PRB 00-05F

Library of Parliament Bibliothèque du Parlement

LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET LE COMMERCE ÉLECTRONIQUE — L'ÉTAT DE LA QUESTION

Margaret Smith
Division du droit et du gouvernement

Le 31 mai 2000

PARLIAMENTARY RESEARCH BRANCH
DIRECTION DE LA RECHERCHE PARLEMENTAIRE

La Direction de la recherche parlementaire de la Bibliothèque du Parlement travaille exclusivement pour le Parlement, effectuant des recherches et fournissant des informations aux parlementaires et aux comités du Sénat et de la Chambre des communes. Entre autres services non partisans, elle assure la rédaction de rapports, de documents de travail et de bulletins d'actualité. Les attachés de recherche peuvent en outre donner des consultations dans leurs domaines de compétence.

N.B. Dans ce document, tout changement d'importance fait depuis la dernière publication est indiqué en **caractère gras.**

CE DOCUMENT EST AUSSI PUBLIÉ EN ANGLAIS

TABLE DES MATIÈRES

PAGE

PAGE

CANADA

LIBRARY OF PARLIAMENT
BIBLIOTHÈQUE DU PARLEMENT

LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET LE COMMERCE ÉLECTRONIQUE — L'ÉTAT DE LA QUESTION

INTRODUCTION

Le « commerce électronique », c'est-à-dire les affaires traitées par voie électronique, couvre de multiples activités. On peut lui donner une définition large ou étroite. La première englobe les transactions effectuées à l'aide de la technologie numérique, notamment sur les réseaux ouverts, tels qu'Internet, et sur les réseaux fermés, tels que ceux qui servent aux échanges de données électroniques ou aux transactions par cartes de débit et de crédit. Quant à la définition étroite, elle se limite aux transactions effectuées sur Internet(1).

Le commerce électronique regroupe trois types de transactions : entre entreprises, entre entreprises et consommateurs, et les services publics. Jusqu'à maintenant, la majeure partie des transactions ont eu lieu entre entreprises ou entre des entreprises et l'administration publique, et sur des réseaux fermés plutôt que sur Internet. De fait, environ 80 p. 100 des échanges s'effectuent d'entreprise à entreprise(2). Mondialement, le commerce d'entreprise à entreprise sur Internet devrait atteindre 2 960 milliards de dollars US d'ici à 2003(3).

Malgré la place dominante occupée actuellement par les transactions d'entreprise à entreprise, on prévoit que la prochaine étape du développement du commerce électronique à l'échelle internationale sera une augmentation rapide des transactions entre les entreprises et les consommateurs. Partout dans le monde, les gouvernements et le secteur privé cherchent donc à réduire ou à supprimer les obstacles au commerce sur Internet.

---

(1) Canada, *Stratégie canadienne sur le commerce électronique*, 1998, p. 1, http://e-com.ic.gc.ca.

(2) *Ibid*., p. 4.

(3) Canada, Groupe de travail sur le commerce électronique, *Fiche récapitulative des statistiques sur le commerce électronique au Canada*, 26 août 1999.

On s'accorde à dire que l'inquiétude des consommateurs au sujet de la confidentialité des renseignements personnels gêne considérablement l'essor du commerce électronique. D'après les sondages, le public préfère nettement que les renseignements personnels soient protégés sur Internet. Selon une enquête Angus Reid de 1998, plus de 80 p. 100 des Canadiens estiment que les renseignements personnels doivent demeurer strictement confidentiels; 65 p. 100 estiment qu'il n'est aucunement acceptable pour les sociétés de vendre, d'échanger ou de partager des listes détaillées de renseignements personnels avec d'autres organisations; neuf Canadiens sur dix désapprouvent fortement les entreprises qui font le trafic des renseignements personnels sans le consentement des intéressés; et 94 p. 100 jugent important qu'il existe des dispositifs sûrs pour protéger les renseignements personnels sur Internet[(4)]. Même si le commerce électronique est appelé à se développer considérablement, la réticence des consommateurs devrait continuer de poser problème tant que les questions relatives à la sécurité, à la protection de la vie privée et aux recours ne seront pas résolues de manière satisfaisante.

Grâce aux progrès techniques, il est de plus en plus facile de recueillir des renseignements personnels par Internet. Il y a plusieurs façons de le faire. Premièrement, l'utilisateur du Web peut donner les renseignements délibérément. Deuxièmement, il peut utiliser un logiciel qui interagit directement avec un site Web (certains sites, par exemple, obligent l'utilisateur à télécharger un logiciel particulier et ainsi à révéler son identité). Troisièmement, il peut fournir des renseignements personnels à son insu, en remplissant un questionnaire ou un formulaire d'inscription pour obtenir l'accès à un site particulier ou figurer dans un répertoire. Quatrièmement, des mouchards ou « cookies » peuvent être utilisés pour établir le profil des utilisateurs d'après leurs habitudes de navigation et leurs intérêts. Le mouchard est une petite quantité de codes informatiques introduits sur le disque dur qui permettent de suivre la navigation de l'utilisateur sur un site et que l'on réutilise, lorsque l'utilisateur revient sur le même site, pour, par exemple, adapter la publicité au client. Le mouchard ne donne ni le nom ni l'adresse électronique de l'usager, mais il peut révéler ses habitudes d'achat et stocker ces renseignements dans une base de données. Cinquièmement, il

---

(4) Industrie Canada, Bureau de la consommation, *Bulletin trimestriel sur la consommation*, vol. 4, n° 1, mars 1999, p. 2, http://strategis.ic.ca/SSGF/ca01128f.html.

est possible, au moyen de logiciels et de répertoires statistiques, de maintenir des registres sur chaque site et chaque page auxquels les usagers accèdent. Ces données, basées sur l'enregistrement de chaque clic de la souris, sont souvent recueillies à l'insu et sans le consentement du consommateur(5).

Les renseignements personnels peuvent avoir une grande valeur. De fait, la réussite d'un site Web peut reposer en grande partie sur leur collecte et leur utilisation. Les bases de données qui contiennent des renseignements sur les habitudes d'achat, les préférences et les caractéristiques démographiques des gens peuvent être utilisées pour faire du démarchage sur mesure ou être vendues à d'autres entreprises(6). Ainsi l'information est l'essence même d'Internet, mais celui-ci offre de nouvelles possibilités d'en faire mauvais usage et de s'ingérer dans la vie privée des gens(7).

Au cours des vingt dernières années, les gouvernements des États-Unis, du Canada, de l'Australie et de l'Europe ont étudié la façon dont les renseignements personnels sont recueillis, utilisés et divulgués, ainsi que les garanties qui sont en place pour en assurer une bonne protection. Cela a donné lieu à toute une série de rapports, de lignes directrices, de codes types et de lois, qui représentent des principes généralement reconnus du traitement équitable de l'information.

Certes ces règles, comme toutes les mesures de protection de la vie privée, concernent aussi bien le secteur public que le secteur privé. Toutefois, notre exposé porte surtout sur le traitement des renseignements personnels par le secteur privé dans le contexte du commerce électronique. Nous examinerons les efforts des gouvernements du Canada, des États-Unis, du Royaume-Uni et de l'Australie, de même que les initiatives d'autoréglementation du secteur privé.

---

(5) Dale A. J. Dietrich, *Legal Issues Affecting Canadian Based Electronic Commerce Undertakings*, document présenté lors de la série sur la propriété intellectuelle destinée à l'industrie des technologies de l'information, Centre d'études sur la propriété intellectuelle, Université du Nouveau-Brunswick, mai 1998, p. 41.

(6) Ann Cavoukian, Commissaire à l'information et à la protection de la vie privée/Ontario : *Privacy: The Key to Electronic Commerce*, avril 1998, p. 4.

(7) Dietrich (1998), p. 40.

LES PRATIQUES ÉQUITABLES DE TRAITEMENT DE L'INFORMATION

Plusieurs des mesures de protection des renseignements personnels reposent sur cinq grands principes :

1. Avis/Connaissance
2. Choix/Consentement
3. Accès/Participation
4. Intégrité/Sécurité
5. Application/Recours(8).

1. Avis/Connaissance

En vertu de ce principe, le consommateur est avisé des pratiques de traitement de l'information de l'organisation avant qu'elle ne recueille le moindre renseignement personnel. Il peut décider en connaissance de cause de divulguer ou non des renseignements le concernant et dans quelle mesure le faire. L'avis précise :

- l'identité de celui qui recueille les renseignements;
- la façon dont les renseignements seront utilisés;
- les destinataires possibles des renseignements;
- le type de renseignements recueillis et la façon dont ils sont recueillis, si cela n'est pas évident;
- s'il est obligatoire ou facultatif de fournir les renseignements, et les conséquences qu'il peut y avoir à ne pas les fournir;
- ce que l'organisation qui recueille les renseignements a fait pour en assurer la confidentialité, l'intégrité et la qualité(9).

---

(8) United States, Federal Trade Commission, *Privacy Online : A Report to Congress*, juin 1998, p. 10, http://www.ftc.gov/reports/privacy3/fairinfo.htm.

(9) *Ibid.*, p. 7.

2. Choix/Consentement

Un autre principe du traitement équitable de l'information est celui du choix ou du consentement du consommateur, à savoir que celui-ci doit avoir des options quant à la façon dont les renseignements personnels qui le concernent seront utilisés. Cela s'applique tout particulièrement aux utilisations secondaires des renseignements, c'est-à-dire celles qui dépassent les utilisations nécessaires à la réalisation de la transaction envisagée(10).

Il existe essentiellement deux grandes options : la possibilité d'accepter et la possibilité de refuser. Quand il a la possibilité d'accepter, l'usager doit donner son consentement avant que la collecte, l'utilisation ou la divulgation des renseignements personnels puisse se faire. La possibilité de refuser implique que les renseignements peuvent être recueillis, utilisés ou divulgués, sauf si la personne prend des mesures pour empêcher que cela se fasse.

3. Accès/Participation

Le troisième principe essentiel — l'accès — concerne la capacité d'une personne d'accéder aux renseignements personnels qui la concernent et de vérifier si ces renseignements sont exacts et complets(11).

4. Intégrité/Sécurité

En vertu de ce principe, les données doivent être exactes et sûres. Cela implique la mise en place de mesures de gestion et de mesures techniques destinées à protéger les renseignements contre toute perte, ainsi que contre un accès, une destruction, une utilisation ou une divulgation non autorisés. Sur le plan de la gestion, ces mesures comportent des dispositions organisationnelles destinées à limiter l'accès et à faire en sorte que les personnes qui jouissent de cet accès n'utilisent pas les renseignements à des fins non autorisées. Les mesures de sécurité technique comprennent, entre autres, le cryptage aux fins de transmission et de stockage, la limitation de l'accès par le recours à des mots de passe et l'emmagasinage des données sur des serveurs ou des ordinateurs protégés, inaccessibles par modem(12).

---

(10) *Ibid.*, p. 8.

(11) *Ibid.*

(12) *Ibid*., p. 9.

5. Application/Recours

Des mécanismes efficaces d'application des règles sont essentiels pour la protection des renseignements personnels. Il existe plusieurs façons de procéder, y compris l'autoréglementation du secteur privé, les lois qui mettent en place des recours privés pour les consommateurs, ou encore une réglementation assortie de sanctions civiles et pénales(13).

LA PROTECTION DE LA VIE PRIVÉE À L'ÉCHELON INTERNATIONAL

A. L'OCDE — Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel

L'un des premiers efforts plurinationaux visant l'établissement de lignes directrices pour la protection des renseignements personnels a été fait par l'Organisation de coopération et de développement économiques (OCDE). En 1980, l'OCDE a en effet adopté huit principes concernant la protection des renseignements personnels dans les secteurs public ou privé. Fruit d'un consensus parmi les pays membres, ces principes sont contenus dans les *Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel*(14) :

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

(13) *Ibid.*, p. 10-11.

(14) Organisation de coopération et de développement économiques, *Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel*, 1980.

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 personnelles 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 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, ou divulgation non autorisés.

Le 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 du 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 d'un fichier, ou par d'autres voies, confirmation du fait que le maître du fichier détient ou non des données la concernant ;

(b) de se faire communiquer les données les 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;

(d) de contester les données la concernant et, si la contestation est bien 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.

Même si les lignes directrices de l'OCDE sont volontaires et n'ont pas force de loi, elles ont servi de base au système de protection de la vie privée dans de nombreux pays. Elles n'ont toutefois pas mené à l'harmonisation escomptée des régimes de protection des données(15).

(15) Tom Wright, *Privacy Protection Models for the Private Sector*, Commissaire à l'information et à la protection de la vie privée/Ontario, 1996, p. 4.

B. L'Union européenne — 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

En 1995, le Conseil des ministres de l'Union européenne a adopté la *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*(16), que les membres de l'UE étaient tenus de mettre en application à l'échelon national avant le 24 octobre 1998.

La directive a deux objectifs : protéger les personnes physiques à l'égard du traitement des données à caractère personnel, et assurer la libre circulation des données personnelles entre les États membres grâce à l'harmonisation des lois nationales portant sur la protection de ces données.

La Directive de l'UE contient toute une série de principes relatifs à la qualité des données. Les États membres doivent veiller à ce que les données personnelles soient :

- 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;
- conservées pendant une durée n'excédant pas la durée nécessaire(17).

De plus, sous réserve de plusieurs exceptions, les données personnelles ne peuvent être traitées que si la personne concernée y a consenti sans ambiguïté. Les exceptions comprennent le traitement nécessaire à l'exécution d'un contrat ou le respect d'une obligation légale, ou encore la sauvegarde de l'intérêt vital ou légitime de la personne concernée ou du responsable du traitement(18).

De même, encore une fois sous réserve de certaines exceptions, il est interdit de traiter les données à caractère personnel qui révèlent l'origine raciale ou ethnique, les opinions

---

(16) Union européenne, *Directive 95/46/EC du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques et à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données*, Journal officiel n° L.281, 23/11/1995, p. 31.

(17) *Ibid*., article 6.

(18) *Ibid.*, article 7.

politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale, ainsi que de traiter les données relatives à la santé et à la vie sexuelle(19).

La Directive de l'UE accorde un certain nombre de droits à la personne faisant l'objet d'une collecte de données à caractère personnel : la personne doit être informée de l'identité du responsable des données, des finalités du traitement auxquelles les données sont destinées, des destinataires des données et de l'existence de droits d'accès à ces données et de rectification(20). Lorsque les données n'ont pas été collectées auprès de la personne concernée, le responsable du traitement doit lui fournir les mêmes informations, à moins que cela se révèle impossible ou implique des efforts disproportionnés, en particulier s'il s'agit d'un traitement à des fins statistiques ou pour une recherche historique ou scientifique(21).

La Directive de l'UE prévoit que la personne concernée a le droit de s'opposer au traitement des données à des fins de marketing direct(22). Elle stipule également que les personnes ont le droit à un recours judiciaire en cas de violation de leurs droits, ainsi qu'à une réparation(23).

Chaque État membre doit nommer une autorité indépendante publique chargée de surveiller l'application de la Directive de l'UE. Cette autorité de contrôle doit disposer 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 de l'UE(24).

La Directive encourage également l'élaboration de codes de conduite par les associations professionnelles et d'autres organisations(25).

L'article 25 de la Directive traite du transfert des données à caractère personnel entre les États membres de l'UE et des pays tiers. Ces transferts ne peuvent avoir lieu que si le pays tiers en question assure « un niveau de protection adéquat » pour ces données. La définition du « niveau de protection adéquat » revêt beaucoup d'importance pour les pays non membres de

(19) *Ibid.*, article 8.

(20) *Ibid.*, article 10.

(21) *Ibid.*, article 11.

(22) *Ibid.*, article 14.

(23) *Ibid.*, articles 22 et 23.

(24) *Ibid.*, article 28.

(25) *Ibid.*, article 27.

l'UE. La Directive précise que le caractère adéquat du niveau de protection offert par un pays tiers doit s'apprécier au regard de toutes les circonstances relatives au transfert, notamment la nature des données, la finalité et la durée du traitement envisagé, les pays d'origine et de destination finale, les règles de droit, générales ou sectorielles, en vigueur dans le pays tiers, ainsi que les règles professionnelles et les mesures de sécurité qui y sont respectées(26).

Lorsque la Commission juge que le pays tiers n'assure pas un niveau de protection adéquat, les États membres doivent empêcher le transfert des données vers ce pays. La Directive poursuit toutefois en prévoyant que le transfert des données vers un pays tiers qui n'assure pas la protection adéquate peut quand même se faire, 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 d'un contrat entre le responsable du traitement et un tiers dans l'intérêt de la personne concernée;
- le transfert soit rendu juridiquement obligatoire pour la sauvegarde d'un intérêt public important, ou pour la constatation, l'exercice ou la défense d'un droit en justice;
- le transfert soit nécessaire à la sauvegarde de l'intérêt vital de la personne concernée;
- le transfert intervienne au départ d'un registre public qui est ouvert à la consultation du public ou de toute personne justifiant d'un intérêt légitime(27).

Les renseignements personnels peuvent également être transférés dans un pays tiers qui n'assure pas un niveau de protection adéquat, lorsque le responsable du traitement offre des garanties suffisantes au regard de la protection de la vie privée et des droits fondamentaux des personnes, ainsi qu'à l'égard de l'exercice des droits correspondants; ces garanties peuvent notamment résulter de clauses contractuelles appropriées(28).

Par ailleurs, la Commission européenne a proposé la création d'un suffixe de domaine Internet de haut niveau (.ue) assorti d'une politique de protection de la vie privée à

(26) *Ibid.*, paragraphe 25(2).

(27) *Ibid.*, paragraphe 26(1).

(28) *Ibid.*, paragraphe 26(2).

laquelle tous les sites seraient tenus d'adhérer pour pouvoir s'inscrire. La garantie de mesures strictes de protection de la vie privée accroîtra, espère-t-on, la confiance des consommateurs dans Internet et donnera aux sociétés inscrites à ces sites un avantage commercial par rapport à celles qui appliquent des normes moins rigoureuses.

C. Le Conseil de l'Europe — Lignes directrices pour la protection des personnes à l'égard de la collecte et du traitement de données à caractère personnel sur les « inforoutes », qui peuvent être intégrées ou annexées à des codes de conduite

Le 23 février 1999, le Comité des ministres des États membres du Conseil de l'Europe a adopté des *Lignes directrices pour la protection des personnes à l'égard de la collecte et du traitement des données à caractère personnel sur les « inforoutes »*. Ces lignes directrices énoncent des principes relativement à la pratique du traitement équitable des données pour les utilisateurs d'Internet et les fournisseurs de services Internet. Le Conseil suggère que ces lignes directrices soient intégrées dans les codes de conduite destinés aux fournisseurs de services Internet. Les fournisseurs de services Internet devraient, par exemple :

- informer les utilisateurs des risques que fait courir l'utilisation d'Internet à la vie privée avant qu'ils ne souscrivent;
- informer les utilisateurs des moyens techniques qu'ils peuvent utiliser licitement pour diminuer les risques concernant la sécurité des données et des communications;
- n'exercer aucune ingérence dans le contenu des communications, à moins que la loi les y autorise;
- ne pas communiquer de données à moins qu'une telle communication ne soit autorisée par la loi;
- n'utilisent pas les données à des fins de promotion ou de mise en marché[29].

(29) Conseil de l'Europe, Comité des ministres, *Lignes directrices pour la protection des personnes à l'égard de la collecte et du traitement des données à caractère personnel sur les « inforoutes »*, recommandation n° R (99) 5, 23 février 1999, p. 4, http://www.coe.fr/cm/ta/rec/1999/f99r5.htm.

D. Les ministres de l'OCDE — Déclaration relative à la protection de la vie privée sur les réseaux

À la conférence « Un monde sans frontières : concrétiser le potentiel du commerce électronique mondial » tenue à Ottawa en 1998, les ministres de l'OCDE ont produit la *Déclaration relative à la protection de la vie privée sur les réseaux*. Ils y confirment leur engagement à cet égard et conviennent qu'ils prendront les mesures nécessaires pour garantir la mise en œuvre efficace des Lignes directrices de l'OCDE sur la protection de la vie privée sur les réseaux mondiaux, en veillant notamment :

- à encourager l'adoption de politiques en matière de vie privée, qu'elles soient mises en œuvre par le recours à des mécanismes juridiques, administratifs, technologiques ou d'autorégulation;
- à encourager la notification en ligne aux utilisateurs des politiques en matière de vie privée;
- à garantir l'existence de mécanismes efficaces de mise en œuvre permettant à la fois de régler les problèmes de non-respect des principes et des politiques de vie privée et de garantir l'accès à des moyens de réparation;
- à promouvoir l'éducation et la sensibilisation des utilisateurs aux problèmes de respect de la vie privée en ligne et aux moyens dont ils disposent pour protéger leur vie privée sur les réseaux mondiaux;
- à encourager l'utilisation de technologies permettant d'améliorer la protection de la vie privée; et
- à encourager l'utilisation de solutions contractuelles et le développement de solutions contractuelles types pour les flux transfrontières de données en ligne(30).

E. Initiatives américaines

Contrairement à l'Union européenne et au Canada, les États-Unis favorisent une approche non législative de la protection des renseignements personnels sur Internet. Il s'ensuit que l'Administration n'a cessé d'appuyer les initiatives d'autoréglementation du secteur privé,

(30) Organisation de coopération et de développement économiques, *Déclaration relative à la protection de la vie privée sur les réseaux mondiaux*, SG/EC(98)14/Final, octobre 1998, p. 14-15.

bien qu'elle ait indiqué qu'elle réévaluerait sa position s'il s'avérait impossible d'assurer une protection efficace de cette façon.

Cette stratégie est énoncée dans le document produit en 1997 par la Maison blanche et intitulé *A Framework for Global Electronic Commerce* (FGEC), qui établit les principes suivants visant à faciliter l'essor du commerce électronique aux États-Unis :

- Le secteur privé devrait assumer l'initiative.
- Les gouvernements devraient éviter d'imposer indûment des restrictions au commerce électronique.
- Là où leur intervention est nécessaire, les gouvernements devraient appuyer et appliquer un cadre juridique prévisible, minimaliste, cohérent et simple pour le commerce.
- Les gouvernements devraient reconnaître les caractéristiques uniques d'Internet.
- Il faudrait faciliter le commerce électronique sur Internet à l'échelle mondiale(31).

Le FGEC définit neuf secteurs où l'on devrait adopter des accords internationaux pour préserver Internet en tant que support de données non réglementé. Ces secteurs sont regroupés en trois grandes catégories : les questions financières, les questions juridiques et l'accès aux marchés. Les questions juridiques comprennent celle d'un code commercial uniforme (Uniform Commercial Code) pour le commerce électronique, la protection de la propriété intellectuelle, les renseignements personnels et la sécurité(32).

La *Presidential Directive on Electronic Commerce* du 1er juillet 1997 a été conçue pour la mise en oeuvre de la stratégie énoncée dans le FGEC et confiait 13 tâches précises à divers organismes de l'exécutif. L'une d'elles relevait du secrétaire au Commerce et du directeur de l'Office of Management and Budget et visait à encourager le secteur privé et les groupes de défense de la vie privée à élaborer et à adopter dans les 12 mois suivants des codes de conduite

(31) États-Unis, Bureau exécutif du président, *A Framework for Global Electronic Commerce,* 1er juillet 1997, p. 2-3.

(32) *Ibid*., p. 3-4.

efficaces, des règles ainsi que des solutions technologiques assurant la protection des renseignements personnels sur Internet(33).

L'objectif visé était donc de promouvoir l'autoréglementation et, ainsi, d'éviter les mesures réglementaires ou législatives. En juin 1998, la Federal Trade Commission (FTC) a remis au Congrès un rapport décrivant son enquête sur les pratiques suivies dans plus de 1 400 sites Web commerciaux, évalués selon leur respect des principes fondamentaux d'un traitement équitable de l'information. L'enquête a révélé que de nombreux sites Web ne respectaient pas de façon acceptable les principes de protection de la vie privée. Près de 85 p. 100 des sites recueillaient des renseignements auprès des consommateurs, mais seulement 14 p. 100 donnaient avis de leurs pratiques de traitement de l'information, et seulement 2 p. 100 s'étaient dotés d'une politique complète à ce chapitre. En ce qui concerne les sites Web destinés aux enfants, la Commission a constaté que 89 p. 100 recueillaient des renseignements personnels auprès des enfants, mais que seulement 23 p. 100 demandaient à ceux-ci d'obtenir la permission de leurs parents avant de la donner, et que ceux qui permettaient aux parents d'exercer un contrôle sur la collecte et l'utilisation de ces renseignements représentaient une proportion encore plus faible(34).

La FTC a continué d'encourager l'élaboration et l'adoption de mesures d'autoréglementation pour protéger les renseignements personnels sur Internet, mais elle a observé que, malgré ses exhortations et initiatives à cet égard, il n'existait pas encore de régime efficace d'autoréglementation. Elle a réclamé davantage d'incitatifs à l'autoréglementation et l'application généralisée des principes fondamentaux de la protection de la vie privée.

> La Commission a encouragé le secteur privé à répondre, grâce à des mesures d'autoréglementation, aux préoccupations des consommateurs concernant la protection des renseignements qu'ils fournissent en ligne. Internet est un marché en évolution rapide. Une autoréglementation efficace demeure souhaitable, car elle permet aux entreprises de réagir rapidement aux changements technologiques et d'utiliser de nouvelles techniques pour protéger la vie privée des consommateurs. Par conséquent, cette protection pourrait s'avérer adéquate si le secteur privé intégrait des pratiques largement acceptées et équitables prévoyant des mécanismes efficaces

(33) États-Unis, U.S. Government Working Group on Electronic Commerce, *First Annual Report*, novembre 1998, p. 15-16.

(34) United States Federal Trade Commission, *Privacy Online: A Report to Congress*, 1998, p. 2.

> d'exécution. À ce jour, cependant, la Commission n'a pas constaté l'existence d'un système efficace d'autoréglementation.
>
> Comme le montrent les résultats du sondage de la Commission, et malgré son initiative triennale visant à promouvoir l'autoréglementation en réponse aux préoccupations des consommateurs, la grande majorité des entreprises en ligne n'ont pas encore adopté ne fût-ce que des pratiques équitables très élémentaires de traitement de l'information (avis/connaissance). En outre, les lignes directrices commerciales soumises à la Commission ne donnent pas à penser que le secteur privé accepte les principes fondamentaux d'un traitement équitable de l'information. Enfin, à quelques exceptions près, les lignes directrices ne comportent aucun des mécanismes d'exécution pouvant assurer l'efficacité d'un régime d'autoréglementation(35).

Par ailleurs, la Commission recommandait que le Congrès élabore un texte de loi donnant aux parents le contrôle de la collecte et de l'utilisation en ligne des renseignements personnels auprès des enfants, et énonçant des normes minimales à cet égard. Tous les sites Web ayant pour clientèle des enfants seraient tenus de respecter ces normes(36). Par suite des recommandations de la FTC, la *Children's Online Privacy Protection Act of 1998* (COPPA) a été promulguée en 1998. À l'automne de 1999, la FTC a publié sa règle finale pour l'application de la COPPA, dont la date d'entrée en vigueur est le 21 avril 2000.

La COPPA et la règle de la FTC visent les sites Web commerciaux destinés aux enfants de moins de 13 ans et limitent les renseignements recueillis à ce qui est indispensable pour leur participation à une activité. La Loi exige que l'exploitant du site Web affiche bien en vue une politique claire sur la protection de la vie privée et obtienne un consentement parental vérifiable avant de recueillir des renseignements personnels auprès d'un enfant, de les utiliser ou de les divulguer. La Loi prévoit également des règles « refuge » pour les groupes de l'industrie ou d'autres intervenants qui veulent créer des programmes d'autoréglementation. En vertu de la loi, la FTC est autorisée à intenter des poursuites et à imposer des amendes administratives aux contrevenants(37).

---

(35) *Ibid*., p. 24-25.

(36) *Ibid*., p. 25.

(37) United States Federal Trade Commission, « New Rule Will Protect Privacy Online », communiqué de presse, 20 octobre 1999, http://www.ftc.gov/opa/1999/9910/childfinal.htm.

Un rapport plus récent du gouvernement peint un tableau moins sombre de l'autoréglementation. Dans le document publié en 1999 et intitulé *Towards Digital eQuality*, le groupe de travail sur le commerce électronique du gouvernement américain fait observer que les politiques de protection des renseignements personnels sont devenues plus courantes dans les sites Web du secteur privé, et que les efforts d'autoréglementation sont multiples et à caractère exécutoire(38). D'après ce rapport, le secteur privé soutient que près des deux tiers des sites Web commerciaux affichent maintenant des politiques ou des déclarations sur la protection des renseignements personnels, comparativement à 14 p. 100 l'année précédente(39). Le rapport affirme de nouveau que le gouvernement américain croit à l'autoréglementation et ajoute qu'il continuera à suivre la situation afin d'établir si les programmes en question protègent effectivement la vie privée des utilisateurs d'Internet. Ce suivi comprendra un sondage en ligne que la FTC effectuera en 2000 afin de réévaluer le progrès de la mise en oeuvre de pratiques équitables de traitement de l'information.

En décembre 1999, un groupe américain de défense des libertés civiles qui s'intéresse à la protection de la vie privée, au cryptage, à l'accès à l'information et à des questions connexes dans Internet, l'Electronic Privacy Information Center (EPIC), a produit un autre rapport sur le sujet. Celui-ci était moins optimiste en ce qui a trait aux pratiques de protection de la vie privée dans Internet(40). Ayant examiné les politiques et pratiques des 100 sites de magasinage électronique les plus populaires pour vérifier s'ils appliquaient des pratiques équitables de traitement de l'information et s'ils utilisaient des mouchards électroniques et de la publicité ciblée, l'EPIC a découvert que tous recueillaient effectivement des renseignements personnels, mais qu'aucun n'exigeait des consommateurs qu'ils divulguent de tels renseignements au moment d'entrer dans le site ou en le parcourant. La page d'accueil de 51 sites offrait un lien à leur politique de protection de la vie privée, mais 18 sites n'avaient

---

(38) U.S. Government Working Group on Electronic Commerce, *Towards Digital eQuality*, 2e Rapport annuel, 1999, p. 35.

(39) *Ibid*., p. 35-36.

(40) Electronic Privacy Information Center, *Surfer Beware III: Privacy Policies without Privacy Protection*, décembre 1999, http://www.epic.org/reports/surfer-beware3.html.

aucune telle politique. L'EPIC a également observé que 20 sites adhéraient à un programme d'autoréglementation du secteur privé tel que TRUSTe ou BBBOnLine[41].

L'EPIC a observé des écarts considérables entre les politiques des 100 sites pour ce qui est de la protection de la vie privée. Certes un plus grand nombre de sites affichaient des politiques à cet égard, et de nouvelles associations avaient été formées pour promouvoir leur élaboration et sensibiliser le secteur privé à la question de la vie privée, mais, en règle générale, la plupart des politiques ne comportaient pas les éléments nécessaires à des pratiques équitables et n'étaient guère susceptibles d'accorder une véritable protection aux consommateurs[42].

Une autre étude, la Georgetown Internet Privacy Policy Survey, publiée quelques mois avant l'enquête de l'EPIC, examinait dans quelle mesure les sites Web commerciaux affichaient des communications relatives à la protection de la vie privée basées sur des pratiques équitables de traitement de l'information[43]. L'échantillon était composé de 361 sites Web commerciaux (.com) visités par des consommateurs au foyer, le choix ayant été effectué parmi les 7 500 premières adresses URL classées selon l'audience au mois de janvier 1999. L'étude portait sur les trois questions suivantes :

1. Quels renseignements personnels les sites Web recueillent-ils auprès des consommateurs?
2. Combien de sites Web affichent de l'information sur la protection de la vie privée?
3. Ces communications témoignent-elles de pratiques équitables?

Pour ce qui est de la première question, l'enquête a révélé que 92,8 p. 100 des sites recueillaient au moins un type de renseignement nominatif (p. ex. le nom, l'adresse électronique et l'adresse postale); 56,8 p. 100 recueillaient au moins un type de renseignement démographique (p. ex. le sexe, les préférences, le code postal); 56,2 p. 100 des sites recueillaient

---

(41) *Ibid*., p. 3-4.

(42) *Ibid*., p. 6.

(43) Georgetown Internet Privacy Policy Survey, rapport final, juin 1999. Cette étude a été réalisée par le secteur privé et financée par les contributions de 17 entreprises et organismes; http://www.msb.georgetown.edu/faculty/culnanm/gippshome.html.

à la fois des renseignements nominatifs et des renseignements démographiques; et 6,6 p. 100 ne recueillaient aucun de ces renseignements(44).

Selon l'étude, 65,3 p. 100 (236) des 361 sites avaient affiché au moins un type de communications relative à la protection de la vie privée (un avis concernant la politique en matière de vie privée, ou une déclaration sur les pratiques de traitement de l'information), 36 p. 100 (131 sites) avaient affiché les deux types de communications, alors que 34,1 p. 100 (123 sites) n'en avaient affiché aucun(45).

L'étude déterminait si ces communications correspondaient à des pratiques équitables en analysant leur contenu en fonction de quatre éléments (avis, choix, accès et sécurité) et en vérifiant l'information sur la façon de poser des questions ou de présenter des plaintes. Sur les 236 sites Web qui recueillaient des renseignements personnels et affichaient une communication relative à la vie privée, 89,8 p. 100 comportaient au moins une indication associée à l'*avis*; 61,9 p. 100, au moins une indication associée au *choix*; 40,3 p. 100, au moins une indication relative à l'*accès*; 45,8 p. 100, au moins une indication relative à la *sécurité*; et 48,7 p. 100, au moins une indication sur la façon de poser des questions ou de présenter des plaintes(46).

---

(44) *Ibid*., p. 1.

(45) *Ibid*.

(46) *Ibid*. Les communications sur la protection de la vie privée ont été analysées afin de déterminer si elles contenaient de l'information relative aux éléments suivants : avis, choix, accès et sécurité.

Ces quatre éléments associés aux pratiques équitables de traitement de l'information étaient mesurés de la façon suivante :

- À la notion d'*avis* correspondaient des indications sur les renseignements recueillis, la façon dont ils le sont, la façon dont ils seront utilisés, la mesure dans laquelle ils seront réutilisés ou divulgués à des tiers, et la mesure dans laquelle le consommateur est prévenu de l'utilisation ou de la non-utilisation de mouchards électroniques.
- À la notion de *choix* correspondaient des indications sur le choix d'être contacté de nouveau par la même organisation et le choix de permettre ou non la divulgation à des tiers des renseignements personnels non agrégés recueillis sur le site Web.
- À la notion d'*accès* correspondaient des indications sur la possibilité pour les consommateurs d'examiner les renseignements recueillis ou de poser des questions à ce sujet, et la mesure dans laquelle les sites indiquaient leur manière de traiter les renseignements personnels inexacts qu'ils avaient recueillis.
- À la notion de *sécurité* correspondaient des indications sur la protection des renseignements pendant la transmission et l'emmagasinage subséquent.

Le rapport ne tirait aucune conclusion ni n'offrait de recommandation pour ce qui est de l'efficacité de l'autoréglementation comme moyen de protéger la vie privée sur Internet.

S'inspirant en partie de l'étude de Georgetown, la majorité des membres de la FTC a recommandé au Congrès, dans un rapport de 1999(47), de permettre à l'autoréglementation de se développer davantage. Elle a aussi exhorté le secteur privé à travailler davantage à mettre en œuvre des pratiques équitables de traitement de l'information.

En février et en mars 2000, la FTC a de nouveau recensé les pratiques en matière de traitement de l'information en vigueur sur les sites Web commerciaux. Dans un rapport de mai 2000 au Congrès(48), la FTC expose les résultats de son enquête en ligne, qui portait sur la nature et le contenu des communications affichées sur les sites Web commerciaux américains relativement à la protection de la vie privée, et elle évalue l'efficacité de l'autoréglementation en tant que moyen de protéger la vie privée des consommateurs dans le cadre d'opérations en ligne.

La FTC se réjouissait des initiatives d'autoréglementation du secteur privé. En revanche, la majorité de ses membres était d'avis que ces initiatives ne suffisaient pas et ne pouvaient garantir que l'ensemble du cybermarché se conformerait aux normes adoptées par les chefs de file du secteur privé(49). La FTC constatait que 20 p. 100 seulement des sites Web les plus achalandés avaient tant soit peu mis en œuvre les quatre pratiques de traitement équitable de l'information dans leurs communications sur la protection de la vie privée, que moins de la moitié (41 p. 100) des sites examinés respectaient les normes relatives à l'avis et au choix et que 8 p. 100 seulement des sites les plus achalandés affichaient le sceau d'un des programmes d'autoréglementation qui en comportent un(50).

(suite)

On a aussi analysé les communications pour voir si elles contenaient de l'information permettant à un consommateur de poser des questions à l'entreprise sur ses pratiques en matière de protection de la vie privée, ou pour se plaindre d'une atteinte à la vie privée auprès de l'entreprise ou d'une autre organisation.

(47) United States Federal Trade Commission, *Self-Regulation and Privacy Online*, juillet 1999.

(48) United States Federal Trade Commission, *Privacy Online: Fair Information Practices in the Electronic Marketplace*, mai 2000.

(49) *Ibid.*, p. 35.

(50) *Ibid*.

Contrairement à sa politique antérieure, la majorité des membres de la FTC a recommandé au Congrès d'adopter des mesures législatives pour assurer aux consommateurs la protection de leurs renseignements personnels sur Internet. Elle reconnaissait toutefois qu'un cadre législatif devrait ménager une place importante à l'autoréglementation du secteur privé(51).

L'autoréglementation a des ramifications importantes pour ce qui est des relations commerciales entre l'Union européenne et les États-Unis. Alors que l'Union européenne s'est dotée d'un cadre législatif et réglementaire, les États-Unis, sauf en ce qui concerne les renseignements personnels recueillis en ligne auprès des enfants, préconisent l'autoréglementation plutôt que les mesures législatives. La Directive de l'Union européenne sur la protection des données interdit l'échange de renseignements personnels avec les pays qui n'appliquent pas des normes adéquates à cet égard.

Puisque les É.-U. n'ont pas adopté de mesures législatives exhaustives pour la protection des données dans le secteur privé, il est très difficile de savoir si les solutions non législatives répondent aux exigences de la Directive européenne. Afin d'atténuer cette incertitude, le département américain du Commerce a élaboré les « International Safe Harbor Privacy Principles » (ou « principes refuge internationaux en matière de vie privée ».) Ces principes, destinés aux organisations américaines qui reçoivent des données personnelles de l'Union européenne, ont pour objet de satisfaire aux exigences de protection adéquate énoncées à l'article 25 de la Directive européenne. L'adhésion à ces principes n'est pas obligatoire, mais les organisations américaines qui souhaitent jouir des avantages en découlant sont tenues de s'y conformer. Les Safe Harbor Privacy Principles continuent de faire l'objet de négociations avec l'UE. À la fin de février 2000, un accord permettant la circulation ininterrompue de l'information aurait été conclu entre l'Europe et les É.-U., et la conclusion d'un accord définitif était prévue pour la fin de mars 2000(52).

F. Initiatives australiennes

À la suite de consultations poussées avec le milieu des affaires et les consommateurs, le commissaire australien à la protection de la vie privée a publié, en

(51) *Ibid*., p. 36-37.

(52) John Burgess, « Accord Near on Data Privacy », *Washington Post*, 24 février 2000, p. A12.

février 1998, les National Principles for the Fair Handling of Personal Information, qui établissent un cadre permettant aux entreprises de se doter de pratiques pour la protection des renseignements personnels. Après des consultations supplémentaires, il a révisé ces principes en janvier 1999.

En décembre 1998, le gouvernement fédéral australien a annoncé qu'il allait élaborer une loi « légère » pour appuyer et renforcer les initiatives d'autoréglementation du secteur privé(53). À l'heure actuelle, l'Australie n'a aucune loi générale sur le traitement des données personnelles dans le secteur privé, bien que les fournisseurs de crédits et les agences d'évaluation du crédit soient réglementés pour ce qui est de la divulgation de renseignements relatifs au crédit personnel.

En 1999, le gouvernement a rendu publique une version préliminaire des dispositions clés de son programme de protection des renseignements personnels dans le secteur privé. Les codes d'autoréglementation seraient reconnus, mais ils seraient complétés par un mécanisme législatif par défaut et un régime de traitement des plaintes s'appliquant en l'absence de codes. Cette formule se trouverait vraisemblablement à mi-chemin entre l'approche législative et réglementaire de l'Union européenne et l'approche fondée sur l'autoréglementation adoptée aux États-Unis.

Le texte de loi intégrerait des principes nationaux en matière de vie privée ou National Privacy Principles (NPP) visant les pratiques d'une organisation, qu'il s'agisse d'une entité constituée ou non en société, d'un partenariat, d'un organisme communautaire ou de bienfaisance, ou d'un particulier, s'il est propriétaire unique(54).

Le régime proposé prévoit cependant des exceptions dans les cas suivants :

- les renseignements personnels recueillis et utilisés pour les besoins domestiques;
- les dossiers des employés;
- les renseignements personnels recueillis, utilisés et divulgués par les médias afin d'informer le public;

---

(53) Australie, ministère du Procureur général, « The government's proposed legislation for the protection of privacy in the private sector », document d'information, septembre 1999, p. 3, http://law.gov.au/infopaper/infopaper.html.

(54) *Ibid*., p. 11.

- les organismes du secteur public des États et territoires; et
- les petites entreprises(55).

Les propositions exempteraient les petites entreprises (ayant un chiffre d'affaires annuel de 1 000 000 $ ou moins) qui présentent un faible risque pour ce qui est de la protection de la vie privée. Il s'agirait d'entreprises ayant un chiffre d'affaires modeste, ne détenant aucun renseignement sensible et ne communiquant aucun renseignement sur un particulier à une autre personne en échange d'un service, d'un bénéfice ou d'un avantage quelconque(56).

Les dispositions proposées établiraient des NPP pour le secteur privé et permettraient qu'un code d'autoréglementation comporte ses propres principes visant la protection des renseignements personnels ou Code Privacy Principles (CPP), lesquels remplaceraient ou intégreraient tous les NPP et assureraient à tout le moins une certaine protection. Les CPP s'appliqueraient aux organisations du secteur privé ayant convenu d'être liées par un code approuvé qui leur soit propre(57).

Les NPP comprennent les éléments suivants :

Collecte : Ce principe prévoit entre autres que seuls doivent être recueillis les renseignements nécessaires au fonctionnement d'une organisation. Il doit s'agir d'une collecte licite et équitable. Au moment de recueillir les données, il faut indiquer clairement à quoi elles vont servir.

Utilisation et divulgation : Ce principe limite l'utilisation et la divulgation des renseignements aux fins auxquelles ils ont été recueillis. Des fins secondaires sont autorisées dans certaines circonstances, notamment lorsque l'intéressé y consent et lorsque ces fins sont de nature connexe et conformes aux attentes raisonnables de l'intéressé.

Qualité des données : En vertu de ce principe, les organisations doivent s'assurer que les renseignements recueillis sont exacts, complets et à jour.

Sécurité des données : Les organisations doivent veiller à ce que les renseignements personnels en leur possession soient conservés dans des conditions sécuritaires.

Transparence : Les organisations doivent faire preuve de transparence en ce qui a trait au genre de renseignements personnels qu'elles détiennent et ce qu'elles en font.

---

(55) *Ibid*., p. 11-12.

(56) Australie, ministère du Procureur général, « Overview of Key Provisions of Privacy Amendment (Private Sector) Bill », 20 décembre 1999, p. 3-4, http://law.gov.au/privacy/overview.html.

(57) Australie, « The government's proposed legislation for the protection of privacy in the private sector », p. 13.

Accès et correction : Dans la mesure du possible, les organisations doivent permettre aux intéressés de consulter les renseignements personnels qui les concernent et de corriger toute erreur.

Identificateurs : Ce principe décourage les organisations du secteur privé d'utiliser pour une personne l'identificateur déjà affecté à cette personne par un organisme du gouvernement.

Anonymat : Dans bien des circonstances, les particuliers devraient pouvoir demeurer anonymes lorsqu'ils traitent avec des organismes du secteur privé.

Circulation transfrontalière des données : Ce principe fixe les conditions dans lesquelles une organisation peut transférer des renseignements personnels à quelqu'un se trouvant dans un pays étranger. Par exemple, le destinataire étranger doit être assujetti à une loi, à un contrat ou à un mécanisme contraignant qui protège le caractère privé des renseignements en question; sinon, la personne visée doit consentir à leur transfert.

Renseignements sensibles : Ce principe limiterait la collecte de renseignements sensibles sur des particuliers, par exemple ceux révélant l'origine raciale ou ethnique, les opinions politiques, les croyances religieuses ou philosophiques, l'appartenance à un syndicat ou des détails relatifs à la santé ou à la vie sexuelle(58).

La proposition traite en long et en large de l'élaboration de codes pour le secteur privé. Un code approuvé aurait préséance sur les NPP législatifs par défaut; si le code prévoit un mécanisme de traitement des plaintes, celui-ci prévaudrait également sur le mécanisme législatif à cet égard. Il incomberait au commissaire à la protection de la vie privée d'approuver les codes ainsi que les modifications aux codes approuvés. Le commissaire pourrait également révoquer l'approbation d'un code.

Avant de pouvoir être approuvé, un code devrait entre autres :

(a) intégrer tous les NPP ou établir des obligations qui soient à tout le moins équivalentes à celles qui y sont énoncées;

(b) spécifier les organisations liées par le code ou une façon de déterminer celles qui le seraient;

(c) stipuler que seules les organisations ayant consenti à être liées par le code le seraient effectivement;

(58) *Ibid*., p. 13-14.

(d) prévoir une procédure permettant à une organisation de ne plus être assujettie au code et précisant le moment où ce changement entrerait en vigueur;

(e) donner au public une possibilité raisonnable d'offrir des commentaires sur le projet de code;

(f) répondre aux normes prescrites et aux lignes directrices du commissaire pour le traitement des plaintes, si le code comporte un processus à cet égard;

(g) prévoir l'intervention d'un arbitre indépendant; et

(h) prévoir la production d'un rapport annuel sur le fonctionnement du code.

Le gouvernement australien a l'intention de présenter son projet de loi sur la protection des renseignements personnels en 2000, et on s'attend à ce que la loi entre en vigueur le 1er juillet 2001(59).

G. Initiatives britanniques

En tant que membre de l'Union européenne, le Royaume-Uni a dû mettre en œuvre la Directive européenne de 1995 sur la protection des données. La *Data Protection Act 1998*(60) (la « Loi ») donne effet à la Directive dans la législation du Royaume-Uni. Modifiant la *Data Protection Act 1984*, elle a reçu la sanction royale le 16 juillet 1998 et est entrée en vigueur le 1er mars 2000. Elle s'applique aux responsables du traitement de données qui sont établis au Royaume-Uni ou qui y utilisent de l'équipement pour le traitement des données. Elle s'appuie sur un système de notification en vertu duquel les personnes qui veulent traiter des données doivent en informer le commissaire à la protection des données. La Loi donne également des droits légaux aux particuliers (les personnes concernées) en ce qui concerne les renseignements personnels détenus à leur sujet par d'autres personnes.

La Loi définit un certain nombre de termes importants, entre autres « personal data » (données personnelles), « sensitive personal data » (données personnelles sensibles), « data subject » (personne concernée), « data controller » (responsable des données) et « processing » (traitement). Les « données personnelles » s'entendent :

---

(59) *Ibid*., p. 10.

(60) *Data Protection Act 1998*, (R.-U.), 1998 c. 29, http://www.hmso.gov.uk/acts/acts1998/19980029.htm.

> des données concernant une personne vivante qui peut être identifiée
>
> (a) à partir de ces données; ou
> (b) à partir de ces données ou d'autres renseignements qui sont en possession ou sont susceptibles d'entrer en possession du responsable des données;
>
> et englobe toute expression d'opinion au sujet de la personne ainsi que toute indication des intentions du responsable des données ou de toute autre personne à l'égard de cette personne(61).

La Loi crée une nouvelle catégorie de « données personnelles sensibles », assujetties à des mesures de protection additionnelles. Les données personnelles sensibles comprennent les renseignements sur les éléments suivants :

- l'origine raciale ou ethnique;
- les opinions politiques, religieuses ou de nature semblable;
- l'appartenance à un syndicat;
- la santé physique ou mentale;
- la vie sexuelle; et
- perpétration d'une infraction, et les poursuites ou la sentence subséquentes(62).

Pour l'application de la Loi, la « personne concernée » est un particulier au sujet duquel existent des données personnelles, alors que le « responsable des données » est une personne qui détermine pourquoi et comment des données personnelles sont ou seront traitées. Le terme « traitement » est défini de façon assez large, soit obtenir, enregistrer, détenir, adapter, utiliser, divulguer, détruire ou bloquer de l'information ou des données(63).

---

(61) *Ibid*., article 1(1) [traduction].

(62) *Ibid*., article 2.

(63) *Ibid*.

La Loi définit en outre huit principes relatifs à la protection des renseignements personnels :

1. Les données personnelles doivent être traitées de façon équitable et licite, et uniquement si certaines conditions sont respectées.

2. Les données personnelles ne doivent être obtenues qu'à des fins précises et licites, et elles ne doivent pas être utilisées à d'autres fins ou d'une manière incompatible avec ces fins.

3. Les données personnelles doivent être adéquates et pertinentes et ne pas dépasser une quantité raisonnable compte tenu des fins auxquelles elles sont recueillies.

4. Les données personnelles doivent être exactes et, s'il y a lieu, tenues à jour.

5. Les données personnelles ne doivent pas être conservées plus longtemps qu'il n'est nécessaire.

6. Le traitement des données personnelles doit respecter les droits des personnes concernées en vertu de la Loi.

7. Les mesures techniques et organisationnelles voulues doivent être prises pour prévenir le traitement non autorisé ou illicite des données personnelles et la perte, la destruction ou la détérioration accidentelles de ces données.

8. Aucune donnée personnelle ne doit être transférée à un pays ou territoire situé à l'extérieur de l'Espace économique européen, à moins que ce pays ou territoire ne garantisse une protection adéquate des droits et libertés des particuliers en ce qui touche le traitement des données personnelles(64).

Sauf exemption, au moins une des conditions suivantes doit être remplie pour qu'on puisse procéder au traitement de données personnelles :

- la personne concernée a donné son consentement;

- le traitement est nécessaire pour :
  (i) exécuter un contrat auquel la personne concernée est partie, ou
  (ii) prendre des mesures à la demande de la personne concernée en vue de conclure un contrat;

(64) *Ibid*., annexe I, partie I.

- le traitement est nécessaire pour exécuter une obligation juridique qui incombe au responsable des données, dans la mesure où cette obligation ne découle pas d'un contrat;

- le traitement est nécessaire à la protection des intérêts vitaux de la personne concernée;

- le traitement est nécessaire pour :
  (i) l'administration de la justice,
  (ii) l'exercice de fonctions prévues par une disposition législative,
  (iii) l'exercice des fonctions de la Couronne, d'un ministre de la Couronne ou d'un ministère, ou
  (iv) l'exécution de toute autre fonction de nature publique accomplie dans l'intérêt public;

- le traitement est nécessaire compte tenu des intérêts légitimes du responsable des données ou d'autres personnes à qui ces données sont divulguées, sauf lorsque le traitement porte préjudice aux droits et libertés ou aux intérêts légitimes de la personne concernée(65).

Il faut s'abstenir de traiter des données personnelles sensibles dans les cas qui ne satisfont pas à au moins une des conditions susmentionnées et à au moins une des conditions énoncées à l'annexe 3 de la Loi. Normalement, il faut obtenir le consentement explicite de la personne concernée avant de traiter des données personnelles sensibles, à moins que le responsable des données puisse prouver que le traitement est nécessaire en vertu de l'un des critères énoncés à l'annexe 3(66).

---

(65) *Ibid*., annexe 2.

(66) L'annexe 3 prévoit :

- que la personne concernée doit donner son consentement explicite;
- que le traitement est nécessaire à l'exercice d'un droit ou à l'exécution d'une obligation qu'une loi confère ou impose au responsable des données relativement à un emploi;
- que le traitement est nécessaire :

  a) afin de protéger les intérêts vitaux de la personne concernée ou d'une autre personne dans les cas où :

  (i) le consentement ne peut être donné par la personne concernée ou en son nom, ou

  (ii) on ne peut raisonnablement s'attendre à ce que le responsable des données obtienne le consentement de la personne concernée; ou

  b) pour protéger les intérêts vitaux d'une autre personne, dans les cas où le consentement est refusé sans raison valable par la personne concernée ou en son nom;

La Loi confère également aux particuliers les droits suivants en ce qui a trait à leurs données personnelles :

- le droit de consulter les données (articles 7 à 9);

(suite)

- que le traitement :

  a) s'effectue dans le cadre des activités légitimes de toute organisation ou association qui existe pour des motifs politiques, philosophiques, religieux ou syndicaux et qui est sans but lucratif;

  b) est assorti d'une protection adéquate des droits et libertés des personnes concernées;

  c) se limite aux particuliers qui sont membres de l'organisation ou qui ont des contrats réguliers avec elle relativement à ses objectifs; et

  d) exclut la divulgation des données personnelles à un tiers sans le consentement de la personne concernée;

- que l'information contenue dans les données personnelles a été rendue publique par suite de mesures prises délibérément par la personne concernée;

- que le traitement est nécessaire :

  a) à des procédures judiciaires (y compris d'éventuelles procédures judiciaires);

  b) à l'obtention d'un avis juridique; ou

  c) afin d'établir, d'exercer ou de défendre des droits reconnus par la loi;

- que le traitement est nécessaire :

  a) à l'administration de la justice;

  b) à l'exercice d'une fonction prévue par un texte de loi; ou

  c) à l'exercice des fonctions de la Couronne, d'un ministre de la Couronne ou d'un ministère;

- que le traitement est nécessaire pour des raisons médicales (entre autres la médecine préventive, la diagnostic médical, les recherches médicales, la prestation de soins et de traitements ainsi que la gestion de services de santé) et est effectué :

  a) par un professionnel de la santé (au sens de la Loi); ou

  b) par une personne qui est tenue à la confidentialité au même titre que si elle était un professionnel de la santé;

- que le traitement :

  a) concerne des données personnelles sensibles relatives à l'origine raciale ou ethnique;

  b) est nécessaire afin de déterminer ou de contrôler l'existence ou l'absence de l'égalité des chances ou de traitement entre personnes de différentes origines raciales ou ethniques, en vue de promouvoir ou de maintenir une telle égalité; et

  c) s'accompagne de mesures de protection appropriées à l'égard des droits et libertés des personnes concernées.

- le droit d'empêcher le traitement de données s'il est susceptible de causer un préjudice ou de la détresse (article 10);
- le droit d'empêcher le traitement de données pour le marketing direct (article 11);
- des droits relatifs au processus décisionnel automatisé (article 12);
- le droit de réclamer une indemnisation en cas de préjudice découlant d'une violation de la Loi par un responsable des données (article 13);
- le droit de prendre des mesures pour rectifier, bloquer, effacer ou détruire des données inexactes (article 14); et
- le droit de demander au commissaire à la protection des données d'établir si une disposition de la Loi a été violée (article 42).

Sous réserve de certaines exceptions, les responsables de données doivent aviser le commissaire avant d'entreprendre le traitement de données personnelles. La Loi prescrit entre autres de fournir le nom et l'adresse du responsable des données, une description des données personnelles à traiter ainsi que les catégories de personnes concernées auxquelles elles se rapportent, une description des personnes à qui le responsable des données a l'intention de les divulguer, les pays à l'extérieur de l'UE auxquels elles seront transférées, et une description des fins auxquelles elles seront traitées(67).

La Loi prévoit un certain nombre d'exemptions, énoncées à la partie IV (articles 28 à 38) et à l'annexe 7.

Il existe des exemptions motivées par la sécurité nationale(68) et d'autres pour la prévention ou la détection de crimes, l'arrestation ou la poursuite de contrevenants, ou encore la cotisation ou la perception de l'impôt(69). En outre, l'article 30 permet au secrétaire d'État d'exempter des données personnelles concernant la santé physique ou mentale d'une personne ainsi que d'autres catégories de données.

(67) *Ibid*., article 16.

(68) *Ibid*., article 28.

(69) *Ibid*., article 29.

Sous réserve de certaines conditions[70], la Loi prévoit des exemptions à des fins journalistiques, artistiques et littéraires, et pour le traitement de données personnelles à des fins de recherche (statistique ou historique, entre autres). Certaines exemptions visent les données qu'un responsable de données doit rendre publiques en vertu d'une loi[71].

Il y a des exemptions aux dispositions de non-divulgation lorsque la divulgation est exigée par une loi ou par une ordonnance, ou afin d'obtenir un avis juridique ou d'entamer des procédures judiciaires[72]. Une exemption est également prévue à des fins domestiques, lorsqu'une personne traite des données ayant trait à ses affaires personnelles ou aux affaires de sa famille ou de son ménage[73].

La Loi établit le bureau du commissaire à la protection des données, un haut fonctionnaire indépendant qui rend des comptes directement au Parlement.

Le commissaire doit notamment :

- promouvoir l'application de normes de bonne pratique par les responsables des données, et le respect des exigences de la Loi;
- diffuser de l'information au sujet de la Loi et de son fonctionnement;
- après consultation avec les parties prenantes, préparer des codes de pratique pour le traitement des données personnelles;
- encourager les associations commerciales à élaborer des codes de pratique;
- examiner les codes préparés par les associations commerciales[74];
- soumettre un rapport annuel au Parlement[75]; et
- évaluer les demandes afin de déterminer si le traitement des données personnelles respecte la Loi.

(70) *Ibid*., article 32.

(71) *Ibid*., article 34.

(72) *Ibid*., article 35.

(73) *Ibid*., article 36.

(74) *Ibid*., article 51.

(75) *Ibid*., article 52.

La Loi accorde également des pouvoirs de contrainte au commissaire. Au moyen d'avis, le commissaire peut exiger qu'un responsable des données prenne ou s'abstienne de prendre des mesures précises, ou qu'il s'abstienne entièrement de traiter des données personnelles. Le fait de ne pas respecter un tel avis constitue une infraction, à moins que l'inculpé démontre qu'il a fait preuve de diligence raisonnable pour s'y conformer. Ce genre d'avis est susceptible d'appel auprès du Tribunal de la protection des données.

Entre autres, la Loi permet au commissaire de fournir une aide à un particulier qui est partie à des procédures judiciaires relatives à certaines dispositions de la Loi. Bien qu'il ait énormément de latitude à cet égard, le commissaire ne peut accorder son appui que dans la mesure où il croit que l'affaire revêt une grande importance du point de vue de l'intérêt public(76).

La Loi autorise le commissaire à entrer par force et à faire des inspections. S'il a des motifs raisonnables de soupçonner qu'une infraction à la Loi a eu lieu ou est en train d'avoir lieu ou que l'un des principes de la protection des données a été violé ou est en train de l'être, le commissaire peut réclamer un mandat de perquisition pour fouiller les lieux.

La Loi prévoit un certain nombre d'infractions, y compris le fait :

- de traiter des données sans notification préalable;
- de ne pas respecter un avis d'exécution ou un avis d'information;
- de faire en connaissance de cause ou avec témérité une fausse déclaration relativement à un avis d'information;
- de faire intentionnellement de l'obstruction ou de ne pas fournir une aide raisonnable lors de l'exécution d'un mandat;
- sans le consentement du responsable des données, en connaissance de cause ou avec témérité :
  (i) d'obtenir ou de divulguer des données personnelles ou des renseignements y figurant; ou
  (ii) de divulguer à une autre personne le contenu de données personnelles;
- de vendre illégalement des données personnelles; et

(76) *Ibid*., article 53.

- pour le commissaire, de divulguer illégalement de l'information(77).

La Loi rend personnellement responsables des infractions les administrateurs ou les autres responsables d'une entreprise qui les ont commises. Lorsqu'une entreprise commet une infraction avec le consentement ou l'accord de l'administrateur ou du responsable concerné, ou en raison d'une négligence de sa part, cette personne est coupable de l'infraction(78).

H. Initiatives canadiennes

Au Canada, l'élaboration de normes visant à protéger la confidentialité des renseignements dans le secteur privé a essentiellement débuté lorsque le gouvernement fédéral a annoncé qu'il adhérait aux Lignes directrices de l'OCDE, en 1984. Le gouvernement fédéral cherchait alors à encourager le secteur privé à adopter des codes volontaires pour la protection des renseignements personnels(79). Toutefois, à la fin des années 80, le Commissaire à la protection de la vie privée s'inquiétait du peu de progrès accomplis et réclamait des mesures législatives fédérales qui obligeraient les organisations sous réglementation fédérale à élaborer de tels codes(80).

Conscient du potentiel du commerce électronique, le gouvernement a commencé à élaborer, dans la deuxième moitié des années 90, des stratégies et politiques portant sur les considérations commerciales, juridiques, technologiques et sociales auxquelles il donnait lieu.

En 1996, dans un rapport intitulé *La société canadienne à l'ère de l'information*, Industrie Canada déclarait qu'il fallait reconnaître le droit à la vie privée sur le plan législatif, particulièrement en ce qui concerne la conservation de renseignements personnels dans des bases

---

(77) *Ibid*., article 55.

(78) *Ibid*., article 61.

(79) Commissaire à la protection de la vie privée du Canada, *Rapport annuel 1984-1985*, Ottawa, Approvisionnements et Services Canada, 1985.

(80) Commissaire à la protection de la vie privée du Canada, *Rapport annuel 1988-1989*, Ottawa, Approvisionnements et Services Canada, 1989; *Rapport annuel 1989-1990*, Ottawa, Approvisionnements et Services Canada, 1990.

de donnés électroniques(81). La même année, les ministres fédéraux de l'Industrie et de la Justice annonçaient que le gouvernement fédéral allait légiférer afin de protéger la vie privée.

En janvier 1998, Industrie Canada et le ministère de la Justice ont rendu public un document de travail, *La protection des renseignements personnels*, qui soulignait notamment que la confiance des consommateurs était essentielle à la croissance de l'économie de l'information. D'après le document, « une loi qui définit un ensemble de règles communes pour la protection des renseignements personnels aidera à renforcer cette confiance et à instaurer un système équitable où l'usage abusif des renseignements personnels ne pourra conférer un avantage concurrentiel »(82), et une loi fédérale devrait tenir compte des quatre éléments clés suivants :

- des obligations fondées sur des pratiques équitables de traitement de l'information;
- des dispositions administratives pour un organe de surveillance afin de garantir la reddition de comptes;
- des attributions pour des autorités de supervision et des tribunaux;
- des pouvoirs et responsabilités qui favoriseront l'information du public et garantiront un réel respect des obligations(83).

Le document proposait aussi d'élaborer un régime législatif inspiré des lois d'autres pays et du Code type de l'Association canadienne de normalisation. En vertu de cette proposition, la loi canadienne devrait :

- encourager, de la part de ceux qui détiennent des renseignements personnels dans le secteur privé, des pratiques responsables en ce qui concerne la protection des renseignements personnels;
- fournir des directives souples mais efficaces pour la protection de droits exécutoires et de règles du jeu équitables sur le marché, où les renseignements personnels jouent un rôle de plus en plus important;

---

(81) Canada, ministère de l'Industrie, *La société canadienne à l'ère de l'information : Pour entrer de plain-pied dans le XXI^e siècle*, Ottawa, 1996, p. 25.

(82) Canada, Groupe de travail sur le commerce électronique, Industrie Canada, Justice Canada, *La protection des renseignements personnels : Pour une économie et une société de l'information au Canada*, Ottawa, janvier 1998, p. 6.

(83) *Ibid*., p. 11.

- être flexible, simple, efficace et d'utilisation facile pour les consommateurs, avec des droits exécutoires et des mécanismes de recours efficaces;

- être efficiente, efficace sur le plan administratif, et ne pas imposer un trop lourd fardeau à l'industrie, notamment aux petites entreprises;

- être conforme à nos obligations et accords commerciaux internationaux(84).

I. Association canadienne de normalisation — Code type sur la protection des renseignements personnels

Pendant que le gouvernement fédéral cherchait à formuler sa politique sur la protection des renseignements personnels, un comité multilatéral mis sur pied par l'Association canadienne de normalisation (CSA) et composé de représentants du monde des affaires, du gouvernement et de groupes de consommateurs travaillait à l'élaboration d'un code à cet égard. En 1996, ce processus a abouti au *Code type sur la protection des renseignements personnels* de la CSA(85), où sont définis dix principes concernant la protection de la vie privée et le droit d'accès à l'information et fondés sur les *Lignes directrices* de l'OCDE :

Responsabilité : Une organisation est responsable des renseignements personnels dont elle a la gestion et doit désigner une ou des personnes qui devront s'assurer du respect de certains principes.

Détermination des fins de la collecte des renseignements : Les fins auxquelles des renseignements personnels sont recueillis doivent être déterminées par l'organisation avant la collecte ou au moment de celle-ci.

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

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

---

(84) *Ibid*.

(85) Association canadienne de normalisation, *Code type sur la protection des renseignements personnels : Norme nationale du Canada*, CAN/CSA-Q830-96, 1996.

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

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

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

Transparence : Une organisation doit faire en sorte que des renseignements précis sur ses politiques et ses pratiques concernant la gestion des renseignements personnels soient facilement accessibles à toute personne.

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

Possibilité de porter plainte à l'égard du 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 responsables de les faire respecter au sein de l'organisation concernée.

Le Code type de la CSA a été conçu pour servir de modèle que les entreprises peuvent adopter et modifier selon leur situation particulière. Il est intégré au projet de loi C-6 : Loi sur la protection des renseignements personnels et les documents électroniques.

J. Conférence pour l'harmonisation des lois au Canada

En 1996, la Conférence pour l'harmonisation des lois au Canada (CHLC), un organisme indépendant qui travaille à l'uniformisation des lois dans le pays, a recommandé l'élaboration d'une loi régissant la protection des renseignements personnels dans le secteur privé. La CHLC a commencé à rédiger un projet de loi uniforme sur la protection des données, en fonction des objectifs suivants :

- traiter également toutes les entreprises et toutes les organisations non gouvernementales, peu importe leur taille ou leur type d'activités;

- traiter toutes les données personnelles sur un pied d'égalité, abstraction faite de leur degré de sensibilité;

- s'appuyer sur des principes établis, comme ceux énoncés dans le Code type sur la protection des renseignements personnels de l'Association canadienne de normalisation;

- établir un mécanisme administratif pour superviser la mise en œuvre de la loi (comme les commissions existantes de protection des données);

- investir la commission de protection des données du pouvoir de sensibiliser le public au sujet de la protection des données dans le secteur privé;

- pourvoir à des enquêtes sur les plaintes et à une médiation, mais seulement après l'application du processus de traitement des plaintes de l'entreprise (à supposer qu'il y en ait un et qu'il fixe des délais clairs et brefs), tout en prévoyant que, dans des cas exceptionnels, on puisse adresser une plainte directement à la commission;

- permettre à la commission de publier les noms des entreprises qui ne respectent pas la loi sur la protection des données; et

- prévoir des mesures dans les cas d'infraction à la loi(86).

Le travail de la CHLC à ce sujet a été suspendu en 1998, cependant, par suite de la présentation du projet de loi fédéral visant à protéger les renseignements personnels dans le secteur privé.

LÉGISLATION FÉDÉRALE — PROJET DE LOI C-6 : LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET LES DOCUMENTS ÉLECTRONIQUES

Le 1er octobre 1998, le ministre fédéral de l'Industrie déposait le projet de loi C-54 : Loi sur la protection des renseignements personnels et les documents électroniques, à la Chambre des communes. Le Comité permanent de l'industrie de la Chambre des communes, qui en a été saisi, en a fait rapport à la Chambre et a proposé plusieurs amendements. Toutefois, le projet de loi est mort au *Feuilleton* à la prorogation du Parlement, pour ensuite être repris et

(86) Conférence pour l'harmonisation des lois au Canada, *La protection des données dans le secteur privé : Options en vue d'une loi uniforme*, 1996.

déposé en tant que projet de loi C-6 le 15 octobre 1999[87]. Le projet de loi C-6 doit entrer en vigueur en 2001.

Le projet de loi renferme des mesures visant à protéger les renseignements personnels dans le secteur privé, établit un mode de communication électronique pour traiter avec le gouvernement fédéral et clarifie la façon dont les tribunaux doivent évaluer la fiabilité des documents électroniques produits en preuve.

Le projet de loi comporte six parties. Avec l'annexe 1, qui renferme le Code type de la CSA, la partie 1, intitulée « Protection des renseignements personnels dans le secteur privé », fixe les règles régissant la collecte, l'utilisation et la communication des renseignements personnels, ainsi que l'accès à ces renseignements dans le secteur privé. La partie 2, intitulée « Documents électroniques », permet de recourir à des moyens électroniques là où les lois fédérales permettent actuellement de conserver ou de communiquer des renseignements sur support papier. Les autres parties modifient d'autres lois fédérales afin de faciliter l'utilisation et la reconnaissance juridique des documents électroniques. Nous examinons ici en détail la partie 1, pour ensuite passer brièvement la partie 2.

A. Partie 1

La partie 1 du projet de loi C-6 (articles 2 à 30) énonce les définitions, l'objet de la partie, son champ d'application, une « limite » d'application et des situations d'exception qui permettent à une organisation de recueillir, d'utiliser et de communiquer des renseignements personnels à l'insu ou sans le consentement de l'intéressé. Cette partie renferme aussi des dispositions concernant l'accès des particuliers aux renseignements personnels qui les concernent, et les pouvoirs d'enquête et de vérification du Commissaire à la protection de la vie privée.

L'article 2 définit divers termes, notamment l'« activité commerciale », l'« organisation » et le « renseignement personnel ». Une « activité commerciale » signifie « toute activité régulière ainsi que tout acte isolé qui revêtent un caractère commercial de par leur

(87) Projet de loi C-6 : Loi visant à faciliter et à promouvoir le commerce électronique en protégeant les renseignements personnels recueillis, utilisés ou communiqués dans certaines circonstances, en prévoyant l'utilisation de moyens électroniques pour communiquer ou enregistrer de l'information et des transactions et en modifiant la *Loi sur la preuve au Canada*, la *Loi sur les textes réglementaires* et la *Loi sur la révision des lois*, Deuxième session, trente-sixième législature, 48 Elizabeth II, 1999.

nature, y compris la vente, le troc ou la location de listes de donneurs, d'adhésion ou de collecte de fonds ». Une « organisation » « s'entend notamment des associations, sociétés de personnes, personnes et organisations syndicales ». Par « renseignement personnel », le projet de loi désigne « tout renseignement concernant un individu identifiable, à l'exclusion du nom et du titre d'un employé d'une organisation et des adresse et numéro de téléphone de son lieu de travail ».

L'objet de la partie 1 est de réglementer la collecte, l'utilisation et la communication de renseignements personnels de manière à tenir compte à la fois du droit des particuliers à la confidentialité des renseignements personnels qui les concernent et du besoin qu'ont les organisations de recueillir, d'utiliser ou de communiquer des renseignements personnels à des fins qu'une personne raisonnable estimerait acceptables. Le but est de trouver un juste milieu entre le droit des particuliers à la protection de leurs renseignements personnels et les besoins raisonnables qu'ont les organisations de recueillir, d'utiliser et de communiquer des renseignements à des fins économiques.

1. Application

Sous réserve de certaines exceptions, la partie 1 du projet de loi vise toute organisation qui recueille, utilise ou communique des renseignements personnels dans le cadre de ses activités commerciales. Elle s'applique aussi à la collecte, à l'utilisation et à la communication de renseignements personnels relatifs aux employés d'organisations sous réglementation fédérale.

La partie 1 ne s'applique toutefois pas :

- aux institutions fédérales auxquelles s'applique la *Loi sur la protection des renseignements personnels*;
- aux renseignements recueillis, utilisés ou communiqués par un individu uniquement à des fins personnelles ou domestiques; ou
- à une organisation à l'égard des renseignements personnels qu'elle recueille, utilise ou communique uniquement à des fins journalistiques, artistiques ou littéraires(88).

(88) *Ibid.*, paragraphe 4(2).

Le secteur de la santé disposera toutefois d'une année à partir de l'entrée en vigueur de la partie 1 pour satisfaire aux exigences de la loi. Sans l'exempter de l'application de la loi, cette disposition lui donne plus de temps pour s'y préparer.

Le paragraphe 30(1) établit une importante exemption à l'application du projet de loi en stipulant que la partie 1 « ne s'applique pas à une organisation à l'égard des renseignements personnels qu'elle recueille, utilise ou communique dans une province dont la législature a le pouvoir de régir la collecte, l'utilisation ou la communication de tels renseignements, sauf si elle le fait dans le cadre d'une entreprise fédérale ou qu'elle communique ces renseignements pour contrepartie à l'extérieur de cette province ». Le paragraphe 30(2) précise que cette exemption à l'application de la partie 1 dans une province cessera d'avoir effet trois ans après l'entrée en vigueur de l'article 30.

Une fois en vigueur, la partie 1 s'appliquera donc aux organisations du secteur privé sous réglementation fédérale (télécommunications, télédiffusion, banques, transport interprovincial et aviation commerciale). La partie 1 visera aussi les organisations qui recueillent, utilisent ou communiquent des renseignements personnels à l'intérieur d'une province si elles les communiquent à l'extérieur de la province ou du pays à des fins commerciales. Trois ans après son entrée en vigueur, la partie 1 s'appliquera toutefois de manière plus générale aux organisations limitées à une province, même si elles recueillent, utilisent ou communiquent des renseignements personnels uniquement à l'intérieur de la province.

Une province peut adopter ses propres mesures législatives pour assurer la protection des renseignements personnels qui sont recueillis, utilisés ou communiqués sur son territoire. Le gouverneur en conseil peut, en vertu de l'alinéa 26(2)*b*), exclure une organisation, une catégorie d'organisations, une activité ou une catégorie d'activités de l'application de la partie 1 si la province a adopté une loi « essentiellement similaire » à la partie 1. Cette exclusion est toutefois limitée à la collecte, à l'utilisation ou à la communication de renseignements personnels à l'intérieur d'une province. Le commerce interprovincial ou international de renseignements personnels demeure assujetti au projet de loi. Pour l'instant, seul le Québec a adopté une loi régissant la collecte, l'utilisation et la communication de renseignements personnels dans le secteur privé.

L'article 5 oblige les organisations à se conformer aux obligations énoncées dans le Code type de la CSA (incorporé au projet de loi à l'annexe 1) sous réserve des exemptions des articles 6 à 9. Il précise toutefois que l'emploi du conditionnel dans l'annexe 1 indique qu'il s'agit non pas d'une obligation mais d'une recommandation. L'article 5 ajoute le critère de la « fin acceptable » en précisant que les fins auxquelles une organisation peut recueillir, utiliser ou communiquer des renseignements personnels doivent se limiter à celles « qu'une personne raisonnable estimerait acceptables dans les circonstances ».

2. Exemptions

L'article 7, qui énonce les cas où une organisation peut recueillir, utiliser ou communiquer des renseignements personnels à l'insu de l'intéressé et sans son consentement, est essentiel au fonctionnement du régime de protection de la vie privée établi par le projet de loi.

Le paragraphe 7(1) établit qu'une organisation ne peut recueillir des renseignements personnels à l'insu de l'intéressé et sans son consentement que dans les cas suivants :

> *a*) la collecte du renseignement est manifestement dans l'intérêt de l'intéressé et son consentement ne peut être obtenu en temps opportun;
>
> *b*) il est raisonnable de croire que la collecte effectuée au su et avec le consentement de l'intéressé pourrait compromettre l'obtention ou l'exactitude des renseignements, et la collecte est raisonnable à des fins liées à une enquête sur la violation d'un accord ou la contravention du droit fédéral ou provincial;
>
> *c*) la collecte est faite uniquement à des fins journalistiques, artistiques ou littéraires;
>
> *d*) il s'agit d'un renseignement réglementaire auquel le public a accès.

Le paragraphe 7(2) établit une exemption pour ce qui est de l'utilisation des renseignements personnels à l'insu de l'intéressé et sans son consentement dans les cas suivants :

> *a*) dans le cadre de ses activités, l'organisation découvre l'existence d'un renseignement dont elle a des motifs raisonnables de croire qu'il pourrait être utile à une enquête sur une contravention au droit fédéral, provincial ou étranger;
>
> *b*) l'utilisation est faite pour répondre à une situation d'urgence mettant en danger la vie, la santé ou la sécurité de tout individu;

c) sous réserve de certaines conditions, l'utilisation est faite à des fins statistiques ou à des fins d'étude ou de recherche érudites;

c.1) il s'agit d'un renseignement réglementaire auquel le public a accès; ou

d) le renseignement a été recueilli au titre des alinéas 7(1)*a*) ou *b*).

L'article 7(3) permet à une organisation de communiquer des renseignements personnels à l'insu de l'intéressé et sans son consentement dans les cas où la communication :

a) est faite à un avocat qui représente l'organisation;

b) est faite en vue du recouvrement d'une créance que l'organisation a contre l'intéressé;

c) est exigée par assignation, mandat ou ordonnance d'un tribunal en vue de contraindre à la production de renseignements ou exigée par les règles de procédure se rapportant à la production de documents;

c.1) est faite à une institution gouvernementale aux fins de la sécurité nationale, de la défense, de la conduite des affaires internationales, de l'application du droit, de la tenue d'enquêtes ou de l'application du droit canadien ou provincial;

d) est faite à un organisme d'enquête lorsque l'organisation a des motifs raisonnables de croire que le renseignement est afférent à la violation d'un accord ou à une contravention au droit, ou soupçonne que le renseignement est afférent à la sécurité nationale, à la défense ou à la conduite des affaires internationales;

e) est faite à toute personne qui a besoin du renseignement en raison d'une situation d'urgence mettant en danger la vie, la santé ou la sécurité d'une personne;

f) est faite, à certaines conditions, à des fins statistiques ou à des fins d'étude ou de recherche érudites;

g) est faite à une institution à vocation historique ou archivistique;

h) est faite 100 ans ou plus après la création du document contenant le renseignement ou 20 ans après le décès de l'intéressé;

h.1) porte sur un renseignement réglementaire auquel le public a accès;

> *h*.2) est faite par un organisme d'enquête et liée à une enquête sur la violation d'un accord ou la contravention du droit;
>
> *i*) est exigée par la loi.

L'exemption qui permet d'utiliser des renseignements personnels « à des fins statistiques ou à des fins d'étude ou de recherche érudites » comporte, nous l'avons vu, certaines conditions. Elle ne peut être invoquée que si les fins visées ne peuvent être réalisées sans les renseignements en cause, leur caractère confidentiel est assuré, le consentement est difficile à obtenir, et l'organisation informe le commissaire de l'utilisation au préalable. De même, la communication de renseignements à des fins statistiques ou à des fins d'étude ou de recherche érudites est autorisée si toutes ces conditions, sauf la garantie du caractère confidentiel, sont réunies.

3. Accès aux renseignements personnels

Le projet de loi C-6 donne aux particuliers le droit de prendre connaissance des renseignements personnels qui les concernent et d'y faire apporter des corrections, au besoin. Une organisation doit répondre aux demandes d'accès dans les 30 jours, mais peut demander plus de temps dans certaines situations[(89)]. Elle peut refuser de communiquer les renseignements à l'intéressé si la communication révèle, au sujet d'un tiers, un renseignement personnel qui ne peut être retranché d'un document. Cette interdiction est toutefois levée si le tiers consent à la communication ou si l'intéressé a besoin du renseignement parce que sa vie, sa santé ou sa sécurité est en danger.

Une organisation peut, par ailleurs, refuser l'accès à des renseignements personnels lorsque :

- les renseignements sont protégés par le secret professionnel qui lie l'avocat à son client;
- la communication révélerait des renseignements commerciaux confidentiels;
- il est raisonnable de croire que cela pourrait nuire à la vie ou la sécurité d'autrui;

(89) *Ibid.*, article 8.

- les renseignements ont été recueillis à des fins liées à une enquête sur la violation d'un accord ou la contravention du droit fédéral ou provincial; ou

- les renseignements ont été recueillis dans le cadre d'un mécanisme officiel de règlement des différends(90).

La communication est toutefois autorisée si l'individu a besoin des renseignements parce que sa vie, sa santé ou sa sécurité est menacée.

Le projet de loi permet à chacun de porter plainte auprès du Commissaire à la protection de la vie privée du Canada au sujet de la façon dont une organisation se conforme à la Loi ou au Code de la CSA, et autorise le commissaire à faire enquête et à tenter de résoudre le problème.

L'article 11 précise qu'une plainte peut être portée soit par l'intéressé, soit par le commissaire. L'intéressé peut déposer une plainte contre une organisation qui contrevient aux dispositions du projet de loi concernant la collecte, l'utilisation et la communication des renseignements personnels ou l'accès à ces renseignements, ou qui ne se conforme pas à l'une des recommandations du Code type. Le commissaire ne peut toutefois prendre l'initiative d'une plainte que s'il a des motifs raisonnables de croire qu'une enquête s'impose sur une question relative à l'application de la partie 1 du projet de loi.

4. Pouvoirs du Commissaire à la protection de la vie privée

Le projet de loi donne des pouvoirs étendus au commissaire, notamment :

- d'accueillir des plaintes de particuliers et de déposer lui-même des plaintes;

- de mener enquête à l'égard des plaintes;

- de tenter de régler les plaintes par la médiation et la conciliation;

- dans l'année qui suit le dépôt d'une plainte, qu'il en ait pris ou non l'initiative, de produire un rapport à ce sujet;

- à l'égard d'une plainte dont il n'a pas pris l'initiative : avec le consentement du plaignant, de demander à la Section de première instance de la Cour fédérale de tenir une audience, de comparaître devant elle au nom du plaignant qui a demandé

(90) *Ibid.*, article 9.

l'audition de la question, ou, avec l'autorisation de la Cour, de comparaître comme partie à la procédure;

- de vérifier les pratiques de gestion des renseignements personnels d'une organisation s'il a des motifs raisonnables de croire que celle-ci contrevient aux dispositions de la loi concernant la protection des renseignements personnels ou ne se conforme pas à une recommandation du Code type de la CSA;

- de rendre publique toute information relative aux pratiques de gestion des renseignements personnels d'une organisation s'il estime que c'est dans l'intérêt du public;

- de consulter ses homologues provinciaux qui, au titre d'une loi provinciale essentiellement similaire, ont des attributions semblables aux siennes;

- de conclure des ententes avec ses homologues provinciaux afin de coordonner leurs activités, d'entreprendre des travaux de recherche et d'en publier les résultats, et d'élaborer des contrats types en vue de protéger les renseignements personnels recueillis, utilisés ou communiqués d'une province ou d'un pays à l'autre;

- d'offrir au grand public des programmes d'information destinés à faire mieux comprendre l'objet des dispositions sur la protection de la vie privée, d'entreprendre des travaux de recherche relatifs à la protection des renseignements personnels et d'en publier les résultats, et d'encourager les organisations à se donner de politiques détaillées, et notamment des codes de pratique; et

- de faire rapport chaque année au Parlement.

L'article 12 donne au commissaire des pouvoirs étendus pour procéder à l'instruction des plaintes, y compris celui :

- d'assigner et de contraindre des témoins à comparaître devant lui, à déposer et à produire les documents requis;

- de faire prêter serment;

- de recevoir les éléments de preuve indépendamment de leur admissibilité devant les tribunaux;

- de visiter, à toute heure convenable, les locaux d'une organisation;

- de s'entretenir en privé avec toute personne qui se trouve dans ces locaux; et

- d'examiner ou de se faire remettre des copies ou des extraits des documents trouvés dans ces locaux.

Le projet de loi prévoit aussi l'audition d'une affaire devant la Section de première instance de la Cour fédérale. Un plaignant peut demander une audience dans les 45 jours qui suivent la transmission du rapport du commissaire. La Cour peut, entre autres, ordonner à l'organisation de revoir ses pratiques, si elles ne sont pas conformes à la Loi, de publier un avis indiquant les mesures prises pour remédier à ses pratiques, et de verser au plaignant des dommages-intérêts, notamment en réparation de l'humiliation subie(91).

Aux termes du projet de loi, quiconque entrave une enquête du commissaire, détruit des documents avant que tous les recours n'aient été épuisés, ou congédie, suspend ou rétrograde un employé qui divulgue les infractions à la Loi de son employeur, commet un délit passible d'une amende maximale de 100 000 $(92).

L'article 27.1 vise à mettre les employés qui dénoncent leur employeur ou une autre personne qui aurait enfreint la Loi à l'abri d'un congédiement, d'une suspension, d'une rétrogradation, de mesures de discipline ou du harcèlement.

B. Partie 2

La partie 2 du projet de loi C-6 permet de remplacer les documents sur support papier par des documents électroniques dans les communications avec l'administration fédérale et introduit la notion de « signature électronique sécurisée ». Conformément à la Loi, le gouvernement devra prescrire les technologies ou procédés utilisés pour produire une « signature électronique sécurisée » en se fondant sur les critères suivants(93) :

- la signature électronique doit être propre à son utilisateur;
- la personne dont la signature électronique paraît sur un document a le contrôle de la technologie utilisée à cette fin;

---

(91) *Ibid.*, article 16.

(92) *Ibid.*, article 28.

(93) Pour l'application du projet de loi C-6, une « signature électronique » s'entend d'une signature constituée d'une ou de plusieurs lettres, ou d'un ou de plusieurs caractères, nombres ou autres symboles sous forme numérique incorporée, jointe ou associée à un document électronique; une « signature électronique sécurisée » est une signature électronique qui résulte de l'application de toute technologie ou de tout procédé prévu par règlement pris en vertu du paragraphe 48(1).

- la technologie permet d'identifier la personne qui s'en sert pour apposer sa signature électronique; et
- la signature électronique peut être liée au document électronique de façon à pouvoir vérifier si le document a été modifié depuis l'opposition de la signature électronique.

Le projet de loi traite aussi des documents électroniques utilisés comme éléments de preuve devant les tribunaux. Dans une instance judiciaire typique, le tribunal exige habituellement des documents originaux pour s'assurer que les conditions d'une entente n'ont pas été modifiées depuis sa signature. Il est difficile de satisfaire à cette exigence lorsqu'il s'agit de documents électroniques, puisqu'il est impossible de différencier l'original d'un document modifié et que le document n'est pas authentifié par des signatures manuscrites. Le projet de loi exige donc d'utiliser des signatures électroniques sécurisées pour les documents électroniques chaque fois que la loi exige des documents originaux ou une attestation de véracité.

SITUATION DANS LES PROVINCES

A. Québec

Le Québec a été la première entité de l'Amérique du Nord à légiférer à l'égard de la collecte, de l'utilisation, de la communication et de la conservation des renseignements personnels dans le secteur privé(94). Il demeure jusqu'ici la seule province à l'avoir fait. La *Loi sur la protection des renseignements personnels dans le secteur privé* (projet de loi 68) est entrée en vigueur le 1er janvier 1994(95).

La Loi vise la collecte de « renseignements personnels », qu'elle définit comme tout renseignement qui concerne une personne physique et permet de l'identifier. Sauf disposition contraire dans la Loi, il faut obtenir le consentement de l'intéressé pour recueillir, utiliser et communiquer des renseignements personnels à son sujet. La mesure québécoise exige

(94) Cette partie s'inspire fortement de la description que Richard C. Owens donne de la législation québécoise sur la protection de la vie privée dans *La protection de la vie privée dans le secteur des services financiers au Canada*, document de recherche produit pour le Groupe de travail sur l'avenir du secteur des services financiers canadien, septembre 1998, p. 79-82.

(95) L.R.Q., c. P-39.1.

que ce consentement soit manifeste, libre et éclairé, et donné à des fins précises. D'autre part, le consentement n'est valable que le temps nécessaire à la réalisation des fins auxquelles il a été demandé. Une entreprise peut recueillir des renseignements d'un tiers sans le consentement de l'intéressé, pourvu que la Loi l'autorise ou que d'autres conditions énoncées dans la Loi soient réunies. Au moment de la collecte des renseignements, l'entreprise doit informer l'intéressé de ce qu'elle compte en faire.

La Loi établit aussi des règles sur la conservation des renseignements personnels. Ces règles permettent aux intéressés de faire retirer de leur dossier tout renseignement désuet ou qui n'est pas nécessaire à l'objet du dossier. Lorsqu'ils servent à prendre une décision au sujet de l'intéressé, les renseignements doivent être à jour et exacts. Une entreprise doit informer les intéressés de l'existence et de l'objet des dossiers qui les concernent et de leur droit d'accès à ces dossiers.

De manière générale, il est interdit aux entreprises de divulguer, de communiquer ou d'utiliser les renseignements personnels à des fins « non pertinentes à l'objet » des dossiers. D'autres utilisations, divulgations ou communications sont autorisées avec le consentement de l'intéressé ou lorsqu'une exception établie par la Loi s'applique. Celle-ci interdit aussi aux entreprises québécoises de communiquer des renseignements personnels à l'extérieur de la province à moins d'avoir pris « tous les moyens raisonnables pour s'assurer que les renseignements ne seront pas utilisés à des fins non pertinentes à l'objet du dossier ».

Des dispositions spéciales s'appliquent aux « listes nominatives », c'est-à-dire des listes de noms, adresses et numéros de téléphone de personnes physiques. Lorsqu'une entreprise souhaite utiliser sa propre liste nominative pour une campagne de prospection commerciale ou philanthropique, elle doit donner l'occasion à ceux dont le nom figure sur la liste de l'en faire retrancher.

La Loi prévoit aussi qu'un particulier peut demander l'accès aux renseignements personnels qui le concernent et leur rectification. Une entreprise doit confirmer l'existence d'un dossier qui renferme des renseignements personnels et répondre à une demande d'accès dans les 30 jours. Ces dispositions comportent toutefois des exemptions et des limites.

Un recours à la Commission d'accès à l'information du Québec est prévu en cas de désaccord entre un particulier et une entreprise au sujet de l'application de la Loi. Les décisions de la Commission sont exécutoires, mais il est possible d'en interjeter appel.

Une entreprise qui recueille, conserve ou communique des renseignements de manière contraire à la Loi est passible d'amendes de 1 000 $ à 10 000 $ s'il s'agit d'une première infraction et de 10 000 $ à 20 000 $ en cas de récidive. Les dirigeants ou les administrateurs d'une entreprise peuvent être jugés personnellement responsables s'ils autorisent ou ordonnent l'acte délictueux ou y consentent.

La loi québécoise ne comporte pas de code de protection de la vie privée pour les divers secteurs d'activité.

B. Nouveau-Brunswick

En mai 1998, le ministère de la Justice du Nouveau-Brunswick a publié un document de travail dans lequel il examine la possibilité d'étendre au secteur privé l'application des mesures législatives sur la protection de la vie privée(96). Le document visait à déterminer si la vie privée doit être mieux protégée qu'elle ne l'est par les lois actuelles, et par quels moyens. Il comporte des « propositions » pour alimenter la discussion et doit être renvoyé au Comité permanent de modification des lois de l'Assemblée législative du Nouveau-Brunswick pour que celui-ci en fasse l'étude et l'objet d'un débat public.

Lorsqu'ils suggèrent que l'on s'inspire du Code type de la CSA sur la protection des renseignements personnels, les auteurs du document signalent que la portée et le contenu de mesures législatives fondées sur ce code sont susceptibles d'être vastes et que les dix principes du Code type en seraient les composantes clés.

Le document de travail examine l'opportunité d'appliquer les principes du Code type également à toutes les organisations, peu importe leur taille, et celle de donner à une loi sur la protection des données dans le secteur privé toute la portée prévue par le Code ou d'adopter une approche plus ciblée. Ses auteurs rappellent toutefois qu'il faut se garder, dans une mesure législative sur la protection des données, d'imposer aux petites organisations des obligations dont elles risquent de ne pas pouvoir s'acquitter.

---

(96) Nouveau-Brunswick, ministère de la Justice, *Droit à la vie privée : deuxième document de travail*, mai 1998.

Le document étudie aussi l'application d'une éventuelle mesure législative sur la protection des données inspirée par le Code de la CSA, et examine l'opportunité d'établir un recours pénal, un recours civil ou un recours administratif.

C. Manitoba

En 1997, le Conseil consultatif manitobain de l'autoroute électronique affirmait que le Manitoba aurait « intérêt à assumer un rôle de premier plan dans les efforts visant à établir un juste équilibre entre la protection des renseignements personnels et confidentiels d'une part, et l'accès à l'information pour des fins sociales et économiques légitimes, d'autre part »(97). Il recommandait, entre autres, que le gouvernement du Manitoba « encourage fortement le secteur privé à envisager l'adoption de lignes directrices semblables à celles qu'a publiées l'Association canadienne de normalisation au sujet de l'accès à l'information et de la protection des renseignements personnels »(98).

La *Loi sur les renseignements médicaux personnels*, adoptée en 1997 par le Manitoba, réglemente la collecte, l'utilisation et la communication des renseignements médicaux personnels. Elle vise les renseignements personnels de nature médicale qui sont versés aux dossiers et qui permettent d'identifier un particulier, mais non l'information ou les données statistiques utilisées de manière à assurer la confidentialité des particuliers(99).

La Loi donne aux particuliers le droit d'examiner les renseignements médicaux personnels qui les concernent, d'en recevoir une copie et d'en demander la correction. De plus, diverses dispositions protègent la confidentialité des renseignements et la vie privée des particuliers, notamment en :

- limitant la nature et le nombre de renseignements qu'un dépositaire peut obtenir, utiliser ou communiquer;

---

(97) *Rapport du Conseil consultatif manitobain de l'autoroute électronique*, 1997, p. 45.

(98) *Ibid.*, p. 50.

(99) L'information sur le contenu de la *Loi sur les renseignements médicaux personnels* est tirée en grande partie du communiqué du ministre de la Santé du Manitoba, « Promulgation de la Loi sur les renseignements médicaux personnels », 17 décembre 1997, http://www.gov.mb.ca/chc/press/top/1997/12/1997-12-17-02.html.fr.

- exigeant que les intéressés soient informés de la raison pour laquelle les renseignements sont recueillis;

- exigeant que les renseignements soient mis à jour et corrigés avant d'être utilisés ou communiqués;

- obligeant les dépositaires à mettre en pratique et à respecter les directives en matière de conservation et de destruction des renseignements;

- obligeant les dépositaires à établir des garanties administratives, techniques et physiques satisfaisantes afin d'assurer la confidentialité, la sécurité, l'exactitude et l'intégrité des renseignements;

- interdisant la vente de renseignements médicaux personnels; et

- exigeant que l'utilisation de renseignements médicaux personnels maintenus par le gouvernement soit approuvée au préalable par un comité de la protection des renseignements médicaux.

Aux termes de la Loi, commet une infraction, quiconque, entre autres :

- recueille, utilise, vend ou communique des renseignements médicaux personnels en violation de la Loi;

- omet de protéger de façon sûre des renseignements médicaux personnels; et

- détruit ou efface volontairement des renseignements médicaux personnels pour empêcher quelqu'un d'y avoir accès.

Il incombe à l'ombudsman du Manitoba de veiller à l'observation de la Loi et de donner suite aux plaintes reçues de particuliers au sujet du droit d'accès aux renseignements médicaux personnels qui les concernent, ou de la collecte, de l'utilisation ou de la communication de renseignements médicaux personnels.

En mars 1999, le ministre de la Consommation et des Corporations du Manitoba rendait public le document de travail *La protection des renseignements personnels dans le secteur privé* afin de recueillir l'opinion des Manitobains sur cette question. Le document comporte 12 questions sur lesquelles le gouvernement souhaitait obtenir le point de vue du public. Il décrit, entre autres, le rôle crucial que l'information joue dans l'économie et dans l'appareil gouvernemental, les inquiétudes croissantes que suscite la collecte de renseignements personnels, les formules adoptées et les initiatives prises en matière de protection de la vie privée aux États-Unis, dans l'Union européenne et au Canada grâce au Code type de la CSA, le projet

de loi C-54 (devenu C-6) et l'évolution de la situation au Manitoba, y compris la publication du rapport du Conseil consultatif manitobain de l'autoroute électronique. Les auteurs du document font observer que la protection des renseignements personnels n'est pas simple et laissent entendre que le Manitoba aurait intérêt à examiner soigneusement l'incidence que la loi fédérale aura au Manitoba sur les consommateurs et les organisations du secteur privé(100).

D. Colombie-Britannique

En juillet 1999, le gouvernement de la Colombie-Britannique a chargé un comité spécial composé de membres de tous les partis d'examiner la question de la protection des renseignements personnels dans le secteur privé et l'incidence des documents électroniques sur la confidentialité et la liberté d'information des résidants de la province, puis de formuler des recommandations. C'est dans ce contexte que la British Columbia Information, Science and Technology Agency a rendu public, en octobre 1999, un document de travail intitulé *Protecting Personal Privacy in the Private Sector*(101).

Selon le document, il importe d'établir un cadre réglementaire efficace pour assurer la protection des renseignements personnels des résidants de la province et d'informer ceux-ci de leurs droits. Les auteurs ajoutent qu'une action efficace dépendra d'un ensemble de solutions, dont la sensibilisation des consommateurs, les techniques de permettant d'accroître la protection de la vie privée, les codes de pratique et les normes, accompagnées d'une mesure législative qui impose une forme de surveillance(102). Ils estiment aussi qu'il est surtout important de mettre les particuliers à l'abri de la collecte, de l'utilisation et de la communication inacceptables des renseignements personnels, notamment dans les domaines qui ne seront pas visés par le projet de loi C-6(103).

---

(100) Manitoba, ministère de la Consommation et des Corporations, *La protection des renseignements personnels dans le secteur privé*, mars 1999, http://www.gov.mb.ca/cca/paperfre.pdf.

(101) British Columbia Information, Science and Technology Agency, *Protecting Personal Privacy in the Private Sector*, octobre 1999, http://www.ista.gov.bc.ca/agency/IMCPD/FOIPP/PSP-100799.htm.

(102) *Ibid.*, p. 7.

(103) *Ibid.* Le document précise que la mesure fédérale ne protégera ni les dossiers des employés d'entreprise du secteur privé sous réglementation provinciale, ni les renseignements personnels recueillis dans des contextes non commerciaux tels que les hôpitaux privés, les écoles privées et les organismes de bienfaisance.

Le document pose dix questions pour alimenter la discussion.

AUTORÉGLEMENTATION

Plusieurs entreprises, groupes de divers secteurs d'activités et organisations du secteur privé ont tenté de se doter de pratiques équitables de traitement de l'information en élaborant et en adoptant volontairement des lignes directrices et des codes de pratique. Les codes les plus connus sont notamment ceux de l'Association des banquiers canadiens, de l'Association canadienne du marketing, de l'Association canadienne des compagnies d'assurances de personnes et du Bureau d'assurance du Canada. Ces codes se divisent, de manière générale, en cinq catégories :

Codes propres à une entreprise : codes élaborés par des entreprises à défaut d'instruments sectoriels de plus grande portée ou en attendant l'élaboration de tels instruments.

Codes de pratique sectoriels : codes élaborés par un groupe du secteur privé qui constate la nécessité de politiques et de pratiques cohérentes et assujetties à des règles conçues en fonction de la spécificité de son secteur et de la structure réglementaire en place.

Codes fonctionnels : codes définis selon l'activité à laquelle une organisation se livre.

Codes technologiques : codes visant des pratiques indiscrètes précises associées aux technologies de l'information et de la communication.

Codes professionnels : codes établis à l'intention d'associations et de sociétés professionnelles(104).

Lorsque les mesures législatives visant à assurer la protection des renseignements personnels dans le secteur privé sont moins importantes, les codes de pratique volontaires constituent un élément important des initiatives dans ce domaine. L'administration fédérale américaine a même encouragé l'autoréglementation comme moyen de favoriser la croissance du commerce électronique.

---

(104) Ann Cavoukian, *Privacy as a Fundamental Human Right vs. Economic Right: An Attempt at Reconciliation*, Commissaire à l'information et à la protection de la vie privée/Ontario, septembre 1999, p. 6.

A. Avantages et inconvénients de l'autoréglementation

L'autoréglementation comporte à la fois des avantages et des inconvénients, dont certains sont examinés dans le document de 1996 intitulé *Privacy Protection Models for the Private Sector* et exposés ci-après.

La souplesse est l'un des grands avantages de l'autoréglementation. Ses partisans soutiennent que la réglementation, solution trop rigide, tend à prendre du retard sur les progrès technologiques et les utilisations des renseignements personnels; qui plus est, elle est difficile à modifier. Par contre, l'autoréglementation permet aux entreprises de prendre une expansion rapide, d'adopter des politiques et des codes de conduite en fonction de l'évolution de la situation et des nouveaux enjeux, et d'adapter les codes de pratique aux besoins d'un secteur particulier(105). Les codes volontaires permettent aussi aux entreprises de maintenir l'équilibre entre, d'une part, la protection de la vie privée et, de l'autre, des intérêts divergents et les contraintes du traitement et de l'utilisation des données au jour le jour(106).

Les consommateurs peuvent être avantagés par l'autoréglementation. Comme les codes volontaires sont habituellement propres à des secteurs ou à des enjeux particuliers, ils sont souvent plus détaillés et plus pertinents que les mesures législatives, dont la portée est forcément beaucoup plus grande. De plus, les responsables de l'application des codes étant moins éloignés du niveau auquel se produisent les différends, des codes volontaires peuvent faciliter l'accès aux mécanismes de recours(107).

L'absence de rouages bureaucratiques et d'interventions gouvernementales est un autre avantage de l'autoréglementation, dont les partisans font valoir que la réglementation est coûteuse et constitue un fardeau à la fois pour les entreprises, les consommateurs et les contribuables. L'autoréglementation permet aussi d'éviter de créer des structures bureaucratiques et de dépenser des deniers publics(108).

---

(105) Tom Wright, *Privacy Protection Models for the Private Sector*, décembre 1996, p. 10.

(106) *Ibid.*

(107) *Ibid.*

(108) *Ibid.*

Les codes volontaires présentent toutefois des inconvénients, notamment :

- un manque de mesures efficaces visant à les faire respecter et (ou) de mécanismes d'appel à des tiers indépendants;
- l'absence ou l'inefficacité des sanctions en cas de non-conformité;
- l'insuffisance des réparations en cas d'infraction au code;
- le manque d'indépendance des organismes d'autoréglementation;
- la participation restreinte des organisations du secteur privé; et
- l'absence de normes d'équité objectives pour la protection des données(109).

Des travaux de recherche ont fait ressortir les points faibles des codes de protection de la vie privée adoptés par les organisations canadiennes. Une étude du Centre pour la défense de l'intérêt public, mentionnée dans le document *Privacy Protection Models for the Private Sector*, a décelé des faiblesses dans plusieurs des 12 codes de pratiques examinés et arrive à la conclusion que ces codes ne protègent pas suffisamment la vie privée. Les problèmes décelés comprenaient :

- le rôle restreint des consommateurs dans l'élaboration des codes;
- l'exclusion des consommateurs de l'administration des codes;
- l'administration au niveau soit de l'entreprise, soit du secteur d'activité;
- le peu de recours à la publicité comme moyen d'assurer le respect des codes;
- la portée insuffisante des codes;
- le manque de surveillance;
- les faibles niveaux de respect des codes;
- la faiblesse des sanctions; et
- l'absence de recours ultime pour les consommateurs(110).

(109) *Ibid.*, p. 10-11.

(110) *Ibid*, p. 11.

B. Mesures pour améliorer les codes et les politiques de protection de la vie privée dans le secteur privé

Il ne suffit pas d'élaborer une politique ou un code de pratique en matière de protection de la vie privée et de l'afficher sur un site Web pour assurer une protection adéquate des renseignements personnels. Pour améliorer cette protection et offrir aux cyberconsommateurs une certaine assurance que la confidentialité de leurs renseignements personnels sera protégée, des organismes non gouvernementaux ont élaboré des programmes volontaires auxquels les organisations qui exploitent des sites Web peuvent participer et assurer ainsi aux utilisateurs que leurs politiques de protection de la vie privée se conforment à certains principes.

Trois des programmes volontaires les plus connus sont TRUSTe, CA WebTrust et BBBOnLine.

1. TRUSTe

Les sites Internet qui se conforment aux principes établis par TRUSTe en matière de protection de la vie privée et acceptent de respecter son processus de surveillance et de règlement des différends avec les consommateurs peuvent en afficher le logo ou le sceau. Les utilisateurs savent aussi que le site Web indiquera quels renseignements personnels sont recueillis, à quoi ils serviront, avec qui ils seront échangés, qui recueille l'information, quelles sont les options de l'utilisateur, quels mécanismes de sécurité sont utilisés pour éviter les abus ou la perte, et de quelle façon les utilisateurs peuvent rectifier l'information pour en contrôler la diffusion(111).

Les entreprises qui participent au programme TRUSTe font l'objet de vérifications périodiques qui permettent d'établir si elles respectent les principes de la protection de la vie privée.

2. CA WebTrust

Le service CA WebTrust est un service mis au point conjointement par l'Institut Canadien des Comptables Agréés et l'American Institute of Certified Public Accountants. Un

(111) TRUSTe, Frequently Asked Questions, http://www.truste.org/webpublishers/pub_faqs.html.

site Web qui satisfait aux principes de WebTrust est autorisé à afficher son sceau et ainsi garantir aux consommateurs qu'il se conforme aux principes et aux critères de WebTrust concernant la transparence des pratiques commerciales, l'intégrité des opérations et la protection de l'information.

Pour conserver sa certification WebTrust, un site doit faire l'objet d'un contrôle au moins tous les trois mois(112).

3. BBBOnLine

Aux États-Unis, le Council of Better Business Bureaus (CBBB) a mis au point, par l'entremise de sa filiale BBBOnLine, un programme d'autoréglementation de la protection de la vie privée sur Internet.

Tout comme TRUSTe et CA WebTrust, le programme BBBOnLine permet aux organisations d'afficher son sceau sur leurs sites Web si elles prouvent qu'elles ont adopté et qu'elles respectent des politiques en matière de protection de la vie privée qui répondent aux exigences du programme.

Les organisations participant au programme doivent s'engager, entre autres(113) :

- à collaborer à l'application des règles de vérification pertinentes;
- à prendre part au programme de règlement des différends en matière de protection de la vie privée de BBBOnLine et à respecter les décisions prises dans ce contexte;
- à informer BBBOnLine de tout changement important de politique ou de pratique en matière de protection de la vie privée;
- à prendre des mesures raisonnables pour s'assurer que personne ne puisse avoir accès sans autorisation à des renseignements concernant une personne identifiée ou identifiable recueillis par Internet;
- à donner aux particuliers l'occasion de se désister ou d'interdire par ailleurs toute utilisation des renseignements personnels qui les concernent et permettent de les identifier à des fins autres que celles auxquelles ces renseignements ont été fournis;

(112) WebTrust, http://www.cica.ca/cica/cicawebsite.nsf/public/SPWT_faqgen.

(113) BBBOnLine, http://www.bbbonline.org/businesses/privacy/eligibility.html.

- à offrir aux particuliers le choix d'accepter ou non la communication de renseignements à des tiers à des fins de prospection commerciale;

- à s'assurer que les renseignements recueillis en ligne sont exacts, complets et opportuns compte tenu des fins auxquelles ils sont destinés et à donner aux particuliers l'accès aux renseignements personnels qui ont été ainsi recueillis à leur sujet et qui permettent de les identifier;

- à se doter d'une politique de protection de la vie privée facile à lire, et à indiquer dans un langage clair et simple :

    1. qui recueille l'information;
    2. le genre de renseignements recueillis concernant des personnes identifiées ou identifiables et l'usage qu'on compte en faire;
    3. les choix offerts aux particuliers concernant l'utilisation de ces renseignements et les personnes à qui ils sont communiqués;
    4. l'engagement de l'organisation concernant la sécurité des données;
    5. la façon de se renseigner au sujet de la politique appliquée au site Web en matière de protection de la vie privée;
    6. le fait que l'organisation participe au programme de protection de la vie privée de BBBOnLine et la façon d'en apprendre plus long au sujet du programme;
    7. toutes filiales, divisions d'exploitation ou gammes de produits connexes qui ne font pas partie du programme de protection de la vie privée;
    8. tout renseignement concernant une personne identifiée ou identifiable recueilli sur le site Web qui est communiqué à des entrepreneurs, des filiales ou d'autres tiers qui ne sont pas visés par une politique commune en matière de protection de la vie privée;
    9. les choix offerts aux utilisateurs concernant les renseignements communiqués à des filiales ou à des tiers qui ne sont pas visés par une politique commune de protection de la vie privée,
    10. les mesures prises par l'organisation pour s'assurer de l'exactitude des renseignements concernant une personne identifiée ou identifiable qui sont conservés d'une façon qui permet d'identifier la personne;
    11. la démarche qu'une personne doit suivre pour avoir accès aux renseignements personnels la concernant et pouvant l'identifier recueillis sur Internet et pour les rectifier;
    12. si d'autres organisations recueillent sur ce site des renseignements permettant d'identifier une personne quand celle-ci réalise sur ce site une opération commerciale avec ces organisations;
    13. les renseignements recueillis qui ne sont pas visés par la politique sur la protection de la vie privée.

Quelque 1 000 sites Internet arborent le sceau d'au moins un de ces services de protection de la vie privée.

4. Online Privacy Alliance

Un autre organisme, Online Privacy Alliance, a été créé aux États-Unis en 1998 pour promouvoir l'autoréglementation de la protection de la vie privée des consommateurs sur Internet. Il compte maintenant environ 90 membres, soit des entreprises et associations transnationales qui s'engagent à appliquer sur Internet des politiques de protection de la vie privée conformes à ses lignes directrices et à prendre part à des processus efficaces d'autoréglementation du respect de la vie privée.

Lorsqu'elle se joint à l'Alliance, une organisation convient que, dans le cadre d'activités en ligne ou de commerce électronique, ses politiques de protection des renseignements concernant une personne identifiée ou identifiable comprendront au moins les éléments suivants :

- *adoption et application d'une politique de protection de la vie privée* : une entreprise qui se livre au commerce électronique doit se donner une politique de protection de la confidentialité de l'information concernant une personne identifiée ou identifiable;

- *avis et communication* : la politique de protection de la vie privée d'une organisation doit être facile à trouver, à lire et à comprendre, et accessible avant la collecte ou la demande de renseignements personnels ou au moment où elle a lieu; elle doit aussi indiquer clairement quelle information est recueillie et à quelles fins, signaler la communication éventuelle de l'information à des tiers, exposer les choix concernant la collecte, l'utilisation et la communication de l'information recueillie, énoncer l'engagement de l'organisation à protéger les données et les mesures prises pour assurer la qualité des données et l'accès aux données, et indiquer clairement quel mécanisme de responsabilisation l'organisation utilise, ainsi que la façon de communiquer avec elle;

- *choix/consentement* : les particuliers doivent avoir la possibilité de décider comment les données recueillies en ligne qui permettent de les identifier peuvent être utilisées à des fins autres que celles de la collecte initiale;

- *sécurité des données* : l'organisation doit assurer la fiabilité de l'information concernant une personne identifiée ou identifiable, la protéger contre la perte et les abus, et en assurer l'intégrité;

- *qualité des données et accès* : les organisations qui créent, maintiennent, utilisent ou diffusent de l'information concernant des personnes identifiées ou identifiables doivent prendre des mesures raisonnables pour s'assurer que les données sont exactes,

complètes et opportunes compte tenu des fins auxquelles elles sont destinées et établir des mécanismes pour corriger les erreurs éventuelles(114).

L'administration américaine attribue aux organismes comme Online Privacy Alliance, TRUSTe, BBBOnLine et CA WebTrust une grande partie des progrès réalisés sur le plan des codes de protection de la vie privée dans le secteur privé aux États-Unis(115).

CONCLUSIONS

Au cours des vingt dernières années, la protection des renseignements personnels a pris une importance considérable dans le domaine de la politique publique. Au départ, la collecte et l'utilisation de ces renseignements soulevait une certaine inquiétude surtout à cause des grandes quantités de données détenues par les administrations publiques. Aussi, plusieurs gouvernements ont-ils décidé d'assujettir la collecte et l'utilisation des renseignements par le secteur public à des lois protégeant la vie privée. Depuis lors, ce sont plutôt la collecte et l'utilisation des renseignements par le secteur privé qui retiennent l'attention. Les entreprises recueillent de grandes quantités de renseignements provenant de plusieurs sources, y compris les achats des consommateurs, les renseignements donnés volontairement par la clientèle et l'usage de logiciels qui permettent de consigner les activités effectuées sur Internet.

Les progrès rapides de la technologie ont accru la capacité des entreprises d'obtenir, d'utiliser et de diffuser des renseignements sur les particuliers par des moyens qui n'existaient même pas il y a quelques années. Ce phénomène suscite chez plusieurs la crainte que des renseignements les concernant ne soient utilisés d'une façon qu'ils ne peuvent prévoir, sans leur consentement ou à leur insu.

Le développement du commerce électronique s'accompagne d'une inquiétude croissante au sujet de la protection des renseignements personnels dans le cadre de transactions sur Internet. Les sondages indiquent d'ailleurs que la protection de la vie privée constitue une préoccupation majeure pour beaucoup de gens, et tant qu'aucune solution satisfaisante ne sera apportée, il est vraisemblable que le commerce électronique ne continuera pas de se développer autant qu'il le pourrait.

---

(114) Online Privacy Alliance, http://www.privacyalliance.org/.

(115) *Towards Digital eQuality* (1999), p. 36.

Toutefois, cette inquiétude n'est que l'un des motifs pour lesquels le secteur privé doit se doter de meilleures mesures de protection des renseignements personnels. La mondialisation des échanges en est un autre. Les entreprises fonctionnent plus que jamais dans un contexte planétaire et celles qui recueillent, conservent, utilisent ou communiquent des renseignements personnels ne peuvent se permettre d'ignorer que la protection de la vie privée est maintenant un élément important du commerce international. La Directive de l'Union européenne sur la protection des données, par exemple, restreint la communication des renseignements personnels entre les États membres et ceux qui n'ont pas adopté de mesures suffisantes pour protéger ces renseignements.

Les entreprises savent que leur compétitivité dépend de leur aptitude à protéger les renseignements personnels : en effet, les pays et les firmes qui auront manifestement pris des mesures dans ce sens jouiront sans doute d'un avantage auprès des consommateurs.

Si l'on admet généralement la nécessité d'adopter des mesures pour protéger les renseignements personnels, notamment dans le cadre de transactions sur Internet, et assurer ainsi l'avenir du commerce électronique, le débat se poursuit entre les tenants d'une réglementation gouvernementale et les défenseurs d'une autoréglementation du secteur privé comme meilleur moyen d'assurer cette protection.

Jusqu'à maintenant, plusieurs solutions ont été adoptées. La directive de l'UE implique l'adoption d'un modèle législatif. En application de cette directive, la *Data Protection Act 1998* du Royaume-Uni établit un régime législatif détaillé pour la protection des renseignements personnels dans le secteur privé. Cette loi prévoit l'adoption de codes par les associations d'entreprises et d'autres organisations, mais non leur reconnaissance sur le plan juridique. Néanmoins, ces codes joueront vraisemblablement un rôle important dans l'interprétation et l'application de cette loi.

Au Canada, une loi fédérale visant à protéger les renseignements personnels dans le secteur privé a été adoptée et doit entrer en vigueur en 2001. Comme la loi britannique, la *Loi sur la protection des renseignements personnels et les documents électroniques* prévoit le recours à des codes dans le secteur privé, sans toutefois leur conférer le moindre statut juridique.

En Australie, la loi envisagée irait un peu plus loin, puisqu'elle donnerait force de loi aux codes autorisés par le commissaire à la protection de la vie privée. Moyennant cette approbation, un code pourra donc remplacer les principes énoncés dans la loi.

Aux États-Unis, le gouvernement a toujours refusé d'assujettir le secteur privé à des mesures législatives, sauf en ce qui concerne la protection de la vie privée des enfants sur

Internet. Très favorable à l'autoréglementation du secteur privé, l'administration américaine encourage ce dernier à élaborer ses propres codes de pratique et de protection de la vie privée. À ce jour, les mesures d'autoréglementation ont fait l'objet de commentaires variés. Une étude révèle que les politiques de plusieurs sites Web ne respectent pas les principes essentiels du traitement équitable de l'information et sont insuffisantes pour assurer une protection réelle. D'autres études font état de résultats plus encourageants. La création de services indépendants de surveillance et de résolution des différends dans le domaine de la vie privée est considérée comme une étape importante pour la mise en place d'initiatives volontaires d'auto-réglementation.

L'approche américaine, favorable à l'autoréglementation, est une cause de friction sur le plan commercial entre les États-Unis et l'Union européenne. D'ailleurs, des négociations en cours cherchent à établir si l'autoréglementation peut répondre à la norme européenne du « niveau de protection adéquat » concernant la communication de renseignements personnels entre les pays appartenant à l'UE et les autres.

Il est trop tôt pour savoir si l'approche réglementaire prévaudra sur l'autoréglementation. Il est très probable qu'on en arrivera à une solution hybride. Même là où des lois existent et où les codes en matière de vie privée n'ont pas de statut juridique, il sera important que les divers secteurs d'activité élaborent des codes qui reflètent les principes de base fixés par les lois et en adaptent l'application à leurs situations particulières. Par contre, là où les codes sont appelés à constituer la base de la protection de la vie privée, il faudra peut-être élaborer des lois qui fixeront des exigences de base — la méthode que semble avoir choisie l'Australie. L'approche américaine, favorable à l'autoréglementation, fonctionnera probablement si la majorité des entreprises qui font des affaires sur Internet adoptent des mesures de protection conformes aux principes des pratiques équitables de traitement de l'information et démontrent, en devenant membres d'associations indépendantes de surveillance et de résolution des différends, qu'elles assurent un niveau de protection suffisant. Si trop peu d'entreprises participent ou si les mesures de protection s'avèrent inadéquates, les États-Unis pourraient devoir changer leur position et envisager de prendre des mesures législatives.