est possible que le transfert s'effectue malgré tout, moyennant les dérogations prévues dans les dispositions contractuelles. En particulier, l'article 26 stipule qu'un transfert pourra être autorisé malgré l'absence de lois « adéquates » à condition que le responsable du traitement offre des garanties au regard de la protection de la vie privée, par le biais de clauses contractuelles appropriées. On retrouve un concept analogue dans la première Convention européenne; en fait, le Conseil de l'Europe a publié un modèle de contrat international visant la protection de la vie privée en vertu de la Convention.³⁷² Le cas de la RailwayCard allemande illustre une situation où la protection contractuelle aura servi à permettre le transfert de données à caractère personnel entre des succursales allemandes et américaines de la Citibank.³⁷³

On sait que la RailwayCard est un document utilisé par les cheminots allemands pour obtenir des remises sur le prix des billets. En 1994, la société des chemins de fer allemande a conclu une entente avec la filiale allemande de Citibank (banque établie aux États-Unis), en vertu de laquelle la RailwayCard serait offerte jumelée à une carte de crédit Visa. Ainsi, l'information sur les titulaires de la carte serait transférée vers une filiale de la Citibank située dans les États du Dakota du Sud et du Nevada, où les cartes seraient produites. Ce projet a provoqué un débat public considérable, d'autant plus que les personnes à qui la RailwayCard avait été proposée au départ étaient forcées d'accepter ce jumelage.³⁷⁴ La crainte du public tenait au fait que la société des chemins de fer, monopole en Allemagne, avait vendu l'information sur les cheminots à une banque américaine qui serait probablement appelée à se servir de ces données pour une multitude d'activités de prospection et de marketing direct.³⁷⁵ Le commissaire berlinois à la protection des données a soutenu que, même si les articles 25 et 26 de la directive UE n'avaient pas été incorporés dans les textes de loi allemands, aucun transfert de données vers les États-Unis ne se devrait se faire tant qu'on n'aurait pas respecté la teneur de ces articles. Résultat pratique : une entente contractuelle passée entre les filiales allemandes et américaines de la Citibank concernées par le programme RailwayCard.

³⁷² Consultative Committee of the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, *Model Contract to Ensure Equivalent Data Protection in the Context of Transborder Data Flows with Explanatory Memorandum* (Strasbourg, Conseil de l'Europe, novembre 1992). Extraits du modèle de contrat reproduits dans *Sourcebook on Business and Global Data Protection* (Hackensack, N.J.: Privacy and American Business, 1996), p. 245ff.

³⁷³ L'étude du cas RailwayCard s'inspire de l'article publié par le sous-commissaire berlinois à la protection des données, Alexander Dix : *The German RailwayCard: A Model Contractual Solution of the 'Adequate Level of Protection' Issue* dans *Privacy Beyond Borders: The 18th International Privacy and Data Protection Conference* (Ottawa, septembre 1996).

³⁷⁴ Finalement, la RailwayCard allait être offerte avec option Visa. Une vaste majorité de titulaires RailwayCard optèrent pour l'offre de carte non jumelée à la Visa.

³⁷⁵ Dix, *supra*, note 373, p. 2.

Ce contrat prévoit diverses dispositions visant à assurer le respect de la vie privée pour les personnes concernées par le transfert de données vers les États-Unis.³⁷⁶ Ainsi, les deux parties ont convenu de s'en remettre à la protection offerte par la loi allemande en ce qui a trait au maniement des données sur les titulaires de la carte. Les parties en présence ont accepté de ne pas transférer de données personnelles vers de tierces parties à des fins commerciales, à deux exceptions près.³⁷⁷ La filiale américaine s'est engagée à nommer des surveillants à la protection des données et d'accepter des visites sur place par le commissaire berlinois à la protection des données ou par un cabinet américain de vérification agissant pour le compte dudit commissaire. (En fait, les agents chargés de la réglementation des banques aux États-Unis et en Allemagne se sont entendus sur les modalités de vérification des données dans ce compte.) Et, ce qui est peut-être plus significatif, la filiale américaine a accepté que les résidents allemands aient envers elle des droits de protection identiques à ce que leur confèrent les textes de loi allemands. De la sorte, les titulaires auraient un droit d'accès et de rectification des données personnelles, et le droit d'intenter un procès pour dédommagement dans le cadre des lois allemandes particulièrement sévères au chapitre de la responsabilité. La mise à exécution de l'entente pourrait aller devant les tribunaux allemands; il semblerait que les lois en vigueur en Allemagne ne présentent pas la même barrière à la connexité que ce qu'on retrouve dans le système de la common law.³⁷⁸

Dans un récent article, le sous-commissaire berlinois a soutenu que la solution contractuelle qu'il proposait satisfaisait aux critères des articles 25 et 26 de la directive UE. Toutefois, il a souligné que la démarche ne devrait pas servir de solution de remplacement à la promulgation de lois assurant la protection de la vie privée aux États-Unis et dans d'autres pays hors de l'Europe. À ce propos, il a affirmé que le libellé même de la directive UE indique que les dérogations aux principes de la protection « adéquate » (article 25) ont valeur d'exception plutôt que de norme. « Militer en faveur de clauses contractuelles standard comme solution modèle pour tous les flux de données transfrontières Europe-pays tiers aurait pour conséquence d'inverser le rapport établi entre le principe et la dérogation, en vertu de la loi européenne. »³⁷⁹ Il a également noté que le cas de la RailwayCard était assez inusité, en ce sens qu'il avait été marqué par l'intervention d'agents de réglementation ainsi que par l'ouverture des responsables de la Citibank à une solution de type contractuel. Finalement, les ententes contractuelles ne pourront pas remplacer le recours à un mécanisme de surveillance centrale dans les pays étrangers comme le Canada et les États-Unis. La méthode prévoyant des droits de vérification spéciaux selon des modalités contractuelles mènerait à l'application de diverses normes par les différentes autorités étrangères sur leur territoire respectif.

³⁷⁶ *Ibid.*, pp. 4-5.

³⁷⁷ Premièrement, l'information personnelle sur l'usage de la carte Visa pourrait être transférée à d'autres filiales Citibank, pour la prospection de services financiers. Deuxièmement, l'information personnelle concernant les utilisateurs de la version ordinaire de la RailwayCard ne pourrait être transférée qu'aux fins de marketing de la RailwayCard version jumelée Visa.

³⁷⁸ Dix, *supra*, note 373, pp. 4-5.

³⁷⁹ Dix, *supra*, note 373, p. 6.

Toutefois, dans le cas des transferts vers des institutions canadiennes réglementées à l'échelon fédéral, les circonstances particulières ayant entouré l'affaire de la RailwayCard pourraient probablement se présenter. Les institutions financières réglementées sont en général des institutions d'envergure et de renom; en outre, le Bureau du surintendant des institutions financières au Canada pourrait se montrer plutôt ouvert à la collaboration afin que les transferts importants se matérialisent. Il se pourrait donc que l'affaire RailwayCard constitue un modèle permettant les transferts entre systèmes européens et institutions financières du Canada, en dépit de ce qu'affirme l'article 25 de la directive UE.

À la lumière de ce qui précède, il semble prématuré de s'engager dans une voie spécifique pour assurer la protection de la vie privée avec alignement potentiel sur les normes européennes. D'abord, on constate un manque de clarté dans les conditions préalables. Ensuite, il y a très peu de précédents sur lesquels se guider. Enfin, l'affaire de la RailwayCard allemande porte à croire qu'il serait possible de procéder à certains transferts en se fiant à des prescriptions contractuelles plutôt que législatives dans les pays tiers. Si un tel dispositif risque bien d'être trop lourd pour un usage généralisé, aucune expérience vécue ne démontre que la directive UE soit aujourd'hui une source de problèmes. Nous ignorons également si la démarche sectorielle avec autoréglementation sera jugée « adéquate » ou non aux fins de l'Union européenne. Il apparaît donc que l'expectative demeure la meilleure solution à l'heure actuelle.

Législation de la vie privée au Royaume-Uni

Le *Data Protection Act 1984*³⁸⁰ a reçu la sanction royale en juillet 1984 et a été introduit graduellement jusqu'au plein effet en 1987. Cette loi britannique avait été promulguée à la suite d'efforts déployés par des membres de l'industrie privée, qui craignaient que le Royaume-Uni ne soit exclu des réseaux de transfert de données entre États européens.³⁸¹ La loi énonce un modèle d'enregistrement pour la protection des données, dans le cadre duquel toute personne intéressée à faire du traitement automatique de données doit s'inscrire auprès du Data Protection Registrar. Certes, les mesures d'application et les recours individuels prévus dans le cadre de cette loi en font un élément positif, mais il reste que la nécessité d'un enregistrement en bonne et due forme semble créer des obstacles bureaucratiques non seulement pour les utilisateurs des données mais aussi pour les particuliers souhaitant accéder à l'information qui les concerne personnellement.

³⁸⁰ *Data Protection Act 1984*, chap. 35.

³⁸¹ Voir Tom Onyshko, *Access to personal information: British and Canadian Legislative approaches* (1989), vol. 18, *Manitoba Law Journal*, p. 213 (pp. 236-237).

Aperçu du *Data Protection Act 1984*

Le *Data Protection Act 1984* régleme dans une large mesure l'exploitation de l'information par les utilisateurs de données automatisées. La loi s'applique à tout utilisateur qui est maître du contenu et de l'exploitation des données ayant été stockées de manière à permettre un traitement automatique³⁸² vis-à-vis un individu vivant et susceptible d'être identifié par cette information.³⁸³

Un utilisateur de données n'est pas autorisé à détenir de l'information personnelle au sujet d'un particulier à moins de s'être inscrit auprès du Data Protection Registrar; tout manquement à cet égard constitue une infraction criminelle.³⁸⁴ Au moment de s'inscrire, utilisateur de données doit fournir, entre autres, une description des éléments ci-dessous : nature des données à entreposer, et finalité du stockage ou de l'exploitation prévus; source d'où provient l'information; identité de toute personne à qui l'information pourrait être divulguée; liste des pays étrangers vers lesquels les données pourraient être transférées, de manière directe ou indirecte.³⁸⁵ Si, à une date ultérieure, l'utilisateur entend divulguer l'information à une personne dont le nom ne figure pas sur le registre, ou s'il entend réunir les données à d'autres fins, il doit faire une nouvelle demande auprès du Registrar pour apporter les modifications qui s'imposent.³⁸⁶ Tout manquement à cet égard constitue également une infraction criminelle.

L'utilisateur de données est tenu d'adhérer aux huit principes de protection figurant dans la loi, qui s'inspirent fortement des principes de la Convention édictée par le Conseil de l'Europe, régissant la collecte, le stockage, le traitement, la nature et l'exploitation des données, ainsi que les droits de la personne concernée. Même si un manquement à l'un de ces principes ne constitue pas *en soi* une infraction criminelle, le Data Protection Registrar pourra agir pour radier l'utilisateur coupable si, à son avis, ledit manquement porte – ou est susceptible de porter – préjudice ou de causer une détresse.³⁸⁷

La loi accorde certains droits aux personnes concernées par le transfert de données. Ainsi, quiconque souhaite accéder aux données le concernant peut faire une demande écrite à cet effet, moyennant certains frais, demande qu'il soumettra à l'utilisateur de données. Par la suite, ce dernier devra fournir à la personne concernée copie de l'information qu'il détient à son endroit.³⁸⁸ Ladite personne devra présenter des demandes distinctes lorsqu'elle a fait l'objet de plusieurs

³⁸² La loi ne porte pas sur les renseignements contenus dans des registres manuels.

³⁸³ Voir art. 1 du *Data Protection Act 1984* pour les définitions des termes « data user », « data subject », « data » et « personal data ». L'opinion qu'on exprime à propos de quelqu'un entre dans la catégorie des données personnelles. La loi présente certaines exemptions à l'obligation de s'inscrire qui est faite à tous les utilisateurs de données. Ainsi, les données personnelles détenues par un particulier et qui ne visent que la gestion des affaires de la personne, de la famille ou du foyer sont exemptes (art. 33), de même que les données concernant la rémunération ou le régime de retraite dans le cadre d'un emploi, plus certaines transactions de vente (art. 32).

³⁸⁴ *Data Protection Act 1984, supra*, note 385, art. 5. On notera que les façonniers (services de travaux d'ordinateur) sont également tenus de s'enregistrer.

³⁸⁵ *Data Protection Act 1984, supra*, note 385, art. 4.

³⁸⁶ *Ibid.*, art. 6.

³⁸⁷ *Ibid.*, art. 11.

³⁸⁸ *Ibid.*, art. 21.

inscriptions séparées (données stockées à différentes fins). La loi prévoit également des procédures civiles lorsqu'un mauvais usage de l'information à caractère personnel porte préjudice. La personne concernée a droit à une indemnité pour tout préjudice ou détresse imputable à l'inexactitude, la perte, la destruction illicite ou la divulgation non autorisée des données par l'utilisateur.³⁸⁹ Par ailleurs, le tribunal pourra, moyennant demande à cet effet et sous réserve de certaines conditions, ordonner la rectification ou la suppression de n'importe quelles données détenues par un utilisateur.³⁹⁰

La loi donne naissance à l'entité du Data Protection Registrar qui, outre la tenue d'un registre des utilisateurs de données, a la responsabilité de promouvoir le respect des principes de protection des données. À cet effet, le Registrar est habilité à poursuivre tout utilisateur qui omet de s'enregistrer ou qui, avec témérité et en toute connaissance de cause, agit de manière qui contrevient à l'inscription au registre. Le Registrar peut également rejeter une demande d'enregistrement par un utilisateur s'il a des raisons de croire que celui-ci est susceptible de contrevenir à n'importe lequel des principes régissant la protection des données.³⁹¹ Si le Registrar estime qu'un utilisateur enregistré à enfreint n'importe lequel des principes, il peut servir audit utilisateur un avis d'exécution (« enforcement notice »), lui demandant de corriger la situation,³⁹² ou un avis de radiation (« de-registration notice ») qui vient annuler l'enregistrement de l'utilisateur.³⁹³ Le Registrar peut également servir à l'utilisateur un avis d'interdiction de transfert (« transfer prohibition notice »), qui peut empêcher ce dernier de procéder au transfert de données personnelles à l'extérieur du Royaume-Uni. De plus, le Registrar a pour mandat d'encourager la production de codes de conduite dans le secteur privé. Toutefois, à la différence de ce qui se passe en Nouvelle-Zélande, les codes du secteur privé n'ont pas force de loi au Royaume-Uni.

L'entrée en vigueur de cette loi qui régleme fortement la protection des données constituait un net revirement par rapport à la tendance du gouvernement britannique en faveur de la déréglementation.³⁹⁴ Même si la loi avait été mise en vigueur par souci de respecter les obligations afférentes au traité, le caractère universel du système d'enregistrement a fait l'objet de critiques considérables. Un membre du comité de l'opposition a d'ailleurs dit de ce document qu'il était non moins qu'un avant-projet d'enregistrement (« Data Registration Bill »), et a déclaré craindre que le Registrar et son personnel ne deviennent que

³⁸⁹ *Ibid.*, art. 22 et 23.

³⁹⁰ *Ibid.*, art. 24.

³⁹¹ *Ibid.*, art. 7(2).

³⁹² *Ibid.*, art. 10.

³⁹³ *Ibid.*, art. 11.

³⁹⁴ M. Stallworthy, « Data Protection: Regulation in a Deregulatory State », (1990) 11 *Statute Law Review* 130, p. 130

de simples agents affectés à la consignation des nombreuses demandes reçues. Par conséquent, plutôt que d'avoir une certaine maîtrise de la situation, le Registrar se retrouverait coincé dans l'administration des tâches quotidiennes. Il serait donc incapable de fournir la moindre assurance réelle quant à la protection des données.³⁹⁵

Dans les faits, le système d'enregistrement a produit des résultats supérieurs à ce que les commentaires ci-dessus pourraient laisser croire, mais il reste que le respect et le mécanisme de mise en œuvre des prescriptions ont déçu.³⁹⁶ Le rapport annuel produit en 1995 par le Office of the Data Protection Registrar admet d'ailleurs que l'enregistrement était un obstacle à franchir : à preuve, le nombre d'enregistrements et de renouvellements, clairement insuffisant.³⁹⁷ Le Registrar a récemment demandé une simplification du système, et une augmentation du nombre d'exemptions possibles.

Amendements envisagés par suite de la directive UE

Les États membres signataires de la directive UE sont tenus d'avoir une loi nationale assurant l'application de la directive au 24 octobre 1998 au plus tard. En dépit des grandes similitudes entre le *Data Protection Act 1984* et la directive UE, il existe un certain nombre de différences significatives qui nécessiteront des amendements à la loi.³⁹⁸ Ainsi, la directive UE prévoit des restrictions sur les processus décisionnels entièrement automatisés et stipule que les personnes concernées pourront s'opposer à un traitement des données à leur endroit (même si ce traitement est licite), ainsi qu'à l'utilisation des données aux fins de prospection par marketing direct. On trouvera également des différences dans la réglementation découlant de la directive, au sujet du transfert de données personnelles hors du cadre de l'Union européenne.

Au départ, le gouvernement britannique était en faveur d'une intervention minimale, et prévoyait apporter uniquement des changements rendant la loi compatible avec les prescriptions de la directive UE. Par contre, le Registrar of Data Protection préconisait des changements fondamentaux.³⁹⁹ En particulier, il a recommandé au gouvernement de « simplifier grandement le processus d'enregistrement en procédant à des exemptions massives et à un allègement du

³⁹⁵ P. Snape, *HC Debs*, Standing Committee H, col. 70 (26 avril 1983), cité dans Stallworthy, *supra*, note 394, p. 143.

³⁹⁶ *Ibid.*

³⁹⁷ The Office of the Data Protection Registrar, *Annual Report 1995*, chapitre 4, <http://www.open.gov.uk/dpr/chap4.htm>.

³⁹⁸ U.K. Home Office, *Consultation Paper on the EC Data Protection Directive (95/46/EC)* (mars 1996), http://www.open.gov.uk/home_off/ccpd/dataprot.htm.

³⁹⁹ « Le Registrar préférerait voir adoptée par le Parlement une loi entièrement nouvelle et homogène portant sur la protection des données, s'appliquant clairement à la protection de la vie privée et incorporant de façon centrale les huit principes de protection préexistants afin de bien établir les droits des individus et le devoir des responsables du traitement, et établissant une structure souple pour l'administration et la mise en vigueur, structure qui pourra s'ajuster à l'évolution, à l'application et au contexte social de la technologie. » Voir The Office of the Data Protection Registrar, *Consultation Paper on the EC Data Protection Directive (95/46/EC): Response of the Data Protection Registrar* (juillet 1996), <http://www.open.gov.uk/dpr/answer/content.htm>.

fardeau bureaucratique ». ⁴⁰⁰ De la sorte, le temps et les ressources du Registrar pourraient être consacrés au traitement des données qui présentent un risque réel pour les personnes concernées; les exemptions concernant les avis devraient être accordées aux utilisateurs dont l'intervention est le moins susceptible d'enfreindre les droits des personnes concernées. ⁴⁰¹

Dans son document *Data Protection: the Government's Proposals*, ⁴⁰² le Home Office exprime sa volonté de réduire le fardeau inutile imposé aux entreprises et, par voie de conséquence, d'accepter un bon nombre de recommandations formulées par le Registrar. De manière plus significative, Londres entend mettre en vigueur des critères simplifiés en ce qui a trait aux avis et à l'enregistrement. Dans le nouveau système, l'utilisateur de données a moins de détails à fournir, dispose de plusieurs méthodes de notification (y compris l'accès en ligne) et met en œuvre un format grandement simplifié, incluant le recours à des lots standard. De plus, certaines opérations de traitement des données pourraient ne pas faire l'objet d'avis, notamment, dans les cadres suivants : administration de la paie du personnel, administration des achats et des ventes, publicité, prospection et marketing, relations publiques et administration générale. Les exigences de notification ne s'appliqueraient pas aux fichiers manuels. Parmi les autres changements à apporter à la nouvelle loi : élargissement de la protection de manière à couvrir certaines données traitées manuellement, et ouverture d'un droit à réparations devant tribunal en cas d'atteinte au respect de la vie privée.

Loi québécoise sur la protection des données dans le secteur privé

Comme on a pu le voir plus tôt, la *Loi sur la protection des renseignements personnels dans le secteur privé* ⁴⁰³ du Québec (également connue sous l'appellation de projet de loi 68) est entrée en vigueur en janvier 1994. Cette loi s'inscrit dans le sillage d'une autre loi portant sur le secteur public, ⁴⁰⁴ et vient étayer diverses dispositions concernant le secteur privé qui figurent dans le *Code civil* de la province. ⁴⁰⁵ Cette loi s'applique à une vaste gamme d'entités du secteur privé, y compris les sociétés commerciales, les entreprises individuelles (ou entreprises à propriétaire unique), les sociétés en nom collectif, les organismes et les associations. Diverses dispositions s'appliquent à la collecte, à l'exploitation et au transfert de données à caractère personnel; en outre, la loi prescrit les droits du particulier à accéder à l'information qui le concerne et à demander des corrections lorsque celles-ci s'imposent. Des dispositions particulières s'appliquent aux listes de noms utilisées à des fins de prospection, ainsi qu'aux transferts d'information concernant des résidents du Québec, à destination de tierces parties situées hors

⁴⁰⁰ *Ibid.*, <http://www.open.gov.uk/dpr/answer/summary.htm>.

⁴⁰¹ *Ibid.*, <http://www.open.gov.uk/dpr/answer/ans6-7.htm>.

⁴⁰² U.K. Home Office, *Data Protection: the Government's Proposals* (juillet 1997), <http://www.homeoffice.gov.uk/datap3.htm>.

⁴⁰³ L.R.Q. chap. P-39.1. Pour de plus amples renseignements sur cette loi, se reporter à la Partie II qui traite de la législation québécoise sur la protection de la confidentialité dans le secteur privé.

⁴⁰⁴ *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, L.R.Q. chap. A-2.1.

⁴⁰⁵ Voir le *Code civil du Québec*, art. 35 à 41.

de la province. Tout litige relié aux prescriptions de la loi sera soumis à l'entité responsable, qui devra le trancher en vertu de la législation québécoise sur l'accès à l'information dans les secteurs public et privé, c'est-à-dire la Commission d'accès à l'information.

La loi québécoise présente des similitudes avec les lois européennes en matière de protection des données, sans toutefois faire appel à l'enregistrement ou au permis obligatoire. Comme l'indiquait l'avocat et président de la commission québécoise dans une revue juridique, le législateur québécois a adapté une démarche européenne au contexte nord-américain : « Par conséquent, on ne trouve aucune mention d'inscription obligatoire dans un registre central par les personnes qui détiennent des fichiers à caractère personnel, exception faite des agents chargés de réunir ce genre de renseignements – presque exclusivement des agences d'évaluation du crédit. »⁴⁰⁶ Les auteurs ont affirmé que l'absence d'un système d'enregistrement généralisé a permis de faciliter l'intégration de la loi au secteur privé.

Il y a eu relativement peu de commentaires sur la loi et sa mise en œuvre. Dans un article publié il y a quelque temps déjà, l'avocate montréalaise Christine Carron faisait une mise en garde contre l'impact négatif de la loi 68 sur les milieux d'affaires québécois : « De par ses nouvelles exigences, la loi provoquera certainement une augmentation des coûts d'exploitation des entreprises; on se demande donc si, réellement, les salariés, les consommateurs, les entrepreneurs et la société en général en sortiront gagnants. »⁴⁰⁷ Toutefois, le président de la Commission d'accès à l'information a laissé entendre que cette loi ne constitue pas un changement fondamental dans les pratiques commerciales déjà en vigueur puisque de nombreuses entreprises québécoises se sont déjà dotées de politiques en matière de protection de la vie privée.⁴⁰⁸ Par ailleurs, les documents obtenus de la Commission n'indiquent pas qu'il y a eu beaucoup de plaintes dans le secteur privé. En effet, au cours de l'exercice 1995-1996, la Commission a reçu 151 plaintes relatives au secteur privé, puis 224 autres au cours de l'exercice suivant.⁴⁰⁹ Nous n'avons pas connaissance d'une étude qui aurait évalué le coût d'une mise en conformité avec les prescriptions de la loi.

⁴⁰⁶ Paul-André Comeau et André Ouimet, *Freedom of Information and Privacy: Quebec's Innovative Role in North America* (1995), vol. 80, *Iowa Law Review*, p. 651 (p. 668).

⁴⁰⁷ Voir Christine A. Carron, *Overview of the Quebec Act Respecting Personal Information in the Private Sector* dans *I've Got A Secret: The Duty of Confidentiality in the Private Sector* (Toronto, Association du Barreau canadien – Ontario, mars 1994), p. 14.

⁴⁰⁸ Le président devait faire ces commentaires quelques mois avant l'entrée en vigueur de la loi : Paul-André Comeau, *The Protection of Personal Information in the Private Sector: An Important Step Forward by Quebec's National Assembly*, présentation faite dans le cadre de la 6^e Annual Conference of Privacy, Laws and Business à Oxford (R-U), 28 juin 1993, p. 13.

⁴⁰⁹ Voir Commission d'accès à l'information du Québec, *Vie privée et transparence administrative au tournant du siècle* (juin 1997), p. 1.3.3 et Graphique 10, <http://www.cai.gouv.qc.ca/sunset1.htm>.

Lois sur la confidentialité des données en Nouvelle-Zélande

La Nouvelle-Zélande a étendu les principes de protection des données au secteur public comme au secteur privé par le biais du *Privacy Act 1993*. Il s'agit là de la plus récente loi néo-zélandaise à traiter du respect de la vie privée⁴¹⁰, loi qui présente un certain nombre de caractéristiques d'intérêt, dont le caractère exécutoire conféré aux codes de conduite approuvés, ainsi que des dispositions particulières réglementant les activités d'appariement de données qui ont été autorisées.

Aperçu du *Privacy Act 1993* néo-zélandais

Au cœur du *Privacy Act* promulgué par le gouvernement néo-zélandais, on retrouve les douze « Information Privacy Principles », qui traitent de la collecte, du stockage, de la nature et de l'usage des données à caractère personnel, de même que des droits de la personne concernée à accéder et à corriger cette information.⁴¹¹ Les principes s'appliquent à l'information détenue par chaque entité (*agency*)⁴¹², définie comme étant « toute personne ou réunion de personnes, morale ou physique, dans le secteur public ou le secteur privé ». ⁴¹³ Chaque entité devra disposer d'au moins un agent à la protection de la vie privée, dont le rôle consistera à inciter au respect des principes de confidentialité, répondre aux demandes de renseignements personnels et collaborer avec le Commissaire à la protection de la vie privée pour le règlement des plaintes reçues.⁴¹⁴

Bien que les « Information Privacy Principles » ne diffèrent pas réellement des principes présentés dans la plupart des codes de conduite et des textes de loi, il existe un certain nombre de différences dignes d'intérêt. Ainsi, le principe 2 de la loi exige que l'information recherchée par une entité soit obtenue directement auprès de la personne concernée, hormis un certain nombre d'exceptions. Le principe 12 ajoute un nouvel élément, absent des textes de loi canadiens.

⁴¹⁰ Au cours des années 50 et 70, la Nouvelle-Zélande s'est dotée de législation visant à assurer la protection des renseignements personnels réunis dans les domaines de la santé, de la fiscalité, des statistiques et de l'application de la loi. Le *Official Information Act*, entré en vigueur le 1^{er} juillet 1983, conférait aux particuliers le droit exécutoire d'accéder aux renseignements détenus par les services publics et ministères ainsi que par les entreprises d'État, et de corriger l'information s'il y a lieu. En 1988, l'organisme chargé de surveiller l'application du *Official Information Act* devant la Chambre basse (Chambre des représentants), recommandait des amendements à la loi (*Official Information Act*) pour réglementer la collecte et l'exploitation des données personnelles. Le gouvernement travailliste prévoyait apporter les modifications nécessaires mais il fut défait aux élections générales. Passé dans l'opposition, le *Labour* a continué à souligner l'urgence d'une protection de la vie privée; en 1991, il présentait à cet effet un projet de loi d'initiative parlementaire. À la suite de ce projet de loi et compte tenu des craintes du public à l'endroit d'un certain programme d'interconnexion proposé, le gouvernement allait déposer sa propre loi. Le *Privacy Commissioner Act*, promulgué le 18 décembre 1991, devait permettre à l'État d'aller de l'avant dans son programme d'interconnexion. Plus tard, le *Privacy Act 1993* allait être promulgué, en mai 1993 plus exactement. Se reporter à John Howells, *The Privacy Act of 1993: A New Zealand Perspective* (1995), vol. 17, *Comparative Labor Law Journal*, p. 107.

⁴¹¹ *Privacy Act 1993*, art. 6.

⁴¹² *Ibid.*, art. 8.

⁴¹³ *Ibid.*, art. 2. Cet article contient un certain nombre d'exceptions à la règle.

⁴¹⁴ *Privacy Act 1993*, art. 23.

L'entité en question n'est pas autorisée à affecter un identificateur spécifique à la personne concernée, à moins qu'une telle action ne soit nécessaire à la bonne marche des activités de l'entité. De plus, une fois l'identificateur attribué, celui-ci ne pourra en aucun cas être utilisé par une autre entité indépendante. Étant donné que l'identificateur répond à une finalité spécifique, il est impossible pour l'État (par exemple) d'attribuer à chaque citoyen un numéro personnel qui serait utilisé pour l'ensemble des interactions avec ce dernier.

La loi prévoit quatre principes additionnels, connus sous le nom de « Public Register Privacy Principles » et qui s'appliquent à l'administration des registres publics.⁴¹⁵ Aux termes de la loi, les services publics chargés d'administrer les registres publics sont considérés comme des « entités » en vertu de la loi et, par voie de conséquence, sont assujettis *et* aux « Information Privacy Principles » *et* aux « Public Register Privacy Principles ». Les quatre « Public Register Privacy Principles » sont les suivants :

On ne pourra accéder à l'information confidentielle tenue dans un registre public qu'au moyen des références de recherche compatibles avec le mode d'indexation ou d'organisation du registre.

L'information à caractère personnel obtenue d'un registre public ne devra faire l'objet d'aucun tri ni d'aucune combinaison avec des données personnelles obtenues d'un autre registre public dans le but d'établir, à titre onéreux, une base de renseignements personnels dont la forme serait différente de ce qu'on trouverait directement dans le registre.

L'information personnelle qui est déposée dans un registre public ne sera pas transmissible par des moyens électroniques, à moins que l'objet de la transmission soit d'ouvrir l'accès à un membre du public qui souhaite interroger le registre.

L'accès à l'information dans le registre public sera offert à titre gracieux ou moyennant des frais modiques.⁴¹⁶

La loi néo-zélandaise contient des clauses particulières au sujet des codes de conduite s'appliquant au secteur public ou au secteur privé.⁴¹⁷ Un code de conduite établi par le Commissaire à la protection de la vie privée constitue un document exécutoire et obligatoire. Il est susceptible de modifier un ou plusieurs des « Information Privacy Principles » au moyen d'exemptions ou de prescription de normes qui seront plus ou moins sévères. En outre, un code peut décider de la manière dont les principes seront appliqués. En bref, un code décidera de la manière dont les entités intervenant dans une activité, une industrie, une profession ou un secteur

⁴¹⁵ *Ibid.*, art. 59. Les principaux registres publics incluent le registre de l'état civil (naissances et décès), le registre des titres, le registre des sièges d'entreprises, les listes électorales, les registres de permis de conduire et d'immatriculation, ainsi que le registre des droits de sûreté. Pour une liste complète, se reporter à l'appendice 2 du *Privacy Act 1993*.

⁴¹⁶ *Privacy Act 1993*, art. 59.

⁴¹⁷ Dans certaines situations, les codes de conduite auront la valeur de règlements : *Privacy Act 1993*, art. 50.

particuliers se soumettront aux « Information Privacy Principles ». Les codes pourront être mis en œuvre soit par le Commissaire à la protection de la vie privée, soit par une « entité » (le plus souvent, des corporations, des ordres professionnels ou des services officiels.⁴¹⁸) Toutefois, avant de mettre en circulation un code de conduite, le Commissaire doit faire l'annonce publique d'un avant-projet de code et des détails qui y sont pertinents; les parties concernées disposeront alors d'un certain délai pour faire au Commissaire des propositions au sujet du code. Une bonne partie du code de conduite devra porter sur les principes de la confidentialité et sur la manière d'assurer l'application de chacun d'entre eux. Il est également prévu que les codes incluent un certain nombre d'exemples pratiques.⁴¹⁹

À l'heure actuelle, il n'existe que trois codes de conduite : le *Health Information Privacy Code 1994*,⁴²⁰ le *Superannuation Schemes Unique Identifier Code 1995* et le *EDS Information Privacy Code 1997*.⁴²¹ Le Commissaire, agissant de concert avec les entités des secteurs d'activité concernés, est à l'origine de tous ces codes. Le Health Information Code s'applique à diverses entités et porte sur différentes informations à caractère médical; ses douze règles de confidentialité reprennent, pour l'essentiel, ce qui figure dans les Information Privacy Principles de la loi, à quelques différences près visant à adapter les principes de la loi au contexte spécifique des services de santé.⁴²² Le Superannuation Code a été établi à la demande de la Association of Superannuation Funds of New Zealand dans le but d'amender le principe 12 de la loi de façon à permettre la circulation des identificateurs spécifiques attribués par l'employeur, circulation qui se ferait entre le lieu de travail et le siège des fiduciaires des régimes de pension de retraite

⁴¹⁸ Voir Office of the Privacy Commissioner of New Zealand, *Guidance Note on Codes of Practice under Part VI of the Privacy Act*, art. 2.0, <http://io.knowledge-basket.co.nz/privacy/guide/cop.htm>.

⁴¹⁹ *Ibid.*, art. 5 et 6. Selon ce qui figure dans le rapport annuel 1994-1995, seuls deux codes de conduite ont été établis au cours de l'année. Voir Office of the Privacy Commissioner of New Zealand, *Report of the Privacy Commissioner for the Year Ended June 1995* (1995), art. 3.2, <http://io.knowledge-basket.co.nz/privacy/anr>. Dans un document plus récent, on apprend que seulement quelques codes de conduite ont été établis à ce jour, et que le Commissaire à la protection de la vie privée est à leur origine. Voir Office of the Privacy Commissioner of New Zealand, *Review of the Privacy Act 1993: Discussion Paper No. 4 – Codes of Practice and Exemptions* (septembre 1997), <http://www.knowledge-basket.co.nz/privacy/discpp/discpr4.htm>.

⁴²⁰ Le *Health Information Privacy Code 1994* s'est substitué au *Health Information Privacy Code 1993* (provisoire). Le code provisoire établi peu après la promulgation du *Privacy Act* avait été mis en œuvre sans qu'on soit passé par le processus de consultation exigé par la loi. Voir Bruce Slane, *Centralised Databases: People, Privacy and Planning* (document présenté par le Commissaire à la protection de la vie privée, dans le cadre de la rencontre entre les directeurs néo-zélandais et australien chargés de la technologie de l'information dans les services de la santé, le 18 février 1998), <http://www.knowledge-basket.co.nz/privacy/speeches/itdirect.htm>.

⁴²¹ Le *EDS Information Privacy Code 1997* s'est substitué au *GCS Information Privacy Code 1994*. Précisons que la GCS Limited était une entreprise d'État qui traitait des données « délicates » destinées aux services publics; par la suite, cette société a été privatisée et appartient maintenant à la EDS (NZ) Limited.

⁴²² Par exemple, la règle 11 du Code autorise une plus grande divulgation de l'information que ne le fait le principe 11, bien que dans des secteurs plus circonscrits, tandis que la règle 12 permet à certaines entités figurant dans l'annexe du Code d'affecter un numéro identificateur spécifique à un particulier, même si une autre entité utilise déjà le même numéro à l'endroit de la personne en question.

associés à l'emploi.⁴²³ Le code EDS s'applique à la compagnie EDS (NZ) Ltd., société fermée qui traite des données fournies par un certain nombre d'organismes publics. En vertu du code, la société EDS (NZ) Ltd. ne peut transférer de données obtenues d'entités désignées à l'extérieur de la Nouvelle-Zélande, à moins de consentement écrit par l'entité concernée et après avis au Commissaire.⁴²⁴

Cette loi régleme également certains programmes d'interconnexion entrepris par des entités publiques. On définit ces systèmes comme étant des programmes qui permettent de comparer des fichiers personnels portant sur dix personnes au moins dans le but de produire ou de vérifier des renseignements sur ces personnes.⁴²⁵ Les dispositions spéciales de la loi entrent en jeu lorsque des entités publiques cherchent à entreprendre des programmes d'interconnexion autorisés en vertu d'autres textes de loi néo-zélandais. La loi comporte une liste restreinte d'entités « spécifiées »,⁴²⁶ tandis que la liste des programmes d'interconnexion « autorisés » figure en annexe.⁴²⁷ (Lorsqu'une entité publique a recours à un programme d'interconnexion qui n'entre pas dans la liste des programmes « autorisés » mais qui est par ailleurs permmissible selon ce qui figure dans les Information Privacy Principles, nulle disposition particulière ne régleme le programme.⁴²⁸) Pour faire des programmes d'interconnexion, les entités spécifiées doivent conclure des ententes qui limitent la divulgation de l'information.⁴²⁹ Il se peut que l'entité spécifiée qui exploite un programme d'interconnexion ne reçoive qu'un accès limité à l'autre base de données; les transferts informatiques en ligne nécessitent l'approbation du Commissaire.⁴³⁰ Si une entité spécifiée entend adopter certaines mesures à l'endroit de quelqu'un sur la foi des données d'un programme d'interconnexion, elle doit transmettre à la personne concernée un préavis écrit de cinq jours.⁴³¹ Les agences spécifiées devront transmettre au Commissaire le détail des données dans le programme d'interconnexion autorisé. Outre ces

⁴²³ Voir Office of the Privacy Commissioner of New Zealand, *Report of the Privacy Commissioner for the Year Ended June 1995* (1995), art. 3.2, <http://www.knowledge-basket.co.nz/privacy/anr/04repcop.htm>. Selon M. Blair Stewart du bureau du Commissaire néo-zélandais à la protection de la vie privée, les représentants de l'industrie ont été invités par le Commissaire à produire le code; ceux-ci ayant été incapables de s'acquitter de la tâche, le Commissaire a dû se charger lui-même de la rédaction de l'avant-projet.

⁴²⁴ Voir Office of the Privacy Commissioner of New Zealand, *Report of the Privacy Commissioner for the Year Ended June 1995* (1995), art. 3.2, <http://io.knowledge-basket.co.nz/privacy/anr>. Voir également l'introduction au document EDS Information Privacy Code 1997.

⁴²⁵ *Privacy Act 1993*, art. 97.

⁴²⁶ *Ibid.*

⁴²⁷ Voir la troisième annexe au *Privacy Act 1993*, où figurent les clauses autorisant l'interconnexion des données traitées dans les lois suivantes : *Births and Deaths Registration Act*, *Penal Institutions Act*, *Marriage Act*, *Customs Act*, *Inland Revenue Department Act*, *Immigration Act*, *Education Act* et *Accident Rehabilitation and Compensation Insurance Act*.

⁴²⁸ Voir Office of the Privacy Commissioner of New Zealand, *Review of the Privacy Act 1993: Discussion Paper No. 7 – Information Matching* (septembre 1997), <http://io.knowledge-basket.co.nz/privacy/discpp/discpr7.htm>, sous la rubrique « The Scheme for Enforcement – What information matching activities ought to be controlled? ».

⁴²⁹ *Privacy Act 1993*, art. 99.

⁴³⁰ Voir art. 3 de l'annexe 4 au *Privacy Act 1993*. Voir également Office of the Privacy Commissioner of New Zealand, *Information Matching: Fact Sheet No. 5* (août 1993), <http://io.knowledge-basket.co.nz/privacy/facts/fact5.htm>.

⁴³¹ *Privacy Act 1993*, art. 103.

dispositions particulières applicables aux entités publiques, la loi prévoit qu'un code de conduite peut, dans certains cas, imposer des restrictions quant aux activités d'interconnexion qu'exercent les entités du secteur privé.⁴³²

La mise en application de la loi est confiée au Commissaire à la protection de la vie privée, au Commissaire aux débats et au tribunal de révision des plaintes. Les tâches du Commissaire à la protection de la vie privée incluent l'établissement de codes de conduite, l'évaluation des lois ou politiques au regard de l'effet sur la confidentialité, la sensibilisation du public à l'endroit des principes de confidentialité, la promotion de ces principes et la suite à donner aux plaintes.⁴³³ Un particulier peut porter plainte devant le Commissaire à la protection de la vie privée, pour toute atteinte qui serait faite à sa vie privée et qui lui causerait des pertes ou des dommages, une humiliation significative, une atteinte à la dignité ou d'autres conséquences néfastes. Il y a « atteinte » en cas d'infraction à un principe ou à un code de conduite, ou encore en cas de non-respect du règlement qui régit l'interconnexion.⁴³⁴ Il y a également « atteinte » lorsque l'entité refuse à un particulier le droit d'accéder aux données qui le concernent ou de modifier ces dernières, et ce sans le moindre motif valable.⁴³⁵ Le Commissaire à la protection de la vie privée est habilité à faciliter le règlement des plaintes,⁴³⁶ à convoquer des rencontres obligatoires visant un règlement de l'affaire,⁴³⁷ et à transmettre les demandes au Commissaire aux débats s'il est lui-même incapable de résoudre le problème.⁴³⁸ À son tour, le Commissaire aux débats ou la personne lésée pourra saisir de ce dossier le tribunal de révision des plaintes, tribunal qui a l'autorité nécessaire pour accorder des réparations s'il est convaincu d'une prépondérance des probabilités voulant que l'action entreprise par l'accusé porte atteinte à la vie privée de la victime présumée. Ce tribunal pourra déclarer que l'action de l'accusé constitue une atteinte à la vie privée de la personne concernée, et ordonner à l'accusé de cesser toute atteinte de ce genre ou de prendre des mesures précises pour remédier à son ingérence. Le tribunal pourrait aussi ordonner toute autre forme de réparation qu'il jugera adéquate, y compris le versement de dommages-intérêts.⁴³⁹

Justification pour l'élargissement de la confidentialité au secteur privé

Lors d'une présentation faite dans le cadre d'une récente conférence sur le droit bancaire, le Commissaire néo-zélandais à la protection de la vie privée, Bruce Slane, a abordé les raisons

⁴³² *Ibid.*, art. 46(4).

⁴³³ *Ibid.*, Partie III, art. 12 à 26.

⁴³⁴ *Ibid.*, art. 66(1).

⁴³⁵ *Ibid.*, art. 66(2).

⁴³⁶ *Ibid.*, art. 74.

⁴³⁷ *Ibid.*, art. 76.

⁴³⁸ *Ibid.*, art. 77.

⁴³⁹ *Ibid.*, art. 85. Le Rapport annuel 1994-1995 indique que 78 p. cent des 827 plaintes reçues au cours de l'année et qui étaient du ressort du Commissaire ont été réglées sans que le Commissaire n'ait à formuler à leur endroit d'opinion définitive. Par ailleurs, 47 p. cent des plaintes traitaient de demandes d'appel concernant la décision d'une entité de ne pas partager certains renseignements personnels. La plupart des autres types de plainte étaient des allégations de divulgation, surtout dans le domaine de la santé. Le Rapport annuel indique également que 58 p. cent des plaintes visaient le secteur privé. Voir Office of the Privacy Commissioner of New Zealand, *Report of the Privacy Commissioner for the Year Ended June 1995* (1995), art. 3.3, <http://io.knowledge-basket.co.nz/privacy/anr>.

justifiant l'élargissement de la confidentialité au secteur privé.⁴⁴⁰ Étant donné que plusieurs entreprises d'État passeront ou ont déjà passé au secteur privé, M. Slane a affirmé qu'il serait illogique d'insister pour que les activités d'une entreprise particulière soient touchées par les prescriptions de la loi sur la confidentialité lorsque cette entreprise est propriété de l'État, mais qu'elles ne soient plus visées par la loi du moment que ladite entreprise a été privatisée. En outre, étant donné que les secteurs du crédit, des banques et des télécommunications contiennent parfois une combinaison d'entreprises d'État et d'entreprises privées, il faudrait que les lois sur la protection de la vie privée s'appliquent à tous de manière à rendre les choses équitables. Selon M. Slane, il est faux de tenir pour acquis que seul le secteur public a besoin d'être légiféré sous prétexte que l'État *uniquement* peut exiger qu'on lui remette de l'information à caractère confidentiel. En réalité, bien des entreprises du secteur privé exigent ce genre de renseignements avant d'offrir leurs services. Les gens s'inquiètent plus de la *manière* dont l'information les concernant sera utilisée que de savoir qui a obtenu ou qui détient l'information. Finalement, M. Slane a indiqué que le recours à des lois sectorielles n'était pas souhaitable compte tenu du coût, en temps et en argent, associé à cette formule – d'autant plus qu'il faudrait alors faire face à d'importants groupes de pression, ce qui pourrait donner des critères d'application disparates.

M. Slane a précisé que la Bankers Association était, au départ, opposée à l'application de la loi dans le secteur privé en général, et dans le secteur bancaire en particulier; ses dirigeants estimaient alors que les banques étaient déjà frappées de plusieurs obligations à caractère législatif. Dans la pratique, les banques n'ont eu aucune grande difficulté à respecter la loi; elles ont fait l'objet d'un nombre relativement peu élevé de plaintes des consommateurs, et n'ont pas cherché à mettre en œuvre un code de conduite. M. Slane a aussi abordé la question des coûts d'observation, notant au passage qu'un régime de protection volontaire pourrait, s'il s'avérait efficace, revenir bien moins cher. En fait, le problème de la confidentialité ne disparaîtrait pas en l'absence d'une loi; les entreprises auraient toujours à en tenir compte, ce qui fait qu'il y aura toujours des frais à engager à ce chapitre.

Révision du *Privacy Act*

Le Commissaire à la protection de la vie privée réévalue à l'heure actuelle le fonctionnement du *Privacy Act* pour savoir s'il est nécessaire d'y apporter des amendements. Il étudie les commentaires reçus quant à la pertinence de nouvelles clauses sur les infractions, ou à la compétence des tribunaux en matière de principes de confidentialité. La loi actuelle met l'accent sur les recours civils. Même si le non-respect d'un principe ne constitue pas une infraction, la loi

⁴⁴⁰ Bruce Slane, Privacy Law Issues – Reform Proposals and their Impact on the Financial Industry; notes pour une présentation par le Commissaire néo-zélandais à la protection de la vie privée dans le cadre de la 14^e Annual Banking Law and Practice Conference, tenue le 22 mai 1997; <http://www.knowledge-basket.co.nz/privacy/speeches/banksyd2.htm>.

pourra, lorsqu'un individu est ainsi lésé, apporter une solution au problème et exiger une réparation.⁴⁴¹ Autre facteur à l'étude : les coûts d'observation. On reconnaît que des coûts d'observation prohibitifs pourraient ralentir la croissance et l'emploi, nuire au caractère concurrentiel sur la scène internationale et, en fait, constituer un obstacle à l'observation des normes fixées. Aujourd'hui, la loi n'impose pas de coûts de base, et il n'existe dans les frais d'enregistrement ou d'adhésion aucun montant qui y corresponde. Les entités doivent se doter de leurs propres marches à suivre et de leurs propres imprimés administratifs.⁴⁴² Finalement, on s'interroge aussi sur la pertinence d'une réglementation du flux de données transfrontières.⁴⁴³

Évolution de la législation australienne

Le gouvernement du Commonwealth d'Australie a considéré à un certain moment élargir au secteur privé les lois qui protègent la confidentialité des données, avant d'en décider autrement il n'y a pas si longtemps. En effet, l'Australie a partiellement introduit les lignes directrices de l'OCDE en promulguant le *Privacy Act 1988*, qui prévoit que les ministères et organismes publics observent plusieurs des préceptes inclus dans les Information Privacy Principles. Toutefois, la loi australienne ne s'applique pas au secteur public, puisqu'elle ne réglemente que le secteur privé (pour les activités d'évaluation du crédit et les numéros de fichier d'impôt).

En 1995, une commission permanente de la Chambre des représentants déposait un document qui recommandait de façon unanime l'élargissement jusque dans le secteur privé des Information Privacy Principles figurant dans la loi.⁴⁴⁴ Pour les membres de la Commission, il semblait nécessaire de doter le pays d'une politique nationale en matière de confidentialité, compte tenu de la vague de privatisation et de la sous-traitance des services publics dans le secteur privé. De plus, ce genre de politique devenait nécessaire s'il fallait relever les défis posés par l'avènement de l'autoroute de l'information. En 1996, la Law Reform Commission recommandait la mise en œuvre d'un dispositif législatif à l'échelle nationale ayant pour but la protection de la confidentialité dans le secteur public et le secteur privé.⁴⁴⁵ Plus tard au cours de la même année, un document de travail établi par le bureau du Procureur général prônait l'élargissement du cadre

⁴⁴¹ Office of the Privacy Commissioner of New Zealand, *Review of the Privacy Act 1993: Discussion Paper No. 1 – Structure and Scope* (septembre 1997), <http://www.knowledge-basket.co.nz/privacy/discpp/discpr1.htm>.

⁴⁴² Office of the Privacy Commissioner of New Zealand, *Review of the Privacy Act 1993: Discussion Paper No. 9 – Compliance and Administration Costs* (septembre 1997), <http://www.knowledge-basket.co.nz/privacy/discpp/discpr9.htm>.

⁴⁴³ Office of the Privacy Commissioner of New Zealand, *Review of the Privacy Act 1993: Discussion Paper No. 12 – New Privacy Protections* (septembre 1997), <http://www.knowledge-basket.co.nz/privacy/discpp/discpr12.htm>.

⁴⁴⁴ House of Representatives Standing Committee on Legal and Constitutional Affairs, *In Confidence: A Report of the Inquiry into the Protection of Confidential Personal and Commercial Information Held by the Commonwealth* (1995).

⁴⁴⁵ Law Reform Commission, *Report of the Review by the Australian Law Reform Commission and the Administrative Review Council of the Federal Freedom of Information Act 1982*, présenté au Parlement le 24 janvier 1996.

législatif de manière à couvrir également le secteur privé.⁴⁴⁶ Ce document décrivait une approche mixte, en vertu de laquelle les principes à caractère statutaire s'appliqueraient à moins que ne soit approuvé un code de conduite axé sur les principes régissant la protection de la vie privée. Les codes pourraient être personnalisés en fonction des différents secteurs d'activité, et permettraient donc une certaine souplesse dans le secteur privé.

L'enquête publique sur les systèmes financiers australiens (Australian Financial System Inquiry), chargée d'étudier les problèmes que rencontre ce secteur d'activité en Australie, a fait son rapport début mars 1997 (le « rapport Wallis »).⁴⁴⁷ L'enquête publique a fait plusieurs recommandations au secteur des services financiers, en partant du principe que les règles de confidentialité s'appliquant au marché devraient être les mêmes que celles qui se retrouvent dans l'économie en général.⁴⁴⁸ Fait révélateur, le rapport Wallis devait recommander l'adoption du principe du consentement par défaut dans le contexte de l'échange de données. Ainsi, une institution financière pourrait faire circuler l'information dont elle dispose dans la mesure où le client ne fait rien pour indiquer son objection; toutefois, l'institution serait tenue de simplifier le processus de refus mis à la disposition du client.⁴⁴⁹ Le rapport Wallis a conclu que toute réglementation portant sur la protection de la vie privée devrait consister en un juste compromis entre, d'une part, les préoccupations du public à ce sujet et, d'autre part, la capacité des institutions financières d'exploiter cette information à des fins commerciales et de fournir des services financiers de manière plus efficace. C'est pourquoi les codes de conduite devraient être administrés à l'échelle nationale et s'appliquer à toutes les entreprises prestataires de services financiers, y compris les institutions non financières appelées à offrir ce genre de services.⁴⁵⁰

En dépit de tout cela, la proposition d'étendre l'emprise de la loi au secteur privé n'allait pas aboutir. Dans un communiqué de presse daté du 21 mars 1997, le premier ministre australien a soutenu que la proposition imposerait un fardeau démesuré au secteur privé : « Au moment où tous les chefs d'État s'entendent sur la nécessité de réduire le fardeau de la réglementation, il ne semble pas productif de proposer de nouveaux régimes de réglementation. »⁴⁵¹ Le premier ministre a également demandé à ses homologues de la fédération australienne de ne pas promulguer de loi de ce genre dans leurs États respectifs. Ce revirement de politique au sein du gouvernement fut mal accueilli par les groupes en faveur de la protection de la vie privée, sur la scène nationale comme sur la scène internationale. Ainsi, le groupe Privacy International devait-il noter que « la loi bénéficiait d'un important appui au sein des entreprises et dans le

⁴⁴⁶ Attorney General's Department, *Privacy Protection in the Private Sector* (septembre 1996), <http://www.agps.gov.au/customer/agd/clrc/privacy.htm>.

⁴⁴⁷ *Final Report of the Financial System Inquiry* (Australie, 18 mars 1997).

⁴⁴⁸ *Ibid.*, p. 17.

⁴⁴⁹ *Ibid.*, recommandation 100, chap. 66, pp. 519-521.

⁴⁵⁰ *Ibid.*, recommandation 101, chap. 66; pp. 516-517 et 521-523.

⁴⁵¹ Communiqué de presse du premier ministre John Howard (21 mars 1997), <http://www.efa.org.au/Issues/Privacy/pmpr0321.html>.

grand public »⁴⁵² et que « la décision du gouvernement va carrément à l'encontre de la politique internationale en la matière ».⁴⁵³

Un document d'étude publié en août 1997 par le Commissaire australien à la protection de la vie privée tente de délimiter une option d'autoréglementation.⁴⁵⁴ Le document convient que l'opinion est partagée entre la formule légiférée et la formule d'autoréglementation, mais que les entreprises favorisent systématiquement l'option qui représente le moins de coûts d'observation et qui réduit les chevauchements avec les autres réglementations ou les conflits entre juridictions différentes. De plus, les sociétés commerciales australiennes bénéficient du flux d'informations transfrontières et ont donc des réserves à l'endroit de la directive UE. Le mécanisme proposé comporte trois composantes : des principes ou des normes de traitement pour les renseignements à caractère personnel; des mécanismes faisant en sorte que les entreprises adhèrent à la formule, et encouragent et contrôlent le respect des principes; enfin, des mécanismes permettant de donner suite aux plaintes reçues et d'y apporter des solutions valables. Le document reconnaît la difficulté d'obtenir les résultats voulus à l'aide d'un régime autoréglementé, et préconise un système dans lequel les entreprises s'engageraient à respecter les règles du jeu et à offrir des réparations en cas d'infraction. La surveillance serait assurée par un administrateur indépendant, auquel s'ajouterait un organisme indépendant permettant aux personnes intéressées d'interjeter appel. Le gouvernement fédéral de l'Australie semble faire face aux mêmes restrictions constitutionnelles que celles qu'on retrouve au Canada.

Jusqu'à tout récemment, les différents États australiens ne disposaient pas vraiment de lois spécifiques à la protection de la vie privée; toutefois, on relève aujourd'hui plusieurs initiatives en ce sens dans les États de Nouvelle-Galles du Sud, de Victoria et de Queensland. Ainsi, en Nouvelle-Galles du Sud, la loi envisagée permettrait l'établissement de codes de conduite à coup de réglementation; ces codes pourraient être élargis en vue d'une application aux entités du secteur public et du secteur privé, et seraient d'application obligatoire.⁴⁵⁵ L'État de Victoria a

⁴⁵² Privacy International, « Looking for Answers on Government's Privacy U-Turn », de *Privacy International Online Privacy Archive* (avril 1997), http://www.privacy.org/pi/countries/australia/campaign97/coalition_statement_497.html.

⁴⁵³ Privacy International, Open letter from Privacy International to the Prime Minister of Australia, datée du 16 avril 1997, http://www.privacy.org/pi/countries/australia/campaign97/pi_letter_497.html. Voir également Tom Dixon, Voluntary Code Leaves Privacy Exposed, *Australian Privacy Foundation Media Release*, daté du 19 août 1997, <http://www.efa.org.au/Issues/Privacy/pr0819.html>. M. Dixon, qui est directeur de la Privacy Foundation, a déploré l'inefficacité des lois australiennes sur la protection de la vie privée : « On commence aussi à manquer de temps pour faire la mise à niveau avec les critères de l'Union européenne en matière de protection de la vie privée. Nous n'avons plus que jusqu'à octobre 1998, après quoi les entreprises australiennes seront exclues du commerce international dans le domaine de l'information. Si le gouvernement entend réellement aider les industries australiennes de l'information, il devra se doter de protections compatibles avec les normes les plus rigoureuses du monde. »

⁴⁵⁴ Privacy Commissioner in Australia, *Information Privacy in Australia: A National Scheme for Fair Information Practices in the Private Sector* (août 1997), http://www2.austlii.edu.au/itlaw/national_scheme/national-INFORMAT.html.

⁴⁵⁵ Legal, Constitutional and Administrative Review Committee, *Privacy in Queensland: Issues Paper No. 2* (mai 1997), http://www.parliament.qld.gov.au/committees/legalrev_issues_paper_2.html.

étudié divers régimes de réglementation mais leur adoption demeure aléatoire à la suite du rejet de la loi qui avait été envisagée par le Commonwealth d'Australie⁴⁵⁶ pour le secteur privé. Le Queensland étudie, quant à lui, une loi en matière de confidentialité. Un document de travail émis par le Queensland Legal, Constitutional and Administrative Review Committee envisage plusieurs options permettant d'optimiser le facteur de protection.⁴⁵⁷

⁴⁵⁶ *Ibid.*

⁴⁵⁷ *Ibid.* Les options étudiées dans le document de travail sont les suivantes : on pourrait avoir un délit créé par une loi, ce qui permettrait aux personnes lésées d'intenter un procès pour atteinte au respect de la vie privée, mais il y aurait là certaines difficultés à définir comme il se doit le concept de vie privée. Autrement, on pourrait demander à un Commissaire à la protection de la vie privée ou encore à un comité de faire l'ébauche de codes de conduite, de les recommander, puis d'enquêter sur les plaintes reçues. La mise en application des Information Privacy Principles pourrait revêtir un aspect administratif (auquel cas, ces directives ne s'appliqueraient qu'au secteur public) ou un aspect législatif (leur portée serait alors élargie de manière à recouvrir le secteur privé également). La protection de la vie privée pourrait revêtir la forme d'une autoréglementation au moyen des codes de conduite, option qui ne garantit pas cependant la mise en application de ces codes. Le document de travail ne formule pas de recommandations mais il précise que la démarche État à État risque de s'avérer lourde, onéreuse et peu propice aux échanges de données transfrontières.

V. Protection de la vie privée, pouvoirs constitutionnels et collaboration entre le gouvernement fédéral et les provinces

Introduction

La Partie V traite des pouvoirs constitutionnels en matière de protection de la vie privée au Canada. Elle évalue les positions des instances fédérales et provinciales qui se disputent les pouvoirs en matière de protection de la vie privée, et en conclut que ces pouvoirs sont probablement répartis aux deux échelons de gouvernement. Par la suite, cette partie aborde quelques modèles conceptuels et historiques de la collaboration entre gouvernement fédéral et gouvernements provinciaux, modèles susceptibles d'éclairer une démarche commune menant à la réglementation de la confidentialité.

Pouvoirs constitutionnels en matière de protection de la vie privée

Tout au long de la présente étude sur le secteur des services financiers au Canada, le rôle de la Constitution canadienne et de la répartition des pouvoirs constitutionnels est sous-jacent. Et nous ajoutons à cette combinaison délicate une analyse du pouvoir par rapport au respect de la vie privée *en soi*. Ainsi, on peut dire que, pour l'essentiel, le gouvernement fédéral dispose de certains pouvoirs à l'endroit des banques puisque celles-ci sont des institutions purement fédérales. Les banques seront donc moins touchées que les autres institutions par les lois provinciales. Le gouvernement fédéral a le pouvoir d'incorporer et de réglementer les assureurs, les sociétés de fiducie, les sociétés de prêts et les associations coopératives de crédit. L'exploitation et le fonctionnement de ces institutions sont également soumis à de nombreux règlements provinciaux. Certains prestataires de services financiers ne sont nullement touchés par la réglementation des institutions financières et sont donc uniquement soumis aux lois commerciales génériques qu'on retrouve dans chaque province. Il en découle que certains prestataires de services financiers tombent sous le coup de la réglementation de la confidentialité imposée en vertu des lois sur les institutions financières fédérales, d'autres sont touchés par la réglementation provinciale, s'il y a lieu, et d'autres enfin ne sont nullement touchés par la réglementation du respect de la vie privée, sauf bien sûr s'ils se trouvent en sol québécois.

Le gouvernement fédéral envisage de promulguer des lois pour réglementer la confidentialité en général, ce qui devrait normalement toucher le secteur des services financiers. On peut donc se demander dans quelle mesure le gouvernement fédéral a les pouvoirs nécessaires pour mettre en œuvre ce genre de loi, ou encore s'il sera en mesure de le faire en collaboration avec les provinces.

Certains commentateurs dignes de foi ont indiqué que, à leurs yeux, le gouvernement fédéral ne disposait pas des pouvoirs nécessaires pour édicter des lois sur la protection de la vie privée, même dans les secteurs qui relèvent de sa compétence, comme les banques ou les sociétés de fiducie et sociétés d'assurances incorporées à l'échelon fédéral. D'après nous, cela semble être une exagération, mais à peine.

Articles 91 et 92 de la *Loi constitutionnelle*

Il n'est pas facile de circonscrire les compétences fédérales et provinciales en matière de protection de la vie privée en général, et en matière de protection de la vie privée par les institutions financières en particulier : les rubriques de compétences figurant dans les articles 91 et 92 de la *Loi constitutionnelle* ne contiennent rien qui permette de cerner nettement et sûrement le concept de vie privée, que ce soit dans un sens général ou dans le contexte spécifique des services financiers.⁴⁵⁸ Rien dans l'essence de la vie privée ne permet de rattacher cette réalité à une compétence fédérale ou provinciale, étant donné qu'il s'agit là d'un domaine qui transcende les démarcations et qui a des applications dans différents domaines d'activité – ce qui contraste avec les catégories plus fines qu'on retrouve dans la *Loi constitutionnelle*.⁴⁵⁹

Dans la mesure où des renseignements confidentiels sont divulgués aux banques, on peut dire que celles-ci sont du ressort fédéral, entrant dans la catégorie « Les banques, l'incorporation des banques et l'émission du papier-monnaie » [art. 91(15)]; « Les caisses d'épargne » [art. 91(16)]; L'incorporation fédérale des compagnies en vertu de lois fédérales régissant implicitement les travaux et entreprises qui débordent du cadre provincial [art. 92(10)]; « La réglementation du trafic et du commerce » [art. 91(2)]; ou même La loi criminelle [art. 91(27)]. Le gouvernement fédéral a également des pouvoirs en matière de protection de la vie privée dans le secteur public fédéral. On peut donc dire sans trop risquer de se tromper que les lois fédérales sur la protection de la vie privée sont subordonnées à l'une ou l'autre des rubriques de compétence précitées; ou, pour reprendre la formule de Laskin JA (qui occupait alors ces fonctions), qu'elles démontrent une « relation rationnelle et fonctionnelle » avec un ou plusieurs pouvoirs fédéraux énumérés dans l'article 91 (et dans l'art. 92).⁴⁶⁰

Toutefois, cela ne signifie pas que les rubriques de compétence provinciale énumérées à l'article 92 ne peuvent s'appliquer. Le meilleur exemple en matière de pouvoirs provinciaux serait celui de « La propriété et les droits civils de la province » [art. 92(13)], qui devrait logiquement en venir à s'appliquer aux données confidentielles, comme s'il s'agissait d'une propriété personnelle incorporelle, ou à la vie privée, droit privé exécutoire, comme l'envisage l'article 92(13). Cette rubrique de compétence a servi à confirmer la validité constitutionnelle des lois assurant la protection du consommateur, cadre législatif dont font certainement partie les lois assurant la protection de la vie privée.⁴⁶¹ Il existe également une compétence provinciale

⁴⁵⁸ *Loi constitutionnelle*, 1982.

⁴⁵⁹ *Union Colliery Co. c. Bryden* [1899] A.C. 580 (P.C.), p. 587, par Lord Watson.

⁴⁶⁰ *Papp c. Papp*, [1970] 1 O.R. 331 (Ont. C.A.), p. 336.

⁴⁶¹ *Irwin Toy c. Québec*, [1989] 1 R.C.S. 927, p. 953.

quant à « Généralement toutes les matières d'une nature purement locale ou privée dans la province » [art. 92(16)], même si ce genre de catégorie peut être difficile à gérer vu que, dans presque toutes les situations, un problème particulier de confidentialité pourrait très bien cesser d'être circonscrit à l'échelle locale ou purement provinciale. On pourrait également dire que les lois provinciales sur la protection de la vie privée sont subordonnées ou, à tout le moins, logiquement liées à « L'incorporation des compagnies pour des objets provinciaux » [art. 92(11)], notamment les sociétés d'assurances, sociétés de fiducie ou de prêts, ou associations coopératives de crédit ayant été incorporées par les provinces. Là encore, on ne saurait conclure que la protection de la vie privée relève strictement des instances provinciales, lorsqu'interviennent des éléments au moins aussi marquants que ceux qui figurent aux articles 91 et 92.

La compétence peut être « double », c'est-à-dire qu'on pourra voir intervenir autant le Parlement fédéral que les législatures provinciales.⁴⁶² Exemple de cet état de chose, les infractions au code de la route, dans un contexte où les provinces disposent de leurs propres lois alors même que le *Code criminel* fédéral est lui aussi mis à contribution. Autres secteurs de double juridiction : l'insolvabilité, la réglementation des valeurs mobilières (d'ordinaire, une question de ressort provincial, mais aussi soumise à des sanctions criminelles du fédéral), les pensions alimentaires du conjoint, et la garde des enfants. Dans chacun de ces exemples, deux compétences s'exercent de front, sans que cela n'entraîne trop de conflits. Dans certains cas, il peut s'avérer impossible de respecter simultanément les lois des deux paliers de gouvernement; la primauté des lois fédérales pourra alors justifier un ressort strictement fédéral.⁴⁶³ Selon nous, cela risque peu de se produire dans le cas de la réglementation de la confidentialité.⁴⁶⁴

Pouvoirs fédéraux en matière de trafic et de commerce

Il serait fort surprenant que le gouvernement central parvienne à régler le respect de la vie privée dans les services financiers en en faisant une question de ressort purement fédéral. Toute tentative en ce sens mettrait probablement à contribution les pouvoirs fédéraux en matière économique, pouvoirs indiqués à l'article 91. Le premier de ces pouvoirs fédéraux concerne « La réglementation du trafic et du commerce » [art. 91(2)], mais on notera que ce pouvoir a été restreint de manière à éviter tout conflit avec « le pouvoir de légiférer les contrats dans un secteur d'activité particulier, notamment pour ce qui est des assurances-incendie dans une province en particulier ».⁴⁶⁵ Si cette tension entre pouvoirs fédéraux en matière de trafic et de commerce, et pouvoirs provinciaux en matière de propriété et de droits civils, on accepte généralement bien que les pouvoirs en matière de trafic et de commerce s'appliquent aux échanges interprovinciaux et internationaux, ainsi qu'à ce que Sir Montague Smith a qualifié de « réglementation générale

⁴⁶² *Hodge c. The Queen*, (1883) 9 App. Cas. 117 (P.C.), p. 130, par Sir Barnes Peacock.

⁴⁶³ Voir Peter Hogg, *Constitutional Law of Canada* (Toronto, 1997), pp. 15-11 à 15-12 et 16-1 à 16-6.

⁴⁶⁴ Pour de plus amples renseignements à ce sujet, voir la rubrique (d) Conclusion ci-dessous, dans la Partie V.

⁴⁶⁵ *Citizens' Insurance Co. c. Parsons* (1881) 7 App. Cas. 96 (P.C.), p. 113, par Sir Montague Smith.

du commerce touchant l'ensemble du Dominion »⁴⁶⁶ (*Citizens' Insurance Co. c. Parsons*). Étant donné que la problématique de la confidentialité dans les services financiers ne sera sans doute pas confinée à des entités ou des transactions purement provinciales, on pourrait logiquement s'attendre à ce que le gouvernement fédéral use des pouvoirs en matière de trafic et de commerce pour justifier une compétence exclusive en matière de confidentialité pour tout ce qui est échanges interprovinciaux; par ailleurs, il y a aussi de fortes probabilités qu'on aboutisse à une compétence mixte, selon la classification de la propriété et du droit civil. Sur un autre plan, on notera que les tribunaux ne semblent pas encore vouloir élargir au maximum les pouvoirs en matière de trafic et de commerce. L'application de ces pouvoirs, dans le domaine du trafic interprovincial (la première composante dans *Parsons*) a été récemment rejetée à deux reprises par la Cour suprême.⁴⁶⁷ Et, en tant que pouvoirs de réglementation économique en général (la deuxième composante de *Parsons*), l'option a été presque systématiquement rejetée.⁴⁶⁸ Dans l'affaire *MacDonald c. Vapor Canada*, Laskin CCM a énoncé trois critères pour l'application des pouvoirs généraux en matière de trafic et de commerce : 1) la présence d'un mécanisme de réglementation général; 2) la surveillance par une entité de réglementation; 3) un intérêt envers le trafic en général et non un secteur d'activité en particulier.⁴⁶⁹ À ces trois critères, Dickson CCM en a rajouté deux autres, lors de l'affaire *General Motors c. City National Leasing* : 4) la loi envisagée devrait être telle que les provinces ne pourraient, individuellement ou conjointement, être capables d'agir constitutionnellement; 5) le défaut de faire participer une ou plusieurs provinces ou localités dans le cadre législatif envisagé pourrait remettre en question le bon fonctionnement de ce cadre dans d'autres parties du pays.⁴⁷⁰ Dans le cas d'une réglementation sur la protection de la vie privée dans le secteur des services financiers, seul le premier critère interviendrait. Plus important encore, la difficulté de démontrer que les provinces seraient incapables sur le plan constitutionnel de mettre en œuvre une loi dans ce domaine, étant donné tous les pouvoirs qu'elles détiennent en matière de propriété et de droits civils. Et, compte tenu de la possibilité d'une collaboration entre les instances fédérales et provinciales, on peut difficilement dire qu'un cadre législatif concernant la collecte, le stockage et la divulgation de renseignements personnels serait réellement mis en danger si le gouvernement fédéral n'en avait pas la compétence exclusive.

Paix, ordre et bon gouvernement

Autre option pour le gouvernement fédéral, affirmer que les pouvoirs exclusifs en matière de réglementation sur la protection de la vie privée, que ce soit en général ou de façon plus particulière dans le secteur des institutions financières, s'inscrivent dans la catégorie des pouvoirs

⁴⁶⁶ *Ibid.*; voir également : *Re Farm Products Marketing Act* [1957], R.C.S. 198, pp. 211-212.

⁴⁶⁷ *Dominion Stores c. La Reine*, [1980] 1 R.C.S. 844; et *Brasseries Labatt c. P.g. du Canada*, [1980] 1 R.C.S. 844, p. 866. Voir également l'étude de ces cas dans Hogg, *supra*, note 463, pp. 20-9 à 20-10.

⁴⁶⁸ Voir : *A.-G. Ontario c. A.-G. Canada*, [1937], A.C. 405 (P.C.); *Dominion Stores c. La Reine*; *Brasseries Labatt c. P.g. du Canada*; *MacDonald c. Vapor Canada*, [1977] 2 R.C.S. 134; *General Motors c. City National Leasing* [1989], 1 R.C.S. 641.

⁴⁶⁹ *MacDonald c. Vapor Canada*, *supra*, note 468, p. 661.

⁴⁷⁰ *General Motors c. City National Leasing*, *supra*, note 468, p. 679.

du Parlement fédéral « de faire des lois pour la paix, l'ordre et le bon gouvernement du Canada, relativement à toutes les matières ne tombant pas dans les catégories de sujets par la présente loi exclusivement assignés aux législatures des provinces... » (art. 91). Comme on l'a déjà dit précédemment, la protection de la vie privée n'est pas *exclusivement* du ressort des provinces, ce qui, en théorie, permettrait l'exercice des pouvoirs résiduels fédéraux concernant la paix et l'ordre ainsi que le bon gouvernement (*Peace, Order and Good Government*, ou « **POGG** »).

Le premier élément des pouvoirs POGG correspond aux pouvoirs d'urgence, peu pertinents ici, étant donné qu'on voit mal comment la réglementation du flux des données confidentielles pourrait finir par devenir une urgence nécessitant la mise en œuvre des pouvoirs POGG.⁴⁷¹

Le second élément des pouvoirs POGG correspond au facteur des « lacunes », facteur pouvant servir à justifier la mise en place de pouvoirs fédéraux pour combler une lacune dans la distribution des pouvoirs entre le Parlement fédéral et les législatures provinciales.⁴⁷² Cet élément POGG a déjà servi à circonscrire des pouvoirs dans des domaines qui ne sont pas énoncés expressément dans l'article 91 ou l'article 92, notamment dans les domaines de l'aéronautique, de l'énergie atomique ou des questions touchant à la région de la capitale nationale, ou encore pour lever certaines incohérences dans le texte de la *Loi constitutionnelle* elle-même (ex. : la référence aux compagnies avec « objets provinciaux », à l'article 92(10) sans qu'il y ait de pendant sous forme de compagnies avec objets fédéraux dans l'article 91).⁴⁷³ Peter Hogg note toutefois que l'élément dit « lacunaire » s'applique à « un nombre réduit de cas inusités » mais qu'il ne peut s'appliquer lorsque ce qui fait l'objet de la loi est tout simplement une nouveauté :

Dans la plupart des cas, un type de loi qui est « nouveau » ou qui n'a pas encore été reconnu ne peut pas nécessairement ou logiquement justifier l'application du principe POGG. On pourrait plutôt faire intervenir les critères de la propriété et des droits civils dans la province [art. 92(13)] ou les matières d'une nature purement locale ou privée dans la province [art. 92(16)]. Le choix des bonnes rubriques de compétence sera fait en fonction de la nature des matières « nouvelles », ainsi que de la portée conférée aux différentes rubriques de compétence, dont le facteur POGG ne représente qu'une manifestation parmi d'autres.⁴⁷⁴

⁴⁷¹ Au sujet des pouvoirs d'urgence, se reporter à Hogg, *supra*, note 463, pp. 17-18 à 17-27.

⁴⁷² *Citizens' Insurance c. Parsons; Re Regulation and Control of Radio Communication in Canada*, [1932] A.C. 304 (P.C.), p. 312.

⁴⁷³ *Johannesson c. West St. Paul*, [1952] 1 R.C.S. 292; *Ontario Hydro c. Ontario*, [1993] 3 R.C.S. 327; *Munro c. Commission de la capitale nationale*, [1966] R.C.S. 663.

⁴⁷⁴ Hogg, *supra*, note 463, p. 17-7.

Le troisième élément POGG concerne la « dimension nationale » ou l'« importance nationale ». ⁴⁷⁵ Dans l'affaire de la *Canada Temperance Foundation*, Viscount Simon devait indiquer que l'« épreuve réelle » pour cet élément POGG se retrouverait :

dans la matière réelle de la loi : s'il s'agit d'une matière qui transcende les intérêts et les enjeux purement provinciaux pour devenir, de manière intrinsèque, une question touchant le Dominion dans son ensemble... alors, cette matière sera du ressort du Parlement du Dominion, une affaire concernant la paix, l'ordre et le bon gouvernement du Canada, même si elle touchait par endroits des matières relevant spécifiquement des législatures provinciales. ⁴⁷⁶

L'élément « importance nationale » renvoie à une matière qui « intéresse toutes les parties du Canada ». ⁴⁷⁷ Hogg précise cependant qu'il ne suffit pas de vouloir uniformiser des lois pour pouvoir évoquer le principe de l'importance nationale, sauf dans des cas où cette uniformisation s'impose du fait de l'incapacité des provinces à régler le problème, ou encore lorsque le caractère hétéroclite des différents régimes provinciaux pourrait s'avérer néfaste. ⁴⁷⁸ On sait que les lois sur la protection de la vie privée diffèrent grandement d'une province à l'autre (par exemple, le Québec est la seule province à réglementer cette protection au-delà du secteur public); toutefois, on pourrait très bien dire que les différences d'approche ne nuiront pas nécessairement aux mesures de protection de la vie privée prises à l'échelon national. Il est probable que le manque d'homogénéité ne constituera pas un problème d'importance nationale; sans doute pourra-t-il être atténué grâce à la collaboration entre les différents appareils juridiques.

Dans la référence *Loi anti-inflation*, le juge Beetz devait soutenir que, advenant une situation d'importance nationale, le facteur POGG pourrait s'appliquer uniquement lorsqu'on a affaire à une « matière » suffisamment distincte, et non à un sujet de préoccupation vaguement défini. ⁴⁷⁹ À la source *Crown Zellerbach*, le juge Le Dain apportait la précision ci-dessous :

Pour qu'une matière soit dite d'importance nationale... il faut qu'on y retrouve les critères d'unicité, de spécificité et d'indivisibilité qui la distingueront clairement des matières d'importance provinciale, ainsi qu'une marge d'impact sur les lois de la province qui puisse être compatible avec la répartition fondamentale des pouvoirs législatifs en vertu de la Constitution. ⁴⁸⁰

⁴⁷⁵ *Russell c. The Queen* (1882) 7 App. Cas. 829 (P.C.); *A.-G. Ontario c. A.-G. Canada*, [1896] A.C. 348 (P.C.); *A.-G. Ontario c. Canada Temperance Foundation*, [1946] A.C. 193 (P.C.); *Johannesson c. West St. Paul*, [1952] 1 R.C.S. 292; *Munro c. Commission de la capitale nationale*, [1966] R.C.S. 663; *La Reine c. Crown Zellerbach*, [1988] 1 R.C.S. 401.

⁴⁷⁶ *A.-G. Ontario c. Canada Temperance Foundation*, *supra*, note 475, pp. 205-206.

⁴⁷⁷ Hogg, *supra*, note 463, pp. 17-12 à 17-13.

⁴⁷⁸ *Ibid.*

⁴⁷⁹ *Concernant la Loi anti-inflation*, [1976] 2 R.C.S. 373, pp. 457-458.

⁴⁸⁰ *Crown Zellerbach*, *supra*, note 475, p. 432.

Il en découle que le facteur d'importance nationale ne peut servir simplement à permettre l'élargissement des pouvoirs fédéraux lorsque le gouvernement central entrevoit régler ainsi un problème aux implications profondes en dépit de la compétence des provinces en la matière.⁴⁸¹ S'il fallait que le facteur POGG soit ainsi exploité, *la totalité* des pouvoirs provinciaux seraient remis en cause.

Dernier critère permettant de satisfaire à l'élément d'importance nationale : la nouveauté. Pour reprendre les mots du juge Pigeon, dans *La Reine c. Hauser*,

... point essentiel pour faire de la Loi sur les stupéfiants une conséquence des pouvoirs résiduels du gouvernement fédéral (c'est-à-dire le facteur POGG) : il s'agit là d'une loi adoptée en fin de compte pour faire face à un problème réellement nouveau qui n'existait pas au moment de la signature de l'acte constitutionnel, et qui ne peut évidemment pas entrer dans la catégorie « Matières d'une nature purement locale ou privée »⁴⁸²

— ou, sans doute, dans la classe de la propriété et des droits civils dans la province. Hogg précise d'ailleurs au moyen d'une annotation qu'il entend par *nouveauté* une nouveauté conceptuelle plutôt qu'historique.⁴⁸³ Il conclut, soit dit en passant, que la doctrine de la « nouveauté » est peu pertinente et peu utile pour ce qui est de reconnaître les champs d'application propres aux pouvoirs résiduels du gouvernement central; toutefois, la décision prise par le juge Pigeon continue de faire autorité. S'il est vrai que les textes de loi provinciale en matière de protection de la vie privée ainsi que les préoccupations du public à l'endroit d'éventuels abus sont relativement récents (une protection juridique de ce genre aurait sans doute paru bizarre en 1867), on est en droit de se demander si ce genre de loi constitue, sur le plan conceptuel, une matière nouvelle (comparer avec l'énergie atomique). Il serait peut-être plus juste de dire que certaines initiatives récentes tendent à élargir l'application des normes en matière de confidentialité jusque dans de nouveaux domaines d'application, mais ne constituent pas un besoin qu'on pourra juger, en soi, nouveau. Il devient donc difficile d'affirmer que la loi sur la confidentialité, loi générique ou loi spécifique traitant des institutions financières, ne peut absolument pas entrer dans la catégorie des « Matières d'une nature purement locale ou privée », pour reprendre les mots de Monsieur le juge Pigeon, ni dans celle de « La propriété et les droits civils dans la province ».

Conclusion

Compte tenu que la *Loi constitutionnelle* de 1982 n'attribue pas clairement les champs de compétence pour ce qui est de la protection de la vie privée en général (pour ne pas dire de la vie privée dans le contexte des institutions financières), il pourrait y avoir partage de compétences dans ce domaine, notamment entre les échelons de gouvernement fédéral et provinciaux. Il serait encore plus juste d'affirmer qu'il s'agit là d'une affaire de ressort purement provincial, sauf en ce

⁴⁸¹ W.R. Lederman, « Unity and Diversity in Canadian Federalism » (1975) 53 *La revue du barreau canadien* 597.

⁴⁸² [1979] 1 R.C.S. 984, pp. 1000-1001.

⁴⁸³ Hogg, *supra*, note 463, p. 17-17.

qui a trait au secteur de la fonction publique fédérale. Comme on a pu le voir, l'un ou l'autre palier de gouvernement pourrait invoquer les rubriques de compétence énumérées dans les articles 91 et 92. Du point de vue fédéral, il s'agit là d'éléments reliés spécifiquement aux banques et aux activités bancaires, aux entreprises incorporées par des instances fédérales et à d'autres travaux et entreprises dont le cadre déborde celui des provinces, des banques, de la loi criminelle, ainsi que du trafic et du commerce; par contre, selon l'optique provinciale, il s'agit de l'incorporation de compagnies pour des objets provinciaux, de la propriété et des droits civils dans la province, et de matières d'une nature purement locale ou privée dans la province.

Le gouvernement fédéral pourrait chercher à réglementer la protection de la vie privée en en faisant un domaine exclusif, soit par le biais du pouvoir économique qu'il détient en matière de trafic et de commerce, soit en faisant intervenir la composante de l'importance nationale, en ce qui a trait aux pouvoirs résiduels fédéraux (POGG). Quoiqu'il en soit, les limites judiciaires qui restreignent l'élargissement des pouvoirs fédéraux par l'un ou l'autre de ces moyens empêcheraient probablement Ottawa de revendiquer l'exclusivité de la compétence. Du point de vue pratique et politique, le gouvernement du Canada hésiterait sans doute à passer pour un usurpateur de pouvoirs déjà inscrits dans les textes de loi provinciaux, pouvoirs dont on ne pourra démontrer ni l'inadéquation ni l'interférence avec de légitimes projets fédéraux en matière de confidentialité. Si la protection de la vie privée doit, de manière générale, être assurée, cela se fera dans le cadre d'une collaboration entre les instances fédérales et provinciales, étant donné que les deux échelons de gouvernement ont des préoccupations légitimes en la matière, et compte tenu du fait que le flux des données confidentielles ne respecte pas les frontières et qu'il nécessite par conséquent une démarche de collégialité.⁴⁸⁴

Pour ce qui est maintenant du secteur des services financiers, le gouvernement peut réglementer les entreprises qui relèvent des instances fédérales. Cela se justifie parfaitement dans le secteur bancaire, en ce sens que même si la protection de la vie privée semble être de compétence provinciale, il existe aussi un élément inhérent à la réglementation bancaire; d'autant plus que l'intrusion fédérale dans l'affaire de compétence provinciale semble justifiée du fait qu'elle ne sera que marginale. Autre exemple pertinent, celui de la *Loi sur les télécommunications*, qui réglemente la protection de la vie privée par rapport aux sociétés de télécommunications. Il est possible que la réglementation de type « inforoute », qui fait nécessairement appel à des installations de télécommunications et à des échanges commerciaux multijuridictionnels, justifie l'élargissement du champ de réglementation; il est cependant improbable que ladite

⁴⁸⁴ Pour certains modèles de collaboration entre les gouvernements fédéral et provinciaux, voir « Some Lessons in Federal-Provincial Legislative Cooperation » et « Uniform Law Conference Privacy Act Deliberations » dans Ian Lawson, *Privacy and the Information Highway: Regulatory Options for Canada* (Industrie Canada, 1996), dont le texte peut être consulté à l'adresse suivante : <http://strategis.ic.gc.ca/SSG/ca00265e.html>. Voir également : William A.W. Neilson, « Interjurisdictional Harmonization of Consumer Protection Laws and Administration in Canada » dans Ronald C.C. Cuming, éd., *Perspectives on the Harmonization of Law in Canada: Collected Research Studies of the Royal Commission on the Economic Union and Development Prospects for Canada* (Toronto, 1985), pp. 76-87.

réglementation s'étend à chaque entité faisant la collecte de données. Résultat : le gouvernement fédéral semble uniquement prêt à légiférer dans les sphères qui relèvent de sa compétence.

Modèles pour une collaboration entre les instances fédérales et provinciales

Dans un État unitaire, comme la Nouvelle-Zélande ou le Royaume-Uni, il est assez simple de réglementer la protection de la vie privée. Ce qui n'est pas le cas dans un système fédéral, où cette protection touche une grande variété de secteurs commerciaux de même que différentes compétences constitutionnelles. L'étude comparative du fédéralisme a permis d'établir un certain nombre de modèles pour la collaboration entre les échelons national et infranational, qui seront succinctement décrits ci-dessous.

Le premier modèle prend l'État unitaire comme point de départ, en affirmant le droit du gouvernement national à des revendications de compétence face à ce qui, au Canada, correspondrait à l'échelon provincial. Au Canada, cela ne s'appliquerait que difficilement, et ne pourrait se réaliser que par le biais de certains principes constitutionnels étudiés dans la section précédente : les pouvoirs économiques d'ordre général que le gouvernement fédéral détient en matière de réglementation du trafic et du commerce, les pouvoirs résiduels en matière de « paix, ordre et bon gouvernement », ou la doctrine de la primauté des lois fédérales.⁴⁸⁵ Les secteurs d'activité dans lesquels le gouvernement fédéral a affirmé une compétence exclusive incluent l'énergie atomique et l'aéronautique. Il est également possible que le gouvernement du Canada cherche à imposer des normes nationales dans des secteurs dont la réglementation est autrement laissée aux provinces, notamment le domaine de la santé. Ce que Ronald C.C. Cuming nomme « harmonisation instituée ».⁴⁸⁶ Ce modèle de relations fédéral-provincial était peut-être courant dans les années soixante-dix et quatre-vingt, qui avaient vu, pour reprendre les mots de Patrick Monahan, un fédéralisme « hiérarchique » ou « unilatéral », contrairement à la démarche collégiale adoptée dans les années soixante.⁴⁸⁷ Gérald A. Beaudoin note également l'alternance entre les formes tantôt centraliste tantôt décentralisante du fédéralisme dans l'histoire récente du Canada.⁴⁸⁸ Certes, l'exercice des pouvoirs fédéraux serait souhaitable du point de vue de l'uniformité de la réglementation, de la facilité d'administration et de la centralisation du

⁴⁸⁵ Se reporter à la Partie V, sous la rubrique « Pouvoirs constitutionnels en matière de protection de la vie privée », sous-rubrique « Paix, ordre et bon gouvernement ».

⁴⁸⁶ Ronald C.C. Cuming, *Harmonization of Law in Canada: An Overview*, dans Ronald C.C. Cumming, éd., *Perspectives on the Harmonization of Law in Canada: Collected Research Studies of the Royal Commission on the Economic Union and Development Prospects for Canada* (Toronto, 1985), pp. 25-28. Voir également : William A.W. Neilson, *Interjurisdictional Harmonization of Consumer Protection Laws and Administration in Canada*, dans Ronald C.C. Cumming, éd., *Perspectives on the Harmonization of Law in Canada: Collected Research Studies of the Royal Commission on the Economic Union and Development Prospects for Canada* (Toronto, 1985), p. 88.

⁴⁸⁷ Patrick Monahan, *The Charter, Federalism and the Supreme Court of Canada* (Toronto, 1987), pp. 144-149.

⁴⁸⁸ Voir Gérald A. Beaudoin, « Fédérations et confédérations », dans *Essais sur la Constitution* (Ottawa, 1979), p. 67.

processus décisionnel, mais un certain nombre de raisons militent contre une telle démarche empruntée du concept de l'État unitaire, et qui pourrait s'avérer indésirable ou inefficace. Dans un premier temps, les possibilités d'affirmation d'une exclusivité des pouvoirs fédéraux sont limitées par certains facteurs de restreinte dans le système juridique, facteurs déjà abordés plus tôt dans la présente partie. Ces limitations font que les velléités de centralisation des pouvoirs n'aboutiront pas, faute d'arguments réellement convaincants. Deuxième facteur, sans doute plus important, une telle approche pourrait envenimer les relations entre l'État fédéral et ses homologues provinciaux; on notera toutefois que même un système très collégial peut dégénérer pour sombrer dans la querelle et la chicane, et ne pas produire de consensus. De plus, l'harmonisation passe par la capacité de convaincre plutôt que par le pouvoir de légiférer. Cette faculté de persuasion est directement liée aux cordons de la bourse fédérale, comme c'est le cas actuellement dans le dossier de la santé. Il faut cependant noter que la capacité du gouvernement fédéral d'instaurer des normes en matière de santé diminue rapidement et corrélativement aux paiements de transfert. Or, nous ne voyons aucune raison ou justification qui permette de rattacher des paiements de transfert à l'établissement de lois en matière de protection de la vie privée.

Contrairement à la démarche hiérarchique ou unilatérale, le principe de « subsidiarité » adopté par les communautés européennes pourrait être pertinent au fédéralisme : il s'agit du principe selon lequel les pouvoirs reviendraient, en fonction de l'efficacité, à l'échelon national (ou local) plutôt qu'à l'échelon supranational.⁴⁸⁹ Contrairement au modèle de fédéralisme hiérarchique ou centraliste, les systèmes fédéraux pourraient opter pour une plus grande autonomie des entités subordonnées, à tel point d'ailleurs que la fédération pourrait se transformer en une confédération plus souple, composée essentiellement d'entités souveraines avec (le plus souvent) des liens économiques.⁴⁹⁰ À défaut de confédération, il existe d'autres formes de fédéralisme décentralisé, notamment le modèle asymétrique, qui confère à certaines sous-parties des pouvoirs plus importants qu'à d'autres sous-parties du même échelon (ainsi, la Bavière, qui dispose de pouvoirs étrangers aux autres *Länder* au sein de la République fédérale d'Allemagne).⁴⁹¹ Le fédéralisme asymétrique peut mener à l'avènement d'une autre variante, dite fédéralisme concurrentiel, en vertu de laquelle les territoires constituants peuvent établir leurs propres normes et se livrer à la concurrence de façon à attirer les industries, les investissements ou les

⁴⁸⁹ Voir Direction générale aux Affaires économiques et financières de la Commission des Communautés européennes, « One Market, One Money », *European Economy*, vol. 44 (octobre 1990), p. 33, cité dans Thomas J. Courchene, *In Praise of Renewed Federalism* (Institut C.D. Howe, The Canada Round: A Series on the Economics of Constitutional Renewal, No. 2) (Toronto et Calgary, 1991), p. 7; Peter M. Leslie, *The Maastricht Model: A Canadian Perspective on the European Union* (Kingston, Ontario, 1996), pp. 59-60.

⁴⁹⁰ Beaudoin, supra, note 488, pp. 65-74.

⁴⁹¹ *Ibid.* Voir également : Preston King, *Federalism and Federation* (Baltimore, 1982), pp. 24-38 et 38-55; Richard Simeon et Mary Janigan, éd., *Toolkits and Building Blocks: Constructing a New Canada* (Toronto et Calgary, 1991), pp. 120-122, 123-129, 133-139, 142-181; Bertus de Villiers, éd., *Evaluating Federal Systems* (Dordrecht, Boston et Londres, 1994); Daniel J. Elazar, éd., *Federal Systems of the World: A Handbook of Federal, Confederal and Autonomy Arrangements*, 2^e édition (Harlow, Essex, 1994).

immigrants.⁴⁹² Une certaine décentralisation serait compatible avec les six autres modèles de collaboration entre instances fédérales et provinciales dégagés par Cuming, modèles qui seront succinctement abordés plus loin. La protection de la vie privée est une problématique intéressante en ce sens qu'elle concerne les droits de chaque citoyen; il serait donc probable qu'elle puisse être traitée à l'échelon local, conformément aux normes en vigueur dans la communauté. Ce qui contredit parfaitement l'objectif de rentabilité économique. Par conséquent, la balance pourrait pencher en faveur de normes nationales, voire supranationales. Selon nous, il y a fédéralisme compétitif du moment que le Québec promulgue ses propres lois pour assurer de manière exhaustive la protection de la vie privée. Dans le modèle de fédéralisme concurrentiel, les pouvoirs en place se disputent les avantages offerts, notamment l'augmentation des recettes publiques ou certains profits politiques, comme de l'emploi pour l'électorat. On voit difficilement ce que le Québec aurait à gagner d'une loi particulière en matière de confidentialité; aucune province ne semble vouloir assumer un leadership dans ce domaine. Sans doute, la protection de la vie privée constituera un facteur qui revêt un certain intérêt, mais elle ne devrait pas jouer un rôle particulièrement significatif.

Le deuxième modèle de Cuming est celui de la législation à effet miroir, en vertu de laquelle l'échelon de gouvernement national promulgue des lois d'ensemble qui seront dupliquées par les échelons inférieurs (provinces ou États) puis administrées par une autorité réglementante commune.⁴⁹³ Le Canada a tenté d'adopter ce modèle dans le domaine des télécommunications, et il serait peut-être en train de le faire maintenant en ce qui a trait à la réglementation des valeurs

⁴⁹² Le débat sur le fédéralisme concurrentiel (source de nivellement par la base?, c'est-à-dire uniformisation des lois en fonction des critères les moins élevés) a eu cours aux États-Unis, pour les chartes d'entreprises et, dans une bien moindre mesure, au Canada. Voir : W.L. Cary, « Federalism and Corporate Law: Reflections upon Delaware » (1974), 83 *Yale Law Journal* 663; R. Romano, « The State Competition Debate in Corporate Law » (1987), 8 *Cardozo Law Review* 709; C.M. Tiebout, « A Pure Theory of Local Expenditures » (1956), 64 *J. Pol. Econ.* 416; R.K. Winter, « State Law, Shareholder Protection, and the Theory of the Corporation » (1977), 6 *Journal of Legal Studies* 251; P. Dodd et R. Leftwich, « The Market for Corporate Charters: 'Unhealthy Competition' versus Federal Regulation » (1980), 53 *Journal of Business Law* 259; F.H. Easterbrook, « Antitrust and the Economics of Federalism » (1983), 26 *Journal of Law & Economics*, 23; B. Baysinger et H. Butler, « The Role of Corporate Law in the Theory of the Firm » (1985), 28 *Journal of Law & Economics* 179; R. Romano, « Law as a Product: Some Pieces of the Incorporation Puzzle » (1985), 1 *J. Law Econ. & Org.* 225; J.R. Macey et G.P. Miller, « Toward an Interest-Group Theory of Delaware Corporate Law » (1987), 65 *Texas Law Review* 469; D.R. Fischel et al., « The Regulation of Banks and Bank Holding Companies » (1987), 73 *Virginia Law Review* 301; W.E. Oates et Robert M. Schwab, « Economic Competition among Jurisdictions: Efficiency Enhancing or Distortion Inducing? » (1988), 35, *J. Pub. Econ.* 333; Note, « To Form a More Perfect Union? – Federalism and Informal Interstate Competition » (1989), 102 *Harvard Law Review* 842; L.A. Bebchuk, « Federalism and the Corporation: The Desirable Limits on State Competition in Corporate Law » (1992), 105 *Harvard Law Review* 1435; R. Revesz, « Rehabilitating Interstate Competition: Rethinking the 'Race-to-the-Bottom' Rationale for Federal Environmental Regulation » (1992), 67 *New York University Law Review* 1210; R.J. Daniels, « Should Provinces Compete? – The Case for a Competitive Corporate Law Market » (1991), 36 *Revue de droit de McGill* 130, pp. 133-134; J.I. MacIntosh, « The Role of Interjurisdictional Competition in Shaping Canadian Corporate Law: A Second Look », *Law and Economics Working Paper Series 18* (Toronto, Faculté de droit, Université de Toronto, 1993). Voir également : Neil Guthrie, « A Good Place to Shop: Choice of Forum and the Conflict of Laws » (1995), 27 *Ottawa Law Review* 201, pp. 204-205.

⁴⁹³ Neilson, *supra*, note 486, pp. 89-90. Voir également : Lawson, *supra*, note 484.

mobilières, mais c'est là un dispositif qui, de façon générale, n'a pas réellement porté fruit au Canada. Par contre, l'Australie s'est dotée d'une bonne législation à effet miroir pour réglementer les entreprises et les valeurs mobilières, au niveau du gouvernement central et des gouvernements des différents États.⁴⁹⁴

Le modèle abstentionniste, troisième modèle, présuppose le choix exercé par un palier de gouvernement de ne pas intervenir dans une sphère d'activité en particulier, préférant laisser à l'autre échelon de gouvernement le soin de légiférer et de réglementer. On trouve un exemple de ce modèle dans les pratiques commerciales, pour lesquelles un certain nombre de provinces ne se sont pas dotées de lois, laissant ainsi le terrain libre à la *Loi sur la concurrence*.⁴⁹⁵

Avec le quatrième modèle, dit modèle contractuel, les échelons de gouvernement national et infranationaux négocient la répartition des pouvoirs avant de promulguer des lois, ce qui s'est produit notamment dans le domaine de l'agriculture.⁴⁹⁶ Une démarche voisine, la législation conditionnelle, prévoit que les échelons infranationaux aient une alternative, autrement dit le choix entre une loi fédérale et leur propre loi.⁴⁹⁷ Lorsqu'il n'y a pas de loi à l'échelon infranational (au niveau des provinces ou des États), c'est la loi fédérale qui s'applique automatiquement. C'est le cas, notamment, de certaines dispositions contenues dans la *Loi sur la concurrence*. L'inconvénient de la formule, c'est qu'elle peut sembler coercitive, comme devait le démontrer le bref épisode de la *Loi visant à assurer la protection des emprunteurs et déposants*.⁴⁹⁸ En effet, le gouvernement du Canada, inquiet du manque de cohérence dans les lois provinciales en matière de protection du consommateur, avait présenté en 1977 la *Loi visant à assurer la protection des emprunteurs et déposants*, pour uniformiser les critères nationaux. Toutefois, faute d'avoir suffisamment consulté les provinces et les institutions financières, il dut retirer cette loi, cédant ainsi aux critiques pour qui la loi empiétait abusivement sur les pouvoirs des provinces, faisait double emploi, semait la confusion et n'était pas fondée sur une consultation adéquate. Légère variante sur le thème du mode conditionnel serait le système dans lequel les provinces peuvent choisir de se retirer du cadre législatif fédéral plutôt que d'y adhérer, et donc de s'occuper de secteurs qui auraient été normalement dévolus à la sphère de compétence fédérale. On en trouve un exemple dans le système québécois de la fiscalité et des régimes de retraite, qui se substitue au mécanisme fédéral sur le territoire de la province. Avec ce genre d'entente, il est clairement possible d'appliquer aussi le modèle contractuel, étant donné que la négociation aura précédé l'établissement de structures formelles.⁴⁹⁹

⁴⁹⁴ Voir Neilson, *supra*, note 486, pp. 102-111.

⁴⁹⁵ *Ibid.*, p. 90.

⁴⁹⁶ *Ibid.*, p. 91.

⁴⁹⁷ *Ibid.*, pp. 91-92.

⁴⁹⁸ Pour un historique de ce projet de loi éphémère, se reporter à la référence Neilson, *supra*, note 486, pp. 76-82.

⁴⁹⁹ Voir l'étude de la question dans Courchene, *supra*, note 489, p. 88. Courchene voit là la base d'un fédéralisme renouvelé et décentralisé, axé sur la « concurrence avec la primauté des lois provinciales », pp. 86-92.

Un cinquième modèle, peut-être plus représentatif de l'expérience canadienne, serait celui des lois parallèles, dans lequel chaque palier de gouvernement établit ses lois sachant au départ que les autres instances pourraient en faire autant.⁵⁰⁰ Exemples : les domaines du droit des sociétés, de l'insolvabilité, du droit de la famille et des lois sur la forêt. Dans bien des cas, la double législation dans un domaine n'est pas source de conflit (ainsi, dans le droit des sociétés, ce sera soit la loi fédérale, soit la loi provinciale sur les sociétés par actions – « corporations » dans certaines provinces – qui s'appliquera, selon ce qui avait été choisi par l'organe d'incorporation). Dans d'autres cas, le chevauchement peut s'avérer problématique, au point de nécessiter l'application du principe de la primauté des lois fédérales pour résoudre les conflits entre les instances de gouvernement. Bien souvent, par contre, la concurrence entre appareils judiciaires différents s'avère bénéfique aux consommateurs.

Un dernier modèle de collaboration entre le gouvernement fédéral et les gouvernements provinciaux serait le modèle de partenariat (ou modèle de complémentarité), dans le cadre duquel la consultation interjuridictionnelle permettrait de coordonner les différentes lois.⁵⁰¹ Comme le note Ian Lawson, le mieux est alors de faire intervenir des groupes de travail réunissant des cadres supérieurs de la fonction publique, qui se réuniront pour harmoniser les lois et s'assurer que leur mise en application par les différents échelons de gouvernement puisse fonctionner.⁵⁰² Ronald C. Cuming appelle ce processus « harmonisation institutionnalisée »; il signale que cela pourrait être réalisé par des groupes de travail provenant d'organismes comme la Conférence sur l'uniformisation des lois du Canada, l'Association du barreau canadien, les commissions fédérale et provinciales de réforme du droit, ainsi que par les comités de représentants de la fonction publique.⁵⁰³ À l'évidence, le modèle de partenariat pourrait s'appliquer de concert avec certains autres modèles, notamment le modèle contractuel ou conditionnel, même là où, ajoute-t-il, le gouvernement fédéral a des pouvoirs exclusifs.⁵⁰⁴ Le modèle de partenariat semble être à l'étude actuellement, grâce aux efforts entrepris par la Conférence sur l'uniformisation des lois du Canada, visant à élaborer une législation modèle.

Le législateur pourra davantage encore tracer la voie à suivre sur le marché. En amenant les institutions fédérales à promulguer des lois sur la protection de la vie privée, et à y assurer une certaine sensibilisation, il contribuera à élever les normes du marché, de sorte que les institutions qui ne sont pas couvertes par les lois fédérales seront forcées de remonter leurs propres normes compte tenu de la demande du marché. Bien sûr, si la demande ne devait se matérialiser, on pourrait dire que cette protection était superflue au départ et que les institutions réglementées par les instances fédérales ont été désavantagées. Ce qui, bien sûr, ne permettrait pas de réaliser tous les objectifs des politiques publiques. Autre mécanisme possible : le recours aux pratiques commerciales promulguées par la Société d'assurance-dépôts du Canada (SADC), organisme

⁵⁰⁰ Neilson, *supra*, note 486, pp. 92-93.

⁵⁰¹ *Ibid.*, pp. 93-94.

⁵⁰² Lawson, *supra*, note 484.

⁵⁰³ Cuming, *supra*, note 486, pp. 31-47. Voir également ce qu'il dit sur « l'harmonisation bureaucratique », pp. 28-31.

⁵⁰⁴ Neilson, *supra*, note 486, pp. 93-94.

dont la plupart, mais non la totalité, des institutions de dépôts provinciales font partie. Ces normes sont d'application obligatoire pour les membres, ce à quoi veillent des organismes de réglementation. Par conséquent, il est faux de dire que la protection de la vie privée a été négligée dans l'assurance-dépôts; en fait, les sociétés membres s'indignent déjà du fardeau que représentent les normes de la SADC.

VI. Réponses circonstanciées aux questions posées

Introduction

On trouvera dans la Partie VI des réponses détaillées aux sept questions posées par les auteurs de la présente étude. La Partie VI traite des sujets suivants : l'adéquation des lois en matière de protection de la vie privée qui régissent actuellement les institutions financières; la nécessité d'une protection accrue compte tenu des technologies et tendances nouvelles dans les services financiers; la mesure dans laquelle il faudra adapter la réglementation de la protection de la vie privée de manière spécifique au secteur des services financiers; la mesure dans laquelle la directive UE et d'autres instruments de réglementation étrangers rendent nécessaire le renforcement de la réglementation sur la protection des données personnelles, vu les ententes de réciprocité; le modèle qui, le cas échéant, conviendrait le mieux à un renforcement de la réglementation canadienne; les leçons à tirer, s'il y a lieu, des efforts entrepris ailleurs pour mettre en place un mécanisme de protection de la vie privée dans un contexte multijuridictionnel; et finalement les risques que posent les situations de propriété réciproque entre institutions financières, et la prestation de services multiples par une même entité.

- 1. Les lois canadiennes sur la protection de la vie privée qui régissent les prestataires de services financiers répondent-elles aux besoins des consommateurs de ces services? Dans l'affirmative, répond-on à ces besoins de manière uniforme à travers tout le secteur des services financiers, ou plutôt selon des modalités limitées à certains types de prestataires ou à certaines juridictions?**

Adéquation de la protection existante

Les lois qui régissent actuellement les prestataires de services financiers de ressort fédéral ne sont pas exhaustives, mais elles sont complétées par des éléments de droit coutumier et par des codes de conduite volontaires. Les projets de règlement devraient donner du muscle aux codes de conduite volontaires. L'homogénéité de cette protection variera quelque peu à travers l'industrie, atteignant un niveau optimal parmi les grandes banques.⁵⁰⁵ Il est probablement vrai d'affirmer que les politiques de protection les plus poussées se retrouvent dans les grandes institutions. Cela s'explique en partie du fait que ces institutions possèdent des structures administratives plus importantes pour régler les questions associées à la protection des données, et du fait que celles-ci traitent avec une clientèle dont l'effectif est supérieur à celui d'une petite société de fiducie provinciale qui offrirait ce service dans le cadre de régimes de retraite d'entreprise, par exemple, ou encore d'une banque de l'annexe II, qui traiterait essentiellement

⁵⁰⁵ Il existe un certain nombre d'exceptions à ces généralités; par ailleurs, rien ne nous permet d'affirmer que certains types d'institutions, ou que certaines institutions en particulier, ont attiré un nombre particulièrement élevé de plaintes.

avec des entreprises clientes. De façon générale, le faible nombre de plaintes des consommateurs à l'endroit du respect de la vie privée, ainsi que la nature des prescriptions du droit coutumier, du droit en équité et des codes de conduite, laissent croire que le *statu quo* serait adéquat.

Homogénéité dans l'ensemble du secteur

À l'heure actuelle, les lois ainsi que le droit coutumier et le droit en équité assurent une certaine protection aux consommateurs. Toutefois, hors Québec, les lois manquent d'homogénéité. Ainsi, les textes de lois fédérales qui s'appliquent aux institutions financières exigent des administrateurs qu'ils adoptent des politiques en matière de confidentialité, que les institutions prennent les mesures nécessaires pour garantir l'exactitude des données et interdire l'accès aux personnes non autorisées, et que les banques et les compagnies d'assurances s'abstiennent de certains usages de l'information. Nous croyons que l'entrée en vigueur des projets de règlement viendra renforcer ces différentes prescriptions fédérales. Divers textes de lois provinciales contiennent des dispositions pertinentes quant à la circulation de l'information et à la protection de la vie privée, y compris des prescriptions régissant les coopératives de crédit ou caisses populaires et l'évaluation du crédit des consommateurs. Le droit coutumier protège la vie privée grâce à l'obligation tacite de tenir le secret, et à la possibilité de faire intervenir des codes de protection dans le cadre de l'entente passée entre le client et l'institution. Hors du cadre contractuel, diverses actions en responsabilité délictuelle et actions en équité permettent des recours pour atteintes à la vie privée; toutefois, les actions en justice comme les actions en équité coûtent cher en temps et en argent, sans compter qu'il s'avère souvent difficile de faire la preuve des préjudices réellement subis. Ce qui revient à dire qu'à l'extérieur du Québec la loi protégeant la vie privée est moins homogène que le voudraient les experts. Il faudra cependant soigneusement évaluer le fardeau additionnel que constitue, pour les institutions, l'obligation de respecter la confidentialité, en regard des avantages pouvant découler d'une telle obligation.

L'adoption par les institutions financières de codes de conduite permet de renforcer la protection de la vie privée.⁵⁰⁶ Ces codes prévoient un certain nombre de principes qui régissent la collecte et l'utilisation des renseignements personnels, en plus de préciser les droits des personnes concernées à accéder aux données et, le cas échéant, à les rectifier. Même si ces codes relèvent d'une application volontaire, tout porte à croire que les institutions s'y conforment et qu'ils constituent un cadre fort raisonnable pour la délimitation de la confidentialité des données.

Il importe de noter que la réglementation fédérale ne porte que sur les institutions fédérales. Nous avons décrit ailleurs la réglementation provinciale touchant les institutions provinciales.⁵⁰⁷ Toutefois, d'importantes parties du secteur des services financiers demeurent pour l'essentiel non réglementées quant à la protection des renseignements personnels, sauf, bien sûr, au Québec.

⁵⁰⁶ Pour de plus amples renseignements à ce sujet, voir la rubrique « Codes des associations industrielles » à la Partie II.

⁵⁰⁷ Voir la Partie II à la rubrique « Dispositions législatives visant les institutions financières et la protection des renseignements personnels », sous-rubrique b) « Lois provinciales et questions connexes ».

Cela ne signifie nullement que les pratiques mises en œuvre par les entreprises nécessitent une réglementation plus sévère. On conviendra toutefois que l'information financière concernant un particulier et qui se trouverait aux mains d'une firme de crédit à la consommation ou d'une société de prêts provinciale n'est pas moins « délicate » que celle dont dispose une banque.

Les possibilités d'améliorations

Comme on l'a déjà vu,⁵⁰⁸ il serait possible d'optimiser le modèle de codes de protection. On pourrait en effet ajouter certaines dispositions précisant davantage l'utilisation pouvant être faite du consentement implicite, la finalité de la collecte, les possibilités de collecte auprès de tierces parties, et les motifs justifiant le refus du droit d'accès à l'information. De plus, les codes devraient explicitement permettre aux personnes concernées de se retirer des programmes qui font usage de renseignements personnels à des fins de publipostage, tout en exigeant des institutions qu'elles prennent les mesures raisonnables dans les circonstances pour s'assurer qu'un pareil retrait se matérialise dans les faits.

Autre source de préoccupation : l'existence de structures permettant d'évaluer les plaintes formulées en vertu des codes de protection, et ce de l'extérieur des institutions. Le secteur bancaire canadien s'est doté d'un pareil mécanisme, en la personne d'un ombudsman.⁵⁰⁹ Celui-ci devrait pouvoir assurer à l'évaluation des plaintes une certaine objectivité, et donc un règlement équitable par les différentes banques concernées. Cependant, dans le domaine des assurances, des sociétés de fiducie et des coopératives de crédit, cette formule n'existe pas. Précisons que, *en soi*, l'ombudsman n'est pas toujours la solution optimale; dans le secteur des assurances, il existe un code de protection qui ouvre accès à la médiation en dernier recours pour régler les litiges en matière de protection de la vie privée. C'est peut-être d'ailleurs une solution tout à fait pratique et rentable au problème.

Finalement, il est deux autres questions qui pourraient être traitées par les institutions, les secteurs d'activité et, s'il y a lieu, les instances chargées de la réglementation. D'abord, à l'heure actuelle, on constate que les imprimés standard qu'utilisent les institutions pour demander le consentement du client relativement à l'accès et à la divulgation ont peut-être été libellés en des termes trop généraux. Il faudrait, en règle générale, reformuler l'énoncé de façon plus spécifique, de manière à n'obtenir rien de plus que le consentement à l'accès puis à la divulgation des renseignements personnels visés par la relation établie avec l'institution. Ensuite, l'information sur l'état de santé, obtenue aux fins de l'assurance, ne devrait pas servir à d'autres usages (notamment, l'approbation ou le rejet d'une demande de crédit). Il faudrait que soit permise de manière explicite l'utilisation limitée des renseignements sur l'état de santé, dont la collecte sera liée à la demande de prêt, pour les besoins de l'assurance-crédit qui accompagne ce genre de demande.

⁵⁰⁸ Voir les mesures abordées dans la Partie VII, à la rubrique « Codes de conduite pour la confidentialité » et à la rubrique « Imprimés types et renseignements sur l'état de santé ».

⁵⁰⁹ Pour de plus amples renseignements sur les difficultés que présente l'obtention des codes de protection auprès de certaines institutions, se reporter à la Partie II, sous la rubrique « Codes des associations industrielles ».

2. Dans quelle mesure l'avènement des nouvelles technologies ou l'internationalisation de la prestation des services financiers provoqueront-ils le besoin d'une protection accrue de la vie privée?

Dans la mesure où les nouvelles technologies bancaires offrent de nouvelles voies pour la prestation de services financiers (notamment les transactions bancaires sur PC et Internet), la principale préoccupation porte sur la protection des données transmises au moyen de l'ordinateur et des réseaux de télécommunications.⁵¹⁰ Pour des raisons évidentes, les prestataires des services financiers ne ménagent pas leurs efforts pour s'assurer que les données seront transmises, codées et stockées de manière sécuritaire. Quoi qu'il en soit, il existe tellement d'autres besoins associés à la sécurité des données – notamment l'intégrité de la transaction et le risque de fraude informatique – qu'il n'est pas nécessaire, selon nous, d'adopter une loi qui mette l'accent sur cet aspect particulier de la protection de la vie privée.

On peut s'attendre à ce que, à l'avenir, l'« exploration de données » soit mise à plus grande contribution par les institutions financières du Canada. Cette exploration est une des préoccupations nouvelles au chapitre de la protection de la vie privée. En fait, elle ne produit, en soi, que des résultats bruts, illustrant des modèles de comportement et pouvant servir aux activités de commercialisation et de mise au point de produits par l'institution. Sans doute, la compilation de résultats bruts est une activité qui n'est pas réellement « personnelle » de par sa nature, et qui ne soulève donc pas la question de la protection des données *en soi*. Toutefois, dès lors que ces techniques d'exploration pourront servir à dégager plus tard le nom des personnes auxquelles on pourra appliquer les enseignements – et le marketing direct sert précisément à faire cela –, on se trouve à poser la question du respect de la vie privée. Pour préserver une certaine maîtrise des renseignements personnels qui les concernent, les particuliers devraient pouvoir choisir de se retirer d'activités de marketing ciblé. Par conséquent, l'institution devrait faire le nécessaire pour s'assurer que la demande formulée par la personne concernée aboutisse concrètement.

À deux grands égards, le phénomène de l'internationalisation risque de militer en faveur d'une réglementation plus serrée. D'abord, la perspective de devoir s'ajuster à des normes de protection plus élevées pour continuer à assurer le flux transfrontières des données arrivant au Canada en provenance d'États de l'Union européenne, par exemple. Ensuite, le risque de voir les institutions financières établies au Canada rechercher des « paradis informationnels » pour le stockage ou le traitement des données dans un pays étranger, afin de contourner les mesures de protection prises au Canada. Il faut dire cependant que les institutions financières réglementées à l'échelon fédéral sont, à l'heure actuelle, limitées dans leur capacité de transfert des données pour traitement hors-Canada, étant tenues d'entreposer certaines informations à l'intérieur des frontières canadiennes. De plus, comme rien ne permet jusqu'ici d'affirmer que les institutions financières sont en quête de paradis informationnels, il peut être injustifié de songer qu'elles le feront un jour.

⁵¹⁰ Pour de plus amples renseignements sur les technologies et tendances nouvelles, se reporter à la Partie III.

Une autre crainte que provoque l'internationalisation : la possibilité que des individus puissent transmettre des données par l'Internet au profit de prestataires étrangers de services financiers. Toutefois, vu les options particulièrement limitées qui s'offrent pour le moment aux instances de régulation canadiennes, il faudra tout simplement que le consommateur continue d'être vigilant (*caveat emptor*).

3. Dans quelle mesure faut-il personnaliser la réglementation en fonction du secteur des services financiers?

On peut reformuler la question en se demandant plutôt si la réglementation de la protection de la vie privée *devrait* être taillée sur mesure pour le secteur des services financiers. La collecte et le maniement des données personnelles ne changent pas vraiment, qu'il s'agisse d'institutions financières ou d'autres types d'entreprises. Le procédé est essentiellement le même. La seule chose qui diffère, c'est la sensibilité des particuliers relativement aux données concernant leurs finances ou leur état de santé.

Ceux qui penchent pour la personnalisation noteront que le secteur des services financiers traite aussi bien des fichiers sur les états de santé que des fichiers sur la situation financière – deux types d'information dont la protection suscite un certain nombre d'interrogations.⁵¹¹ Cette protection s'imposerait compte tenu de l'effet néfaste que produit une information inexacte sur l'état de santé ou l'état des finances, et vu le caractère « délicat » de cette information justement. Peut-être que, dans les faits, il s'agit là du seul type d'information dont la protection doit être réglementée. D'un autre côté, étant donné que les renseignements sur l'état de santé et l'état financier sont justement aussi délicats, on constate une augmentation des obligations juridiques à leur endroit, ce qui dans une large mesure évite d'alourdir le mécanisme de réglementation. C'est dans d'autres sphères de l'activité humaine que la protection des données marque le pas et que, par conséquent, on pourrait envisager un renforcement de la réglementation – dans la mesure, bien entendu, où l'information visée mérite une telle protection.

Il est vrai que la tendance en Europe et ailleurs dans le monde est aujourd'hui de protéger les renseignements personnels de manière globale. Cela ne signifie pas cependant qu'une démarche sectorielle plus posée serait mauvaise. On constate néanmoins de fortes pressions politiques visant une fin à la généralisation des principes, vu le caractère abstrait du débat sur la protection de la vie privée, débat axé sur le modèle des principes de l'OCDE plutôt que sur la rectification de problèmes particuliers dans ce domaine. De plus, il est possible qu'une protection « adéquate » en vertu de l'article 25 de la directive UE nécessite l'adoption de critères nationaux uniformes, même si, au départ, cela ne semble pas du tout garanti.

⁵¹¹ Se reporter à la recherche menée par Les Associés de recherche Ekos inc. (note 76 et le texte qui l'accompagne).

4. La directive UE, ou éventuellement n'importe quel texte de loi exigeant la réciprocité pour la protection de la vie privée, crée-t-elle le besoin d'une réglementation accrue dans ce domaine pour faciliter le flux transfrontières des données?

Selon l'article 25 de la directive UE, le transfert vers un pays tiers de données à caractère personnel ne peut avoir lieu que si le pays en question assure un niveau de protection adéquat, au regard de toutes les circonstances relatives au transfert envisagé.⁵¹² La démarche précise par laquelle les États européens évalueront l'adéquation de la protection demeure floue, et le restera probablement, étant donné que le processus laisse forcément une certaine place au jugement. Le document produit par le groupe de l'Union européenne dégage un certain nombre de facteurs qui entreront en ligne de compte, mais n'explique pas vraiment comment ceux-ci s'appliqueront aux cas particuliers. À l'heure actuelle, il n'existe pas de difficulté particulière dans nos transferts des données; et il semblerait d'ailleurs que le secteur des services financiers se soit doté d'une protection jugée « adéquate ». À part l'article 25, l'article 26 de la directive UE autorise le transfert de données vers des pays tiers n'assurant pas un niveau de protection adéquat, à certaines conditions (notamment, le consentement indubitable de la personne concernée, ou la nécessité d'un transfert pour la conclusion ou l'exécution d'un contrat signé ou pour l'intérêt de la personne concernée).

Vu le côté aléatoire qui sous-tend l'évaluation de cette adéquation, il sera difficile pour le législateur canadien de prévoir quelle est la combinaison de réglementation, de législation et de codification nationales permettant de satisfaire aux prescriptions de l'article 25. Généralement, l'approche adoptée pour la protection de la vie privée en vertu de la directive UE semble devoir grandement aux traditions socio-juridiques de l'Europe, et risque donc de ne pas être bien reçue au Canada. Il est clair que la démarche préconisée par la directive UE diffère notablement de la démarche sectorielle proposée pour la réglementation aux États-Unis, notre principal partenaire commercial. Résultat pratique, le Canada sera sans doute le mieux servi par une démarche qui ne cherche pas à calquer le modèle ou le niveau de protection offerts en Europe. Si l'on se fie au cas de la RailwayCard allemande,⁵¹³ il apparaît possible que de nombreux transferts de renseignements personnels se poursuivent entre l'Europe et le Canada même après l'entrée en vigueur de la directive UE, par le biais d'une protection de type contractuel. Si, plus tard, d'importants problèmes devaient survenir, il serait justifié d'amender la législation et la réglementation canadiennes en matière de protection de la vie privée pour redresser la situation.

⁵¹² Pour davantage de renseignements sur la directive UE, se reporter à la Partie IV.

⁵¹³ Pour plus de renseignements sur l'affaire de la RailwayCard allemande, se reporter aux notes 373 à 379 ainsi qu'au texte qui les accompagne.

5. S'il devait s'avérer nécessaire de réglementer davantage la protection de la vie privée dans le secteur des services financiers, de quelle structure de réglementation devrait-on s'inspirer pour le contexte canadien?

Modèles de réglementation potentiels

S'il devait s'avérer nécessaire de se doter de règlements additionnels pour protéger la vie privée, les décideurs devront soigneusement évaluer la structure qui convient le mieux au contexte canadien. Car il existe plusieurs modèles potentiels.⁵¹⁴ Ainsi, le Royaume-Uni est un exemple de système où il est nécessaire de s'enregistrer avant de pouvoir traiter l'information confidentielle. Cela a l'avantage de permettre aux personnes concernées de consulter, si elles le souhaitent, un registre central où figurent toutes les institutions qui exploitent l'information de cette nature. Le Québec, par contre, est doté d'une loi qui, à défaut d'exiger l'enregistrement, énonce des principes détaillés pour protéger la vie privée, principes qui doivent être respectés par le secteur privé. De plus, il est possible de soumettre à une entité publique les plaintes portées contre des institutions du secteur privé. La Nouvelle-Zélande, quant à elle, s'est dotée d'une loi qui énonce des principes généraux en matière de protection de la confidentialité, principes qui doivent être mis à exécution dans le secteur privé. En vertu de la loi néo-zélandaise, les codes établis par le secteur privé peuvent modifier l'obligation d'origine législative ou s'y substituer dans le but d'assurer le respect des principes de protection de la vie privée, ce qui n'empêchera pas les particuliers de porter plainte, le cas échéant, auprès du commissaire néo-zélandais à la protection de la vie privée. Le modèle à adopter (ou la combinaison d'éléments provenant de différents modèles) dépendra de divers facteurs – dont les coûts, la protection et les révisions indépendantes recherchées par les décideurs.

Au chapitre des coûts, il est probable qu'une loi exprimant de manière détaillée les obligations législatives que devront suivre les institutions financières sera la formule la plus onéreuse – formule qui, en plus, imposera peut-être un certain nombre d'obligations inadéquates. La loi pourrait emprunter une démarche spéciale ou contenir un certain nombre de clauses particulières forçant une institution à changer son règlement interne (notamment ses méthodes d'archivage). C'est le cas de la législation québécoise, qui exige la présence d'une finalité dûment exprimée pour autoriser la tenue de fichiers sur la personne concernée. Cependant, il est possible que les institutions aient structuré leurs fonds de renseignements de sorte qu'il n'existe pas de « fichiers » identifiables par rapport à une personne en particulier. De plus, comme on vit à l'âge de la polyvalence de l'information et de l'« exploration de données », il se peut que les fichiers existants ne présentent pas de finalité identifiable. Cette information sera alors utilisée en fonction des besoins changeants de l'institution et selon les associations ou modélisations particulières que le processus d'exploration pourra dégager. De plus, des droits détaillés à l'accès et à la rectification des données – surtout s'ils sont assortis de courts délais d'exécution et de l'interdiction de recouvrer les coûts en facturant la personne concernée – imposeront des coûts administratifs additionnels aux institutions financières.

⁵¹⁴ Pour de plus amples renseignements sur le cadre législatif du Royaume-Uni, du Québec et de la Nouvelle-Zélande, se reporter à la Partie IV.

L'ampleur de la protection recherchée est intimement liée au facteur coût. Pour une protection optimale de la vie privée, certains spécialistes préconisent le recours à des obligations et des restrictions détaillées qui seraient d'origine législative. Ainsi, ces experts seraient en faveur de l'obligation pour les institutions d'identifier clairement les usages ultérieurs des données réunies, de répondre gratuitement et dans de courts délais aux demandes d'accès à l'information, d'obtenir un consentement écrit pour les utilisations particulières chaque fois que cela s'avère possible, et de présenter à tous les clients un résumé de la politique en matière de confidentialité. Certes, de telles obligations permettraient de garantir un niveau de protection relativement élevé, mais elles imposeraient aussi des coûts additionnels aux institutions. De surcroît, d'autres mesures de protection seraient susceptibles d'imposer des « coûts » nouveaux en ce sens que les institutions financières touchées ne seraient pas capables d'exploiter leurs fonds de renseignements de manière concurrentielle. Par exemple, certains experts en confidentialité seraient en faveur d'une loi qui limite sérieusement la capacité pour une institution financière d'explorer ses fonds de renseignements, en plus de limiter les possibilités de circulation de données entre filiales ou subdivisions offrant des services distincts. De pareils coûts seraient répercutés aux consommateurs sous la forme de services plus élémentaires, assortis de coûts administratifs.

La plupart des observateurs conviennent qu'une démarche axée sur les principes exprimés dans les lignes directrices de l'OCDE ou dans le code type de l'Association canadienne de normalisation serait raisonnable. Toutefois, la question épineuse consiste à savoir dans quelle mesure la loi devrait étayer les principes d'application et permettre la mise en œuvre du dispositif au moyen de codes dans les institutions. Ainsi, dans le cadre néo-zélandais, la loi peut exprimer des principes de base, tout en laissant aux codes de conduite le soin de gérer la mise en application détaillée du mécanisme. Ou encore, au Québec, la loi pourrait elle-même contenir des clauses circonstanciées décrivant les modalités pratiques des principes qui régissent la protection de la vie privée. Cependant, même si la loi prévoit une description détaillée des principes de confidentialité, reste à savoir le rôle précis que joueront les codes des secteurs d'activité ou des institutions au niveau de la mise à exécution. Ainsi, ces codes pourraient ne pas se substituer aux prescriptions circonstanciées figurant dans les textes de loi, mais être plutôt reconnus comme des moyens d'interprétation pertinents permettant de voir de quelle façon des prescriptions particulières peuvent s'appliquer à certains secteurs d'activité ou à certaines situations. Le fait de s'appuyer sur des codes de conduite pour mettre en application les principes régissant la confidentialité, ou l'utilisation de ces codes comme aides à l'interprétation, pourrait assurer une meilleure collaboration de la part des secteurs d'activité, ainsi que leur autoréglementation. Si les codes sont appelés à jouer un rôle important dans la mise en application des lois, cela pourrait entraîner la mise sur pied de mécanismes de révision indépendants permettant de s'assurer que lesdits codes reflètent équitablement les principes régissant la confidentialité. Ainsi, les associations d'industries pourraient être appelées à soumettre leurs codes à un processus de révision auprès du Commissariat à la protection de la vie privée ou auprès du Bureau du surintendant des institutions financières. Ce processus pourrait nécessiter des audiences publiques ou des présentations par des groupes de consommateurs.

La question de l'exécution et du processus de révision indépendant est liée aux coûts et à la protection recherchés. Selon certains experts en la matière, le meilleur dispositif d'application consisterait en un organisme public et indépendant qui aurait la responsabilité de vérifier les pratiques courantes dans les institutions, de mener des enquêtes et de se prononcer sur les plaintes déposées par les particuliers. Bien sûr, cette démarche présuppose, par rapport à un système plus autoréglementé, des coûts accrus. Du point de vue des entreprises, il serait préférable d'avoir une situation semblable au *statu quo*, c'est-à-dire où les institutions sont pour l'essentiel responsables de l'application du dispositif et où les plaintes sont le plus souvent traitées dans le cadre du règlement interne. Une solution intermédiaire consisterait à permettre l'autoréglementation dans la plupart des cas, mais avec possibilité de révision par un organisme public indépendant advenant des plaintes ou des difficultés particulières. De la sorte, les plaintes seraient, le cas échéant, déposées dans le cadre du règlement interne de l'institution; toutefois, si la personne concernée était insatisfaite de l'issue, elle pourrait avoir le droit de soumettre son cas à un organisme indépendant, pour interjeter appel ou demander une nouvelle audience de sa requête. Au Canada, cela pourrait signifier que les plaintes non réglées à l'interne iraient devant le Commissariat fédéral à la protection de la vie privée ou devant le Bureau du surintendant des institutions financières. Finalement, une autre solution de compromis consisterait à avoir un système semblable à celui de l'ombudsman dans le secteur bancaire canadien, et ce pour tous les secteurs qui offrent des services financiers. Les associations des industries pourraient être appelées à ouvrir des bureaux d'ombudsman autonomes, que viendront consulter les personnes concernées qui s'estiment insatisfaites des résultats obtenus à l'interne.

Sélection du modèle approprié

La présente étude a abordé plusieurs modèles de protection de la confidentialité. Tous incorporent les principes énoncés par l'OCDE; on pourrait discuter longuement des différences en matière de sévérité, mais il reste que tous ces modèles ont démontré qu'ils fonctionnaient. Il semble raisonnable toutefois d'inférer qu'un mécanisme de réglementation rigide et à grande échelle se traduirait par des coûts considérables et aurait moins de chances de succès qu'un mécanisme plus souple et plus léger. Le choix de la méthode souple s'appuie d'ailleurs sur une observation d'ensemble quant à la réglementation de la confidentialité dans le secteur des services financiers canadiens : le faible niveau de plaintes et, dans l'ensemble, la conformité des codes de conduite par rapport aux principes régissant le respect de la vie privée.

Il semblerait que le modèle de réglementation optimal serait celui qui permet la plus grande faculté d'adaptation à des circonstances changeantes. Un système qui permettrait la mise au point et la personnalisation de règlements au niveau des secteurs d'activité serait sans doute le mieux approprié. Certains sondages indiquent une méfiance du public à l'endroit de l'autoréglementation.⁵¹⁵ Cela pourrait s'expliquer par l'impression qu'il existe un problème de type systémique au chapitre de la confidentialité, et que l'agent et la cible de la réglementation ne font qu'un. Toutefois, le système avec autoréglementation a donné naissance au code type de la

⁵¹⁵ Voir les notes 79 and 91, ainsi que le texte qui les accompagne.

CSA (ACNOR), code qui a été fort bien reçu et qui offre un excellent niveau de protection de la vie privée. Les principes de la CSA ont d'ailleurs été incorporés par les modèles de code de l'Association des banquiers canadiens et d'autres associations. En deux mots, la démarche d'autoréglementation employée au Canada fonctionne. Bien sûr, le système peut être amélioré. On trouvera d'ailleurs dans la présente étude plusieurs améliorations possibles à ce système.⁵¹⁶

Toutefois, s'il fallait opter pour une démarche davantage légiférée, probablement sous la pression d'instances étrangères, un système de type néo-zélandais pourrait convenir.⁵¹⁷ Les principes régissant le respect de la vie privée seraient décrits dans les textes de loi; par la suite, ces principes seraient mis en application par le biais de codes de conduite approuvés par l'industrie plutôt que par des textes de loi. Une telle démarche permettrait une vérification objective des codes mis en place sur le marché, ce qui supprimerait tout risque d'intérêts personnels. En outre, nous croyons que l'actuel système de surveillance pourrait continuer de fonctionner dans le cadre d'un tel mécanisme. L'ombudsman du secteur bancaire au Canada pourrait procéder à une révision indépendante des plaintes de consommateurs à l'endroit du secteur bancaire. D'autres secteurs pourraient être incités à adopter des mesures susceptibles de mener à une médiation ou à un arbitrage indépendants des plaintes formulées par les particuliers insatisfaits par l'issue de leurs requêtes à l'interne.

Dans la présente étude, nous avons déjà indiqué à plusieurs reprises le caractère efficace des règles du marché quant aux risques de divulgation d'information confidentielle. Même si cela n'est pas nécessairement accepté par les tenants de la réglementation, le marché constitue une force non négligeable qui peut bien réglementer les comportements de l'entreprise en matière de confidentialité. L'argument en faveur de ces forces est double. D'abord, le client a intérêt à préserver le caractère confidentiel de l'information, et les institutions ont intérêt à préserver leur clientèle. Par conséquent, les deux parties ont un intérêt commun. (De plus, on notera que les institutions elles-mêmes ont intérêt à préserver la confidentialité et l'exactitude de leurs fonds de données, indépendamment des intérêts de la clientèle.) Deuxièmement, les consommateurs se plaindront s'ils constatent que la protection de la vie privée est inadéquate, ce à quoi les institutions auront à répondre. En général, il semble que les choses vont bien dans l'actuelle combinaison de règles du marché et de restrictions de droit coutumier concernant les institutions, du moins si l'on se fie au faible niveau des plaintes déposées devant les institutions, les ombudsmans et des associations d'industries.

⁵¹⁶ Les améliorations incluent certains changements mineurs aux codes régissant la confidentialité, plus l'ajout de clauses nouvelles aux codes en matière de confidentialité, pour permettre aux particuliers de se retirer des programmes d'« exploration de données » et de marketing direct; des dispositions garantissant que les codes soient facilement accessibles au grand public; de nouvelles méthodes de révision pour les plaintes n'ayant pas abouti; des changements aux imprimés administratifs de manière à restreindre la portée des indications qui y figurent; et peut-être des mesures faisant en sorte que les renseignements sur l'état de santé, réunis à des fins d'assurances, ne servent pas à d'autres fins. Se reporter à la Partie II, sous la rubrique « Codes des associations industrielles », sous-rubrique e) « Observations concernant les codes des associations »; voir également la Partie VII, à la rubrique « Codes de conduite pour la confidentialité ».

⁵¹⁷ Pour de plus amples renseignements sur le *Privacy Act* de la Nouvelle-Zélande, se reporter à la Partie IV, sous la rubrique « Lois sur la confidentialité des données en Nouvelle-Zélande ».

6. Le Canada a-t-il des leçons à tirer des efforts déployés pour l'introduction d'un mécanisme de protection élargie dans un cadre multijuridictionnel?

Il n'existe que quelques exemples touchant à la mise en œuvre de régimes de protection dans des systèmes multijuridictionnels qui puissent intéresser le Canada. Le meilleur exemple est sans contredit celui de l'Union européenne. Toutefois, la directive UE doit faire l'objet de certaines réserves pour les Canadiens. Car son adoption visait d'abord une homogénéité de la réglementation à des fins commerciales – autrement dit, faciliter le transfert de données entre États membres de l'Union européenne. Or, le Canada n'a à l'heure actuelle aucune préoccupation de cette sorte.⁵¹⁸ De plus, la directive UE constitue un compromis entre diverses législations et approches nationales. Or, les lois canadiennes en matière de confidentialité ne sont pas aussi hétéroclites que celles des États européens. De surcroît, la nature même du droit civil (droit romano-germanique) ainsi que les cultures européennes qu'on retrouve dans ces pays devrait faire de la directive UE un document qui reflète essentiellement les origines qui lui sont propres.⁵¹⁹

L'expérience de la directive UE porte à croire que la mise en œuvre d'une directive unique qui puisse s'appliquer à divers États nécessite certains compromis. Différents États voudront faire en sorte que certains éléments de leur législation se retrouvent (ou, à tout le moins, sont reconnaissables) dans la directive. Dans le cadre canadien, cela pourrait signifier que les résultats optimaux seront conditionnés par la mise au point conjointe avec les gouvernements provinciaux d'une politique générale en matière de confidentialité. Au Québec, cela pourrait cependant poser des problèmes significatifs puisque cette province est déjà dotée d'un cadre juridique qui n'est pas nécessairement compatible avec celui des autres provinces ou de l'État central. Or, dans un monde idéal, le même niveau de protection devrait être offert dans tous les territoires et provinces pour ne pas imposer aux institutions présentes sur la scène nationale des systèmes multinormes.

7. Quels sont les risques que pourraient constituer, pour la protection de la vie privée, le phénomène de propriété réciproque entre institutions financières, ainsi que la prestation de différents services financiers par une même entité?

La propriété réciproque entre institutions financières permet le partage d'information entre agents de prospection pour divers types de services financiers, dans le but de créer une machine de marketing plus précise. Lorsqu'une même institution offre un vaste nombre de produits et de

⁵¹⁸ Même si les textes de loi québécois régissant le secteur privé contiennent des dispositions qui limitent le transfert de données personnelles vers l'extérieur de la province, il semblerait que ces dispositions n'aient pas eu d'impact important sur la circulation des données entre les provinces.

⁵¹⁹ Dans une certaine mesure, il faudrait voir sous le même jour l'expérience législative du Québec. La *Loi sur la protection des renseignements personnels dans le secteur privé* reflète certains principes fondamentaux en matière de confidentialité, incorporés dans la dernière édition du *Code civil* de la province. Toutefois, les autres juridictions canadiennes, de type « common law », se distinguent du système judiciaire québécois, unique en son genre dans la Confédération.

services, il lui devient possible d'avoir de nombreuses applications pour les mêmes données personnelles. De plus, on pourrait être tenté d'exploiter certains types de données du simple fait de leur présence : ainsi, s'il fallait que les fichiers traitant des états de santé deviennent d'accès universel dans une institution tout simplement parce que celle-ci travaille dans les assurances, ces fichiers pourraient servir à d'autres fins. Dans la mesure où cela peut être source de préoccupations, il faudrait noter, par exemple, que le code établi par l'Association des banquiers canadiens interdit l'échange d'information entre une banque et une société d'assurances affiliée.⁵²⁰

Malheureusement, les implications d'une propriété réciproque entre différents prestataires de services financiers est une question fortement politisée. Par conséquent, il importe de distinguer les craintes à l'endroit du caractère concurrentiel de celles qui touchent au caractère confidentiel. Au Canada, on retrouve un important groupe de pression constitué notamment de courtiers d'assurances et de courtiers en valeurs mobilières qui voient leur position sur le marché être menacée par les conglomérats de banques. On ne s'attardera pas, dans la présente étude, aux facteurs concurrentiels. La capacité d'échanger des données entre différents prestataires de services ou entre différentes subdivisions au sein d'une même entreprise prestataire est susceptible d'optimiser le rendement et de produire une baisse des coûts à la consommation. Or, il arrive souvent qu'une amélioration du rendement engendre des pressions sur les intervenants moins rentables sur le marché. La présente étude n'abordera pas la question de savoir si l'atténuation des effets sur le rendement constitue un objectif de politique publique qui serait souhaitable. Nous craignons simplement que les restrictions sur la circulation des données, dans le but d'ajouter au caractère concurrentiel d'une entreprise, ne soient confondues avec les restrictions sur le flux de ces mêmes données, cette fois-ci pour des motifs touchant à la protection de la vie privée. L'importance et le caractère aléatoire des préoccupations dans ce domaine favorisent leur exploitation par différents groupes de pression. Il faut savoir que les problèmes de confidentialité qu'on peut retrouver dans différentes parties du secteur des services financiers ne varient pas de façon significative. Par contre, la question du chevauchement des services et de l'accès à l'information par divers services financiers est bien plus épineuse que certains participants voudraient le laisser croire. Nous croyons que la politique gouvernementale ne devrait pas contribuer à alourdir ces craintes en levant la démarcation qui sépare la réglementation des marchés de la réglementation de la confidentialité.

Il peut arriver que, du fait d'une réglementation, certains services ne puissent être offerts que par des filiales distinctes. Dans d'autres cas, ces services seront dispensés par le biais d'une seule et même entité juridique. Les démarcations entre différents secteurs ont, pour l'essentiel, disparu. La vente d'assurances par les succursales de banque est l'un des rares réseautages qui est limité de par la loi. Le fait que des services soient offerts ou non par une seule et même entité participe d'une drôle de combinaison de facteurs comme les aléas de l'histoire et la politique de

⁵²⁰ Association des banquiers canadiens, *Confidentialité, modèle de code pour protéger les renseignements personnels des clients des banques* (1996), art. 5.4. De plus, les directives, lignes directrices et codes adoptés par les associations d'assureurs prévoient que les sociétés d'assurances n'échangeront pas avec d'autres institutions les données relatives à la clientèle assurée, à part quelques rares exceptions.

diversification (qui n'ont rien à voir avec le principe de la confidentialité), ainsi que de l'ingénuité des conseillers et agents de normes pour inventer de nouveaux produits qui puissent contourner les restrictions imposées. Les compagnies d'assurances vendent des fonds réservés, mais qui ne sont à toutes fins utiles rien d'autre que des fonds mutuels. Elles offrent des produits qui ressemblent grandement à des dépôts, et sont habilitées à émettre des cartes de crédit. Les courtiers en valeurs mobilières détiennent des fonds pour lesquels ils paient de l'intérêt, tout comme s'il s'agissait de dépôts. Aux États-Unis, ceux-ci peuvent d'ailleurs être virés par chèque. De plus en plus, les différents types d'institution seront appelés à se ressembler ou à appartenir à la même entité, présentant ainsi une seule et même façade aux yeux du grand public et étant gérés par un seul ensemble de politiques internes, notamment en matière de respect de la confidentialité. Il suffit pour en être convaincu de songer aux assurances CIBC, à la Société de fiducie TD, et à la Banque Manuvie. Toutefois, à défaut d'un consentement, l'information ne pourra être partagée entre des personnes morales différentes, même en cas de propriété commune. Rien ne semble justifier logiquement cette situation, étant donné que la répartition des services offerts entre des personnes morales distinctes n'a pas grand-chose à voir avec les intérêts du client en matière de confidentialité, mais plutôt avec une capacité de réglementation accrue, des considérations de prudence et, le plus souvent, l'efficacité attribuée aux groupes pression lorsque vient le moment de protéger leur territoire économique. Par conséquent, on jugera acceptables les consentements de type général portés sur les contrats, pour permettre la circulation de l'information au sein d'un groupe de sociétés particulier.

Les groupes de consommateurs se sont dits inquiets devant l'usage possible de l'information pour vendre d'autres produits, une situation susceptible de donner au consommateur l'impression qu'il est tenu de faire l'achat s'il souhaite préserver ses services bancaires. Selon nous, cela ne devrait pas constituer la base d'une nouvelle réglementation ou politique. D'abord, il ne s'agit pas réellement d'un problème de respect de la vie privée. Une institution cherchera à écouler ses produits, qu'elle ait recours ou non à l'information personnelle. Si, par la suite, elle utilise l'information à sa disposition pour procéder à un publipostage d'assurances destiné aux personnes le plus susceptibles de se prévaloir de l'offre – ce qui permettra de réduire les frais de courrier de neuf dixièmes –, tant mieux pour elle. Si, par contre, elle est contrainte d'envoyer dix fois plus de lettres, il reste que les mêmes personnes ayant déjà une relation avec l'institution se verront proposer les nouveaux produits. Il s'agit donc davantage d'un problème de ventes liées que d'un problème de confidentialité. Dans le secteur des services financiers, il n'y a pas grand-chose qui laisse penser à des pratiques monopolistiques de ventes liées.⁵²¹

⁵²¹ Pour de plus amples renseignements sur la problématique des ventes liées, voir Owens, Onyshko et Goode, *supra*, note 24.

VII. Conclusions

Introduction

La Partie VII présente les conclusions des auteurs en ce qui a trait à la réglementation de la protection de la vie privée vis-à-vis les prestataires de services financiers. En particulier, la Partie VII étudie les intérêts en matière de confidentialité ainsi que les besoins de réglementation en général, les codes de conduite en matière de confidentialité qui existent déjà dans le secteur des services financiers, les imprimés standard utilisés par les prestataires de services financiers, l'information en matière de santé que s'échangent les assureurs, la réglementation des agences d'évaluation du crédit et des compagnies d'assurances, les conséquences de la directive UE, ainsi que celles des tendances et technologies nouvelles, d'une part, et du phénomène de propriété réciproque parmi les prestataires de services financiers, d'autre part.

Intérêts en matière de confidentialité et besoin de réglementation

Les intérêts en matière de confidentialité découlent de la collecte, de l'exploitation et de la communication de données sur l'état des finances et de la santé, dans le secteur des services financiers. Ces intérêts tombent sous le coup des lois existantes, du droit commun et des codes de conduite. Une protection accrue sera accordée par le biais des réglementations proposées dans le cadre des lois fédérales sur les finances en vertu des prescriptions par ces motifs dans le projet de loi C-82 (le « projet de règlement »). La protection qui existe à l'heure actuelle à l'endroit des prestataires de services financiers réglementés à l'échelon fédéral est moins stricte que dans certains autres territoires, notamment dans les États de l'Union européenne, mais plus stricte que d'autres pays encore, comme les États-Unis. Dans l'ensemble, on peut dire que la structure qu'on retrouve actuellement au Canada incorpore les principes et les aspects propres à un régime de protection moderne.

Compte tenu du faible nombre de plaintes portées à l'endroit des institutions financières, et vu la nature des mesures existantes en matière de confidentialité, une analyse de rentabilité tendrait à favoriser une certaine prudence dans les réformes à venir. On notera toutefois que, pour protéger la vie privée du consommateur ainsi que la confidentialité des données qui s'y rattachent, les institutions ont déjà adopté des pratiques qui permettraient de s'adapter facilement à un resserrement de la réglementation dans le domaine. Par conséquent, il importe de préciser comme il faut les coûts additionnels pouvant découler d'éventuelles réformes.

Étant donné que les régimes de protection sont plus sévères dans certains territoires, comme dans les États de l'Union européenne, le Canada risque de subir des pressions l'amenant à remonter la barre. Si Ottawa devait décider d'obtempérer, il faudrait s'assurer que les nouvelles mesures se

caractérisent par une certaine souplesse. Or, l'usage actuel des codes de conduite volontaires répond bien à ce critère. D'autres mesures encore pourraient s'inspirer du modèle néo-zélandais⁵²² par exemple, modèle qui permet la formulation de codes de conduite de concert avec les entités qui font la collecte de données et qui sont le plus susceptibles d'être touchées par ces codes.

La réglementation des codes de conduite n'a pas à être taillée sur mesure en fonction des besoins propres au secteur des services financiers. Les principes et les préoccupations en matière de confidentialité sont les mêmes dans tous les autres secteurs de l'économie où l'on procède à la collecte, l'exploitation et la divulgation d'informations à caractère personnel. Toutefois, ce qui peut changer, c'est peut-être le degré de préoccupation. Comme on pourrait s'y attendre, les sondages démontrent que le public s'inquiète bien davantage dès lors qu'il s'agit de données sur l'état des finances ou l'état de la santé.⁵²³ Par conséquent, on pourrait bien décider de réglementer seulement les activités commerciales qui touchent à ces données, quitte à évaluer la pertinence d'une réglementation ultérieure portant sur d'autres types de renseignements, jugés moins « délicats ».

En principe, les activités de n'importe quel prestataire de services financiers auront toujours les mêmes implications pour ce qui est de la protection de la vie privée. Les conclusions de la présente étude valent aussi bien pour les firmes de crédit à la consommation et les sociétés de cartes de crédit que pour les banques et compagnies d'assurances. Il pourrait y avoir une légère différence quant au degré de préoccupation, mais la problématique demeure essentiellement la même. Toutefois, le gouvernement fédéral ne semble pas avoir l'autorité pour promulguer des règlements sur la confidentialité à l'extérieur du cadre de la réglementation fédérale des services financiers; résultat pratique, les mesures touchant les firmes de crédit et les compagnies de cartes de crédit, ainsi que les autres activités apparentées, devront, le cas échéant, découler de lois provinciales. À notre connaissance, aucun comportement particulier et aucun ensemble de plaintes ne semblent exister qui justifieraient l'établissement d'une telle réglementation dans ce secteur. S'il fallait que des lois ou des règlements provinciaux soient adoptés, il est important de veiller à l'homogénéité à travers le Canada de façon à ce que de grandes entreprises établies dans différentes provinces n'aient pas à se soumettre à des règles contradictoires.

Codes de conduite pour la confidentialité

La présente étude décrit un certain nombre d'intérêts en matière de confidentialité, touchés par la prestation de services financiers et reconnus dans la théorie de la protection de la vie privée. Les principes modernes de la confidentialité – comme ceux qu'on retrouve dans les lignes directrices de l'OCDE⁵²⁴ – traitent de ces intérêts. Au Canada, ces principes sont intégrés à des codes de

⁵²² Pour de plus amples renseignements sur le *Privacy Act* de la Nouvelle-Zélande, voir la Partie IV, à la rubrique « Lois sur la confidentialité des données en Nouvelle-Zélande ».

⁵²³ Se reporter à la recherche menée par Les Associés de recherche Ekos inc. (note 76 et le texte qui l'accompagne).

⁵²⁴ Voir la note 15 et le texte qui l'accompagne.

conduite qui ont été adoptés par des associations d'industries et des institutions financières individuelles. Toutefois, comme on a pu le voir ailleurs dans cette étude,⁵²⁵ certains codes modèles pourront être optimisés grâce à l'ajout de certaines directives sur le consentement implicite, sur la finalité de la collecte de données, sur l'exploitation potentielle par de tierces parties, et sur les motifs clairs pouvant justifier l'interdiction d'accès à l'information.

En outre, les codes de protection de la vie privée devraient permettre aux personnes qui le souhaitent de se retirer de programmes qui utilisent les renseignements personnels à des fins de marketing direct, en plus d'exiger des institutions qu'elles prennent les mesures raisonnables et nécessaires pour faire en sorte que le retrait du programme se fasse de manière réelle.⁵²⁶ Les risques en matière de confidentialité demeurent modestes dans le cas des programmes de marketing direct. On ne peut donc pas parler de divulgation de renseignements « délicats ». Toutefois, pour une question de principe, il serait bon de donner aux personnes concernées la possibilité de maîtriser un tant soit peu l'usage qui est fait de l'information les concernant. De plus, le public est de plus en plus irrité et préoccupé par les sollicitations intempestives faites par courrier ou par téléphone. Il serait raisonnable de se contenter d'une option de « retrait du système » dans la mesure où l'on ne dispose d'aucune preuve attestant de sérieux problèmes associés à de telles pratiques. On pourrait aussi envisager une protection accrue, en exerçant l'option d'« entrée » dans le système, qui nécessiterait pour l'institution qu'elle obtienne au préalable le consentement écrit et explicite de la personne concernée. Toutefois, cette deuxième modalité entraînera des coûts d'administration supérieurs puisqu'il faudra aller chercher l'autorisation des clients individuels.

Certains codes émanant des institutions ne sont pas facilement accessibles au public.⁵²⁷ Or, les institutions et leur clientèle seraient mieux servies si l'on déployait des efforts raisonnables pour rendre la documentation d'appoint disponible sur demande. En fait, certaines diront même que les institutions devraient remettre à leur clientèle l'information nécessaire quant à la protection des renseignements qu'elles sont prêtes à leur accorder. Si une telle exigence devait être formulée, elle devrait l'être de façon collégiale, car elle pourrait bien représenter des coûts élevés et s'avérer difficile à mettre en œuvre, dans l'état actuel des systèmes informatiques.

Le plus souvent, les régimes de protection de la vie privée prévoient que les personnes concernées pourront, s'il y a lieu, porter plainte auprès d'une personne chargée de la réglementation ou d'un arbitre impartial. Dans le cas des banques, l'ombudsman joue ce rôle.⁵²⁸

⁵²⁵ Voir la Partie II à la rubrique « Codes des associations industrielles », sous-rubrique e) « Observations concernant les codes des associations ».

⁵²⁶ On notera que certains codes existant déjà (y compris celui de l'Association des banquiers canadiens) prévoient que la personne concernée pourra, à certaines conditions, retirer le consentement qu'elle avait donné à l'utilisation des renseignements qui la touchent. En outre, le code de l'ABC affirme que la banque devra obtenir le consentement du client avant d'utiliser l'information qui le concerne à des fins de prospection. Voir les notes 276 et 277, ainsi que le texte qui les accompagne.

⁵²⁷ Pour de plus amples renseignements sur les difficultés entourant l'obtention des codes de conduite auprès de certaines institutions, se reporter à la Partie II, sous la rubrique « Codes des associations industrielles ».

⁵²⁸ Pour de plus amples renseignements sur le rôle joué par l'Ombudsman du secteur bancaire, voir les notes 95, 96, 296 et 297, ainsi que le texte qui les accompagne.

Cependant, le secteur bancaire dispose d'un énorme bassin de clients et de transactions à partir duquel il pourra appuyer le rôle de l'ombudsman. Ailleurs, pour les petits regroupements de prestataires de services financiers, il pourrait être insuffisant de mettre en place un pareil dispositif d'ombudsman. La solution pourrait consister en une mise sur pied, par les codes de conduite servant de modèle aux associations d'industries, de mécanismes de médiation et d'arbitrage pour résoudre les cas de litige spécifiques. Par exemple, le modèle de code du BAC (Bureau d'assurance du Canada) prévoit le recours à un processus de médiation indépendante si l'on ne parvient pas à régler le différend concernant l'interdiction d'accès à l'information;⁵²⁹ il s'agit là d'un mécanisme de résolution de dernier recours, relativement peu onéreux puisqu'il n'entraîne pas nécessairement la mise en place de structures permanentes. Les associations d'industries (autres que l'Association des banquiers canadiens) pourraient adopter une démarche semblable pour régler des plaintes n'ayant pu aboutir dans le cadre des mécanismes internes de l'institution.

Les observations qui précèdent ne constituent pas un aveu d'échec mais bien plutôt le portrait des éléments pouvant être optimisés en fonction des notions idéales de protection de la vie privée. En général, les codes canadiens reflètent les principes établis en matière de protection ainsi que des mesures nécessaires pour en assurer l'application.⁵³⁰ Ces codes constituent la base d'un système réaliste d'autoréglementation qui a été mis sur pied par les principales associations d'industries pour les besoins propres au secteur des services financiers.

Imprimés types et renseignements sur l'état de santé

Un secteur qui devra être travaillé par les institutions, les associations d'industries et, s'il y a lieu, par les personnes chargées de la réglementation, c'est le libellé des imprimés types qui sont utilisés par les prestataires de services financiers. En effet, les imprimés et les conventions autorisant la collecte et le partage des données personnelles devraient respecter, et non pervertir, les principes régissant l'utilisation et la collecte, principes établis dans les codes sur la protection de la vie privée.⁵³¹ Chaque fois que cela s'avère possible ou nécessaire, les institutions devront demander le consentement du client avant de procéder à la collecte ou au partage des données qui le concernent. Toutefois, et en règle générale, cet assentiment devrait se limiter à certains types de circonstances ou de destinataires. Ainsi, les imprimés utilisés par les banques pourraient permettre l'accès aux données personnelles, ainsi que leur partage, pour des motifs exclusivement liés à la relation établie entre la banque et le client. Les autorisations d'accès ou de partage *quel que soit* le motif gagneraient à être remplacées par une formulation plus précise.

⁵²⁹ Bureau d'assurance du Canada, *Modèle de code sur les renseignements personnels* (1996), art. 4.9.1.

⁵³⁰ On verra, dans les tableaux de l'annexe A, dans quelle mesure les modèles de code permettent l'application des principes en matière de confidentialité.

⁵³¹ Pour une analyse de certains imprimés établis par les banques, se reporter aux notes 136 à 141, ainsi qu'au texte qui les accompagne.

L'information sur l'état de santé qui se trouve réunie à des fins d'assurances ne devrait pas servir à l'évaluation du crédit.⁵³² Bien entendu, certains renseignements en matière de santé sont parfaitement pertinents à l'évaluation du crédit, mais ils devraient alors faire l'objet d'une collecte et d'une utilisation spécifiques à cet effet et à ce contexte. C'est là une préoccupation qu'on retrouve dans les codes de conduite existant déjà. Le code de l'Association des banquiers canadiens prévoit que les banques ne pourront tirer de renseignements personnels du dossier médical qu'à des fins bien précises – et qu'elles n'en divulgueront la nature ni à leurs filiales ni aux sociétés affiliées.⁵³³ De même, les lignes directrices et le code adoptés par les associations d'assureurs prévoient que les compagnies d'assurances ne pourront partager avec d'autres institutions l'information concernant les assurés, si ce n'est dans certaines situations bien particulières.⁵³⁴ Toutefois, le projet de code établi par la Centrale des caisses de crédit du Canada (CCCC) prévoit que les données médicales réunies par une caisse de crédit pourront servir à l'étude du crédit ainsi qu'aux besoins d'assurances qui y sont associés.⁵³⁵ On suppose que, dans ce contexte, le lien qu'on fait ici s'applique à l'assurance-crédit, elle-même liée à la demande de crédit, pratique qui semblerait justifiée. Règle générale, les assureurs tout comme les octroyeurs de crédit ont tellement intérêt à préserver l'intégrité et la franchise du processus qu'on les voit mal en train de donner au public l'impression que les renseignements serviront à d'autres fins que ce qui avait été prévu au départ. Nous n'avons pas eu connaissance d'abus fréquents qui auraient été commis à cet égard dans l'industrie.

Agences d'évaluation du crédit et compagnies d'assurances

Deux autres dossiers relèvent de la compétence des provinces.⁵³⁶ Les agences d'évaluation du crédit suscitent d'importantes interrogations pour ce qui est du respect de la vie privée, compte tenu de l'importance du rôle qu'elles jouent dans l'économie moderne, et de l'effet direct que les rapports de crédit ont sur les particuliers. En général, et de façon plus ou moins régulière, les agences sont réglementées à l'échelon provincial. On recommande d'ordinaire des dispositions législatives exigeant que les personnes concernées soient informées du recours à une agence de crédit, de l'emplacement de l'agence, de la personne-ressource qui y travaille, et du droit de consulter les rapports établis. En outre, l'échange d'information entre les assureurs, par le biais du Bureau de renseignements médicaux (MIB), pourrait devenir une pratique réglementée, de la même manière que l'échange d'information entre agences de crédit. Les réformes entreprises par les différentes provinces devraient être homogènes.

⁵³² Pour de plus amples renseignements, se reporter aux notes 283 à 285, ainsi qu'au texte qui les accompagne.

⁵³³ Association des banquiers canadiens, *Confidentialité – Modèle de code, pour protéger les renseignements personnels des clients des banques* (1996), art. 5.4.

⁵³⁴ Association canadienne des compagnies d'assurances de personnes, *Droit à la vie privée, lignes directrices n° 96*, art. 6; Bureau d'assurance du Canada, *Modèle de code sur les renseignements personnels* (1996), art. 4.3.2.

⁵³⁵ Centrale des caisses de crédit du Canada, *Credit Union Code for the Protection of Personal Information* (avant-projet) (1996), art. 5.4.

⁵³⁶ Pour de plus amples renseignements sur ces questions, se reporter à la Partie II, sous la rubrique « Dispositions législatives visant les institutions financières et la protection des renseignements personnels », sous-rubrique b) Lois provinciales et questions connexes.

Implications de la directive UE

Tout semble indiquer qu'il n'existe pas de problèmes en ce qui a trait au transfert de données personnelles entre l'Union européenne et le Canada. De plus, l'expérience accumulée par la directive UE⁵³⁷ est assez embryonnaire, étant donné que ce document n'a pas encore été pleinement mis en œuvre en Europe. Ce serait donc une erreur que de voir dans ce régime embryonnaire et marqué culturellement, établi par la directive UE, un modèle à suivre pour le Canada. Les mesures actuelles prises par le secteur des services financiers, surtout si elles devaient faire l'objet d'une sanction législative nouvelle par le biais des projets de règlement, pourraient bien répondre au critère de protection « adéquate » en vertu de l'article 25 de la directive UE. Le secteur financier canadien, réglementé à l'échelon fédéral, pourrait figurer sur une « liste blanche partielle », pour reprendre les mots qu'on retrouve dans la récente déclaration de principe du groupe UE.⁵³⁸ Quoiqu'il en soit, le respect des dispositions de l'article 25 dans la directive UE semble particulièrement problématique. Tendre vers le respect de ces dispositions revient à augmenter la charge de la réglementation, à un moment où l'on ignore encore ce que signifie exactement « protection adéquate ».

Tendances, technologies, et propriété réciproque

En plus de ce qui précède, il existe un certain nombre de problèmes reliés aux tendances et aux technologies nouvelles, ainsi qu'au phénomène de propriété réciproque parmi les institutions financières.⁵³⁹ Dans l'ensemble, les technologies de tendance nouvelle ne soulèvent pas de problèmes qui nécessitent, à l'heure actuelle, une réglementation officielle. Par contre, l'intensification de l'« exploration de données » à des fins de marketing direct porte à croire que les personnes concernées devraient pouvoir se retirer de ce genre de programme en donnant à leur institution un avis à cet effet. Quant au phénomène de la propriété réciproque, il pourrait permettre à différentes subdivisions des institutions d'exploiter des renseignements personnels en élargissant le champ d'application. Nous croyons cependant que le risque posé par la propriété réciproque ne justifie pas le recours à une réglementation allant au-delà de ce qui a déjà été recommandé ailleurs dans la présente étude.

⁵³⁷ Pour de plus amples renseignements sur la directive UE, se reporter à la Partie IV.

⁵³⁸ Pour de plus amples renseignements sur le document publié par le groupe UE, voir la note 366 et le texte qui l'accompagne.

⁵³⁹ Pour de plus amples renseignements sur les technologies et les tendances nouvelles, se reporter à la Partie III.

Annexe A : Sommaire et tableaux comparatifs détaillés : Comparaison des codes sectoriels et de certaines lois en matière de protection des renseignements personnels

Le texte qui suit est un tableau récapitulatif du degré de conformité à certains principes de protection des renseignements personnels de divers codes sectoriels et textes de loi visant la protection des renseignements personnels. Selon l'objet de la comparaison, le résultat est exprimé en degrés (« faible », « moyen », « élevé ») ou par une mention indiquant si une disposition déterminée est incluse (« oui », « non »). Dans une certaine mesure, le tableau est intrinsèquement trompeur. Premièrement, il résulte d'un exercice de jugement inévitablement subjectif. Deuxièmement, les différences entre les degrés sont souvent légères au point d'être pratiquement négligeables. Troisièmement, il est trompeur de supposer qu'il existe une incarnation parfaite de chaque principe et qu'une dérogation à celui-ci traduit un manque de volonté à l'égard de la protection des renseignements personnels. Les circonstances dans lesquelles les activités sont exercées comportent plusieurs facteurs d'adaptation des principes à la réalité, y compris une analyse de rentabilité réaliste ainsi que tout intérêt propre à l'égard de la valeur économique du partage des données. Les évaluations du degré de conformité sont faites en fonction de l'application pratique la plus stricte exprimant un principe déterminé plutôt qu'en fonction du degré d'incarnation du principe visé. Il faut aussi souligner qu'une cote « faible » n'est pas nécessairement une évaluation négative. Dans certaines circonstances, il se peut qu'il soit peu pratique de se conformer à la norme. Par exemple, le *Data Protection Act* du Royaume-Uni prévoit une action au civil relative aux données inexactes. Il s'agit d'un exemple de recours à la pleine force de la loi en vue de l'exécution des principes qui mérite donc une cote élevée, mais ce recours est peu pratique étant donné le coût et la lenteur des tribunaux. Dans certains cas, cette situation se reflète par le fait que l'ensemble des codes sectoriels présentent un faible degré de conformité, même s'ils sont en réalité pleinement « conformes », mais omettent certaines des dispositions excessives de l'incarnation la plus stricte d'une norme.

Tableau sommaire comparatif (UE, Québec, A.B.C., A.C.C.A.P., B.A.C.)

Élément de comparaison ⁵⁴⁰	Union européenne (UE) <i>Directive relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (1995)</i>	Québec <i>Loi sur la protection des renseignements personnels dans le secteur privé, L.R.Q., ch. P-39.1 (1994)</i>	Association des banquiers canadiens (ABC) <i>Confidentialité – Modèle de code (1996)</i>	Association canadienne des compagnies d'assurances de personnes inc. (ACCAP) <i>Droit à la vie privée</i> Ligne directrice n° 96	Bureau d'assurance du Canada (BAC) <i>Modèle de code sur les renseignements personnels (1997)</i>
1. Type de document	Directive de l'Union européenne	Législation applicable au secteur privé au Québec	Modèle de code à l'intention des banques	Modèle de lignes directrices à l'intention des assureurs-vie et maladie	Modèle de code à l'intention des assureurs I.A.R.D.
2. Application	Secteurs public et privé	Secteur privé	Membres de l'ABC	Membres de l'ACCAP	Assureurs I.A.R.D. qui adoptent le code
3. Exécution	Élevé	Élevé	Moyen	Faible	Faible à moyen
4. Définition des renseignements personnels	Oui	Oui	Oui	Oui	Oui
5. Définition du consentement	Oui	Oui	Oui	Non	Oui
6. Principe de la limitation en matière de collecte (OCDE)	Moyen	Élevé	Moyen	Faible	Moyen
7. Principe de la qualité des données (OCDE)	Élevé	Moyen à élevé	Moyen	Moyen à élevé	Moyen
8. Principe de la spécification des finalités (OCDE)	Élevé	Moyen à élevé	Faible	Faible	Faible
9. Principe de la limitation de l'utilisation (OCDE)	Élevé	Élevé	Élevé	Élevé	Moyen
10. Principe des garanties de sécurité (OCDE)	Élevé	Moyen	Moyen	Moyen	Moyen
11. Principe de la transparence (OCDE)	Élevé	Faible	Moyen	Faible	Moyen
12. Principe de la participation individuelle (OCDE)	Élevé	Élevé	Moyen	Faible	Moyen à élevé

Élément de comparaison ⁴⁰	Union européenne (UE) <i>Directive relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (1995)</i>	Québec <i>Loi sur la protection des renseignements personnels dans le secteur privé, L.R.Q., ch. P-39.1 (1994)</i>	Association des banquiers canadiens (ABC) <i>Confidentialité – Modèle de code (1996)</i>	Association canadienne des compagnies d'assurances de personnes inc. (ACCAP) <i>Droit à la vie privée</i> Ligne directrice n° 96	Bureau d'assurance du Canada (BAC) <i>Modèle de code sur les renseignements personnels (1997)</i>
13. Principe de la responsabilité (OCDE)	Élevé	Élevé	Moyen	Faible	Faible à moyen
14. Dispositions spécifiques en matière de consentement	Faible	Élevé	Moyen	Faible	Moyen
15. Dispositions limitant le transfert extraterritorial	Oui	Oui	Non	Non	Non
16. Élément présentant un intérêt particulier	Oui Il existe des mesures particulières concernant le traitement des données à caractère personnel, le traitement des données sensibles et la prise de décision automatisée.	Oui Il existe des mesures particulières concernant les « listes nominatives » qui sont définies comme des listes de « noms, adresses ou numéros de téléphone de personnes physiques ». (Art. 22)	Non	Non	Non

Tableau sommaire comparatif (ACFC, C.C.C.C., A.C.N., R.-U., N.-Z.)

Élément de comparaison ⁵⁴¹	Association des compagnies de fiducie du Canada (ACFC) <i>La vie privée des clients : une responsabilité de confiance (1993)</i>	Centrale des caisses de crédit du Canada <i>Credit Union Code for the Protection of Personal Information, projet (1996)</i>	Association canadienne de normalisation <i>Code type sur la protection des renseignements personnels (1996)</i>	Royaume-Uni <i>Data Protection Act 1984 (ch. 35)</i>	Nouvelle-Zélande <i>Privacy Act 1993</i>
1. Type de document	Modèle de code pour les sociétés de fiducie	Projet de modèle de code à l'intention des caisses de crédit	Modèle de code à l'intention des entreprises	Législation fondée sur les principes de l'OCDE	Législation fondée sur les principes de l'OCDE
2. Application	Sociétés de fiducie qui adoptent le code	Caisses de crédit qui adoptent le code	Entreprises qui adoptent le code	Secteurs public et privé	Secteurs public et privé
3. Exécution	Faible	Faible à moyen	Faible	Élevé	Élevé
4. Définition des renseignements personnels	Oui	Oui	Oui	Oui	Oui
5. Définition du consentement	Non	Oui	Oui	Non	Non
6. Principe de la limitation en matière de collecte (OCDE)	Moyen	Faible à moyen	Faible à moyen	Moyen à élevé	Moyen à élevé
7. Principe de la qualité des données (OCDE)	Moyen à élevé	Moyen	Moyen	Élevé	Élevé
8. Principe de la spécification des finalités (OCDE)	Faible	Faible	Faible	Élevé	Moyen à élevé
9. Principe de la limitation de l'utilisation (OCDE)	Moyen	Moyen	Moyen	Élevé	Moyen
10. Principe des garanties de sécurité (OCDE)	Moyen	Moyen	Moyen	Moyen	Moyen
11. Principe de la transparence (OCDE)	Faible	Moyen	Moyen	Élevé	Élevé
12. Principe de la participation individuelle (OCDE)	Moyen	Moyen	Moyen	Élevé	Élevé
13. Principe de la responsabilité (OCDE)	Faible	Faible à moyen	Faible	Élevé	Élevé
14. Dispositions spécifiques en matière de consentement	Faible	Moyen	Moyen	Faible	Faible
15. Dispositions limitant le transfert extraterritorial	Non	Non	Non	Oui	Non
16. Élément présentant un intérêt particulier	Non	Non	Non	Oui	Oui

Tableau comparatif (U.E., Québec, A.B.C., A.C.C.A.P., B.A.C.)

Élément de comparaison	Union européenne (UE) <i>Directive relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (1995)</i>	Québec <i>Loi sur la protection des renseignements personnels dans le secteur privé, L.R.Q., ch. P-39.1 (1994)</i>	Association des banquiers canadiens (ABC) <i>Confidentialité – Modèle de code (1996)</i>	Association canadienne des compagnies d'assurances de personnes inc. (ACCAP) <i>Droit à la vie privée Ligne directrice n° 96</i>	Bureau d'assurance du Canada (BAC) <i>Modèle de code sur les renseignements personnels (1997)</i>
1. Type de document	Directive de l'UE qui doit être adoptée sous forme de loi nationale par les membres de l'Union européenne.	Législation applicable au secteur privé au Québec, fondée sur les principes de l'OCDE. Il est à souligner que le secteur public est visé par une législation antérieure sur l'accès à l'information et la protection de la vie privée.	Modèle de code à l'intention des banques, fondé sur les principes du code type de la CSA. Le code de l'ABC est présenté sous forme de principes et de paragraphes explicatifs.	Modèle de lignes directrices à l'intention des assureurs-vie et maladie fondé sur les principes de l'OCDE. Les lignes directrices sont accompagnées de notes explicatives.	Modèle de code à l'intention des assureurs I.A.R.D. fondé sur les principes du code type de la CSA. Le code du BAC est présenté sous forme de principes accompagnés de paragraphes explicatifs.
2. Application	La directive de l'UE s'applique aux secteurs privé et public.	Secteur privé La Loi s'applique au secteur privé au Québec généralement.	Membres de l'ABC Le Code prévoit que les membres de l'ABC doivent se munir de codes de protection des renseignements personnels conformes au Code.	Membres de l'ACCAP Les lignes directrices se veulent une norme minimale pour les membres de l'ACCAP.	Assureurs I.A.R.D. qui adoptent le Code
3. Exécution	Élevé L'application des dispositions de la directive de l'UE se fait au moyen d'un recours judiciaire dont les personnes physiques et les autorités publiques peuvent se prévaloir.	Élevé La Commission d'accès à l'information du Québec applique la loi.	Moyen L'application du Code se fait au moyen de politiques de protection des renseignements personnels et de procédures de conformité établies par les banques. Toutefois, les personnes insatisfaites du processus de traitement des plaintes d'une banque peuvent porter plainte auprès de l'Ombudsman bancaire canadien.	Faible L'application des lignes directrices se fait au moyen de politiques de protection des renseignements personnels et des procédures de plaintes établies par les assureurs.	Faible à moyen L'application du Code se fait par voie de politiques de protection des renseignements personnels et de procédures de plaintes établies par les assureurs. Dans le cas du refus d'accès aux renseignements, le Code prévoit la possibilité d'une médiation devant une partie indépendante.
4. Définition des renseignements personnels	Oui « "Données à caractère personnel", toute information concernant une personne physique identifiée ou identifiable; est réputée identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, psychique, économique, culturelle ou sociale ». (Art. 2)	Oui « Est un renseignement personnel, tout renseignement qui concerne une personne physique et permet de l'identifier ». (Art. 2)	Oui « Renseignements sur une personne cliente d'une banque. Il s'agit notamment des coordonnées suivantes : nom, adresse, âge, sexe, numéros d'identification, revenu, emploi, actif, passif, source de capitaux, antécédents de remboursement, références personnelles et dossier médical. On peut aussi y trouver à qui la banque a fourni des renseignements et si le crédit a été ou non consenti ». (Définitions)	Oui « "Renseignements personnels" : s'entend de tout renseignement relatif à un particulier, identifié ou identifiable, y compris – mais sans s'y limiter – les renseignements médicaux et financiers ». (Art. 2) Les notes mentionnent ce qui suit : « "Renseignements personnels" s'entend de renseignements relatifs à des particuliers identifiés ou identifiables, mais non de statistiques ou d'autres données concernant des particuliers non identifiables ».	Oui « Enregistrement de renseignements concernant un client, quelle que soit sa forme. Il peut s'agir notamment du nom d'une personne, de son adresse, de son numéro de téléphone, de sa date de naissance, de sa situation de famille, de son état civil, de sa profession ou de son occupation, de ses dossiers médicaux et de santé, de son actif, de son passif, de ses revenus, de sa cote de crédit, du fait qu'un crédit lui a été octroyé ou refusé, de ses antécédents de crédit et de paiement, de ses antécédents en matière d'assurance, y compris son dossier de sinistres, et de son dossier de conducteur ». (Définitions)

<p>Élément de comparaison</p>	<p>Union européenne (UE) <i>Directive relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (1995)</i></p>	<p>Québec <i>Loi sur la protection des renseignements personnels dans le secteur privé.</i> L.R.Q., ch. P-39.1 (1994)</p>	<p>Association des banquiers canadiens (ABC) <i>Confidentialité – Modèle de code (1996)</i></p>	<p>Association canadienne des compagnies d'assurances de personnes Inc. (ACCAP) <i>Droit à la vie privée</i> Ligne directrice n° 96</p>	<p>Bureau d'assurance du Canada (BAC) <i>Modèle de code sur les renseignements personnels (1997)</i></p>
<p>5. Définition du consentement</p>	<p>Oui « Consentement de la personne concernée », toute manifestation de volonté, libre, spécifique et informée par laquelle la personne concernée accepte que des données à caractère personnel la concernant fasse l'objet d'un traitement ». (Art. 2)</p>	<p>Oui « Le consentement à la communication ou à l'utilisation d'un renseignement personnel doit être manifeste, libre, éclairé et être donné à des fins spécifiques. Ce consentement ne vaut que pour la durée nécessaire à la réalisation des fins pour lesquelles il a été demandé. Un consentement qui n'est pas donné conformément à [ce qui précède] est sans effet ». (Art. 14)</p>	<p>Oui « Acquiescement libre. Le consentement peut être explicite, implicite ou fourni par un mandataire autorisé. Le client peut exprimer son consentement explicite de vive voix, par écrit ou électroniquement. Le consentement explicite est non équivoque et ne nécessite aucune inférence de la part de la banque qui obtient le consentement. Il y a consentement implicite lorsque l'action ou l'inaction d'un client permet de déduire raisonnablement qu'il y a consentement. (Définitions)</p>	<p>Non</p>	<p>Oui « Acquiescement libre à ce qui se fait ou est proposé. Le consentement peut être exprimé ou implicite. Le consentement exprimé se donne de façon explicite, de vive voix ou par écrit. Le consentement explicite est non équivoque et n'oblige pas l'assureur I.A.R.D. qui demande le consentement du client à l'inferer. Le consentement implicite survient lorsque les actes ou l'inaction du client permettent raisonnablement de déduire qu'il y a consentement ». (Définitions)</p>
<p>6. Principe de la limitation en matière de collecte (OCDE) Il conviendrait d'assigner des limites à la collecte des données de caractère personnel et toute donnée de ce type devrait être obtenue par des moyens licites et loyaux et, le cas échéant, après en avoir informé la personne concernée ou avec son consentement.</p>	<p>Moyen Les données doivent être collectées pour des « finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement d'une manière incompatible avec ces finalités ». (Art. 6)</p>	<p>Élevé Pour recueillir des renseignements personnels, l'entreprise qui constitue un dossier sur une personne doit le faire en raison d'un intérêt sérieux et légitime (Art. 4) Une entreprise ne peut recueillir que les renseignements « nécessaires » à l'objet du dossier. (Art. 5). Une entreprise ne peut refuser d'acquiescer à une demande de biens ou de services ni à une demande relative à un emploi à cause du refus de la personne qui formule la demande de lui fournir un renseignement personnel, sauf dans l'une ou l'autre des circonstances suivantes : la collecte est nécessaire à la conclusion ou à l'exécution d'un contrat, la collecte est autorisée par la loi, ou s'il y a des motifs raisonnables de croire qu'une telle demande n'est pas licite. (Art. 9)</p>	<p>Moyen « La banque respecte certaines limites quant à la quantité et à la nature des renseignements personnels qu'elle recueille. Elle réunit les renseignements personnels pour les seules fins déjà précisées au client, et procède de façon équitable et légale ». (Principe 4) La banque ne recueille de renseignements que pour : comprendre les besoins du client; déterminer l'adéquation et l'accessibilité des produits et des services pour le client; établir et gérer les produits et les services qui répondent à ces besoins; fournir des services courants; satisfaire aux exigences des lois et règlements. (Paragr. 2.2)</p>	<p>Faible « Seuls des moyens licites seront utilisés pour recueillir des renseignements personnels. (Art. 3) Tous les efforts jugés raisonnables seront faits pour s'assurer que les renseignements personnels recueillis par la société sont : a) pertinents, c'est-à-dire qu'ils servent à mener efficacement les opérations de la société... » (Art. 4)</p>	<p>Moyen « L'assureur I.A.R.D. ne peut recueillir que les renseignements personnels nécessaires aux fins déterminées et doit procéder de façon honnête et licite ». (Art. 4.4) L'assureur recueillera des renseignements personnels aux seules fins : d'établir et de maintenir des communications avec les clients; d'évaluer les risques avec prudence; d'enquêter sur les demandes d'indemnités et les régler; de détecter et de réprimer une fraude; d'offrir et de fournir des produits et services qui répondent aux besoins des clients; de dresser des statistiques; d'observer des lois; et d'une activité à laquelle il peut se livrer aux termes des lois fédérales, provinciales ou territoriales applicables. (Paragr. 4.2.1)</p>

<p>Élément de comparaison</p> <p>7. Principe de la qualité des données (OCDE)</p> <p>Les données de caractère personnel devraient être pertinentes par rapport aux finalités en vue desquelles elles doivent être utilisées et, dans la mesure où ces finalités l'exigent, elles devraient être exactes, complètes et tenues à jour.</p>	<p>Union européenne (UE)</p> <p><i>Directive relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (1995)</i></p> <p>Élevé</p> <p>Les données doivent être traitées « loyalement et licitement ». Les données doivent être « adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et pour lesquelles elles sont traitées ultérieurement ». Les données doivent être « exactes et, si nécessaire, mises à jour ». (Art. 6)</p>	<p>Québec</p> <p><i>Loi sur la protection des renseignements personnels dans le secteur privé. L.R.Q., ch. P-39.1 (1994)</i></p> <p>Moyen à élevé</p> <p>Les renseignements doivent être à jour et exacts au moment où ils sont utilisés pour prendre une décision. (Art. 11)</p>	<p>Association des banquiers canadiens (ABC)</p> <p><i>Confidentialité – Modèle de code (1996)</i></p> <p>Moyen</p> <p>« La banque conserve des renseignements personnels aussi précis, complets, à jour et pertinents que l'exigent les fins auxquelles ils sont collectés et que la banque fait des efforts raisonnables pour « réduire au minimum le risque » de fonder une décision à l'égard d'un client sur des renseignements personnels inexacts, incomplets ou désuets.</p>	<p>Association canadienne des compagnies d'assurances de personnes Inc. (ACCAP)</p> <p><i>Droit à la vie privée</i></p> <p><i>Ligne directrice n° 96</i></p> <p>Moyen à élevé</p> <p>« Tous les efforts jugés raisonnables seront faits pour s'assurer que les renseignements personnels recueillis par la société sont : a) pertinents, c'est-à-dire qu'ils servent à mener efficacement les opérations de la société; b) aussi précis et complets que possibles, et conséquents aux raisons pour lesquelles on les a recueillis ». (Art. 4) Les notes mentionnent que l'objectif visé par la disposition relative à la qualité des données est de « s'assurer que les renseignements obtenus proviennent de sources sûres et que seuls les renseignements pertinents soient recueillis ».</p>	<p>Bureau d'assurance du Canada (BAC)</p> <p><i>Modèle de code sur les renseignements personnels (1997)</i></p> <p>Moyen</p> <p>« Les renseignements personnels doivent être aussi exacts, complets et à jour que l'exigent les fins auxquelles ils sont utilisés ». (Art. 4.6) Le degré de respect de la norme susmentionnée dépend de l'usage des renseignements compte tenu des intérêts du client. Les renseignements devraient être suffisamment exacts, complets et à jour pour « réduire au minimum » la possibilité que des renseignements erronés soient utilisés pour prendre une décision.</p>
<p>8. Principe de la spécification des finalités (OCDE)</p> <p>Les finalités en vue desquelles les données de caractère personnel sont collectées devraient être déterminées au plus tard au moment de la collecte des données et lesdites données ne devraient être utilisées par la suite que pour atteindre ces finalités ou d'autres qui ne soient pas incompatibles avec les précédentes et qui seraient déterminées dès lors qu'elles seraient modifiées.</p>	<p>Élevé</p> <p>Si des données sont collectées auprès d'une personne concernée, le responsable du traitement des données doit fournir : l'identité du responsable; les finalités du traitement des données; toute information supplémentaire telle que les destinataires des données, le fait de savoir si la réponse aux questions est obligatoire et les conséquences éventuelles d'un refus de répondre, ainsi que l'existence de droits d'accès et de rectification des données. (Art. 10). Lorsque les données ne sont pas collectées auprès de la personne concernée, le responsable du traitement des données est encore tenu de fournir les informations dès l'enregistrement des données ou lors de leur communication à un tiers. (Art. 11)</p>	<p>Moyen à élevé</p> <p>Une entreprise qui recueille des renseignements directement auprès de la personne doit l'informer de l'objet du dossier, de l'utilisation des renseignements, de l'endroit où sera déposé son dossier et de ses droits d'accès ou de rectification. (Art. 8)</p> <p>Une entreprise ayant pour objet le prêt d'argent et qui prend connaissance de rapports de crédit doit informer la personne concernée de son droit d'accès et de rectification du rapport déposé par l'agence d'évaluation du crédit. L'entreprise doit communiquer la teneur du rapport de crédit consulté en vue de prendre une décision au sujet de la personne. (Art. 19)</p>	<p>Faible</p> <p>« La banque précise les fins auxquelles doivent servir les renseignements personnels, avant ou au moment de leur collecte ». (Principe 2) La banque recueille des renseignements surtout auprès du client, mais aussi auprès de sources telles que des agences d'évaluation du crédit, des employeurs et d'autres prêteurs. (Paragr. 4.2)</p>	<p>Faible</p> <p>« Les raisons pour lesquelles on demande des renseignements personnels à un particulier lui seront données lors de la collecte ou avant celle-ci, et toute modification de ces raisons lui sera communiquée ». (Art. 5) Les notes mentionnent que si une autorisation est obtenue pour recueillir des renseignements dans le cadre de l'évaluation des risques ou du traitement des demandes de règlement, ces renseignements ne peuvent être utilisés à des fins n'ayant pas de rapport avec celles mentionnées sans que la personne concernée en soit informée.</p>	<p>Faible</p> <p>« Les fins pour lesquelles des renseignements personnels sont recueillis doivent être déterminées par l'assureur I.A.R.D. avant ou au moment de la collecte ». (Art. 4.2) Les assureurs obtiendront des renseignements personnels principalement auprès de leurs clients d'assurances, mais aussi auprès de tiers tels que d'autres assureurs I.A.R.D., des courtiers et des réseaux d'information en matière de production ou de sinistres. (Paragr. 4.4.1)</p>

<p>Élément de comparaison</p> <p>9. Principe de la limitation de l'utilisation (OCDE)</p> <p>Les données de caractère personnel ne devraient pas être divulguées, ni fournies, ni utilisées à des fins autres que celles spécifiées conformément au principe de la spécification des finalités], si ce n'est :</p> <p>a) avec le consentement de la personne concernée; ou b) lorsqu'une règle de droit le permet.</p>	<p>Union européenne (UE)</p> <p><i>Directive relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (1995)</i></p> <p>Élevé</p> <p>Les données de caractère personnel doivent être « collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement de manière incompatible avec ces finalités ».</p> <p>Un traitement ultérieur à des fins historiques, statistiques ou scientifiques sera considéré compatible pour autant que des garanties soient prévues. (Art. 6)</p>	<p>Québec</p> <p><i>Loi sur la protection des renseignements personnels dans le secteur privé.</i> L.R.Q., ch. P-39.1 (1994)</p> <p>Élevé</p> <p>Une entreprise ne peut communiquer ni utiliser des renseignements à des fins non pertinentes à l'objet du dossier à moins que la Loi ne l'y autorise ou que la personne n'y consente. (Art. 13) Il existe un ensemble de plus d'une douzaine d'exceptions permettant la communication de renseignements sans le consentement de la personne. (Art. 18) Une disposition particulière autorise la communication de renseignements à des fins de recherche. (Art. 21) L'utilisation des renseignements contenus dans un dossier n'est permise, une fois l'objet du dossier accompli, qu'avec le consentement de la personne, sous réserve du délai prévu par la loi ou par un calendrier de conservation établi par règlement. (Art. 12)</p>	<p>Association des banquiers canadiens (ABC)</p> <p><i>Confidentialité – Modèle de code (1996)</i></p> <p>Élevé</p> <p>« La banque n'utilise ni ne divulgue des renseignements personnels qu'aux fins pour lesquels ils ont été recueillis, à moins que le client ne consente à ce qu'ils soient utilisés ou divulgués à d'autres fins.</p> <p>Dans certaines circonstances exceptionnelles, la banque a le devoir public ou le droit de divulguer des renseignements personnels sans le consentement du client pour protéger son propre intérêt ou l'intérêt public.</p> <p>La banque ne conserve les renseignements personnels que pour la durée d'utilité et les fins qu'elle a précisées ». (Principe 5)</p> <p>Les paragraphes explicatifs du principe 5 autorisent la divulgation ou l'utilisation des renseignements dans différentes circonstances. Ils établissent aussi des dispositions particulières pour les dossiers médicaux. Les dossiers médicaux ne sont constitués que pour des fins spécifiques. La banque et ses filiales ne se divulguent pas réciproquement des dossiers médicaux. « Par exemple, la banque ne peut pas utiliser les renseignements personnels tirés du dossier médical d'un client de l'une de ses filiales pour évaluer une demande de prêt ».</p> <p>(Paragr. 5.4)</p>	<p>Association canadienne des compagnies d'assurances de personnes Inc. (ACCAP)</p> <p><i>Droit à la vie privée</i> Ligne directrice n° 96</p> <p>Élevé</p> <p>« Les renseignements personnels ne seront pas communiqués ou utilisés à des fins autres que celles données à la personne concernée, sauf : i) si la personne concernée y consent ou ii) si la loi l'exige ou iii) si cela est jugé nécessaire pour déterminer le droit d'une personne de recevoir des prestations ou pour protéger la société contre les actes criminels, la fraude et les fausses déclarations pouvant avoir des conséquences importantes en rapport avec un contrat d'assurance ou iv) dans l'intérêt public. » (Art. 6)</p> <p>Les notes mentionnent qu'une autorisation incluse dans une demande d'adhésion peut permettre la communication à des entités précises (telles que l'employeur) ou à des fins précises. Aussi, les renseignements peuvent être utilisés ou divulgués sans le consentement de la personne concernée lorsqu'elle est assignée à comparaître ou lorsqu'il y a enquête ou surveillance en raison de soupçons de fraude ou en vue de la préparation d'une poursuite judiciaire.</p>	<p>Bureau d'assurance du Canada (BAC)</p> <p><i>Modèle de code sur les renseignements personnels (1997)</i></p> <p>Moyen</p> <p>« Les renseignements personnels ne doivent pas être utilisés ou communiqués à des fins autres que celles auxquelles ils ont été recueillis à moins que le client concerné n'y consente ou que la loi ne l'exige. On ne doit conserver les renseignements personnels qu'aussi longtemps que nécessaire pour la réalisation des finalités déterminées ». (Art. 4.5)</p> <p>Toutefois, il existe des cas dans lesquels les assureurs I.A.R.D. divulguent des renseignements personnels « dans le cadre de pratiques prudentes d'assurances » : pour les fins suivantes : partager le risque avec d'autres sociétés d'assurances; échanger des renseignements personnels à des fins de production, de règlements des sinistres, de classification et de tarification; à des entreprises qui fournissent des biens et services aux sociétés d'assurances et à des clients comme des organismes de traitement des données, des gestionnaires de contrôle des sinistres; et à des intermédiaires d'assurances, tels que les courtiers et les agents. (Paragr. 4.5.1)</p>
-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Élément de comparaison	Union européenne (UE) <i>Directive relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (1995)</i>	Québec <i>Loi sur la protection des renseignements personnels dans le secteur privé, L.R.Q., ch. P-39.1 (1994)</i>	Association des banquiers canadiens (ABC) <i>Confidentialité – Modèle de code (1996)</i>	Association canadienne des compagnies d'assurances de personnes inc. (ACCAP) <i>Droit à la vie privée Ligne directrice n° 96</i>	Bureau d'assurance du Canada (BAC) <i>Modèle de code sur les renseignements personnels (1997)</i>
<p>10. Principe des garanties de sécurité (OCDE)</p> <p>Il conviendrait de protéger les données de caractère personnel, grâce à des garanties de sécurité raisonnables, contre des risques tels que la perte des données ou leur accès, destruction, utilisation, modification ou divulgation non autorisés.</p>	<p>Élevé</p> <p>Le responsable du traitement des données doit mettre en œuvre les mesures techniques et d'organisation appropriées pour protéger les données à caractère personnel contre la destruction accidentelle ou illicite, la perte accidentelle, l'altération, la diffusion ou l'accès non autorisés. (Art. 17)</p> <p>Lorsque le traitement des données est effectué par un tiers pour le compte du responsable du traitement des données, celui-ci doit obtenir des garanties suffisantes au regard des mesures de sécurité techniques et d'organisation. Le tiers doit être régi par un contrat imposant l'obligation de prendre des mesures de sécurité et de n'obéir qu'au responsable du traitement des données.</p>	<p>Moyen</p> <p>Une entreprise qui recueille, détient, utilise ou communiquer des renseignements personnels sur autrui doit prendre « des mesures de sécurité propres à assurer le caractère confidentiel des renseignements ». (Art. 10)</p>	<p>Moyen⁵⁴²</p> <p>« La banque protège les renseignements personnels par des mesures de sécurité qui tiennent compte du risque en cause ». (Principe 7)</p> <p>Des renseignements peuvent être divulgués à un tiers pour impression de chèques, traitement des données ou recouvrement de créances ou encore pour la fourniture d'autres biens et services. Toutefois, la banque exige du tiers qu'il protège ces renseignements. (Paragr. 7.5)</p>	<p>Moyen</p> <p>« Les renseignements personnels seront considérés confidentiels et des mesures exhaustives pour en assurer la confidentialité seront adoptées par les sociétés ».</p> <p>Les agents, les courtiers, les promoteurs de régimes et les autres personnes ou organismes agissant au nom des sociétés devront se conformer aux lignes directrices. (Art. 9)</p>	<p>Moyen</p> <p>« Les renseignements personnels doivent être protégés au moyen de mesures de sécurité correspondant à leur degré de sensibilité ». (Art. 4.7)</p>
<p>11. Principe de la transparence (OCDE)</p> <p>Il conviendrait d'assurer, d'une façon générale, la transparence des progrès, pratiques et politiques, ayant trait aux données de caractère personnel. Il devrait être possible de se procurer aisément les moyens de déterminer l'existence et la nature des données de caractère personnel et les finalités principales de leur utilisation, de même que l'identité du maître du fichier et le siège habituel de ses activités.</p>	<p>Élevé</p> <p>Les États membres prennent des mesures pour assurer la publicité des traitements. En particulier, les États membres prévoient la tenue d'un registre des traitements. Ce registre peut être consulté par toute personne. (Art. 21) Aussi, le responsable du traitement des données doit aviser l'autorité de contrôle établie par l'État membre avant de procéder à tout traitement intégralement ou partiellement automatisé. Des dispenses spécifiques de l'exigence de notification sont prévues.</p>	<p>Faible</p> <p>Il n'existe pas de dispositions particulières concernant la transparence, bien que d'autres obligations (telles que l'obligation de fournir des renseignements sur la collecte ou la consultation d'un rapport de crédit) puissent couvrir certains aspects de la transparence.</p>	<p>Moyen</p> <p>« La banque fait preuve d'ouverture quant aux normes et à ces méthodes qu'elle utilise pour gérer les renseignements personnels. Le client a accès à ces normes et à ces méthodes... » (Principe 8) Sur demande, la banque met à la disposition des exemplaires de son code de protection des renseignements personnels.</p>	<p>Faible</p> <p>« Chaque société doit adopter une politique de transparence quant à ses pratiques et principes en matière d'utilisation et de protection des renseignements personnels... » (Art. 7) Toutefois, il est à souligner que la note explicative de ce principe ne traite que du droit d'accès des particuliers aux renseignements personnels.</p>	<p>Moyen</p> <p>« L'assureur I.A.R.D. doit mettre à la disposition de ses clients des renseignements précis sur sa politique et ses pratiques concernant la gestion des renseignements personnels ». (Art. 4.8) Un client devrait pouvoir obtenir sans efforts déraisonnables de l'information au sujet de cette politique et de ces pratiques.</p>

<p>Élément de comparaison</p> <p>12. Principe de la participation individuelle (OCDE)</p> <p>Toute personne physique devrait avoir le droit :</p> <p>a) d'obtenir du maître d'un fichier, ou par d'autres voies, confirmation du fait que le maître du fichier détient ou non des données la concernant;</p> <p>b) de se faire communiquer les données la concernant i) dans un délai raisonnable;</p> <p>ii) moyennant, éventuellement, une redevance modérée; iii) selon des modalités raisonnables; et iv) sous une forme qui lui soit aisément intelligible;</p> <p>c) d'être informée des raisons pour lesquelles une demande qu'elle aurait présentée conformément aux alinéas a) et b) est rejetée et de pouvoir contester un tel rejet;</p> <p>d) de contester les données la concernant et, si la contestation est fondée, de les faire effacer, rectifier, compléter ou corriger.</p>	<p>Union européenne (UE)</p> <p><i>Directive relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (1995)</i></p> <p>Élevé</p> <p>La directive de l'UE prévoit des droits d'accès et de rectification ainsi que certaines exceptions.</p> <p>Détails : Les dispositions relatives à l'accès et à la rectification prévues dans la Loi complètent les droits prévus dans le <i>Code civil du Québec</i>. Une entreprise doit répondre à une demande d'accès dans un délai de 30 jours et l'omission de répondre est réputée être un refus de l'accès. (Art. 32) L'accès doit être gratuit, sauf pour des frais raisonnables de transcription, de reproduction ou de transmission des renseignements. (Art. 33) Après avoir obtenu l'accès, une personne peut demander la suppression des renseignements personnels dont la collecte n'est pas autorisée par la loi. (Art. 28) L'accès peut être refusé pour différentes raisons personnelles, y compris : un refus temporaire par une entreprise de services professionnels dans le domaine de la santé s'il en résulterait un préjudice grave pour la personne, le refus de l'accès à une personne âgée de moins de 14 ans à des renseignements de nature médicale ou sociale, le refus lorsque l'accès risque de nuire à une enquête sur un crime ou une infraction, le refus lorsque l'accès risque d'avoir un effet sur une procédure judiciaire dans laquelle la personne ou l'entreprise a un intérêt, et le refus lorsque les renseignements contiennent des informations au sujet d'un tiers peut être sérieusement à ce tiers. (Art. 37 à 40)</p> <p>Rectification : En plus de la rectification des données, la personne physique peut demander l'effacement ou le verrouillage si le traitement des données la concernant n'est pas conforme à la directive de l'UE. La personne concernée peut exiger la notification aux tiers à qui les données ont été communiquées de toute rectification, de l'effacement ou du verrouillage des données, si cela ne s'avère pas impossible ou disproportionné. (Art. 12 et 13)</p>	<p>Québec</p> <p><i>Loi sur la protection des renseignements personnels dans le secteur privé. L.R.Q., ch. P-39.1 (1994)</i></p> <p>Moyen</p> <p>Le Code prévoit des droits d'accès et de rectification. La banque n'est tenue de communiquer une rectification à un tiers qu'« au besoin ».</p> <p>Accès : L'accès doit être donné au client dans un délai raisonnable et à un coût minime ou gratuitement. L'accès peut être refusé dans des cas « spécifiques » dont les suivants : l'extraction est trop coûteuse, les renseignements font allusion à d'autres personnes, les renseignements sont assujettis au secret professionnel, il s'agit de renseignements exclusifs de la banque et les renseignements ne peuvent être divulgués légalement. (Principe 9)</p> <p>Rectification : Lorsqu'un client démontre que les renseignements sont « inexacts, incomplets, désuets ou non pertinents » la banque procède à leur révision. La banque divulgue les renseignements personnels révisés aux tiers qui ont reçu les anciens renseignements « au besoin ». Si la banque refuse une demande de révision des renseignements, le client peut contester cette décision. La banque devrait prendre note de cette contestation et, au besoin, la communiquer aux tiers. (Paragr. 6.4 et 6.5)</p>	<p>Association des banquiers canadiens (ABC)</p> <p><i>Confidentialité – Modèle de code (1996)</i></p> <p>Faible</p> <p>Les lignes directrices prévoient des droits d'accès et de rectification. La liste d'exceptions n'est pas exhaustive. Le droit de rectification est bref et il ne traite pas de la question de savoir si l'assureur devrait communiquer une rectification à un tiers.</p> <p>Détails : « a) Après s'être dûment identifiés et en avoir fait la demande par écrit à la société dans des formes acceptables par elle, les particuliers seront informés des renseignements personnels contenus à leur sujet dans les dossiers de la société. La société peut fournir des renseignements moyennant des frais administratifs raisonnables. Il est possible que certains renseignements médicaux ne puissent être obtenus auprès du médecin du particulier.</p> <p>b) Quand l'information ne pourra être communiquée à la personne en cause, on lui en fournira les raisons.</p> <p>c) Les particuliers pourront clarifier les renseignements que détiennent les sociétés à leur sujet ou corriger les erreurs qu'ils contiennent. L'information erronée ou incomplète sera rectifiée et tout écart relevé sera pris en note ». (Art. 7)</p> <p>Les notes mentionnent que les assureurs peuvent refuser de divulguer des renseignements « à moins qu'il soit inacceptable, du point de vue juridique, de le faire » et dans des cas où les renseignements sont obtenus auprès d'organismes spécialisés dans la surveillance.</p>	<p>Association canadienne des compagnies d'assurances de personnes Inc. (ACCAP)</p> <p><i>Droit à la vie privée</i></p> <p><i>Ligne directrice n° 96</i></p> <p>Moyen</p> <p>Le Code prévoit des droits d'accès et de rectification. La liste des exceptions n'est pas exhaustive. Le Code propose une médiation devant une partie indépendante en cas de refus d'accès à l'information. L'assureur est tenu de communiquer une rectification à un tiers « s'il y a lieu ».</p> <p>Accès : L'accès devrait être donné dans un délai raisonnable et à un coût minime sinon nul. Les exceptions en matière devraient être « restreintes et précises ». Les motifs de refus d'accès peuvent comprendre : le coût prohibitif, le fait que les renseignements personnels contiennent des détails sur d'autres personnes, l'existence de raisons d'ordre juridique, de raisons de sécurité ou de raisons liées à des secrets commerciaux exclusifs et le fait que les renseignements sont visés par le privilège du secret professionnel de l'avocat ou par le privilège applicable en cas de procédures judiciaires. L'assureur peut choisir que les renseignements médicaux sensibles soient communiqués par un médecin. (Art. 4.9)</p> <p>Accès refusé : Si une demande d'accès est rejetée, le client doit être informé de la façon de contester ce refus et notamment : être invité à transmettre une lettre au président de l'assureur, obtenir l'engagement de la part de l'assureur d'établir un dialogue, et d'obtenir l'engagement de la part de l'assureur de participer à un processus de médiation indépendante si les parties ne parviennent pas à régler le différend. Le Bureau d'assurance du Canada aidant les parties à prendre des dispositions en vue de cette médiation indépendante. (Paragr. 4.9.1)</p> <p>Rectification : Lorsqu'un client démontre que des renseignements sont inexacts ou incomplets, l'assureur doit modifier ces renseignements. « S'il y a lieu », les renseignements modifiés doivent être communiqués à des tiers ayant accès à l'information en question. Lorsqu'un différend n'est pas réglé à la satisfaction du client, le fond de la plainte devrait être enregistré et « s'il y a lieu », les tierces parties ayant accès à l'information en question devraient être informées de ce différend. (Paragr. 4.9.5 et 4.9.6)</p>	<p>Bureau d'assurance du Canada (BAC)</p> <p><i>Modèle de code sur les renseignements personnels (1997)</i></p> <p>Moyen</p> <p>Le Code prévoit des droits d'accès et de rectification. La liste des exceptions n'est pas exhaustive. Le Code propose une médiation devant une partie indépendante en cas de refus d'accès à l'information. L'assureur est tenu de communiquer une rectification à un tiers « s'il y a lieu ».</p> <p>Accès : L'accès devrait être donné dans un délai raisonnable et à un coût minime sinon nul. Les exceptions en matière devraient être « restreintes et précises ». Les motifs de refus d'accès peuvent comprendre : le coût prohibitif, le fait que les renseignements personnels contiennent des détails sur d'autres personnes, l'existence de raisons d'ordre juridique, de raisons de sécurité ou de raisons liées à des secrets commerciaux exclusifs et le fait que les renseignements sont visés par le privilège du secret professionnel de l'avocat ou par le privilège applicable en cas de procédures judiciaires. L'assureur peut choisir que les renseignements médicaux sensibles soient communiqués par un médecin. (Art. 4.9)</p> <p>Accès refusé : Si une demande d'accès est rejetée, le client doit être informé de la façon de contester ce refus et notamment : être invité à transmettre une lettre au président de l'assureur, obtenir l'engagement de la part de l'assureur d'établir un dialogue, et d'obtenir l'engagement de la part de l'assureur de participer à un processus de médiation indépendante si les parties ne parviennent pas à régler le différend. Le Bureau d'assurance du Canada aidant les parties à prendre des dispositions en vue de cette médiation indépendante. (Paragr. 4.9.1)</p> <p>Rectification : Lorsqu'un client démontre que des renseignements sont inexacts ou incomplets, l'assureur doit modifier ces renseignements. « S'il y a lieu », les renseignements modifiés doivent être communiqués à des tiers ayant accès à l'information en question. Lorsqu'un différend n'est pas réglé à la satisfaction du client, le fond de la plainte devrait être enregistré et « s'il y a lieu », les tierces parties ayant accès à l'information en question devraient être informées de ce différend. (Paragr. 4.9.5 et 4.9.6)</p>
---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

<p>Élément de comparaison</p> <p>13. Principe de la responsabilité (OCDE)</p> <p>Tout maître de fichier devrait être responsable du respect des mesures donnant effet aux principes énoncés ci-dessus.</p>	<p>Union européenne (UE)</p> <p><i>Directive relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (1995)</i></p> <p>Élevé</p> <p>La Directive ne traite pas du principe de responsabilité en particulier, mais d'autres dispositions traitent de certains aspects de la responsabilité (c'est-à-dire l'obligation d'informer la personne physique de la collecte ou de l'utilisation des données, et l'obligation imposée aux responsables du traitement des données de s'inscrire auprès des autorités publiques). L'application se fait par l'intermédiaire des autorités judiciaires et au moyen de recours judiciaires.</p>	<p>Québec</p> <p><i>Loi sur la protection des renseignements personnels dans le secteur privé.</i></p> <p>L.R.Q., ch. P-39.1 (1994)</p> <p>Élevé</p> <p>La Loi ne traite pas du principe de responsabilité en particulier, mais d'autres dispositions traitent de certains aspects de la responsabilité (c'est-à-dire, l'obligation d'informer la personne au moment de la collecte des données et l'obligation d'informer la personne de certains renseignements si un rapport de crédit est utilisé). L'application se fait par l'intermédiaire d'un organisme public qui a le pouvoir d'entendre les plaintes.</p>	<p>Association des banquiers canadiens (ABC)</p> <p><i>Confidentialité – Modèle de code (1996)</i></p> <p>Moyen</p> <p>Le Code renferme un exposé général de la responsabilité et des procédures internes de règlement des plaintes. Une personne qui n'est pas satisfaite du processus de traitement des plaintes de sa banque peut porter plainte à l'Ombudsman bancaire canadien.</p> <p>Responsabilité : « La banque est responsable de tous les renseignements personnels en sa possession, y compris les renseignements personnels divulgués à des tiers pour traitement. La banque établit des normes et des méthodes et désigne une ou plusieurs personnes responsables de s'assurer du respect du code de confidentialité ». (Principe 1)</p> <p>Plaintes : Chaque banque dispose de politiques et de procédures régissant la réception, l'enquête et la réponse en matière de plaintes. La banque fait enquête sur toutes les plaintes. Si une plainte est motivée, la banque y remédie. Si le client n'est pas satisfait de la manière dont la banque a répondu à sa plainte, il peut communiquer avec le Bureau du surintendant des institutions financières ou l'Ombudsman du secteur bancaire. (Principe 10)</p>	<p>Association canadienne des compagnies d'assurances de personnes Inc. (ACCAP)</p> <p><i>Droit à la vie privée</i></p> <p>Ligne directrice n° 96</p> <p>Faible</p> <p>Les lignes directrices traitent brièvement de la responsabilité et de la nécessité d'établir des procédures internes pour traiter les plaintes.</p> <p>Responsabilité : L'avant-propos des lignes directrices mentionne que « les sociétés d'assurances doivent suivre de près des règles strictes sur la protection des renseignements confidentiels qu'elles détiennent ».</p> <p>Responsabilité : « Pour s'assurer d'agir conformément aux lignes directrices, chaque société :</p> <p>a) nommera un cadre supérieur responsable de l'enregistrement des plaintes; b) établira des mécanismes d'enregistrement et de traitement des plaintes. Les particuliers insatisfaits du mécanisme de traitement des plaintes d'une société pourront communiquer avec le bureau des responsables de la réglementation de l'assurance de leur territoire de compétence ». (Art. 8).</p>	<p>Bureau d'assurance du Canada (BAC)</p> <p><i>Modèle de code sur les renseignements personnels (1997)</i></p> <p>Faible à moyen</p> <p>Le Code traite en général de la responsabilité et des procédures internes de plaintes. Le Code prévoit la possibilité d'une médiation devant un médiateur indépendant en cas de refus d'accès à l'information.</p> <p>Responsabilité : « L'assureur I.A.R.D. est responsable des renseignements personnels dont il a la gestion et doit désigner une ou des personnes qui devront s'assurer du respect des principes énoncés ci-dessous ». (Art. 4.1)</p> <p>Plaintes : L'assureur doit établir des mécanismes pour recevoir les plaintes. Il doit faire enquête sur toutes les plaintes et si une plainte est jugée fondée, il doit la régler. Les clients doivent être informés de leur droit de porter plainte. Par exemple, les clients insatisfaits peuvent porter plainte aux autorités de réglementation. (Voir l'art. 4.10 en général). Aussi, en cas de refus d'accès à l'information, le Code prévoit la possibilité d'une médiation devant un médiateur indépendant. (Paragr. 4.9.1)</p>
-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

<p>Élément de comparaison</p>	<p>Union européenne (UE)</p> <p><i>Directive relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (1995)</i></p>	<p>Québec</p> <p><i>Loi sur la protection des renseignements personnels dans le secteur privé.</i> L.R.Q., ch. P-39.1 (1994)</p>	<p>Association des banquiers canadiens (ABC)</p> <p><i>Confidentialité – Modèle de code (1996)</i></p>	<p>Association canadienne des compagnies d'assurances de personnes Inc. (ACCAP)</p> <p><i>Droit à la vie privée</i> Ligne directrice n° 96</p>	<p>Bureau d'assurance du Canada (BAC)</p> <p><i>Modèle de code sur les renseignements personnels (1997)</i></p>
<p>14. Dispositions spécifiques en matière de consentement</p>	<p>Faible</p> <p>La Directive ne traite pas en détail du consentement, mais le consentement est mentionné dans les dispositions permettant l'utilisation des données à une nouvelle fin.</p>	<p>Élevé</p> <p>La Loi ne traite pas en détail du consentement, mais le consentement est mentionné dans les dispositions permettant l'utilisation de renseignements à une nouvelle fin. La Loi fixe une norme très élevée en ce qui a trait à la nature du consentement. (Voir ci-dessus la définition de la notion de consentement).</p>	<p>Moyen</p> <p>« La banque fait un effort raisonnable pour s'assurer que le client comprend dans quelles circonstances elle utilise et divulgue des renseignements personnels. Elle obtient son consentement avant ou au moment de recueillir, d'utiliser ou de divulguer les renseignements personnels le concernant.Le consentement d'un client peut être explicite, implicite ou fourni par un mandataire autorisé... toutefois, la banque peut recueillir, utiliser ou divulguer des renseignements personnels sans le consentement du client pour des motifs d'ordre juridique ou reliés à la sécurité ou, dans certains cas, pour des questions liées à leur traitement ». (Principe 3) Le client peut retirer son consentement, sous réserve de restrictions d'ordre contractuel, dans la mesure où la banque en est avisée dans un délai raisonnable et où le consentement ne s'applique pas à un produit de crédit à l'égard duquel la banque doit obtenir et divulguer de l'information après avoir octroyé un crédit. La banque peut demander le NAS pour consulter les dossiers de l'agence d'évaluation du crédit mais elle ne peut exiger ce renseignement.</p>	<p>Faible</p> <p>Les lignes directrices ne traitent pas en détail du consentement. Le consentement est mentionné brièvement dans des dispositions traitant de la collecte de renseignements et de l'utilisation ou de la divulgation de renseignements.</p>	<p>Moyen</p> <p>« Tout client doit être informé et consentir à toute collecte, utilisation ou communication de renseignements personnels qui le concernent, à moins qu'il ne soit pas approprié de le faire ». (Art. 4.3)</p> <p>Des renseignements peuvent être recueillis, utilisés et communiqués dans certaines circonstances telles que celles qui concernent des motifs d'ordre juridique, médical ou de sécurité. Lorsque l'assureur n'est pas en relation directe avec le client (c'est-à-dire lorsque celui-ci fait affaires avec un courtier ou un agent indépendant), il se peut que l'assureur I.A.R.D. ne soit pas en mesure de demander le consentement. Toutefois, si certains types de renseignements sont recueillis – tels que des dossiers médicaux ou hospitaliers, des dossiers d'emploi ou des dossiers concernant l'impôt sur le revenu – l'assureur I.A.R.D. obtiendra le consentement explicite du client. Le consentement peut être retiré sous réserve de restrictions contractuelles et de l'exigence que les assureurs préservent l'intégrité des statistiques et des données nécessaires.</p>

<p>Élément de comparaison</p>	<p>Union européenne (UE)</p> <p><i>Directive relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (1995)</i></p>	<p>Québec</p> <p><i>Loi sur la protection des renseignements personnels dans le secteur privé.</i> L.R.Q., ch. P-39.1 (1994)</p>	<p>Association des banquiers canadiens (ABC)</p> <p><i>Confidentialité – Modèle de code (1996)</i></p>	<p>Association canadienne des compagnies d'assurances de personnes inc. (ACCAP)</p> <p><i>Droit à la vie privée</i> Ligne directrice n° 96</p>	<p>Bureau d'assurance du Canada (BAC)</p> <p><i>Modèle de code sur les renseignements personnels (1997)</i></p>
<p>15. Dispositions limitant le transfert extraterritorial</p>	<p>Oui</p> <p>L'article 25 prévoit que le transfert des données en vue de leur traitement peut se faire seulement si le pays destinataire offre un niveau de protection adéquat. Le caractère adéquat est évalué à la lumière des circonstances relatives à un transfert projeté. « Sont prises en considération la nature des données, la finalité et la durée du ou des traitements envisagés, les pays d'origine et de destination finale, les règles de droit, générales ou sectorielles, en vigueur dans le pays tiers en cause, ainsi que les règles professionnelles et les mesures de sécurité qui y sont respectées ».</p> <p>L'article 26 prévoit certaines exceptions à l'article 25. Par exemple, notwithstanding l'article 25, un transfert peut être effectué si : la personne concernée y a consenti, le transfert est nécessaire à l'exécution d'un contrat conclu avec la personne concernée, le transfert est nécessaire à l'exécution d'un contrat dans l'intérêt de la personne concernée, ou le transfert est nécessaire ou juridiquement obligatoire pour la sauvegarde d'un intérêt public important. Le transfert est aussi possible lorsque le responsable du traitement des données offre des garanties suffisantes au moyen, par exemple, de mesures contractuelles.</p>	<p>Oui</p> <p>Avant de communiquer des renseignements concernant des résidents du Québec à une personne à l'extérieur du Québec, une entreprise située au Québec doit « prendre tous les moyens raisonnables » pour s'assurer que : 1) les renseignements ne seront pas utilisés à des fins non pertinentes à l'objet du dossier ni communiqués à des tiers sans le consentement de la personne concernée sauf dans la mesure où les exceptions prévues par la loi le permettent; 2) les dispositions de la Loi concernant le tranchement de noms de listes nominatives seront suivies. (Art. 17)</p>	<p>Non</p>	<p>Non</p>	<p>Non</p>

<p>Élément de comparaison</p>	<p>Union européenne (UE)</p> <p><i>Directive relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (1995)</i></p>	<p>Québec</p> <p><i>Loi sur la protection des renseignements personnels dans le secteur privé.</i> L.R.Q., ch. P-39.1 (1994)</p>	<p>Association des banquiers canadiens (ABC)</p> <p><i>Confidentialité – Modèle de code (1996)</i></p>	<p>Association canadienne des compagnies d'assurances de personnes inc. (ACCAP)</p> <p><i>Droit à la vie privée</i> Ligne directrice n° 96</p>	<p>Bureau d'assurance du Canada (BAC)</p> <p><i>Modèle de code sur les renseignements personnels (1997)</i></p>
<p>16. Élément présentant un intérêt particulier</p>	<p>Oui</p> <p>Il existe des mesures spéciales concernant le traitement des données à caractère personnel, le traitement des données sensibles et la prise de décision automatisée.</p> <p>Traitement en général : La directive de l'UE interdit le caractère personnel à moins qu'il ne s'agisse de l'une des six exceptions suivantes : la personne concernée a donné son consentement, le traitement est nécessaire à l'exécution d'un contrat, au respect d'une obligation légale, à la sauvegarde de l'intérêt vital de la personne concernée, à l'exécution d'une mission d'intérêt public ou à la réalisation de l'intérêt légitime du responsable du traitement des données (art. 7)</p> <p>Traitement de données délicates : La directive de l'UE interdit généralement le traitement de certains types de données à caractère personnel délicates – c'est-à-dire des données « qui révèlent l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale » ou les données « relatives à la santé et à la vie sexuelle ». Toutefois, il existe un certain nombre d'exceptions à cette interdiction d'ordre général. (Art. 8)</p> <p>Prise de décision automatisée : La directive de l'UE prévoit le droit d'une personne de ne pas être soumise à certains types de prises de décisions automatisées. « Toute personne a le droit de ne pas être soumise à une décision produisant des effets juridiques à son égard ou l'affectant de manière significative, prise sur le seul fondement d'un traitement automatisé de données destiné à évaluer certains aspects de sa personnalité, tels que son rendement professionnel, son crédit, sa fiabilité, son comportement, etc. ». Toutefois, la directive de l'UE autorise une telle prise de décision en vertu d'un contrat ou d'une loi nationale si certaines conditions sont réunies. (Art. 15)</p>	<p>Oui</p> <p>Il existe des mesures spéciales concernant les « listes nominatives » qui sont définies comme des listes de « noms, adresses ou numéros de téléphone de personnes physiques ». (Art. 22)</p> <p>Listes nominatives : Les listes nominatives peuvent être communiquées à un tiers seulement si certaines conditions sont réunies, lesquelles incluent l'exigence selon laquelle, avant la communication, chaque personne mentionnée sur la liste s'est vue accorder une « occasion valable » de faire retrancher son nom de la liste. (Art. 22) Une entreprise peut utiliser une liste nominative de clients, d'employés ou de membres à des fins de prospection commerciale ou philanthropique. Toutefois, chaque personne mentionnée sur la liste doit avoir une « occasion valable » de faire retrancher son nom. (Art. 23) Une entreprise qui utilise une liste nominative à des fins de prospection commerciale ou philanthropique par la poste ou par téléphone doit s'identifier et informer la personne à qui elle s'adresse de son droit de faire retrancher de la liste son nom et les renseignements personnels la concernant. (Art. 24) La personne peut demander de faire retrancher son nom d'une liste par écrit ou verbalement et son nom doit être retranché avec diligence raisonnable. (Art. 25 et 26)</p>	<p>Non</p>	<p>Non</p>	<p>Non</p>

Tableau comparatif (A.C.F.C., C.C.C.C., A.C.N., R.-U., N.-Z.)

Élément de comparaison	Association des compagnies de fiducie du Canada (ACFC) <i>La vie privée des clients : une responsabilité de confiance (1993)</i>	Centrale des caisses de crédit du Canada <i>Credit Union Code for the Protection of Personal Information, projet (1996)</i>	Association canadienne de normalisation <i>Code type sur la protection des renseignements personnels (1996)</i>	Royaume-Uni <i>Data Protection Act 1984 (ch. 35)</i>	Nouvelle-Zélande <i>Privacy Act 1993</i>
1. Type de document	Modèle de code à l'intention des sociétés de fiducie fondé sur les principes de l'OCDE. Le Code de l'ACFC est structuré selon les principes de l'OCDE accompagnés de paragraphes explicatifs.	Projet de modèle de code à l'intention des caisses de crédit fondé sur le code type de la CSA. Le code de la CCCC est présenté sous forme de principes accompagnés de paragraphes explicatifs.	Modèle de code à l'intention des entreprises à adapter à la situation particulière du secteur d'activité de l'entreprise. Le Code de la CSA est présenté sous forme de principes accompagnés de paragraphes explicatifs.	Législation fondée sur les principes de l'OCDE qui régissent l'utilisation des données traitées automatiquement.	Législation néo-zélandaise en matière de protection de la vie privée fondée sur les principes de l'OCDE
2. Application	Sociétés de fiducie qui adoptent le Code	Les sociétés de crédit qui adoptent le Code	Entreprises qui adoptent le Code	Secteurs public et privé La Loi s'applique aux secteurs privé et public et vise le traitement automatisé des renseignements, mais elle ne régit pas les renseignements contenus dans des registres manuscrits.	Secteurs public et privé La Loi s'applique à toutes personnes ou organisations en Nouvelle-Zélande à l'égard des renseignements personnels détenus pour une autre fin que leurs affaires personnelles, familiales ou domestiques.
3. Exécution	Faible L'application se fait par voie de politiques et de procédures de plaintes établies par les sociétés de fiducie.	Faible à moyen L'application se fait par voie de politiques de protection des renseignements personnels et de procédures de plaintes établies par les caisses de crédit. Le Code prévoit que si la plainte d'une personne n'est pas réglée au sein de la caisse de crédit, des procédures devraient être prévues pour la soumettre à la Centrale des caisses de crédit ou à un médiateur ou arbitre indépendant.	Faible L'application se fait par voie de politiques et de procédures de plaintes établies par les entreprises qui adoptent le Code. Le Code prévoit aussi que les entreprises devraient informer les clients des mécanismes de plainte dont ils peuvent se prévaloir, y compris les organismes de réglementation qui acceptent de recevoir les plaintes.	Élevé Le registraire responsable de la protection des données est chargé d'appliquer la Loi et de favoriser le respect des principes. Un recours judiciaire est prévu dans certains cas.	Élevé L'application des dispositions de la Loi se fait par l'intermédiaire du Commissaire à la vie privée, bien que le Commissaire chargé des instances et le Tribunal d'examen des plaintes puissent délivrer des ordonnances en matière de dommages-intérêts ou interdire certaines actions. Chaque organisation ou agence doit désigner au moins un responsable de la protection des renseignements personnels, dont le rôle consiste à favoriser le respect des principes de protection des renseignements personnels et de la Loi. (Art. 23)
4. Définition des renseignements personnels	Oui « Les renseignements personnels signifient les données qui permettent d'identifier et d'établir un rapport avec une personne en particulier. Cela comprend, sans toutefois s'y restreindre, le nom de la personne, son adresse, son âge, ses numéros d'identification, ses éléments d'actif et de passif, son revenu, le nom de tiers à qui des renseignements ont été divulgués, le fait qu'un crédit lui a ou non été accordé et les dossiers relatifs aux paiements ». (Paragr. 2(2))	Oui [TRADUCTION] « Enregistrement de renseignements concernant un individu identifiable, quelle que soit sa forme ». (Définitions)	Oui « Enregistrement de renseignements concernant un individu identifiable, quelle que soit sa forme ». (Paragr. 2.1)	Oui [TRADUCTION] « "Données à caractère personnel" : Données consistant en renseignements qui se rapportent à une personne physique vivante qui peut être identifiée à partir de ces renseignements (ou à partir de ces renseignements et d'autres renseignements en la possession de l'utilisateur de données), y compris toute expression d'opinion au sujet de la personne physique, mais non une indication des intentions de l'utilisateur des données à l'égard de cette personne physique ». (Art. 1)	Oui [TRADUCTION] « "Renseignements personnels" : renseignements au sujet d'une personne identifiable; et inclut des renseignements contenus dans tout registre de décès tenu en vertu de la <i>Births and Deaths Registration Act 1951</i> ». (Art. 2)

Élément de comparaison	Association des compagnies de fiduciaire du Canada (ACFC) <i>La vie privée des clients : une responsabilité de confiance (1993)</i>	Centrale des caisses de crédit du Canada <i>Credit Union Code for the Protection of Personal Information, projet (1996)</i>	Association canadienne de normalisation <i>Code type sur la protection des renseignements personnels (1996)</i>	Royaume-Uni <i>Data Protection Act 1984 (ch. 35)</i>	Nouvelle-Zélande <i>Privacy Act 1993</i>
5. Définition du consentement	Non	Oui [TRADUCTION] « Acquiescement libre à ce qui se fait ou est proposé. Le consentement peut être exprimé ou implicite. Le consentement exprimé se donne de façon explicite, de vive voix ou par écrit. Le consentement explicite est non équivoque et n'oblige pas la caisse de crédit qui demande le consentement de la personne à l'inferer. Le consentement implicite survient lorsque les actes ou l'inaction de la personne permettent raisonnablement de déduire qu'il y a consentement ». (Définitions)	Oui « Acquiescement libre à ce qui se fait ou est proposé. Le consentement peut être exprimé ou implicite. Le consentement exprimé se donne de façon explicite, de vive voix ou par écrit. Le consentement explicite est non équivoque et n'oblige pas l'organisme qui le demande à l'inferer. Le consentement implicite survient lorsque les actes ou l'inaction de la personne permettent raisonnablement de déduire qu'il y a consentement ». (Paragr. 2.1)	Non	Non

Élément de comparaison	Association des compagnies de fiducie du Canada (ACFC) <i>La vie privée des clients : une responsabilité de confiance</i> (1993)	Centrale des caisses de crédit du Canada <i>Credit Union Code for the Protection of Personal Information, projet</i> (1996)	Association canadienne de normalisation <i>Code type sur la protection des renseignements personnels</i> (1996)	Royaume-Uni <i>Data Protection Act 1984</i> (ch. 35)	Nouvelle-Zélande <i>Privacy Act 1993</i>
<p>6. Principe de la limitation en matière de collecte (OCDE)</p> <p>Il conviendrait d'assigner des limites à la collecte des données de caractère personnel et toute donnée de ce type devrait être obtenue par des moyens licites et loyaux et, le cas échéant, après en avoir informé la personne concernée ou avec son consentement.</p>	<p>Moyen</p> <p>« Les sociétés de fiducie membres ne recueillent que les renseignements personnels dont elles ont besoin au sujet de leurs clients pour les fins précisées au paragraphe 6(2) du présent Code... » (Paragr. 4(1)). Le paragraphe 6(2) prévoit les fins suivantes : établir et maintenir des relations avec les clients; offrir et assurer la prestation de produits et services, tel que permis par la loi; se conformer à la loi; et protéger les intérêts des clients et ceux de la société de fiducie. Les sociétés de fiducie ne recueillent des renseignements personnels que par des moyens légaux.</p>	<p>Faible à moyen</p> <p>[TRADUCTION] « La caisse de crédit ne peut recueillir que les renseignements nécessaires aux fins déterminées et doit procéder de façon honnête et licite ». (Principe 4) La caisse de crédit recueille des renseignements pour les fins suivantes : aider à comprendre les besoins du client; déterminer l'adéquation et l'accessibilité des produits et services pour le membre; établir, offrir et gérer des produits et services, qui répondent aux besoins du membre; fournir des services courants; satisfaire aux exigences des lois et règlements. (Paragr. 2.2)</p>	<p>Faible à moyen</p> <p>« <i>Limitation de la collecte</i> : L'organisme ne peut recueillir que les renseignements personnels nécessaires aux fins déterminées et doit procéder de façon honnête et licite ». (Principe 4) Les entreprises ne doivent pas recueillir des renseignements de façon arbitraire. On doit restreindre tant la quantité que la nature des renseignements recueillis à ce qui est nécessaire pour réaliser les fins déterminées.</p>	<p>Moyen à élevé</p> <p>L'utilisateur des données ne peut caractériser personnel qui se conforme à la description des données fournies au registraire au moment de l'enregistrement. (Art. 4 et 5). [TRADUCTION] « Les renseignements contenus dans les données à caractère personnel doivent être obtenus, et les données à caractère personnel doivent être traitées, de façon honnête et licite ». (Principe 1) Pour déterminer si les renseignements ont été obtenus de façon honnête, [TRADUCTION] « il est tenu compte de la méthode au moyen de laquelle ils ont été obtenus, y compris, en particulier, la question de savoir si une personne de qui ils ont été obtenus a été trompée ou incluse en erreur quant à la fin ou aux fins pour lesquelles les renseignements devaient être détenus, utilisés ou divulgués ». (Interprétation du Principe 1)</p>	<p>Moyen à élevé</p> <p>Les principes 2 à 4 en matière de protection des renseignements personnels limitent ou restreignent la collecte des renseignements personnels par les agences (c'est-à-dire toute personne, société ou ministère gouvernemental). [TRADUCTION] « Lorsqu'une agence recueille des renseignements personnels, elle doit les recueillir directement auprès de la personne concernée ». (Principe 2) Les renseignements personnels ne doivent pas être recueillis par des moyens illégitimes ou par des moyens qui sont malhonnêtes ou déraisonnablement intrusifs. (Principe 4)</p>
<p>7. Principe de la qualité des données (OCDE)</p> <p>Les données de caractère personnel devraient être pertinentes par rapport aux finalités en vue desquelles elles doivent être utilisées et, dans la mesure où ces finalités l'exigent, elles devraient être exactes, complètes et tenues à jour.</p>	<p>Moyen à élevé</p> <p>« Au meilleur de leurs capacités, les sociétés de fiducie membres veilleront à ce que les renseignements personnels qu'elles conservent au sujet de leurs clients soient aussi précis, complets pour les fins visées et à jour que possible... » (Paragr. 5(1))</p>	<p>Moyen</p> <p>[TRADUCTION] « Les renseignements personnels doivent être aussi exacts, complets et à jour que l'exigent les fins pour lesquelles ils sont utilisés ». (Principe 6) Le degré de respect de cette norme dépend de l'usage auquel les renseignements sont destinés, compte tenu des intérêts du membre. Les renseignements doivent être suffisamment exacts, complets et à jour pour [TRADUCTION] « réduire au minimum » la possibilité que des renseignements erronés soient utilisés pour prendre une décision au sujet de la personne concernée.</p>	<p>Moyen</p> <p>« <i>Exactitude</i> : Les renseignements personnels doivent être aussi exacts, complets et à jour que l'exigent les fins pour lesquelles ils sont utilisés ». (Principe 6) Le degré de respect de cette norme dépend de l'usage auquel les renseignements sont destinés, compte tenu des intérêts de la personne. Les renseignements doivent être suffisamment exacts, complets et à jour pour « réduire au minimum » la possibilité que des renseignements erronés soient utilisés pour prendre une décision au sujet de la personne concernée.</p>	<p>Élevé</p> <p>[TRADUCTION] « Les données à caractère personnel détenues à une ou plusieurs fins doivent être adéquates, pertinentes et non excessives par rapport à cette ou ces fins ». (Principe 4) [TRADUCTION] « Les données à caractère personnel doivent être exactes et, s'il y a lieu, mises à jour ». (Principe 5) Les données ne doivent pas être [TRADUCTION] « conservées plus longtemps que nécessaire ». (Principe 6)</p>	<p>Élevé</p> <p>[TRADUCTION] « Une agence qui détient des renseignements ne doit pas les utiliser sans prendre les mesures (le cas échéant) qui sont, dans les circonstances, raisonnables pour s'assurer que, compte tenu de la fin pour laquelle les renseignements doivent être utilisés, les renseignements sont exacts, à jour, complets, pertinents et non trompeurs ». (Principe 8) [TRADUCTION] « Une agence qui détient des renseignements personnels ne doit pas conserver les renseignements plus longtemps que nécessaire pour les fins pour lesquelles les renseignements peuvent être légitimement utilisés ». (Principe 9)</p>

Élément de comparaison	Association des compagnies de fiducie du Canada (ACFC) <i>La vie privée des clients : une responsabilité de confiance (1993)</i>	Centrale des caisses de crédit du Canada <i>Credit Union Code for the Protection of Personal Information, projet (1996)</i>	Association canadienne de normalisation <i>Code type sur la protection des renseignements personnels (1996)</i>	Royaume-Uni <i>Data Protection Act 1984 (ch. 35)</i>	Nouvelle-Zélande <i>Privacy Act 1993</i>
<p>8. Principe de la spécification des finalités (OCDE)</p> <p>Les finalités en vue desquelles les données de caractère personnel sont collectées devraient être déterminées au plus tard au moment de la collecte des données et lesdites données ne devraient être utilisées par la suite que pour atteindre ces finalités ou d'autres qui ne soient pas incompatibles avec les précédentes et qui seraient déterminées dès lors qu'elles seraient modifiées.</p>	<p>Faible</p> <p>« Avant ou au moment de recueillir des renseignements, les sociétés de fiducie membres informent leurs clients des raisons pour lesquelles les renseignements personnels sont recueillis ». (Paragr. 6(1)) Les sociétés de fiducie obtiennent des renseignements personnels principalement auprès des clients, mais aussi à des sources extérieures telles que les fournisseurs de crédit, les agences d'évaluation du crédit, les sources de revenus et les références personnelles. Les sociétés de fiducie obtiennent le consentement du client avant de vérifier et de compléter auprès des sources extérieures les renseignements personnels les concernant. (Paragr. 4(4))</p>	<p>Faible</p> <p>[TRADUCTION] « Les fins pour lesquelles les renseignements personnels sont recueillis doivent être déterminée par la caisse de crédit avant ou au moment de la collecte ». (Principe 2) Les fins déterminées doivent être spécifiques au membre auprès de qui les renseignements sont recueillis. Lorsque les renseignements personnels sont utilisés à une autre fin que celle pour laquelle ils ont été recueillis, le consentement du membre est requis à moins que ces nouvelles fins ne soient prévues par une loi.</p>	<p>Faible</p> <p>« <i>Détermination des fins de la collecte des renseignements</i> : Les fins pour lesquelles des renseignements personnels sont recueillis doivent être déterminées par l'organisme avant ou au moment de la collecte ». (Principe 2) Avant de se servir de renseignements personnels à des fins non précisées antérieurement, les nouvelles fins doivent être précisées au préalable avant de les utiliser. À moins que les nouvelles fins auxquelles les renseignements sont destinés ne soient prévues par la loi, il faut obtenir le consentement de la personne concernée avant d'utiliser les renseignements pour cette nouvelle fin. (Al. 4.2.4)</p>	<p>Élevé</p> <p>Au moment de l'enregistrement, l'utilisateur des données doit fournir, notamment, une description de ce qui suit : 1) les données à caractère personnel à détenir et les fins pour lesquelles ces données seront détenues ou utilisées; 2) la source auprès de laquelle les données seront obtenues; 3) toute personne à qui les données peuvent être divulguées; et 4) tout pays à l'extérieur du R.-U. auquel les données peuvent être directement ou indirectement transférées. (Art. 4)</p> <p>L'utilisateur des données doit soumettre une demande au registraire pour apporter des modifications à la description susmentionnées. (Art. 6)</p> <p>De plus, les données à caractère personnel ne sont [TRADUCTION] « détenues que pour une ou plusieurs fins déterminées et légitimes ». (Principe 2)</p>	<p>Moyen à élevé</p> <p>L'agence doit prendre les mesures raisonnables pour s'assurer que la personne auprès de laquelle les renseignements sont recueillis est informée, notamment, du fait que des renseignements sont recueillis, de la fin pour laquelle les renseignements sont recueillis et des destinataires prévus de ces renseignements. Cette information devrait être expliquée avant que les renseignements soient recueillis ou dès que possible. (Principe 3) Une agence ne doit pas recueillir des renseignements personnels à moins que ces renseignements soient recueillis pour une fin légitime et qu'ils ne soient nécessaires à cette fin. (Principe 1)</p>

Élément de comparaison	Association des compagnies de fiducie du Canada (ACFC) <i>La vie privée des clients : une responsabilité de confiance (1993)</i>	Centrale des caisses de crédit du Canada <i>Credit Union Code for the Protection of Personal Information, projet (1996)</i>	Association canadienne de normalisation <i>Code type sur la protection des renseignements personnels (1996)</i>	Royaume-Uni <i>Data Protection Act 1984 (ch. 35)</i>	Nouvelle-Zélande <i>Privacy Act 1993</i>
<p>9. Principe de la limitation de l'utilisation (OCDE)</p> <p>Les données de caractère personnel ne devraient pas être divulguées, ni fournies ni utilisées à des fins autres que celles spécifiées, conformément au principe de la spécification des finalités, si ce n'est : a) avec le consentement de la personne concernée; ou b) lorsqu'une règle de droit le permet.</p>	<p>Moyen</p> <p>« Avant que les sociétés de fiducie membres utilisent les renseignements personnels à des fins autres que celles pour lesquelles ils ont été recueillis ou pour toute autre fin qui serait compatible avec les premières, elles obtiendront le consentement de leurs clients ». (Paragr. 7(1))</p> <p>Les sociétés de fiducie ne divulguent des renseignements personnels à des tiers que si l'une des quatre exceptions suivantes s'applique : le client a consenti, la société de fiducie est dans l'obligation légale de le faire, la société de fiducie a une obligation publique de le faire, ou la société de fiducie est tenue de le faire pour protéger ses propres intérêts (Paragr. 7(2)). Le Code souligne que l'échange de renseignements personnels avec des tiers comme des fournisseurs de crédit et des bureaux d'évaluation du crédit, nécessite le consentement des clients à moins que le Code ne l'autorise.</p>	<p>Moyen</p> <p>[TRADUCTION] « Les renseignements personnels ne doivent pas être utilisés ou communiqués à des fins autres que celles auxquelles ils ont été recueillis à moins que le membre concerné n'y consente ou que la loi ne l'exige. On ne doit conserver les renseignements personnels qu'aussi longtemps que nécessaire pour la réalisation des finalités déterminées ».</p> <p>La caisse de crédit peut divulguer des renseignements personnels sans obtenir le consentement de la personne concernée lorsqu'elle y est tenue par la loi, comme dans le cas d'un subpoena, d'un mandat de perquisition, d'une autre ordonnance judiciaire ou gouvernementale ou de demandes de la part de parties disposant d'un droit d'accès aux renseignements personnels.</p> <p>Le dossier médical du membre peut être utilisé pour une demande de crédit et d'autres fins liées à l'assurance. Le dossier médical ne sera pas recueilli auprès d'une autre organisation ni divulgué à celle-ci.</p>	<p>Moyen</p> <p>« <i>Limitation de l'utilisation, de la communication et de la conservation</i> : Les renseignements personnels ne doivent pas être utilisés ou communiqués à des fins autres que celles auxquelles ils ont été recueillis à moins que la personne concernée n'y consente ou que la loi ne l'exige. On ne doit conserver les renseignements personnels qu'aussi longtemps que nécessaires pour la réalisation des finalités déterminées ». (Principe 5)</p>	<p>Élevé</p> <p>Un utilisateur de données ne peut détenir des données pour une fin autre que celles qui décrites dans l'inscription au registre ni divulguer des données détenues à une personne qui n'est pas décrite dans l'inscription. (Art. 5) [TRADUCTION] « Des données à caractère personnel détenues à une ou plusieurs fins ne doivent pas être utilisées ni divulguées d'une manière incompatible à ces fins ». (Principe 3)</p>	<p>Moyen</p> <p>[TRADUCTION] « Une agence qui détient des renseignements personnels qui ont été obtenus relativement à une fin ne doit pas utiliser ces renseignements à une autre fin. » sous réserve de certaines exceptions. Une agence peut utiliser des renseignements personnels pour une autre fin si, par exemple, elle croit qu'il s'agit d'une fin directement reliée, que la source de renseignements est un document public, ou que l'information est utilisée sous une forme qui ne permet d'identifier la personne concernée. (Principe 10) Une agence ne peut divulguer des renseignements personnels à moins de croire raisonnablement, notamment, que [TRADUCTION] « la divulgation des renseignements vise l'une des fins [ou est directement reliée à l'une des fins] relativement à laquelle les renseignements ont été obtenus ». (Principe 11)</p>
<p>10. Principe des garanties de sécurité (OCDE)</p> <p>Il conviendrait de protéger les données de caractère personnel, grâce à des garanties de sécurité raisonnables, contre des risques tels que la perte des données ou leur accès, destruction, utilisation, modification ou divulgation non autorisés.</p>	<p>Moyen</p> <p>« Les sociétés de fiducie membres mettent en œuvre des mesures de sécurité élaborées en vue de protéger les renseignements personnels sur leurs clients contre la perte ou l'accès, l'utilisation, la divulgation, l'altération ou la destruction non autorisés ». (Paragr. 8(1))</p> <p>Des renseignements peuvent être divulgués à des entreprises telles que celles qui font l'impression des chèques, les bureaux de services informatiques et d'envoi postal et des organismes de perception qui sont tenus de traiter de façon confidentielle ces renseignements. (Paragr. 8(3))</p>	<p>Moyen</p> <p>« <i>Mesures de sécurité</i> : Les renseignements personnels doivent être protégés au moyen des mesures de sécurité correspondant à leur degré de sensibilité ». (Principe 7)</p> <p>Les tiers (tels que les imprimeurs de chèques, les entreprises qui traitent des données, les agences de recouvrement de créances et les agences d'évaluation du crédit) seront tenus de protéger les renseignements personnels qui leur sont divulgués d'une manière conforme aux politiques de la caisse de crédit.</p>	<p>Moyen</p> <p>[TRADUCTION] « Des mesures de sécurité appropriées doivent être prises contre les accès non autorisés aux données à caractère personnel, leur altération, leur divulgation ou leur destruction et contre la perte accidentelle ou la destruction des données à caractère personnel ». (Principe 8)</p>	<p>Moyen</p> <p>Une agence qui détient des renseignements personnels doit s'assurer que les renseignements sont protégés au moyen de mesures de sécurité raisonnables contre la perte, le mauvais usage, ou l'accès non autorisé, l'utilisation, l'altération, ou la divulgation. Lorsqu'il est nécessaire que les renseignements soient communiqués à une personne relativement à la prestation d'un service, [TRADUCTION] « toutes les mesures raisonnables qui sont en le pouvoir de l'agence [doivent être] prises pour empêcher l'utilisation non autorisée ou la divulgation non autorisée des renseignements ». (Principe 5)</p>	<p>Moyen</p> <p>Une agence qui détient des renseignements personnels doit s'assurer que les renseignements sont protégés au moyen de mesures de sécurité raisonnables contre la perte, le mauvais usage, ou l'accès non autorisé, l'utilisation, l'altération, ou la divulgation. Lorsqu'il est nécessaire que les renseignements soient communiqués à une personne relativement à la prestation d'un service, [TRADUCTION] « toutes les mesures raisonnables qui sont en le pouvoir de l'agence [doivent être] prises pour empêcher l'utilisation non autorisée ou la divulgation non autorisée des renseignements ». (Principe 5)</p>

<p>Élément de comparaison</p>	<p>Association des compagnies de fiduciaire du Canada (ACFC) <i>La vie privée des clients : une responsabilité de confiance</i> (1993)</p>	<p>Centrale des caisses de crédit du Canada <i>Credit Union Code for the Protection of Personal Information</i>, projet (1996)</p>	<p>Association canadienne de normalisation <i>Code type sur la protection des renseignements personnels</i> (1996)</p>	<p>Royaume-Uni <i>Data Protection Act 1984</i> (ch. 35)</p>	<p>Nouvelle-Zélande <i>Privacy Act 1993</i></p>
<p>II. Principe de la transparence (OCDE) Il conviendrait d'assurer, d'une façon générale, la transparence des progrès, pratiques et politiques, ayant trait aux données de caractère personnel. Il devrait être possible de se procurer aisément les moyens de déterminer l'existence et la nature des données de caractère personnel et les finalités principales de leur utilisation, de même que l'identité du maître du fichier et le siège habituel de ses activités.</p>	<p>Faible « Les sociétés de fiduciaire membres trait à leurs politiques de protection du caractère confidentiel des renseignements personnels au sujet des clients. Les questions et préoccupations touchant aux politiques d'une société en particulier devraient être soumises à cette dernière ». (Paragr. 3(1))</p>	<p>Moyen [TRADUCTION] « La caisse de crédit doit mettre à la disposition de tout membre des renseignements précis sur ses politiques et ses pratiques concernant la gestion des renseignements personnels ». Les renseignements seront aisément accessibles sous une forme généralement compréhensible. (Principe 8)</p>	<p>Moyen « <i>Transparence</i> : 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 ». (Principe 8) Une personne devrait pouvoir obtenir sans efforts déraisonnables de l'information au sujet des politiques et des pratiques d'une entreprise.</p>	<p>Élevé L'utilisateur des données n'a pas le droit de détenir des données à caractère personnel à moins qu'il ne s'enregistre auprès du registraire à titre d'utilisateur de données ou de bureau informatique. Les inscriptions au registre doivent être accessibles pour fins de consultation par le public. (Art. 9) L'une des obligations du registraire est d'informer le public sur l'application de la Loi. (Art. 36)</p>	<p>Élevé En plus de l'obligation générale du Commissaire à la protection des renseignements personnels qui doit promouvoir une compréhension des principes de protection des renseignements personnels, le Commissaire peut aussi diffuser certaines publications qui peuvent inclure des renseignements tels que la nature des renseignements personnels détenus par une agence, le but et le délai pendant lesquels ils sont détenus, les personnes qui ont le droit d'accès aux renseignements personnels détenus par une agence et les mesures à prendre pour obtenir l'accès. (Art. 21) Le Commissaire peut exiger qu'une agence fournisse des renseignements pour les besoins de ces publications. (Art. 22)</p>

<p>Élément de comparaison</p> <p>12. Principe de la participation individuelle (OCDE)</p> <p>a) Toute personne physique devrait avoir le droit :</p> <p>a) d'obtenir du maître d'un fichier, ou par d'autres voies, confirmation du fait que le maître du fichier détient ou non des données la concernant;</p> <p>b) de se faire communiquer les données la concernant i) dans un délai raisonnable; ii) moyennant, éventuellement, une redevance modérée; iii) selon des modalités raisonnables; et iv) sous une forme qui lui soit aisément intelligible;</p> <p>c) d'être informés des raisons pour lesquelles une demande qu'elle aurait présentée conformément aux alinéas a) et b) est rejetée et de pouvoir contester un tel rejet;</p> <p>d) de contester les données la concernant et, si la contestation est fondée, de les faire effacer, rectifier, compléter ou corriger.</p>	<p>Association des compagnies de fiduciaire du Canada (ACFC)</p> <p><i>La vie privée des clients : une responsabilité de confiance (1993)</i></p> <p>Moyen</p> <p>Des droits d'accès et de rectification sont prévus dans le Code. Le droit d'accès est limité en ce qu'il ne s'applique pas aux opinions et aux jugements sur la personne concernée. La liste d'exceptions n'est pas exhaustive. Toutefois, la société de fiduciaire doit faire « tout ce qui est en son pouvoir » pour transmettre une rectification à un tiers si des renseignements inexacts qui ont pu avoir été transmis peuvent être préjudiciables aux intérêts d'un client.</p> <p>Accès : Les clients ont le droit d'avoir accès aux renseignements les concernant qui sont détenus par leur société de fiduciaire, sauf les opinions et jugements exprimés à leur sujet. La société de fiduciaire donnera accès aux renseignements dans un délai et à un coût raisonnables. L'accès sera accordé à moins qu'il n'y ait une raison « valable » de ne pas le faire.</p> <p>Rectification : Les clients pourront contester l'exactitude, le caractère complet ou la désuétude des renseignements personnels à leur sujet. Les renseignements inexacts ou incomplets seront modifiés et les renseignements superflus seront supprimés. Si une société de fiduciaire divulgue des renseignements inexacts à un tiers et que ces renseignements peuvent être préjudiciables aux intérêts du client, elle fera tout ce qui est en son pouvoir pour transmettre les renseignements corrigés au tiers.</p>	<p>Centrale des caisses de crédit du Canada</p> <p><i>Credit Union Code for the Protection of Personal Information, projet (1996)</i></p> <p>Moyen</p> <p>Le Code prévoit des droits d'accès et de rectification. La liste des exceptions n'est pas exhaustive. La caisse de crédit est tenue de communiquer une rectification au tiers [TRADUCTION] « s'il y a lieu ».</p> <p>Accès : L'accès doit être donné dans un délai raisonnable et à un coût minime sinon nul pour la personne. Les exceptions aux exigences en matière d'accès aux renseignements personnels devraient être « restreintes et précises ». Ces raisons peuvent comprendre le coût prohibitif de l'information à fournir, le fait que les renseignements personnels contiennent des détails sur d'autres personnes, l'existence de raisons d'ordre juridique, de raisons de sécurité ou de raisons de sécurité ou de raisons d'ordre commercial exclusives et le fait que les renseignements sont protégés par le secret professionnel ou dans le cours d'une procédure de nature judiciaire. Dans le cas de renseignements médicaux sensibles, l'entreprise peut préférer que ces renseignements soient communiqués par un médecin. (Al. 4.9.1 à 4.9.4)</p> <p>Rectification : Lorsqu'un membre démontre que des renseignements personnels sont inexacts ou incomplets, l'entreprise doit apporter les modifications nécessaires à ces renseignements. « S'il y a lieu », l'information modifiée doit être communiquée à des tiers ayant accès à ces renseignements. [TRADUCTION] « S'il y a lieu », l'information modifiée doit être communiquée à des tiers ayant accès à l'information en question. Lorsqu'un différend n'est pas réglé à la satisfaction du membre concerné, la caisse de crédit devrait enregistrer le fond de la plainte rejetée. [TRADUCTION] « S'il y a lieu », les tierces parties ayant accès à l'information en question devraient être informées du fait que le différend n'a pas été réglé. (Paragr. 9.6 et 9.7)</p>	<p>Association canadienne de normalisation</p> <p><i>Code type sur la protection des renseignements personnels (1996)</i></p> <p>Moyen</p> <p>Le Code prévoit des droits d'accès et de rectification. La liste des exceptions n'est pas exhaustive. Une entreprise devrait communiquer une rectification à un tiers « s'il y a lieu ».</p> <p>Accès : L'accès doit être donné dans un délai raisonnable et à un coût minime sinon nul pour la personne. Les exceptions aux exigences en matière d'accès aux renseignements personnels devraient être « restreintes et précises ». Ces raisons peuvent comprendre le coût prohibitif de l'information à fournir, le fait que les renseignements personnels contiennent des détails sur d'autres personnes, l'existence de raisons d'ordre juridique, de raisons de sécurité ou de raisons de sécurité ou de raisons d'ordre commercial exclusives et le fait que les renseignements sont protégés par le secret professionnel ou dans le cours d'une procédure de nature judiciaire. Dans le cas de renseignements médicaux sensibles, l'entreprise peut préférer que ces renseignements soient communiqués par un médecin. (Al. 4.9.1 à 4.9.4)</p> <p>Rectification : Lorsqu'un membre démontre que des renseignements personnels sont inexacts ou incomplets, l'entreprise doit apporter les modifications nécessaires à ces renseignements. « S'il y a lieu », l'information modifiée doit être communiquée à des tiers ayant accès à ces renseignements. [TRADUCTION] « S'il y a lieu », l'information modifiée doit être communiquée à des tiers ayant accès à l'information en question. Lorsqu'un différend n'est pas réglé à la satisfaction de la personne concernée, l'entreprise devrait enregistrer le fond de la plainte rejetée. « S'il y a lieu », les tierces parties ayant accès à l'information en question devraient être informées du fait que le différend n'a pas été réglé. (Al. 4.9.5 et 4.9.6.)</p>	<p>Royaume-Uni</p> <p><i>Data Protection Act 1984 (ch. 35)</i></p> <p>Élevé</p> <p>La Loi prévoit des droits d'accès et de rectification, sous réserve d'exceptions énumérées.</p> <p>[TRADUCTION] « Une personne physique dispose des droits suivants :</p> <p>a) à intervalles raisonnables et sans délais ou frais déraisonnables ;</p> <p>i) d'être informée par tout utilisateur de données s'il détient des données à caractère personnel dont elle fait l'objet; et ii) d'avoir accès à toutes données semblables détenues par un utilisateur de données; et</p> <p>b) s'il y a lieu, de faire rectifier ou effacer ces données ». (Principe 7)</p> <p>Lorsque la personne concernée par les données présente une demande écrite, accompagnée de droits, l'utilisateur de données doit lui fournir une copie des renseignements dans les 40 jours. (Art. 21) La personne physique a droit à une indemnisation pour tous dommages ou tous troubles subis en raison de l'inexactitude, de la perte, de la destruction non autorisée ou de la divulgation non autorisée des données détenues par un utilisateur de données. (Art. 22 et 23) Sur demande et sous réserve de certaines conditions, un tribunal peut aussi ordonner la rectification ou l'effacement de toutes données détenues par un utilisateur de données. (Art. 24)</p>	<p>Nouvelle-Zélande</p> <p><i>Privacy Act 1993</i></p> <p>Élevé</p> <p>La Loi prévoit des droits d'accès et de rectification sous réserve de certaines exceptions déterminées.</p> <p>Accès : Une personne a le droit d'obtenir d'une agence la confirmation que celle-ci détient des renseignements personnels et, dans l'affirmative, elle a le droit d'avoir accès à ces renseignements. (Principe 6) Si l'agence ne détient pas les renseignements demandés mais croit qu'une autre agence les détient, elle doit transmettre la demande dans un délai de 10 jours. (Art. 39) L'agence doit répondre dans un délai de 20 jours ouvrables et indiquer si elle se conformera à la demande à moins qu'une prolongation du délai ne soit demandée. (Art. 40 et 41) Si l'agence refuse la demande, elle doit motiver son refus et donner à la personne les renseignements concernant son droit de demander une enquête et un examen du refus. (Art. 44)</p> <p>Rectification : Une personne a le droit de demander une rectification des renseignements personnels détenus par une agence ou une annexe aux renseignements portant qu'une rectification a été demandée, mais n'a pas été apportée. Une agence qui détient des renseignements personnels doit prendre les mesures raisonnables, de sa propre initiative ou à la demande de la personne concernée, pour s'assurer que les renseignements sont [TRADUCTION] « exacts, à jour, complets et non trompeurs ». (Principe 7). Une personne qui présente une demande relative à l'accès ou à la rectification de renseignements détenus dans un document doit recevoir une copie du document ou avoir une possibilité raisonnable de le consulter. (Art. 42)</p>
-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

<p>Élément de comparaison</p>	<p>Association des compagnies de fiducie du Canada (ACFC) <i>La vie privée des clients : une responsabilité de confiance</i> (1993)</p>	<p>Centrale des caisses de crédit du Canada <i>Credit Union Code for the Protection of Personal Information, projet</i> (1996)</p>	<p>Association canadienne de normalisation <i>Code type sur la protection des renseignements personnels</i> (1996)</p>	<p>Royaume-Uni <i>Data Protection Act 1984</i> (ch. 35)</p>	<p>Nouvelle-Zélande <i>Privacy Act 1993</i></p>
<p>13. Principe de la responsabilité (OCDE) Tout maître de fichier devrait être responsable du respect des mesures donnant effet aux principes énoncés ci-dessus.</p>	<p>Faible Le Code traite brièvement de la responsabilité et des procédures internes de plaintes. Responsabilité : « La direction de chaque société de fiducie membre a la responsabilité de veiller à l'application des dispositions du présent Code et elle doit s'assurer que l'on donne suite aux préoccupations exprimées par les clients. Cependant, l'application au jour le jour des modalités de protection de la vie privée peut être confiée à certains employés désignés ». (Paragr. 10(2)) Plaintes : Les sociétés de fiducie disposent de procédures claires et expéditives pour traiter les plaintes des clients. Les clients qui ne sont pas satisfaits de la façon dont leur plainte a été traitée par la société de fiducie peuvent communiquer avec le Bureau du Surintendant des institutions financières. (Paragr. 10(3))</p>	<p>Faible à moyen Le Code traite en général de la responsabilité et des procédures internes de plaintes. Il propose que les plaintes ne soient pas réglées à l'intérieur mais soumises à la Centrale des caisses de crédit ou à un médiateur ou un arbitre indépendant. [TRADUCTION] « Responsabilité : La caisse de crédit est responsable des renseignements personnels dont elle a la gestion et doit désigner une ou des personnes qui devront s'assurer du respect des principes du Code ». (Principe 1) Plaintes : Chaque caisse de crédit disposera de politiques et de procédures pour recevoir les plaintes et y répondre. La caisse de crédit fera enquête sur toutes les plaintes et si une plainte est fondée, elle prendra les mesures appropriées. Si la plainte n'est pas réglée de manière satisfaisante par le responsable désigné de la caisse de crédit, elle peut être soumise au conseil d'administration de la caisse de crédit. Si la plainte n'est pas réglée par le conseil d'administration, il doit y avoir des procédures pour soumettre la plainte à la Centrale des caisses de crédit, à une autorité de réglementation ou à un médiateur ou un arbitre indépendant. (Principe 10)</p>	<p>Faible Le Code traite en général de la responsabilité et de la nécessité de procédures internes de plaintes. Il propose aussi d'informer les personnes de l'existence des autorités de réglementation qui peuvent accepter de recevoir des plaintes. « Responsabilité : Un organisme est responsable des renseignements personnels dont il a la gestion et doit désigner une ou des personnes qui devront s'assurer du respect des principes énoncés ci-dessous ». (Principe 1) « Possibilité de porter plainte contre le non-respect des principes : Toute personne doit être en mesure de se plaindre du non-respect des principes énoncés ci-dessus en communiquant avec le ou les individus responsables de les faire respecter au sein de l'organisme concerné ». (Principe 10) Les entreprises doivent informer les personnes de l'existence des mécanismes de plaintes dont ils peuvent se prévaloir, y compris les organismes de réglementation qui acceptent de recevoir des plaintes. Une entreprise doit faire enquête sur toutes les plaintes et si une plainte est jugée fondée, elle doit prendre les mesures appropriées.</p>	<p>Élevé La Loi ne traite pas du principe de responsabilité, mais certaines de ses dispositions traitent de certains aspects de la responsabilité (c'est-à-dire le devoir des utilisateurs de données de s'inscrire auprès des autorités publiques). L'application se fait par l'intermédiaire des autorités publiques.</p>	<p>Élevé La Loi ne traite pas en particulier du principe de responsabilité mais diverses dispositions traitent de certains aspects de la responsabilité (c'est-à-dire la nomination de responsables des renseignements personnels, l'obligation d'informer la personne au moment de la collecte des données, la publication des renseignements détenus par les agences, le statut réglementaire des codes de pratique adoptés par les agences). L'application se fait par l'intermédiaire des autorités publiques.</p>

Élément de comparaison	Association des compagnies de fiduciaire du Canada (ACFC) <i>La vie privée des clients : une responsabilité de confiance (1993)</i>	Centrale des caisses de crédit du Canada <i>Credit Union Code for the Protection of Personal Information, projet (1996)</i>	Association canadienne de normalisation <i>Code type sur la protection des renseignements personnels (1996)</i>	Royaume-Uni <i>Data Protection Act 1984 (ch. 35)</i>	Nouvelle-Zélande <i>Privacy Act 1993</i>
14. Dispositions spécifiques en matière de consentement	Faible Le Code ne traite pas en détail du consentement. Le consentement est mentionné brièvement dans les dispositions traitant de la collecte de renseignements et de l'utilisation ou de la divulgation de renseignements.	Moyen [TRADUCTION] « Tout membre doit être informé et consentir à toute collecte, utilisation ou communication de renseignements personnels qui le concernent, à moins qu'il ne soit pas approprié de le faire ». (Principe 3) Dans certaines circonstances, il est possible de recueillir, d'utiliser et de communiquer des renseignements à l'insu du membre et sans son consentement, par exemple, pour des raisons d'ordre juridique ou médical ou pour des raisons de sécurité. Pour déterminer la forme que prendra le consentement, la caisse de crédit doit tenir compte de la sensibilité des renseignements. Dans l'obtention du consentement, les attentes raisonnables du membre sont aussi pertinentes. Un membre peut retirer son consentement en tout temps sous réserve de restrictions d'ordre juridique ou contractuel dans la mesure où la caisse en est avisée dans un délai raisonnable et où le consentement ne s'applique pas à un produit de crédit à l'égard duquel la banque doit obtenir et divulguer de l'information après avoir octroyé un crédit.	Moyen « <i>Consentement</i> : Toute personne doit être informée et consentir à toute collecte, utilisation ou communication de renseignements personnels qui la concernent, à moins qu'il ne soit pas approprié de le faire ». (Principe 3) Dans certaines circonstances, il est possible de recueillir, d'utiliser et de communiquer des renseignements à l'insu du client et sans son consentement, par exemple, pour des raisons d'ordre juridique ou médical ou pour des raisons de sécurité. Les organismes qui ne sont pas en relation directe avec le client ne sont pas toujours en mesure d'obtenir le consentement prévu. Pour déterminer la forme que prendra le consentement, l'entreprise doit tenir compte de la sensibilité des renseignements. Dans l'obtention du consentement, les attentes raisonnables de la personne sont aussi pertinentes. Une personne peut retirer son consentement en tout temps sous réserve d'un avis prévu par la loi ou un contrat.	Faible La loi ne traite pas du consentement de la personne concernée par les données.	Faible La Loi traite peu du consentement; le consentement est mentionné dans les dispositions qui restreignent l'utilisation et la divulgation des renseignements personnels.
15. Dispositions limitant le transfert extraterritorial	Non	Non	Non	Oui Le registraire peut signifier un avis d'interdiction de transfert à un utilisateur de données lui interdisant de transférer des données à l'extérieur du Royaume-Uni en permanence ou prises pour assurer la protection des intérêts des personnes visées par les données. Lorsque les transferts de données se font vers des États qui ne sont pas liés par la Convention européenne, le registraire doit être convaincu que le transfert est susceptible de contrevenir à l'un des principes de protection des données avant de signifier l'avis d'interdiction. Lorsque les transferts de données se font vers des États par la Convention européenne, l'avis ne sera pas signifié à moins que le registraire ne soit convaincu qu'un autre transfert à un État qui n'est pas lié par la Convention est susceptible de mener à la violation de l'un des principes de protection des données. (Art. 12)	Non La Loi ne mentionne pas spécifiquement les flux transfrontières de données mais se fonde sur les principes pertinents de protection des renseignements personnels pour régir ces transferts.

Élément de comparaison	Association des compagnies de fiduciaire du Canada (ACFC) <i>La vie privée des clients : une responsabilité de confiance</i> (1993)	Centrale des caisses de crédit du Canada <i>Credit Union Code for the Protection of Personal Information</i> , projet (1996)	Association canadienne de normalisation <i>Code type sur la protection des renseignements personnels</i> (1996)	Royaume-Uni <i>Data Protection Act 1984</i> (ch. 35)	Nouvelle-Zélande <i>Privacy Act 1993</i>
16. Élément présentant un intérêt particulier	Non	Non	Non	Oui Traitement des données sensibles : La Loi prévoit que les principes de protection des données peuvent être modifiés ou complétés par le Secrétaire d'État pour fournir des mesures de protection additionnelles à l'égard des données à caractère personnel consistant en des renseignements quant à l'origine raciale, les opinions politiques ou les croyances religieuses ou autres, l'état de santé physique ou mental ou la vie sexuelle ou les condamnations criminelles de la personne visée par les données. (Art. 2). Note : Un nouveau projet de loi concernant la protection des données qui mettra en œuvre la directive de l'UE en matière de protection des données de 1995 a été présenté. Ce projet de loi a été lu en première lecture à la Chambre des lords et sa deuxième lecture est prévue en février 1998. Le nouveau régime simplifiera les exigences en matière de notification et d'enregistrement. Contrairement à la loi actuelle, elle s'appliquera aussi aux registres non automatisés. La nouvelle loi permettra aux personnes physiques qui estiment qu'il a été porté atteinte à leurs droits à la vie privée de solliciter une mesure de redressement devant les tribunaux, en plus de porter plainte devant l'autorité de surveillance. La nouvelle loi comportera des dispositions sur la prise de décision automatisée, sur le consentement, sur les critères à respecter avant d'entreprendre le traitement, particulièrement dans le cas des données sensibles, et sur les circonstances dans lesquelles des transferts de données à caractère personnel vers des pays offrant une « protection inadéquate » sont susceptibles de se produire.	Oui Il existe des dispositions particulières traitant des identificateurs uniques, des codes de pratique, du recoupement des renseignements et des principes de protection des renseignements personnels des registres publics. Identificateurs uniques Une agence n'est pas autorisée à assigner un identificateur unique à une personne à moins que cette assignation ne soit nécessaire pour permettre à l'agence d'accomplir ses fonctions efficacement. Une fois qu'un identificateur est assigné par une agence, il ne peut être utilisé par une autre agence qui n'y est pas liée. (Principe 12) Codes de pratique Les codes de pratique peuvent, après un avis public et une consultation, être introduits par le Commissaire ou une agence et ils constituent des documents exécutoires et obligatoires en vertu de la Loi. Un code de pratique peut modifier un ou plusieurs des principes de protection des renseignements. (Partie VI, art. 46 à 57) Appariement des données La Loi limite les programmes de recoupement à quelques organismes publics « déterminés » qui sont tenus de signer des ententes en matière de recoupement des renseignements qui imposent des mesures de contrôle en matière de divulgation des renseignements. Un organisme « non déterminé » n'est pas autorisé à participer à un programme de recoupement à moins que certains objectifs soient visés. (Partie X, art. 97 à 109) Principes de protection des renseignements personnels des registres publics La Loi prévoit quatre principes traitant des registres publics. Les ministères gouvernementaux qui administrent des registres publics doivent se conformer aux principes de protection des renseignements personnels en l'absence d'autres lois prépondérantes. (Partie VII, art. 58 à 65)

Table de jurisprudence	Page
<i>A.-G. Ontario c. A.-G. Canada</i> , [1896] A.C. 348 (P.C.)	150
<i>A.-G. Ontario c. A.-G. Canada</i> , [1937], A.C. 405 (P.C.)	148
<i>A.-G. Ontario c. Canada Temperance Foundation</i> , [1946] A.C. 193 (P.C.)	150
<i>Allan Mather c. Columbia House</i> , une cause non publiée dans le cadre de laquelle la Division Générale de la Cour de l'Ontario a rendu une décision le 6 août 1972	53
<i>Concernant la Loi anti-inflation</i> , [1976] 2 R.C.S. 373	150
<i>Australian Securities Commission c. Westpac Banking Corporation</i> (1991), A.C.S.R. 350, 32 F.C.R. 546	63
<i>Banks c. Biensch</i> (1977), 5 A.R. 83 (S.C.)	68
<i>Bernstein of Leigh c. Skyviews & General Ltd.</i> , [1978] 1 Q.B. 479	52
<i>Bhogal c. Punjab National Bank</i> , [1988] 2 All E.R. 296, p. 305 (C.A.)	64
<i>Brasseries Labatt c. P.g. du Canada</i> , [1980] 1 R.C.S. 844	148
<i>Budzich c. Toronto Dominion Bank</i> , [1996] 2 C.T.C. 278	64
<i>Burrows c. Superior Court of San Bernardino County</i> (1974), 13 Cal. 3d 238, 118 Cal. Rptr. 166, 529 P.2d 590	63
<i>Cambridge Water Company c. Eastern Counties Leather</i> , [1994] 1 All E.R. 53	55
<i>Canadian Deposit Insurance Corp. c. Canadian Commercial Bank</i> (1989), 64 Alta. L.R. (2d) 329, 71 C.B.R. (N.S.) 239, 95 A.R. 24, A.W.L.D. 367	65
<i>Canadian imperial Bank of Commerce c. Sayani</i> (1993), 83 B.C.L.R. (2d) 167	66
<i>CIBC c. A.-G. Can.</i> (1962), 35 D.L.R. (2d) 49 (S.C.C)	64
<i>Citizens' Insurance Co. c. Parsons</i> (1881) 7 App. Cas. 96 (P.C.)	147
<i>Cossette c. Dun</i> (1891), 18 S.C.R. 22	54
<i>Dominion Stores c. La Reine</i> , [1980] 1 R.C.S. 844	148
<i>Duchess of Argyll c. duke or Argyll</i> [1967], Ch.D. 302	56
<i>Farm Products Marketing Act</i> [1957], R.C.S. 198	148

<i>Foundation Co. of Canada Ltd. c. Dhillon</i> , [1995] O.J. 3211 (Division générale de la Cour de l'Ontario)	64
<i>Frame c. Smith</i> , [1987] 2 S.C.R. 99	56
<i>General Motors c. City National Leasing</i> [1989], 1 R.C.S. 641	148
<i>Georgia Construction c. Pacific Great Eastern R. Co.</i> , [1929] 4 D.L.R. 161, (S.C.C.)	67
<i>Gillette c. Nissen</i> (1976), 58 D.L.R. (3d) 104 (Alta. S.C.).	54
<i>Grieg c. Grieg</i> [1966] V.R. 376 (S.C)	52
<i>Guertin c. la Banque Royale du Canada</i> (1983), 43 O.R. (2d) 363	63
<i>Haughton c. Haughton</i> , [1965] 1 O.R. 481	64
<i>Hodge c. The Queen</i> , (1883) 9 App. Cas. 117 (P.C.)	147
<i>Hongkong Bank of Canada c. Phillips</i> , [1997] M.J. No. 134 (Man. Q.B.)	64
<i>Hull c. Childs & Huron and Erie Mortgage Corp.</i> , [1951] O.W.N. 116	63
<i>Irwin Toy c. Québec</i> , [1989] 1 R.C.S. 927	146
<i>Jacobsen c. Citizens State Bank</i> (1979), 587 SW2d 480 (Tex. Civ. App.)	63
<i>Johannesson c. West St. Paul</i> , [1952] 1 R.C.S. 292	149
<i>Kabwand Pty. Ltd. c. National Australian Bank Limited</i> (1989), No. G355, Fed. No. 195 (Aust. F.C.)	63
<i>Kingston Thoroughbred Horse Stud and Australian Tax Office No. N85/130</i> (1986) (Administrative Appeals Tribunal)	63
<i>LAC Minerals c. International Corona Resources Ltd.</i> , [1989] 2 S.C.R. 574	56
<i>Libyan Arab Foreign Bank c. Bankers Trust Co.</i> , [1988] 1 Lloyd's Rep. 259	65
<i>MacDonald c. Vapor Canada</i> , [1977] 2 R.C.S. 134	148
<i>Malone c. Commissioner of Police (No. 2)</i> , [1979] 2 All E.R. 620 (Ch.D.)	52
<i>Marcel c. Commissioner of Police of the Metropolis</i> , [1992] 1 All E.R. 72, Ch. 225	64
<i>Midland Doherty Limited c. Rohrer</i> , (1984) 62 N.S.R. (2d) 205 p. 212 (N.S.T.D.)	67
<i>Motherwell c. Motherwell</i> [1976] 6 W.W.R. 550, 1 A.R. 47, 73 D.L.R. (3d) 62 (C.A.)	53

<i>Munro c. Commission de la capitale nationale</i> , [1966] R.C.S. 663	149
<i>Murano c. Bank of Montreal</i> (1995), 31 C.B.R. (3d) 1, 20 B.L.R. (2d) 61	65
<i>Ontario Hydro c. Ontario</i> , [1993] 3 R.C.S. 327	149
<i>Papp c. Papp</i> , [1970] 1 O.R. 331 (Ont. C.A.)	146
<i>Park c. Bank of Montreal</i> , [1997] B.C.J. N° 787	64
<i>Peter Lawrence Crawley et al</i> (1981), 52 F.L.R. 123	63
<i>Pharand Ski Corporation c. Alberta</i> (1991), 7 C.C.L.T. 225 (Alta. Q.B.)	56
<i>Pigg c. Robertson</i> (1977), 549 SW2d 597	63
<i>La Reine c. Crown Zellerbach</i> , [1988] 1 R.C.S. 401	150
<i>La Reine c. Duarte</i> (1990) 65 D.L.R. (4th) 240 (S.C.C)	19
<i>La Reine c. Hauser</i> [1979] 1 R.C.S. 984	151
<i>La Reine c. Lillico</i> (1994), 92 C.C.C. (3d) 90 (Division générale de la Cour de l'Ontario)	65
<i>Reine c. Spencer</i> (1983), 2 C.C.C. (3d) 526 (C.A.), par McKinnon A.C.J.O	64
<i>Regulation and Control of Radio Communication in Canada</i> , [1932] A.C. 304 (P.C.)	149
<i>Robertson c. Canadian Imperial Bank of Commerce</i> , [1995] 1 All E.R. 824 (P.C.)	63
<i>Royal Bank of Canada c. Art's Welding & Machine Shop</i> (1989), 34 C.P.C. (2d) 190	64
<i>Royal Bank of Canada c. Brattberg</i> (1993), 11 Alta. L.R. (3d) 190, 8 W.W.R. 139, 143 A.R. 131, A.W.L.D. 684	65
<i>Russell c. The Queen</i> (1882) 7 App. Cas. 829 (P.C.)	150
<i>Rylands c. Fletcher</i> (1866) L.R. 1 Ex 265, confirmée par (1868) L.R. 3 H.L. 330	55
<i>Sheen c. Clegg</i> , Non publiée. La cause a déjà été décrite dans l'édition du 22 juin 1961 du Daily Telegraph	52
<i>Smith c. Kamloops et la District Elizabeth Fry Society</i> [1995] B.C.J. N° 516 (B.C.S.C.), confirmée par (1996) 136 D.L.R. (4 th) 644 (C.A.)	68
<i>Smorgen c. Australia and New Zealand Banking Group Ltd</i> (1976), 134 C.L.R. 475	63
<i>State c. McCray</i> (1976) 15 Wash. App. 810, 551 P.2d 1376	63

<i>Suburban Trust Co.</i> (1979), 408 A.2d, p. 758	63
<i>Sutherland c. Barclays Bank Ltd.</i> (1938) 5 L.D.A.B. 163	66
<i>Taylor c. Commercial Bank</i> (1903) 174 NY 181, 66 NE 726	63
<i>Tournier c. National Provincial & Union Bank of England</i> [1924] 1 K.B. 461 (C.A.)	62
<i>Union Colliery Co. c. Bryden</i> [1899] A.C. 580 (P.C.)	146
<i>United States Department of Justice c. Reporters Committee for Freedom of the Press</i> , 489 U.S. 749 (1989)	19
<i>Weld-Blundell c. Stephens</i> , [1920] A.C. 956	65
<i>X A.-G. c. A Bank</i> , [1983] 2 All E.R. 464	64
<i>X. c. Y.</i> [1988], 2 All E.R. 648	56

Bibliographie

- Association des banquiers canadiens, Confidentialité – Modèle de code : Pour protéger les renseignements personnels des clients des banques (Toronto, Association des banquiers canadiens, 1996).
- Association des consommateurs du Canada, Consumer Data Protection (Ottawa, Association des consommateurs du Canada, mars 1993).
- Association des consommateurs du Canada, Privacy and Data Protection: Background Paper (Ottawa, Association des consommateurs du Canada, juillet 1992).
- Association des consommateurs du Canada, Privacy in the Age of the Information Highway (Ottawa, Association des consommateurs du Canada, mars 1995).
- Association des consommateurs du Canada, Reform of Financial Services: Retailing of Insurance by Deposit-Taking Institutions (Ottawa, Association des consommateurs du Canada, août 1995).
- Australie, Attorney General's Department, Privacy Protection in the Private Sector (September 1996). <http://www.agps.gov.au/customer/agd/clrc/privacy.htm>.
- Benn, S.I., Privacy, Freedom and Respect for Persons (Lieber-Atherton, 1971).
- Bureau d'assurance du Canada, Modèle de code sur les renseignements personnels (Toronto, Bureau d'assurance du Canada, 1996).
- Burns, P., « The Law and Privacy: The Canadian Experience », (1976) 54 La Revue du Barreau canadien 5.
- Carlin, F.M., « The Data Protection Directive: the introduction of common privacy standards », (1996) 21 European Law Review 65.
- Cate, F.H., « The EU Data Protection Directive, Information Privacy, and the Public Interest », (1995) 80 Iowa Law Review 431.
- Cavoukian, Ann, Data Mining: Staking A Claim on Your Privacy (Ontario, Commissaire à l'information et à la protection de la vie privée, janvier 1998).
- Centrale des caisses de crédit du Canada, Credit Union Code for the Protection of Personal Information (Draft) (Ottawa, Centrale des caisses de crédit du Canada, 1996).
- Downey, Catherine M., « The high price of a cashless society: exchanging privacy rights for digital cash? », (1996) 14 John Marshall Journal of Computer & Information Law.
- Estadella-Yuste, Olga, « The Draft Directive of the European Community Regarding the Protection of Personal Data », (1992) 41 International and Comparative Law Quarterly 170.

Financial System Inquiry, Financial System Inquiry Final Report, vol. 1, 2 et 3 (Canberra, Australie, Australian Government Publishing Service, 1997).

Fried, C., « Privacy », (1968) 77 Yale Law Journal 475.

Gavison, R., « Privacy and the limits of law », (1980) 89 Yale Law Journal 42.

Hammond, R.G., « Quantum Physics, Econometric Models and Property Rights to Information », (1981) 27 La Revue de droit de McGill 47.

Insight Information Inc. Electronic Delivery of Financial Services. (Toronto, Insight Information Inc., 1995).

L'Institut canadien, The Internet and Online Services: Exploring the Legal Implications of Doing Business Electronically (Toronto, L'Institut canadien, 6 et 7 mars 1995).

Lawson, Ian et Woods, David, Protection de la vie privée et autoroute de l'information : Les options du Canada en matière de réglementation. Étude réalisée pour le compte d'Industrie Canada (Ottawa, Industrie Canada, 1996). <http://strategis.ic.gc.ca/SSG/ca00257e.html>.

Lawson, Ian, Privacy and Free Enterprise: The Legal Protection of Personal Information in the Private Sector (Ottawa, Le Centre pour la défense de l'intérêt public, 1992).

Le Centre pour la défense de l'intérêt public et Fédération nationale des associations de consommateurs du Québec, Des frontières à définir : Les Canadiens et les renseignements personnels (Ottawa et Montréal, CDIP et FNACQ, 1995).

Les Associés de recherche Ekos inc., Privacy Revealed: The Canadian Privacy Survey (Ottawa, Les Associés de recherche Ekos inc., 1993).

Lloyd, Ian, « An Outline of the European Data Protection Directive », (1996) 1 The Journal of Information, Law and Technology. <http://elj.warwick.ac.uk/elj/jilt/dp/intros/>.

Louis Harris & Associates et Westin, le D^f Alan F., Rapport Equifax Canada sur les consommateurs et la vie privée à l'ère de l'information (Ville d'Anjou, Québec, Equifax Canada Inc., 1995).

Maxeiner, J.R., « Business Information and "Personal Data": Some Common-Law Observations About the EU Draft Data Protection Directive », (1995) 80 Iowa Law Review 619.

Office of the Privacy Commissioner of New Zealand, Fact Sheets on the Privacy Act 1993 (août 1993). <http://io.knowledge-basket.co.nz/privacy/facts/fact0.htm>.

Office of the Privacy Commissioner of New Zealand, Review of the Privacy Act 1993: Discussion Papers 1 to 12 (septembre 1997). <http://www.knowledge-basket.co.nz/privacy/discpp/intro.htm>.

Ombudsman bancaire canadien, Rapport annuel 1996 (Toronto, Ombudsman bancaire canadien, 1996).

Ombudsman bancaire canadien, Rapport pour les neuf mois terminés au 31 juillet 1997 (Toronto, Ombudsman bancaire canadien, 1997).

Ontario, Commission on Freedom of Information and Individual Privacy, Privacy and Personal Data Protection: Research Publication No. 15 (mars 1980).

Onyshko, Thomas S. et Owens, Richard C., « Debit Cards and Stored Value Cards: Legal Regulation and Privacy Concerns », (1997) 16 National Banking Law Review 65.

Onyshko, Thomas S., « Access to personal information: British and Canadian Legislative Approaches », (1989) 18 Manitoba Law Journal 213.

Onyshko, Thomas S., « Privacy, Access to Information and Transborder Data Transfer », (Smith Lyons, 1997). <http://www.smithlyons.ca/it/privacy/index.htm>.

Onyshko, Thomas S., « The Federal Court and the Access to Information Act », (1993) 22 Manitoba Law Journal 73.

Onyshko, Thomas S., Informational Privacy and the Law in Canada (Mémoire de maîtrise, Université de Toronto, 1995).

Owens, Richard C., Onyshko, Thomas S. et Goode, Peter C., « Reform Proposals Relating to Customer Privacy and Tied Selling in the Federally-Regulated Financial Services Sector », publié dans The Regulation of Financial Institutions: Issues and Perspectives (Scarborough, Ontario, Carswell, 1997).

Owens, Richard et Myers, John, « Privacy in Financial Services: An Overview of Canadian Law », publié dans Retailing Financial Services (Toronto, L'Institut canadien, 1994).

Owens, Richard et Onyshko, Thomas S., « Legal Regulation and Privacy Concerns Relating to Credit Cards, Debit Cards and Stored Value-Cards », publié dans Maximizing Your Upside from Credit/Debit/Smart/Cards (Toronto, L'Institut canadien, 1997).

Owens, Richard, « Legal Issues in the Creation, Management and Exploitation of Corporate Databases », publié dans Protecting and Managing IP Assets (Federated Press, 1997).

Owens, Richard, « Retailing of Financial Services », Exposé présenté à l'occasion d'un colloque organisé par l'Institut canadien (Toronto, L'Institut canadien, 1996).

Owens, Richard, « Some Legal Issues Concerning Databases and Database Marketing », publié dans Retailing Financial Services (Toronto, L'Institut canadien, 1995 et 1996).

Owens, Richard, « Some Privacy Thoughts », publié dans Privacy in Financial Services (Toronto, L'Institut canadien, 1994).

Owens, Richard, « Steering Clear of the Legal Pitfalls of Database and Relationship Marketing », Exposé présenté à l'occasion d'un colloque organisé par l'Institut canadien (Toronto, L'Institut canadien, 1994).

Perey A. et Janisch H., « International Restrictions on the Exchange of Information: Privacy, Transborder Data Flows and Trade in Services », publié dans *Privacy in Financial Services: Striking a Balance between Privacy Rights and Profits* (1994, L'Institut canadien).

Privacy & American Business, *Privacy in Cyberspace: Issues and Solutions*. Documents préparés en vue de la « Third Annual Conference Managing Privacy in Cyberspace and Across National Borders » (Hackensack, N.J., Privacy & American Business, 1996).

Privacy & American Business, *Sourcebook on Business and Global Data Protection*. Documents préparés en vue de la « Third Annual National Conference Managing Privacy in Cyberspace and Across National Borders » (Citicorp Bank, 1996).

Privacy Commissioner of Australia, *Information Privacy in Australia: A National Scheme for Fair Information Practices in the Private Sector* (août 1997). http://www2.austlii.edu.au/itlaw/national_scheme/national-INFORMAT.html.

Prosser, W.L. « Privacy », (1960) 48 *California Law Review* 383.

Rankin, M., « Privacy and Technology: A Canadian Perspective », (1984) 22 *Alberta Law Review* 323.

Reidenberg, Joel R., « Rules of the Road for Global Electronic Highways: Merging the Trade and Technical Paradigms », (1993) 6 *Harvard Journal of Law. & Technology* 287.

Roberts, R.J., « Is Information Property? », (1987) *Intellectual Property Journal* 209.

Rosenbaum, J.I., « The European Commission's Draft Directive on Data Protection », (1992) 33 *Jurimetrics Journal of Law, Science and Technology* 1.

Ryan, E.R., « Privacy, Orthodoxy and Democracy », (1973) 51 *La Revue du Barreau canadien* 84.

Schwartz, P.M., « European Data Protection Law and Restrictions on International Data Flows », (1995) 80 *Iowa Law Review* 471.

Secrétariat général de la Commission européenne, *First Orientations on Transfers of Personal Data to Third Countries – Possible Ways Forward in Assessing Adequacy: Discussion Document Adopted by the Working Party on June 26, 1997*. <http://www.open.gov.uk/dpr/d5020en2.htm>.

Simitis, Spiros, « From the Market to the Polls: The EU Directive on the Protection of Personal Data », (1995) 80 *Iowa Law Review* 445.

Slane, Bruce, Privacy Law Issues – Reform Proposals and their Impact on the Financial Industry. Notes for an Address by the Privacy Commissioner for New Zealand, Bruce Slane, to the Fourteenth Annual Banking Law and Practice Conference (22 mai 1997) <http://www.knowledge-basket.co.nz/privacy/speeches/banksyd2.htm>.

Stallworthy, M., « Data Protection: Regulation in a Deregulatory State », (1990) 11 Statute Law Review 130.

The Office of the Information and Privacy Commissioner of British Columbia, Visions for Privacy in the 21st Century: A Search for Solutions. Documents préparés en vue d'un colloque organisé par The Office of the Information and Privacy Commissioner of British Columbia and The University of Victoria. (Victoria, Colombie-Britannique : The Office of the Information and Privacy Commissioner of British Columbia, 1996).

U.K. Home Office, Consultation Paper on the EC Data Protection Directive (95/46/EC) (mars 1996) http://www.open.gov.uk/home_off/ccpd/dataprot.htm.

U.K. Home Office, Consultation Paper on the EC Data Protection Directive (95/46/EC): Response of the Data Protection Registrar (juillet 1996) <http://www.open.gov.uk/dpr/answer/content.htm>.

U.K. Home Office, Data Protection: the Government's Proposals (juillet 1997) <http://www.homeoffice.gov.uk/datap2.htm>.

Warren, S.D. et Brandeis, L.D., « The Right to Privacy », (1890) 4 Harvard Law Review 193.

Wellbery, B.S., « An Overview of Information Privacy in the United States and European Union », sous la direction de L. Fischer et R. Bennett, Privacy in Electronic Commerce: A Compendium of Essays on the Use of Information (Washington, American Bankers Association, 1997).

Westin, A.F., Privacy and Freedom (New York, Atheneum, 1967).

Wiebe, Andreas, « Harmonization of Data Protection Law in Europe », (1996) 3 The Journal of Information, Law and Technology. <http://lrc.law.warwick.ac.uk/jilt/confs/3dp/default.htm>.

Wright, Tom, Privacy Protection Models for the Private Sector (Toronto, Commissaire à l'information et à la protection de la vie privée de l'Ontario: 1996). http://www.ipc.on.ca/web_site.eng/matters/sum_pap/papers/models-e.htm.