RAPPORT QUINQUENNAL 2011

Technologies et vie privée à l'heure des choix de société

Commission d'accès
à l'information
du Québec

RAPPORT QUINQUENNAL 2011

Technologies et vie privée à l'heure des choix de société

Rapport sur la mise en œuvre de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* et de la *Loi sur la protection des renseignements personnels dans le secteur privé*

Commission d'accès à l'information du Québec

Conception et réalisation : Commission d'accès à l'information du Québec

Dépôt légal – 2011
Bibliothèque nationale du Québec
Bibliothèque nationale du Canada
ISBN : 978-2-550-62430-1 (version imprimée)
ISBN : 978-2-550-62431-8 (version PDF)

CAI

Ce rapport est disponible sur le site Internet de la Commission à l'adresse suivante :
http://www.cai.gouv.qc.ca.

Monsieur Pierre Moreau
Ministre responsable de la Réforme des institutions démocratiques
et de l'Accès à l'information
875, Grande Allée Est
Bureau 3.501
Québec (Québec)
G1R 4Y8

Québec, juin 2011

Monsieur le Ministre,

Conformément aux dispositions de l'article 179 de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (L.R.Q., c. A-2.1) et de l'article 88 de la *Loi sur la protection des renseignements personnels dans le secteur privé* (L.R.Q., c. P-39.1), nous avons le plaisir de vous transmettre le Rapport quinquennal *Technologies et vie privée : à l'heure des choix de société* de la Commission d'accès à l'information du Québec.

Veuillez agréer, Monsieur le Ministre, l'expression de notre sincère considération.

Le président,

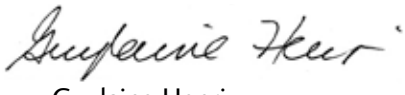
Jean Chartier

Les commissaires,

Teresa Carluccio

Christiane Constant

Hélène Grenier



Guylaine Henri

MOT DU PRÉSIDENT

MOT DU PRÉSIDENT

En 2002, au moment de la publication du dernier rapport quinquennal de la Commission, *Facebook, YouTube, Twitter, Google Street View* et *WikiLeaks* n'existaient pas encore ! Le temps écoulé depuis fait en sorte que notre réflexion sur la législation actuelle doit tenir compte de la réalité d'un espace qui ne cesse de se modifier au gré des technologies de l'information.

Ainsi, plusieurs catégories de renseignements personnels peuvent être diffusées plus rapidement et plus largement que jamais par les individus eux-mêmes dans le cadre de leurs activités. En même temps, tant le secteur public que le secteur privé demeurent avides de telles informations. La puissance du traitement informatique permet de les coupler, les regrouper, les lier entre elles et les stocker de façon illimitée pour générer des analyses de comportement, des fiches de crédit, des habitudes de consommation, des historiques de consultations du Web et ainsi de suite.

C'est pourquoi le présent rapport de la Commission porte une attention particulière à la protection de la vie privée. Il devient de plus en plus pressant, à l'ère numérique, de mettre en place des mesures de protection tenant compte des défis posés par les technologies de l'information sur la vie privée.

Il faut faire face à la réalité puisque les moyens technologiques vont continuer à se développer et à se raffiner. L'information fournie aux utilisateurs en ce qui concerne la divulgation de leurs renseignements personnels et les conséquences qui peuvent en découler doit être simple et transparente.

La Commission est préoccupée par ce qui semble être une certaine insouciance à cet égard. Elle s'inquiète de l'inexistence ou du manque de convivialité des formules d'adhésion ou de consentement à la collecte et à l'utilisation de renseignements personnels proposées ici et là pour accéder à un bien ou à un service. Dans le même ordre d'idées, il y a place à la simplification des politiques de confidentialité affichées par les organismes publics et les entreprises. De plus, si les renseignements devaient être perdus ou piratés, que penser du fait que nos législations actuelles ne prévoient aucune obligation d'en informer les autorités et les personnes concernées ? La protection des renseignements personnels a besoin d'une mise à jour importante à l'ère numérique.

Dans une société où l'information prend de plus en plus d'importance, on constate que les citoyens recherchent désormais une information facilement accessible, selon des besoins qu'ils déterminent eux-mêmes. L'information gouvernementale dont l'État est le dépositaire ne peut échapper à cette évolution. Le droit de savoir, le droit d'être informé, ainsi que la nécessaire transparence des pouvoirs publics sont les fondements préalables à la vie démocratique moderne.

Chacune des recommandations contenues dans ce rapport s'inscrit dans la continuité de l'action de la Commission depuis bientôt 30 ans. Si l'accès à l'information gouvernementale a été le « fer de lance » de l'adoption de la *Loi sur l'accès,* il importe maintenant d'augmenter de façon substantielle la quantité des informations accessibles aux citoyens et de faciliter, dans le respect des droits de chacun, l'accès à cette information.

Aussi, la Commission propose d'adapter le régime d'accès à l'information à la réalité actuelle en ouvrant, sauf exceptions, l'ensemble des données gouvernementales à la consultation et à l'utilisation. Sans pour autant gouverner dans une maison de verre, l'État doit répondre aux préoccupations citoyennes par une transparence accrue et une simplification de l'accès à l'information.

D'autres recommandations contribuent à renforcer le régime d'accès à l'information, notamment celles qui abordent l'assujettissement de certains organismes à la *Loi sur l'accès* et la nécessité pour ceux-ci de respecter les délais prescrits pour justifier un refus d'accès, ce qui serait de nature à faciliter le cheminement du justiciable dans un processus qui doit être simple et rapide pour produire ses effets.

De même, si la protection des renseignements personnels a été la « pierre d'assise » de l'adoption de la *Loi sur la protection dans le secteur privé*, il est essentiel de s'assurer que les recours mis à la disposition des citoyens peuvent être exercés adéquatement et que les entreprises sont représentées par un interlocuteur.

Enfin, l'évolution fulgurante des technologies de l'information préoccupe la Commission et l'amène à interpeller le gouvernement sur les nécessaires moyens dont elle devrait disposer pour remplir adéquatement son mandat de voir à la promotion de la protection des renseignements personnels de nos concitoyens. La constitution de mégabases de données, le vol d'identité, l'utilisation insouciante d'Internet, le profilage des individus, dont les enfants, ne peuvent pas demeurer uniquement les manifestations d'un progrès qui nous dépasse. Il faudra bien un jour ou l'autre s'en préoccuper.

En terminant sur une note plus personnelle, je tiens à souligner que mon arrivée à la présidence de la Commission m'a permis de prendre la mesure de l'engagement indéfectible de mon prédécesseur, Me Jacques Saint-Laurent, qui avait lancé la préparation de ce rapport. Nous nous sommes engagés dans les sillons qu'il avait définis et sa contribution mérite notre reconnaissance.

Depuis ma nomination à la Commission en 2006, j'ai eu l'occasion de tisser des liens privilégiés avec les membres du personnel de l'institution. Au cours des derniers mois, j'ai eu la chance de pouvoir apprécier leur compétence et leur dévouement remarquable. Tous ont su conjuguer leurs efforts et leurs expertises pour produire ce rapport. Au nom de tous mes collègues commissaires, je tiens à les remercier et à leur exprimer ma considération.

JEAN CHARTIER

TABLE DES MATIÈRES

INTRODUCTION

À l'aube du trentième anniversaire de l'adoption de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*[1], il apparaît nécessaire de s'arrêter quelques instants afin de procéder à une rétrospective de l'évolution qui nous a menés au présent *Rapport quinquennal*.

La tâche des vrais démocrates est de voir à ce que le peuple soit de plus en plus au courant, instruit, renseigné sur ses propres intérêts.

(René Lévesque)

Dès 1978, le gouvernement québécois manifeste sa volonté de légiférer en matière d'accès à l'information[2]. En septembre 1980, il met sur pied une *Commission d'étude sur l'accessibilité à l'information gouvernementale et sur la protection des renseignements personnels que le gouvernement détient sur les citoyens* (Commission Paré) qui a pour mandat

> « de définir et recommander au gouvernement les principes, les exemptions et leurs justifications, les modalités d'application et d'administration d'une éventuelle loi d'accessibilité à l'information gouvernementale, y incluant les renseignements personnels que détient le gouvernement sur les citoyens. »[3]

Le Québec s'inscrit alors dans la mouvance d'un bon nombre de pays occidentaux qui cherchent à dynamiser les institutions démocratiques en libéralisant l'accès à l'information gouvernementale.

En mai 1981, la Commission Paré dépose le rapport *Information et liberté*[4]. Fait assez exceptionnel, ce rapport présente une proposition de loi de 163 articles couvrant l'ensemble de ses recommandations afin de s'assurer que son modèle sera bien compris. Cette dernière est retenue par l'Assemblée nationale qui adopte le 22 juin 1982, à l'unanimité, la *Loi sur l'accès*.

Dès lors, les citoyens exerceront un contrôle plus éclairé sur la vie publique, et l'État, une mainmise restreinte et mieux encadrée sur leur vie privée. Cette loi a préséance sur toute loi qui lui est postérieure à moins que celle-ci n'y déroge expressément[5]. Il s'agit là d'un choix éloquent puisque les parlementaires n'hésitent pas à instituer un régime qui les engage pour l'avenir.

Le 16 décembre de la même année, la Commission d'accès à l'information du Québec (Commission) se voit confier le mandat de veiller à l'application de la *Loi sur l'accès*. Le législateur confie à la Commission des fonctions d'adjudication en plus du mandat de surveiller l'application de la *Loi sur l'accès*. Formée à l'époque de trois membres dont un président, la Commission agit comme un tribunal administratif lorsqu'elle révise le refus d'un organisme public d'octroyer à un citoyen l'accès à un document administratif, l'accès à ses renseignements personnels ou de procéder à leur rectification. Elle possède alors un pouvoir décisionnel et non pas un simple pouvoir de recommandation, comme c'est le cas pour nombre d'organismes similaires ailleurs dans le monde. La Commission reçoit aussi le mandat de veiller au respect des obligations imposées aux organismes publics en matière de cueillette, de détention, d'utilisation et de communication de renseignements personnels.

1. L.R.Q., c. A.2-1, ci-après « Loi sur l'accès ».
2. *La politique québécoise de développement culturel*, Québec, Éditeur officiel Québec, 1978.
3. *Décret numéro 2807-80 du 3 septembre 1980 concernant une commission d'étude sur l'accessibilité à l'information gouvernementale et sur les renseignements personnels que le gouvernement détient sur les citoyens.*
4. COMMISSION D'ÉTUDE SUR L'ACCÈS DU CITOYEN À L'INFORMATION GOUVERNEMENTALE ET SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS, *Information et liberté : rapport de la Commission d'étude sur l'accès du citoyen à l'information gouvernementale et sur la protection des renseignements personnels*, Québec, Direction générale des publications gouvernementales, Ministère des communications, 1981.
5. *Loi sur l'accès*, art. 168.

Présidents de la Commission de 1982 à nos jours
M. Jean Chartier
(depuis 2010)
M. Jacques Saint-Laurent
(2004 – 2010)
Mme Diane Boissinot (int)
(2003 – 2004)
Mme Jennifer Stoddart
(2000 – 2003)
M. Paul-André Comeau
(1990 – 2000)
M. Jacques O'Bready
(1988 – 1990)
Mme Thérèse Giroux (int)
(1987 – 1988)
M. Marcel Pépin
(1982 – 1987)

Nous avons laissé, mes collègues et moi, un travail qui peut servir de base à un régime amélioré et plus transparent. Mais qui sera toujours tributaire de la bonne volonté des gouvernements.

(Jean Paré)

Compte tenu de l'importance accordée à la *Loi sur l'accès* dans le corpus législatif québécois, la Commission Paré avait proposé à l'Assemblée nationale une mesure tout à fait nouvelle dans notre droit : l'inclusion dans la loi d'une démarche de réforme continue[6]. Dans le cadre d'une révision quinquennale, la Commission devait faire au gouvernement un rapport sur la mise en œuvre de la loi, sur l'opportunité de la maintenir en vigueur et, le cas échéant, de la modifier[7].

Dans son premier rapport quinquennal[8], la Commission insiste pour qu'on lui accorde expressément un mandat d'information et de promotion auprès des organismes publics et de la population sur les principes qui gouvernent l'accès aux documents publics et la protection des renseignements personnels. Par ailleurs, sans faire de recommandation immédiate, elle souligne l'importance de réfléchir à l'assujettissement du secteur privé à des règles de protection des renseignements personnels.

En 1992, alors que la Commission dépose son deuxième rapport quinquennal[9], toutes les attentions se concentrent sur une priorité législative. L'Assemblée nationale est, en effet, saisie du *Projet de loi nº 68*[10] qui élargit la protection des renseignements personnels au secteur privé.

La Loi sur la protection des renseignements personnels dans le secteur privé[11] entrera en vigueur le 1er janvier 1994, en même temps que le *Code civil du Québec*[12]. Le Québec devient alors le premier gouvernement en Amérique du Nord à assurer la protection des renseignements personnels tant dans le secteur public que dans le secteur privé.

La *Loi sur la protection dans le secteur privé* établit notamment qu'une entreprise doit avoir un intérêt sérieux et légitime pour constituer un dossier sur autrui. Elle doit informer la personne concernée des raisons et des finalités de la collecte et, sauf exceptions, elle ne peut communiquer à un tiers les renseignements personnels contenus dans un dossier à moins que la personne concernée n'y consente.

6. Commission Paré, *préc.*, note 4, p. 11.
7. *Loi sur l'accès*, art. 179, tel que libellé à l'époque.
8. COMMISSION D'ACCÈS À L'INFORMATION DU QUÉBEC, *Une vie privée mieux respectée, un citoyen mieux informé - Rapport sur la mise en œuvre de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, Québec, Commission d'accès à l'information du Québec, 1987.
9. COMMISSION D'ACCÈS À L'INFORMATION DU QUÉBEC, *Un passé éloquent, un avenir à protéger - Rapport sur la mise en œuvre de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, Québec, Commission d'accès à l'information du Québec, 1992.
10. *Loi sur la protection des renseignements personnels dans le secteur privé*, projet de loi n° 68, 2e sess., 34e légis. (Qc).
11. L.R.Q., c. P-39.1, art. 1, ci-après « Loi sur la protection dans le secteur privé ».
12. L.R.Q., c. C-1991, ci-après « C.c.Q. ».

Elle reconnaît aussi au citoyen le droit d'être informé de l'existence d'un dossier le concernant de même que le droit de le consulter et d'en avoir copie. Si des renseignements personnels consignés à son dossier sont inexacts, incomplets ou équivoques, il peut en demander la rectification. Le citoyen dispose également d'un recours à la Commission concernant toute mésentente portant sur l'accès à un renseignement personnel, sa rectification ou encore sur son retrait d'une liste nominative.

Le troisième rapport quinquennal[13] de la Commission inclut des observations sur l'application de la *Loi sur la protection dans le secteur privé*[14]. Si cette loi a soulevé au moment de son adoption nombre d'inquiétudes auprès des entreprises assujetties, la Commission constate que l'intégration de ce nouveau régime s'est déroulée sans trop de bouleversements et de réticences. Au contraire, un certain nombre de grandes entreprises commerciales et financières ont décidé d'étendre l'application des principes de la loi à l'ensemble de leurs clients canadiens.

Le quatrième rapport quinquennal[15] de la Commission marque un tournant. Le droit à l'information est au cœur de ce rapport. Considérant les moyens offerts par les technologies de l'information, la Commission y recommande de mettre en place un nouveau régime d'accès basé sur le principe de la publication automatique de l'information. À un régime où la diffusion des documents doit souvent faire l'objet d'une demande d'accès, la Commission propose de substituer un régime où l'organisme public doit rendre l'information accessible au citoyen, sans que ce dernier n'ait à faire de démarche particulière.

1987 - Premier rapport quinquennal de la Commission : *Une vie privée mieux respectée, un citoyen mieux informé.*

1992 - Deuxième rapport quinquennal de la Commission : Un passé éloquent, *un avenir à protéger.*

1997 - Troisième rapport quinquennal de la Commission : *Vie privée et transparence administrative au tournant du 20e siècle.*

2002 - Quatrième rapport quinquennal de la Commission : *Une réforme de l'accès à l'information : le choix de la transparence.*

Le 14 juin 2006, l'Assemblée nationale, en adoptant le *Projet de loi n°86*[16], donne suite à plusieurs recommandations émises par la Commission en 2002. En outre, elle reporte au 14 juin 2011 l'échéance du cinquième rapport quinquennal de la Commission.

Le changement le plus marquant de cette réforme réside dans l'adoption de mesures de divulgation automatique de l'information gouvernementale. Les organismes visés devront diffuser dans leur site Internet certains documents identifiés par règlement du gouvernement. En d'autres termes, les citoyens auront accès à un grand nombre de documents, plus facilement et plus rapidement, grâce aux possibilités offertes par les technologies de l'information et de la communication.

13. COMMISSION D'ACCÈS À L'INFORMATION DU QUÉBEC, *Vie privée et transparence administrative au tournant du 20e siècle - Rapport sur la mise en œuvre de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels et de la Loi sur la protection des renseignements*, Québec, Commission d'accès à l'information du Québec, 1997.
14. Précité, note 11, art. 88.
15. COMMISSION D'ACCÈS À L'INFORMATION DU QUÉBEC, *Une réforme de l'accès à l'information : le choix de la transparence - Rapport sur la mise en œuvre de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels et de la Loi sur la protection des renseignements*, Québec, Commission d'accès à l'information du Québec, 2002.
16. *Loi modifiant la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels et d'autres dispositions législatives*, projet de loi n°86, (sanctionné – 14 juin 2006), 2e sess., 37e légis. (Qc).

Certaines mesures favorisent une transparence accrue du secteur public en élargissant le champ d'application de la *Loi sur l'accès*. En effet, en donnant suite aux recommandations de la Commission, le législateur étend la notion d'organisme public. Dorénavant, des organismes comme les centres locaux de développement et d'autres liés au monde municipal et scolaire seront assujettis à cette loi. Les ordres professionnels pour leur part seront soumis à un régime hybride : les documents qu'ils détiennent dans le cadre du contrôle de l'exercice de la profession sont soumis à la *Loi sur l'accès* alors que la *Loi sur la protection dans le secteur privé* protégera les renseignements personnels colligés dans le cadre de leur mission associative.

Une autre modification apportée à la *Loi sur l'accès* crée deux sections distinctes au sein de la Commission : une section de surveillance et une section juridictionnelle. Lors de leur nomination par l'Assemblée nationale, les membres de la Commission sont assignés à l'une ou l'autre de ces sections. Cependant, le président, gardien de toute l'organisation, peut assumer des fonctions associées à ces deux sections.

Dans la foulée des recommandations de la Commission visant la divulgation automatique de l'information des organismes publics, le gouvernement a adopté le *Règlement sur la diffusion de l'information et sur la protection des renseignements personnels*[17] en 2008. Les mesures portant sur la diffusion obligatoire et automatique de documents administratifs dans un site Internet sont quant à elles entrées en vigueur en novembre 2009 et établissent la liste des documents devant faire l'objet d'une diffusion. Ce règlement oblige également les organismes publics à prendre des mesures particulières pour la protection des renseignements personnels lors de projets concernant un système d'information ou de prestation électronique de services.

Ce survol des modifications apportées au régime d'accès à l'information et à la protection des renseignements personnels au fil des ans est une prémisse au contenu du présent rapport quinquennal de la Commission. Ce cinquième rapport répond aux exigences de la *Loi sur l'accès*[18] et de la *Loi sur la protection dans le secteur privé*[19], puisqu'il contient des constats relatifs à l'application de ces deux législations et propose des améliorations. Or, la volonté de la Commission est de remplir le mandat qui lui est confié de veiller à l'accès aux documents et à l'information détenue par les organismes publics, tout en assurant, tant dans le secteur public que dans le secteur privé, la protection des renseignements personnels des citoyens québécois.

17. c. A-2.1, r. 0.2, ci-après « Règlement sur la diffusion ».
18. Précité, note 1, art. 179.
19. Précité, note 11, art. 88.

PARTIE 1 :
LA PROTECTION DES RENSEIGNEMENTS PERSONNELS

1.1. LA PROTECTION DES RENSEIGNEMENTS PERSONNELS À L'ÈRE NUMÉRIQUE

L'information préalable à l'expression d'un consentement et le consentement sont deux éléments essentiels en matière de protection des renseignements personnels. Toutefois, il serait naïf de considérer que le fait de cocher une case de type « j'ai lu et j'accepte » ou « j'atteste avoir pris connaissance » signifie que les personnes concernées ont lu et compris les conditions d'utilisation ou la politique de confidentialité associées à un site Web, à un réseau social de type *Facebook*[20] ou *Twitter*[21]. Nombreux sont les utilisateurs qui cochent une telle case sans avoir consulté ces informations, ils ne savent donc pas toujours à quoi ils consentent.

Cette situation s'explique notamment par la longueur et la complexité des documents indiquant les modalités d'utilisation du site ou les engagements relatifs aux renseignements personnels. Elle s'explique aussi par le fait que les internautes doivent cocher une telle case, sans quoi, ils ne peuvent ni commander en ligne, ni s'inscrire à un réseau social, à un programme personnalisé de santé ou encore à certains sites de jeux pour enfants, par exemple.

Dès lors, et sans plus de démonstration, il apparaît nécessaire de simplifier, à l'ère numérique, l'information préalable à l'expression du consentement des personnes concernées et par le fait même l'expression de leur consentement. La Commission considère que des actions doivent être prises afin que les organismes publics et les entreprises adoptent différents mécanismes susceptibles de répondre à ces objectifs.

Les organismes publics et les entreprises qui collectent, communiquent ou utilisent de tels renseignements doivent respecter les principes énoncés dans la *Loi sur l'accès* et dans la *Loi sur la protection dans le secteur privé*. Ces principes s'appliquent quelle que soit la nature du support. Ainsi, un site Web gouvernemental ou commercial ou un réseau social doivent intégrer ces principes dès la conception des processus permettant de recueillir des renseignements personnels et veiller à leur application tout au long du cycle de vie de ceux-ci.

Parmi ces principes, deux retiennent particulièrement l'attention : l'information préalable à l'expression du consentement et le consentement lui-même.

Des renseignements, pour quelle fin ? Les organismes publics et les entreprises ne doivent recueillir que les renseignements personnels nécessaires à l'obtention du bien ou du service offert. Ils doivent indiquer aux personnes concernées les tenants et les aboutissants de la collecte, de la communication ou de l'utilisation de renseignements personnels.

20. http://www.facebook.com (dernière consultation: 06 juin 2011).
21. http://twitter.com (dernière consultation: 06 juin 2011).

Cette obligation d'information préalable à l'expression du consentement s'infère de l'article 65 de la *Loi sur l'accès* en ce qui concerne les organismes publics et de l'article 8 de la *Loi sur la protection dans le secteur privé* pour ce qui est des entreprises. Ces articles se lisent comme suit :

Loi sur l'accès	Loi sur la protection dans le secteur privé
65. *Quiconque, au nom d'un organisme public, recueille verbalement un renseignement personnel auprès de la personne concernée doit se nommer et, lors de la première collecte de renseignements et par la suite sur demande, l'informer :* *1° du nom et de l'adresse de l'organisme public au nom de qui la collecte est faite;* *2° des fins pour lesquelles ce renseignement est recueilli;* *3° des catégories de personnes qui auront accès à ce renseignement;* *4° du caractère obligatoire ou facultatif de la demande;* *5° des conséquences pour la personne concernée ou, selon le cas, pour le tiers, d'un refus de répondre à la demande;* *6° des droits d'accès et de rectification prévus par la loi.* *L'information qui doit être donnée en vertu des paragraphes 1° à 6° du premier alinéa doit être indiquée sur toute communication écrite qui vise à recueillir un renseignement personnel.* *[…]*	**8.** *La personne qui recueille des renseignements personnels auprès de la personne concernée doit, lorsqu'elle constitue un dossier sur cette dernière, l'informer :* *1° de l'objet du dossier;* *2° de l'utilisation qui sera faite des renseignements ainsi que des catégories de personnes qui y auront accès au sein de l'entreprise;* *3° de l'endroit où sera détenu son dossier ainsi que des droits d'accès ou de rectification.*

Un consentement libre et éclairé, jusqu'à quel point ? On retrouve dans la *Loi sur la protection dans le secteur privé* l'idée selon laquelle la personne concernée doit consentir à la collecte, à la communication ou à l'utilisation de ses renseignements personnels. Ce consentement doit être donné par une personne capable d'exprimer sa volonté[22], ou par son représentant. Il doit être libre et éclairé[23]. Ces caractéristiques[24] sont reprises à l'article 14 de la *Loi sur la protection dans le secteur privé* qui se lit comme suit :

> **14.** *Le consentement à la collecte, à la communication ou à l'utilisation d'un renseignement personnel doit être manifeste, libre, éclairé et être donné à des fins spécifiques. Le consentement ne vaut que pour la durée nécessaire à la réalisation des fins pour lesquelles il a été demandé. Un consentement qui n'est pas donné conformément au premier alinéa est sans effet.*

Il est à noter que pareille disposition ne se retrouve pas dans la *Loi sur l'accès*. Toutefois, la Commission applique les critères reconnus dans la *Loi sur la protection dans le secteur privé* au secteur public[25].

À la lumière de ces obligations, il est permis de s'interroger sur la valeur du consentement exprimé en ligne par la personne concernée. Il est tout autant permis de s'interroger sur l'information qu'elle reçoit quant aux conditions d'utilisation et à la politique de confidentialité d'un site Web ou d'un réseau social[26].

Des solutions doivent donc être envisagées concernant les trois problématiques suivantes, à savoir la complexité des politiques de confidentialité, l'absence de repères visuels et les technologies ciblant les individus.

1.1.1. Les politiques de confidentialité simplifiées

La Commission recommande que soit considérée la nécessité de présenter et de communiquer différemment les engagements en matière de protection des renseignements personnels contenus dans des politiques de confidentialité.

Rappelons que l'adoption de ces politiques, notamment par les entreprises en ligne, s'est généralisée au début des années 2000 sous l'impulsion des États-Unis et, plus particulièrement de la *Federal Trade Commission* (FTC). Cet organisme américain indépendant de régulation du commerce a pour mission de protéger les consommateurs en s'assurant que les pratiques déloyales et trompeuses affectant le commerce soient déclarées illégales[27].

La FTC soutient l'effort d'autoréglementation des entreprises en ligne pour informer les personnes concernées de leurs engagements en matière de collecte, de communication ou d'utilisation des renseignements personnels[28]. Néanmoins, elle reconnaît qu'à lui seul cet effort ne parvient pas à garantir pleinement la protection des renseignements personnels. Elle a donc recommandé, en 2000, dans son rapport *Privacy Online: Fair Information Practices in the Electronic Marketplace*[29], une intervention du Congrès américain.

22. C.c.Q., *préc.*, note 12, art. 1385.
23. *Id.*, art. 1399.
24. COMMISSION D'ACCÈS À L'INFORMATION DU QUÉBEC, « Foire aux questions – Entreprises – Que veut-on dire par le terme « consentement » ? ».
25. Voir notamment : ASSOCIATION SUR L'ACCÈS ET LA PROTECTION DE L'INFORMATION, *Guide pratique sur l'accès et la protection de l'information*, vol. 1, Cowansville, Les Éditions Yvon Blais, 2010, p. 3-70; Raymond DORAY et François CHARETTE, *Accès à l'information*, vol. 1, Cowansville, Les Éditions Yvon Blais, 2010, p. 53-5.
26. Voir notamment : Vincent GAUTRAIS et Pierre TRUDEL, *Circulation des renseignements personnels et Web 2.0*, Montréal, Éditions Thémis, 2010, p. 163; Vincent GAUTRAIS, « Les contrats de cyberconsommation sont presque tous illégaux! », (2005) *Revue du Notariat 617.*
27. 15 U. S. C. Sec. 45 (a) (1). (notre traduction)
28. Voir notamment : FEDERAL TRADE COMMISSION, *Privacy Online : A Report to Congress*, June 1998 (ci-après « FTC 1998 »); FEDERAL TRADE COMMISSION, *Self-Regulation and Privacy Online : A Report to Congress*, July 1999.
29. « The Commission believes that industry's limited success in implementing fair information practices online, as well as ongoing consumer concerns about Internet privacy, make this the appropriate time for legislative action. […] Such legislation, in conjunction with self-regulation, would ensure important protections for consumer privacy at a critical time in the development of the online marketplace. », FEDERAL TRADE COMMISSION, Privacy Online : *Fair Information Practices in the Electronic Marketplace – A Report to Congress*, May 2000, p. 38.

Dix ans plus tard, même si elles sont souvent décriées en ce qui concerne leur accessibilité, leur clarté et leur compréhension, les politiques de confidentialité demeurent néanmoins un outil informationnel à considérer puisqu'elles répondent généralement à l'obligation d'information préalable à l'expression du consentement[30]. La Commission encourage ces entités à continuer sur ce chemin tout en recommandant que celui-ci soit simplifié pour favoriser un consentement éclairé.

Ces politiques constituent, en effet, l'outil par lequel les organismes publics et les entreprises informent les personnes concernées de leurs engagements quant à la collecte, à la communication et à l'utilisation de renseignements personnels. Il y est généralement indiqué quels sont les renseignements personnels qui sont collectés, quelles sont les raisons de la collecte, qui aura accès aux renseignements, quelles sont les mesures de sécurité prises pour en assurer la confidentialité ou encore comment les personnes concernées peuvent exercer leur droit d'accès.

« Les recherches indiquent que les jeunes (de même que de nombreux adultes) lisent rarement les politiques de confidentialité des sites Web qu'ils visitent, ce qui n'est pas surprenant puisque les politiques de nombreux sites sont rédigées dans une langue spécialisée, technique ou juridique difficile à comprendre pour la majorité des lecteurs. »

Source : *Résolution sur la vie privée des enfants en ligne*, Résolution adoptée lors de la 30e Conférence internationale des commissaires à la protection des données et de la vie privée, Strasbourg (France), 17 octobre 2008. (nos soulignements)

Toutefois, pour faire en sorte que les politiques de confidentialité répondent mieux à leur rôle informationnel, des discussions ont lieu, ici et ailleurs, quant au moyen de présenter et de communiquer autrement l'information relative au traitement des renseignements personnels à l'ère numérique.

Par exemple, récemment la FTC invitait toute personne à lui présenter des commentaires concernant le fait que « les politiques de confidentialité doivent être claires, courtes et plus standardisées, pour permettre une meilleure compréhension et comparaison des pratiques en matière de vie privée »[31].

La Commissaire à l'information et à la protection de la vie privée de l'Ontario a répondu à cette invitation en indiquant qu'elle est favorable au développement d'applications adaptées aux différents supports afin de protéger les personnes concernées. Elle a reconnu l'importance d'adopter des politiques de confidentialité simplifiées. Elle a également insisté sur la nécessité de mettre en place des pictogrammes informant les individus qu'une entreprise recourt, entre autres, à la géolocalisation ou encore à la technologie sans fil[32].

30. Voir notamment : FEDERAL TRADE COMMISSION, *Protecting Consumer Privacy in an Era of Rapid Change – A Proposed Framework for Businesses and Policymakers*, December 2010, p. 69 et suiv. (ci-après « FTC 2010 »). Il est également à préciser qu'en Australie la *Privacy Act of 1988* encourage le secteur privé à développer des *Privacy Code* (art. 18BA et suiv.). Ces codes doivent être approuvés par l'Office of the Australian Information Commissioner. Après approbation ce code « replace the National Privacy Principles under the [Privacy Act of 1988] for those organisations bound by the code », OFFICE OF THE AUSTRALIAN INFORMATION COMMISSIONER, « Business – Privacy Codes ».
31. FTC 2010, *Id.*, p. 70. (notre traduction)
32. INFORMATION AND PRIVACY COMMISSIONER OF ONTARIO, *Response to the FTC Framework for Protection Consumer Privacy in an Era of Rapid Change*, January 2011, p. 8. (notre traduction)

La Commission considère qu'au lieu de publier une politique sous forme linéaire, les organismes publics et les entreprises doivent proposer une politique condensée et une détaillée.

La politique condensée présente, en quelques paragraphes, les principaux éléments des engagements des organismes publics et des entreprises en matière de protection des renseignements personnels. Cette politique qui s'apparente à un résumé ou une vue d'ensemble doit s'afficher lorsque les internautes cliquent sur le lien « politique de confidentialité » ou « vie privée » d'un site Web ou d'un réseau social. À partir de là, ils doivent pouvoir consulter la politique détaillée du site s'ils désirent avoir plus d'informations sur ces engagements. Par ailleurs, la Commission est d'avis que pareille attitude doit prévaloir quel que soit le support utilisé pour collecter des renseignements personnels. Cette simplification doit s'appliquer aussi bien au papier qu'au numérique.

Cette façon de présenter et de communiquer l'information aux individus est déjà utilisée par certaines entreprises. Elle trouve également application auprès de certains gouvernements. Par exemple, le gouvernement australien propose sur son site Web une politique de confidentialité condensée. À partir de cette politique, il est possible d'accéder pour plus d'informations à une politique détaillée. L'Australie donne ainsi suite à une résolution adoptée, en 2003, lors de la conférence internationale des commissaires à la protection des données et de la vie privée mettant de l'avant l'importance de recourir à plusieurs niveaux de détails pour présenter les politiques de confidentialité dans les secteurs public et privé[33].

Cette approche[34] permet de communiquer les engagements en matière de renseignements personnels dans un format adapté au support. En effet, la lecture d'un document ne s'appréhende pas de la même manière selon qu'il est sur support papier ou informatique. Par conséquent, « des avis très succincts [peuvent] être conçus pour l'affichage des téléphones mobiles et autres appareils de taille réduite »[35].

Par ailleurs, l'attention du lecteur n'étant pas la même face à un support électronique, il est important de présenter des textes ne nécessitant pas ou peu de défilement d'écran. Ainsi, « lorsque l'espace / le temps de communication est limité, les formats multistrates peuvent améliorer la lisibilité des avis »[36].

Partant, le recours à des politiques de confidentialité simplifiées présente plusieurs avantages pour les acteurs suivants :

- **les personnes concernées :** une telle politique permet aux personnes concernées de prendre rapidement connaissance des informations essentielles en matière de protection des renseignements personnels. Les engagements sont résumés et présentés dans un langage et dans une forme accessibles, ils ne sont pas « noyés » dans un texte long et incompréhensible;
- **les organismes publics et les entreprises :** ce format oblige les organismes publics et les entreprises à reconsidérer la présentation de leurs politiques de confidentialité. Il les conduit à décrire dans un langage clair et compréhensible les éléments essentiels à l'expression d'un consentement éclairé. Ce format leur permet donc d'améliorer la compréhension des informations relatives au traitement des renseignements personnels, ce qui peut avoir une incidence sur le consentement des personnes concernées.

33. *Résolution visant l'amélioration des pratiques d'information en matière de protection des données et de la vie privée*, Résolution adoptée lors de la 25e Conférence internationale des commissaires à la protection des données et de la vie privée, Sydney (Australie), 12 septembre 2003. *Infra*, Annexe 2 – Résolutions adoptées par les commissaires à la protection des données et de la vie privée et de l'accès à l'information.
34. Voir notamment : *Berlin Privacy Notices Memorandum*, April 2004; GROUPE DE TRAVAIL « ARTICLE 29 » SUR LA PROTECTION DES DONNÉES, *Avis 10/2004 sur « Dispositions davantage harmonisées en matière d'informations*, WP100, 25 novembre 2004 (ci-après « GROUPE DE TRAVAIL « ARTICLE 29 » - WP 100 »); ORGANISATION DE COOPÉRATION ET DE DÉVELOPPEMENT ÉCONOMIQUES, *Simplifier les notices d'information sur la protection de la vie privée : rapport et recommandations de l'OCDE*, DSTI/ICCP/REG(2006)5/FINAL, 24 juillet 2006; Cynthia CHASSIGNEUX, *Guide pour l'élaboration d'une politique de confidentialité*, Montréal, Chaire L.R Wilson sur le droit des technologies de l'information et du commerce électronique, 2008, p. 3 et suiv.
35. GROUPE DE TRAVAIL « ARTICLE 29 » - WP100, *Id.*, p. 9.
36. *Id.*, p. 8.

1.1.2. Les pictogrammes de protection

La Commission recommande que soit envisagée la possibilité de recourir à des pictogrammes de protection.

Face aux multiples supports (ordinateur, tablette électronique, téléphone intelligent, etc.) sur lesquels une personne peut consulter un site Web, il convient de développer des solutions qui permettent aux internautes de connaître en un « clin d'œil » les engagements des organismes publics et des entreprises en matière de protection des renseignements personnels. Les politiques de confidentialité simplifiées sont un exemple, les pictogrammes de protection en sont un autre.

En effet, on dit souvent qu'une image vaut mille mots. Cela s'illustre notamment en matière de droit d'auteur, plus particulièrement d'œuvres en usage partagé (*creative commons*), où les symboles suivants ont été développés pour informer les utilisateurs des droits accordés par l'auteur sur son œuvre :

	L'œuvre peut être utilisée librement à la condition d'indiquer le nom de son auteur.
	L'œuvre ne peut pas être utilisée pour des fins commerciales sans l'autorisation de son auteur.
	L'œuvre ne peut pas faire l'objet de modification, elle doit être utilisée intégralement.
	L'œuvre peut être modifiée, mais l'œuvre qui en est issue doit mentionner les conditions initialement autorisées par l'auteur.

Source (inspiré de): creativecommons.org (dernière consultation: 06 juin 2011).

À l'instar des panneaux de signalisation routière ou encore des tableaux de valeur nutritive des aliments, ces symboles ont été standardisés afin d'avoir partout la même signification.

En ce qui a trait à la protection des renseignements personnels, les pictogrammes de protection devraient apparaître sur la page d'accueil d'un site Web ou d'un réseau social. Ils devraient également être visibles sur les pages qui conduisent à la collecte de renseignements personnels ou sur un formulaire de consentement. Il est donc important de veiller à ce que ces pictogrammes soient compris de tout le monde, c'est-à-dire aussi bien par les adultes que par les jeunes.

Cependant, si ces pictogrammes facilitent la compréhension des personnes concernées et par conséquent leur permettent d'exprimer un consentement éclairé, ceux-ci ne doivent pas pour autant se substituer aux politiques de confidentialité. Ils doivent les compléter. En effet, les internautes doivent pouvoir cliquer sur le pictogramme pour apprendre davantage sur le partage des renseignements, sur la sécurité, par exemple.

Pareil mécanisme est notamment proposé par TRUSTe, une société américaine sans but lucratif[37] qui, depuis la fin des années 1990, propose différents programmes destinés aux entreprises afin qu'elles se conforment aux principes fondamentaux de protection des renseignements personnels. Sont ainsi offerts des programmes certifiant l'adéquation des politiques de confidentialité à ces principes, à l'accord intervenu entre l'Europe et les États-Unis quant aux transferts de renseignements personnels ou encore à la législation américaine protégeant la vie privée des enfants sur Internet.

Par exemple, avec le programme *Mobile Privacy*[38], la personne concernée consulte une politique de confidentialité sur son téléphone intelligent, des pictogrammes apparaissent à côté de « Collection et Utilisation » ou encore « Profilage et Publicité ». En cliquant sur l'un de ces pictogrammes, elle accède à une politique condensée lisible en un écran. Cette politique indique, par exemple, quels sont les renseignements personnels qui sont collectés et comment ils sont utilisés. Par le biais de cette page, elle peut alors cliquer sur un lien qui la conduit à la politique complète du site en matière de protection des renseignements personnels.

37. http://www.truste.com (dernière consultation: 06 juin 2011).
38. http://www.truste.com/privacy_seals_and_services/enterprise_privacy/mobile_certification.html (dernière consultation: 06 juin 2011).

Source :TRUSTe

Lien vers la politique complète du site

Partant, le recours aux pictogrammes de protection présente plusieurs avantages pour les acteurs suivants :

- **les personnes concernées :** les pictogrammes de protection permettent aux personnes concernées de comprendre plus rapidement les composantes d'une politique de confidentialité et donc d'exprimer un consentement éclairé. Ils leur permettent de garder un contrôle sur le traitement de leurs renseignements personnels par les organismes publics et par les entreprises. Toutefois, ces pictogrammes ne sont qu'un raccourci et ne doivent pas empêcher les personnes concernées de vérifier la politique de confidentialité d'un organisme public ou d'une entreprise;
- **les organismes publics et les entreprises :** les pictogrammes de protection permettent aux organismes publics et aux entreprises de présenter leurs engagements en matière de protection des renseignements personnels d'une façon « ludique », accessible quel que soit le support et compréhensible par tous. Toutefois, l'insertion de ces pictogrammes dans leur plan de communication ne doit pas se substituer à l'adoption d'une politique de confidentialité répondant aux principes de protection des renseignements personnels.

1.1.3. Les technologies ciblant les individus

La Commission recommande de renforcer l'application des principes de protection des renseignements personnels auprès des organismes publics et des entreprises ayant recours à des technologies permettant de surveiller les individus, de localiser ou d'identifier une personne en possession de certains outils technologiques. Il en va ainsi, par exemple, de la vidéosurveillance, de la biométrie, de la géolocalisation ou de l'identification par radiofréquence (puces RFID).

Ces technologies sont présentes, entre autres, dans certains passeports et permis de conduire, dans les cartes d'accès des employés, dans les cartes de plusieurs sociétés de transports au Québec, dans la téléphonie cellulaire ou encore dans certains véhicules professionnels.

Concernant la biométrie, il convient de rappeler que « la création d'une banque de caractéristiques ou de mesures biométriques doit être préalablement divulguée à la Commission d'accès à l'information ».

Source : *Loi concernant le cadre juridique des technologies de l'information*, L.R.Q., c. C-1.1, art. 45.

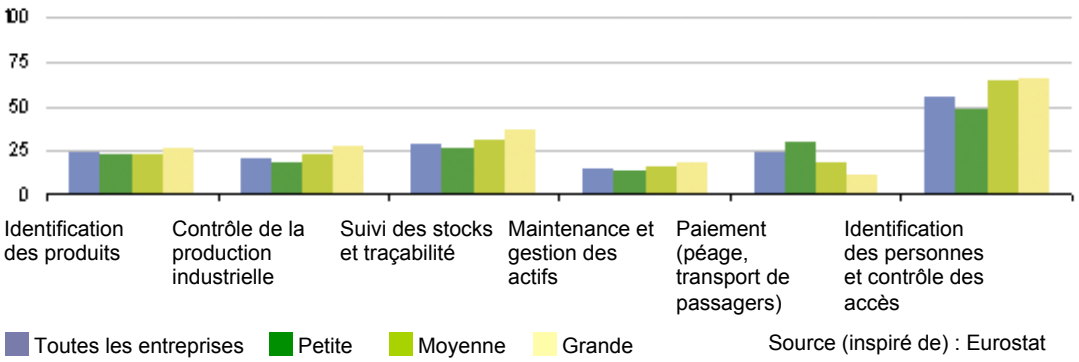
Ces technologies présentent des avantages, notamment en termes de gestion des stocks, de traçabilité d'un bien, de suivi des personnes en perte d'autonomie, de lutte contre la falsification de documents, de prévention des crimes et délits, de commodité pour franchir un poste de contrôle au travail ou frontalier. Elles suscitent néanmoins des risques d'atteinte à la vie privée, notamment lorsqu'elles sont utilisées pour filmer les individus à leur insu, pour suivre leurs déplacements ou encore lorsqu'elles sont associées à des renseignements personnels qui peuvent être lus à distance.

Partant, la Commission s'interroge, entre autres, sur l'information transmise aux personnes utilisant des objets susceptibles de les localiser et de les identifier et par le fait même sur leur consentement à ce qu'un organisme public ou une entreprise collecte et utilise leurs renseignements personnels par le biais de ces technologies.

Cette situation est d'autant plus préoccupante au regard de statistiques publiées par l'office de la statistique de l'Union européenne (Eurostat), démontrant qu'en 2009, les entreprises recourent aux puces RFID majoritairement pour l'identification des personnes ou le contrôle des accès[39].

Dans un document d'analyse intitulé *La technologie d'identification par radiofréquence (RFID) doit-on s'en méfier ?* la Commission affirmait en 2006 :

> « les citoyens ont le droit de connaître les produits identifiés avec la technologie RFID et les spécifications techniques utilisées. Il y aurait lieu de fournir une indication claire, précise et facile à comprendre des produits identifiés avec la technologie RFID, et ce, dans un langage non technique et vulgarisé. »[40]



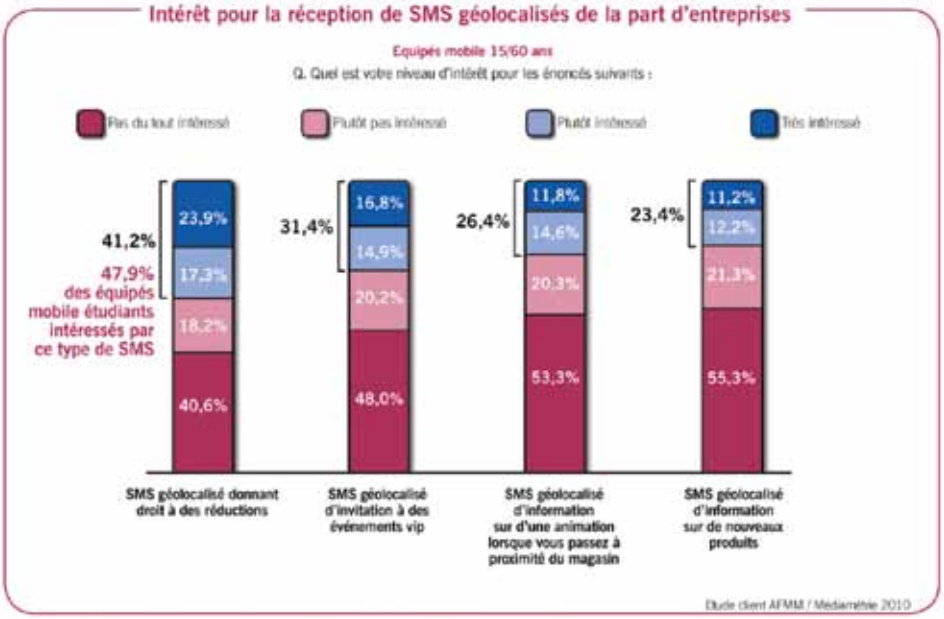
39. EUROSTAT, « Information society statistics », September 2010, http://epp.eurostat.ec.europa.eu/statistics_explained/index.php/Information_society_statistics (dernière consultation: 06 juin 2011).
40. COMMISSION D'ACCÈS À L'INFORMATION DU QUÉBEC, *La technologie d'identification par radiofréquence (RFID) doit-on s'en méfier ?*, Mai 2006, p. 6.

Les organismes publics et les entreprises devraient ainsi s'assurer au moment de délivrer une carte d'accès ou un téléphone intelligent que les utilisateurs ont compris et consentent à ce que de telles technologies puissent les localiser et les identifier en tout temps.

Le recours aux puces RFID, mais aussi aux autres technologies ciblant les individus, devrait donc entraîner une obligation de dénoncer clairement quels sont les renseignements qui seront collectés, à quelle fin ou encore quels sont les moyens offerts aux personnes concernées pour désactiver les fonctions permettant de les localiser ou de les identifier. En effet, ce ne sont pas tous les individus qui sont intéressés à recevoir des messages publicitaires ou des bons de réduction lorsqu'ils passent à proximité d'un commerce, comme l'illustre une étude menée par l'Association Française du Multimédia Mobile et Médiamétrie, une société indépendante de mesure d'audience.

« Le développement rapide de réseaux sociaux par géolocalisation tels que Foursquare ou Gowalla et l'ajout de fonctionnalités similaires dans des réseaux sociaux existants comme Facebook Places ont déjà soulevé de nouveaux problèmes en matière de vie privée. Certains s'inquiètent de l'utilisation et de la transmission des données de géolocalisation dont disposent ces nouveaux modèles d'affaires. Ce débat devrait se poursuivre en 2011 en raison de la progression certaine de ces nouveaux outils. »

Source : CEFRIO, « Un fort potentiel pour l'Internet mobile au Québec », (2010) vol. 1 n° 3 *NeTendances* 14.



Source : ASSOCIATION FRANÇAISE DU MULTIMÉDIA MOBILE, « Indicateurs clés du multimédia mobile et marketing par SMS », Communiqué de presse, 21 juin 2010, p. 5.

Le fait pour les organismes publics et les entreprises de s'assurer que les utilisateurs ont compris le fonctionnement de ces technologies est un aspect qui doit revêtir la même importance que celui d'intégrer les principes de protection des renseignements personnels « dans la conception, le fonctionnement et la gestion des TIC et des systèmes connexes pendant toute la période de conservation des renseignements afin de protéger pleinement la vie privée »[41].

La Commission invite les organismes publics et les entreprises à prendre en considération ces principes en amont et non en aval de leur projet, ce qui est susceptible de réduire leurs coûts de production.

La Commission entend rappeler aux organismes publics et aux entreprises que les principes contenus dans la *Loi sur l'accès* et dans la *Loi sur la protection dans le secteur privé* s'appliquent quelle que soit la technologie permettant de collecter, de communiquer et d'utiliser des renseignements personnels et que ceux-ci doivent être mis en œuvre tout au long du cycle de vie de ces renseignements.

En raison des multiples enjeux découlant de la protection des renseignements personnels à l'ère numérique, la Commission recommande de mieux encadrer l'information transmise aux personnes concernées tout en s'assurant qu'elles expriment un consentement libre et éclairé. Ces obligations doivent profiter à tous, adultes et jeunes. La Commission verra ainsi renforcer son rôle de surveillance et de prévention à l'égard de la protection des renseignements personnels tant dans le secteur public que privé.

Recommandation 1 : La Commission recommande au législateur d'obliger les organismes publics et les entreprises à adopter des politiques de confidentialité simplifiées présentant, en termes clairs et compréhensibles, une vue d'ensemble de leurs engagements en matière de protection des renseignements personnels.

Recommandation 2 : La Commission recommande au législateur d'imposer aux organismes publics et aux entreprises l'utilisation de pictogrammes de protection informant les citoyens de leurs engagements en matière de protection des renseignements personnels.

Recommandation 3 : La Commission recommande au législateur d'obliger les organismes publics et les entreprises à signaler la présence de mécanismes susceptibles d'identifier ou de localiser une personne physique lors de l'utilisation de leurs produits.

Recommandation 4 : La Commission rappelle aux organismes publics et aux entreprises d'intégrer les principes de protection de renseignements personnels dès la conception de leurs biens et services et de les appliquer tout au long du cycle de vie de ces renseignements.

Principes relatifs à la « protection intégrée de la vie privée » (*Privacy by Design*) développés par la Commissaire à l'information et à la protection de la vie privée de l'Ontario :

1. Prendre des mesures proactives et non réactives; des mesures préventives et non correctives.
2. Assurer la protection implicite de la vie privée.
3. Intégrer la protection de la vie privée dans la conception.
4. Assurer une fonctionnalité intégrale selon le paradigme à somme positive [axé sur l'ensemble des fonctionnalités] et non à somme nulle.
5. Assurer la sécurité de bout en bout, pendant toute la période de conservation des renseignements.
6. Assurer la visibilité et la transparence.
7. Respecter la vie privée des utilisateurs.

Source : Ann CAVOUKIAN, « La protection intégrée de la vie privée – Les sept principes fondamentaux », août 2009 (modifié en janvier 2011).

41. *Résolution sur la protection intégrée de la vie privée*, Résolution adoptée lors de la 32e Conférence internationale des commissaires à la protection des données et de la vie privée, Jérusalem (Israël), octobre 2010. *Infra*, Annexe 2 – Résolutions adoptées par les commissaires à la protection des données et de la vie privée et de l'accès à l'information.

1.2. LES NATIFS DU NUMÉRIQUE

La protection des renseignements personnels s'impose à tout âge. Les principes qui la gouvernent s'appliquent que l'on soit d'une génération pour qui l'accès en tout temps et en tous lieux à ses courriels ou encore aux profils de ses amis est essentiel ou d'une génération précédente. Et si la frontière entre la vie publique et la vie privée apparaissait plus prononcée il y a quelques années, force est de constater qu'aujourd'hui les natifs du numérique semblent faire preuve d'une plus grande transparence quant à leurs activités, leurs émotions, leur vie.

Une enquête menée auprès de 25 000 jeunes européens de 9 à 16 ans démontre que 56 % des 11-12 ans, 71 % des 13-14 ans et 78 % des 15-16 ans savent changer les paramètres de confidentialité de leur profil.

Source : Sonia LIVINGSTONE, Kjartan OLAFSSON and Elisabeth STAKSRUD, *Social Networking, Age and Privacy*, April 2011, p. 7. (Enquête réalisée pour le compte d'EUKidsOnline)

Illustration de ce que font les jeunes sur Internet

Activités en ligne	Garçons	Filles
Écrire dans un wiki	7 %	3 %
Faire connaître son opinion sur un produit	11 %	5 %
Transférer des photos vers un site prévu à cette fin	12 %	15 %
Écrire dans son blogue personnel	13 %	25 %
Transférer une vidéo vers un site prévu à cette fin	14 %	9 %
Créer et afficher des contenus vidéo ou musicaux	15 %	9 %
Commenter le blogue d'un autre	22 %	29 %
Regarder des photos sur un site réservé à cette fin	28 %	35 %
Faire des achats en ligne	28 %	18 %
Afficher ou consulter des petites annonces	32 %	26 %
Écouter ou télécharger des films en ligne	38 %	26 %
Échanger des notes de cours	40 %	48 %
Consulter un blogue	41 %	42 %
Effectuer des transactions bancaires	42 %	44 %
Trouver de l'information en ligne avant d'acheter en magasin	44 %	37 %
Participer à un concours	45 %	54 %
Visiter un site de réseautage	57 %	67 %
Participer à des jeux, seuls ou en réseau	58 %	33 %
Écouter ou télécharger de la musique	70 %	71 %
Clavarder	72 %	77 %
Communiquer par courrier électronique	80 %	89 %
Rechercher de l'information	85 %	86 %

Source : Réjean ROY, « Les 12-24 ans : utilisateurs extrêmes d'Internet et des TI », (2009) vol. 7, n° 1 *Réseau CÉFRIO* 3, 5.

Ces natifs sont, en effet, des « utilisateurs extrêmes d'Internet et des TI »[42]. Ils recourent aux blogues, à *Twitter*[43], à *MySpace*[44] ou encore à *Facebook*[45] pour communiquer avec leurs amis d'ici ou d'ailleurs, pour publier des photos et des vidéos, pour savoir où sont leurs amis. Ils naviguent sur Internet pour leurs devoirs, pour se divertir en jouant en ligne, pour télécharger de la musique ou pour se procurer des biens et des services.

Cette transparence peut sembler anodine jusqu'au moment où un utilisateur est victime de vol d'identité[46] ou de cyberintimidation[47]. Ou jusqu'à ce qu'un employeur refuse de retenir la candidature d'une personne en tenant compte de ses faits et gestes de jeunesse. Ou jusqu'à ce que la police soit obligée d'intervenir pour mettre fin à une fête car l'invitation postée sur un réseau social n'a pas été restreinte aux seuls amis de l'organisateur. En effet, plusieurs personnes naviguent en plein paradoxe, estimant que leur page est du domaine privé même si le média est public. Par ailleurs, plusieurs jeunes ne modifient pas, ou ne savent pas comment changer les paramètres de confidentialité établis par les responsables des sites Web et de réseaux sociaux. Leurs profils sont ainsi accessibles à tous et non à leurs seuls amis.

Résultat de cette transparence, les natifs du numérique divulguent un certain nombre de renseignements permettant de les identifier et de les suivre à la trace. Certes ils les communiquent volontairement. Mais connaissent-ils l'usage que font de leurs renseignements personnels les responsables des sites Web commerciaux ou des réseaux sociaux ? Ont-ils consenti à ce que ceux-ci se servent de leurs données à des fins de vente

42. Réjean ROY, « Les 12-24 ans : utilisateurs extrêmes d'Internet et des TI », (2009) vol. 7, n° 1 *Réseau CÉFRIO 3*. Cet article s'inscrit dans le cadre d'une enquête sur la génération C, soit les jeunes nés entre 1984 et 1996, disponible sur le site du Centre francophone d'informatisation des organisations (CÉFRIO).
43. Précité, note 21.
44. http://www.myspace.com (dernière consultation: 06 juin 2011).
45. Précité, note 20.
46. Louis P. ROBERTSON, « La fraude d'identité : connaissez-vous ? », dans *Congrès annuel du Barreau du Québec 2009*, Service de la formation continue du Barreau du Québec, 2009. Selon l'auteur, « les jeunes sont considérés comme un groupe émergent qui deviendra de plus en plus la cible de fraudes d'identité », p. 17 (pdf).
47. Des sites tels que *WebAverti* (http://www.webaverti.ca), *Réseau Éducation-Médias* (http://www.education-medias.ca), *Jeunesse J'écoute* (http://jeunessejecoute.ca), par exemple, proposent des sections consacrées à cette problématique (dernière consultation : 06 juin 2011).

ou de profilage ? Savent-ils dans quel pays leurs informations sont conservées et qui y aura accès ? En un mot, sont-ils conscients des possibles incidents et préjudices engendrés par le dévoilement de leurs renseignements personnels, pour aujourd'hui mais aussi pour demain ? En effet, dès l'instant où elle est publiée en ligne, une information devient permanente.

Ce constat ne vise pas uniquement les natifs du numérique. Toutefois, leur présence de plus en plus nombreuse et leur comportement face aux enjeux des technologies de l'information (TI) et du Web 2.0 quant à leurs renseignements personnels inquiètent un certain nombre d'acteurs concernés, dont la Commission.

Ainsi, selon une recherche menée pour le compte du *Pew Internet & American Life Project*[48], un centre de recherche américain indépendant qui analyse l'impact social d'Internet, en 2010, 95 % des jeunes de 14-17 ans étaient des utilisateurs d'environnements électroniques contre 88 % pour les 12-13 ans[49]. Et si 82 % des 14-17 ans ont un profil en ligne, un peu plus de la moitié des 12-13 ans disent aussi avoir un tel profil[50].

Concernant ces derniers, les résultats s'expliquent notamment par le fait que la plupart des médias sociaux restreignent l'accès aux jeunes de 13 ans et plus. *Facebook* recommande alors

> « vivement aux mineurs de 13 ans et plus de demander l'autorisation à leurs parents avant d'envoyer à quiconque des informations les concernant via internet et [encourage] les parents à sensibiliser leurs enfants aux pratiques d'utilisation d'internet en toute sécurité. »[51]

Néanmoins, comme le révèle cette recherche américaine, il serait naïf de croire que les jeunes de moins de 13 ans ne sont pas présents sur ce réseau, et ce, même si la politique de confidentialité du site indique que « les enfants de moins de 13 ans ne doivent pas s'inscrire sur *Facebook* ni […] fournir d'informations personnelles les concernant »[52].

D'ailleurs, *Facebook* a laissé savoir que 20 000 profils étaient supprimés par jour, ce qui inclut ceux de jeunes de moins de 13 ans[53].

Facebook n'est pas le seul réseau à attirer les jeunes de moins de 13 ans. Des communautés virtuelles destinées principalement à cette clientèle sont présentes sur Internet. Il en va ainsi de *Togetherville.com*[54] dont l'inscription se fait à partir du profil *Facebook* des parents. Tel est aussi le cas du *Club Penguin*[55] dont l'abonnement doit être activé par un adulte. Pour ce faire, un jeune doit d'abord accepter les conditions d'utilisation et la politique de confidentialité du club, se créer un avatar sous la forme d'un pingouin et saisir l'adresse courriel d'un adulte. Par la suite, l'adulte reçoit un message du club l'invitant à finaliser le processus d'abonnement du jeune.

48. http://www.pewinternet.org (dernière consultation: 06 juin 2011).
49. Amanda LENHART, Kristen PURCELL, Aaron SMITH and Kathryn ZICKUHR, *Social Media & Mobile Internet Use Among Teens and Young Adults*, February 2010, p. 5.
50. *Id.*, p. 17.
51. FACEBOOK, *Politique de confidentialité*, dernière mise à jour 22 décembre 2010, http://www.facebook.com/policy.php (dernière consultation: 06 juin 2011).
52. *Id.*
53. COMMITTEE ON CYBER-SAFETY, *Cybersafety issues affecting children and young people*, Canberra (Australia), 21 March 2011, p. 1 et suiv. (Hearing of M. Thompson, Advisory Board and Policy Adviser, Facebook Inc).
54. http://togetherville.com (dernière consultation: 06 juin 2011).
55. http://www.clubpenguin.com (dernière consultation: 06 juin 2011).

Illustration de la page visant à dénoncer l'utilisation par un jeune de moins de 13 ans du site Facebook

Signaler un enfant mineur

Nous avons étudié le compte signalé et avons pris les mesures nécessaires selon nos règlements. Vous ne recevrez de confirmation que lorsque nous aurons pris des mesures, mais nous étudions tous les signalements. Si vous avez signalé le compte d'un enfant dont la date de naissance est fausse et que l'âge de cet enfant peut être facilement confirmé comme en-dessous de 13 ans, nous supprimerons immédiatement le compte. Vous ne recevrez aucune confirmation de cette décision, mais vous ne serez plus à même de voir le profil de l'enfant sur le site. Si l'âge de l'enfant signalé n'est pas facilement vérifiable comme en-dessous de 13 ans, alors, nous ne pourrons prendre des mesures à l'encontre du compte. Dans ce cas, si vous n'êtes pas parent de l'enfant, nous vous encourageons fortement à demander aux parents de nous contacter personnellement à l'aide de ce formulaire.

Votre adresse électronique :
Adresse électronique à laquelle nous pouvons vous contacter. Si vous êtes en mesure d'accéder à votre adresse électronique de connexion, saisissez-la ici.

URL du profil que vous souhaitez signaler :
Veuillez copier/coller l'URL de son profil.

Prénom et nom de la personne que vous souhaitez signaler :

Adresse électronique associée au profil :

Réseaux auxquels le profil appartient :
Par exemple, le réseau régional de San Francisco.

Âge réel de l'utilisateur : Veuillez sélectionner une réponse :

Votre relation avec l'utilisateur : Veuillez sélectionner une réponse :

Questions ou informations pertinentes supplémentaires :

Envoyer Annuler

Source : http://www.facebook.com (dernière concultation : 06 juin 2011)

Face à l'engouement toujours grandissant des environnements électroniques, les commissaires à la protection des données et de la vie privée[56], réunis en conférence internationale, ont adopté la *Résolution sur la vie privée des enfants en ligne*[57]. Cette dernière met l'accent sur la nécessaire collaboration entre les gouvernements, les entreprises et les autorités de protection des consommateurs et de protection des renseignements personnels pour développer des outils permettant d'éduquer et de sensibiliser les jeunes aux risques liés à l'utilisation des TI. Elle insiste également sur l'importance d'adopter des moyens visant à limiter ou à interdire le traitement des renseignements personnels des enfants notamment à des fins publicitaires. Elle recommande aussi aux responsables des sites Web commerciaux ou des réseaux sociaux de simplifier leur politique de confidentialité[58].

Face aux enjeux inhérents à la collecte, à la communication et à l'utilisation des renseignements personnels des jeunes à l'ère numérique, la Commission recommande différentes avenues. Une première concerne la sensibilisation et l'éducation des natifs du numérique. Une seconde a trait à l'implication des entreprises face à cette problématique. Néanmoins, pour que ces avenues ne demeurent pas lettre morte, elles doivent s'accompagner d'une prise de conscience collective. En effet, la protection des renseignements personnels des jeunes est l'affaire de tous car le présent indélébile des générations montantes est tributaire de notre vigilance.

56. Depuis 2002, la Commission peut participer aux conférences fermées tenues lors des conférences internationales des commissaires à la protection des données et de la vie privée. Voir notamment : *Résolution concernant l'accréditation de nouvelles autorités*, Résolution adoptée lors de la 24e Conférence internationale des commissaires à la protection des données et de la vie privée, Cardiff (Royaume-Uni), 2002.
57. *Résolution sur la vie privée des enfants en ligne*, Résolution adoptée lors de la 30e Conférence internationale des commissaires à la protection des données et de la vie privée, Strasbourg (France), 17 octobre 2008. *Infra*, Annexe 2 – Résolutions adoptées par les commissaires à la protection des données et de la vie privée et de l'accès à l'information. Cette résolution internationale vient confirmer celle adoptée le 4 juin 2008 par les commissaires à la protection de la vie privée et responsable de la surveillance de la protection de la vie privée du Canada à Régina (Saskatchewan – Canada).
58. *Supra*, 1.1.1. Les politiques de confidentialité simplifiées.

1.2.1. Sensibilisation et éducation des jeunes

La Commission s'est vu confier par l'Assemblée Nationale le mandat d'assurer la promotion de la protection des renseignements personnels[59] tant auprès des adultes que des jeunes. En effet, les lois de protection des renseignements personnels s'appliquent à toute personne quel que soit son âge.

À ce propos, s'il est important de sensibiliser les jeunes aux risques et défis que présentent les environnements électroniques pour leurs renseignements personnels, il convient également d'informer leurs parents et leurs enseignants de ces enjeux. Même si les jeunes préfèrent généralement faire leurs propres expériences loin du contrôle des adultes, il est essentiel que ces derniers puissent, le cas échéant, les accompagner dans leur apprentissage et répondre à leurs éventuelles questions pour les encourager à réfléchir sur la protection de leur vie privée pendant leurs sessions en ligne.

Cette approche « à large spectre » a déjà été utilisée par la Commission dans son document *Inforoute, attention zone scolaire*[60] qui s'adresse aux commissions scolaires, aux établissements d'enseignement privé, aux écoles, aux personnels enseignants, aux élèves et aux parents. La Commission y suggérait certaines pistes pour que la création de sites Web et l'utilisation d'Internet en milieu scolaire respectent les principes de protection des renseignements personnels. Par exemple, il était recommandé aux commissions scolaires et aux écoles de sensibiliser les élèves aux enjeux d'Internet concernant leurs renseignements personnels et superviser les activités pédagogiques pour éviter que les jeunes ne tiennent des propos malveillants sur le Web ou visitent des sites destinés aux adultes.

Par ailleurs, il est prévu au *Plan stratégique 2009-2012* de la Commission qu'elle mette en place des activités de sensibilisation pour informer les jeunes des enjeux inhérents à l'utilisation des TI sur les renseignements personnels[61]. Des activités de promotion ont ainsi été réalisées dans le cadre de la *Journée internationale de la protection des données* et de la *Semaine du droit à l'information.*

S'inscrivant dans cette approche préventive, l'Association francophone des autorités de protection des données personnelles[62] a produit de la documentation à l'intention des jeunes de 6 à 13 ans[63]. Au Québec, ce matériel est diffusé par le biais de la Commission.

Il s'agit d'un signet, d'une affiche et d'un dépliant sur le thème *Internet : c'est moi qui décide !* présentant des « trucs et des astuces » pour éviter les pièges des environnements électroniques. Ce matériel tend à responsabiliser les jeunes. Les informations qu'ils publient sur Internet constituent des renseignements personnels sur eux, leur famille et leurs amis. Internet et le Web 2.0 étant de véritables terrains de jeux pour les jeunes, cette documentation vise à leur donner les outils nécessaires pour les aider à faire les bons choix, à comprendre les conséquences de leurs activités en ligne et à développer une certaine « pudeur numérique ».

59. *Loi sur l'accès*, art. 122.1.
60. COMMISSION D'ACCÈS À L'INFORMATION DU QUÉBEC, *Inforoute, attention zone scolaire*, 1999.
61. COMMISSION D'ACCÈS À L'INFORMATION DU QUÉBEC, *Plan stratégique 2009-2012*, Québec, Commission d'accès à l'information du Québec, 2009, p. 10.
62. L'Association francophone des autorités de protection des données personnelles (AFAPDP) a été créée le 24 septembre 2007, lors de la première Conférence des Commissaires à la protection des données de la Francophonie. Me Chartier, président de la Commission, assume depuis février 2011 la présidence de cette association. Il succède à Me Saint-Laurent, ancien président de la Commission (2004-2010), qui occupait ce poste depuis 2007. Comme indiqué dans ses statuts, cette association a pour objectifs de mettre en place des programmes de coopération entre ses membres, d'encourager des recherches « sur des questions et pratiques relatives à la protection des données personnelles », de proposer une expertise pour « l'adoption de textes législatifs nationaux ou d'instruments internationaux » ou encore de « fournir un forum de réflexion et d'échange ».
63. Cette documentation a été réalisée en partenariat avec l'Organisation Internationale de la Francophonie.

« Les enfants et les élèves doivent être éduqués de façon à devenir des citoyens autonomes dans la société de l'information. À cet effet, il est fondamental qu'ils apprennent dès leur plus jeune âge l'importance du respect de la vie privée et de la protection des données. Ces notions leur permettront par la suite de prendre des décisions en connaissance de cause sur les informations qu'ils souhaitent divulguer, à qui et dans quelles conditions. La protection des données doit être systématiquement intégrée dans les programmes scolaires, en fonction de l'âge des élèves et de la nature des matières enseignées. »

Source : GROUPE DE TRAVAIL « ARTICLE 29 » SUR LA PROTECTION DES DONNÉES, *Avis 2/2009 sur la protection des données à caractère personnel de l'enfant (Principes généraux et cas particulier des écoles)*, WP 160, 11 février 2009, p. 21. Ce groupe de travail est un organe consultatif européen indépendant.

La diffusion de ce matériel par la Commission s'inscrit dans son rôle de promotion de la protection des renseignements personnels. Cette façon de faire correspond aussi à l'approche de plusieurs autorités en la matière.

Ainsi, par exemple, la Commission Nationale de l'Informatique et des Libertés en France (CNIL) a notamment développé une affiche, un questionnaire en ligne et une application que les jeunes peuvent télécharger gratuitement sur un *iPhone*, *iPod touch* ou *iPad* pour apprendre « à rester net sur le web! »[64]. Le Commissariat à la protection de la vie privée du Canada (CPVPC) a développé pour sa part le site Web « ma vie privée, mon choix, ma vie » qui propose différentes ressources destinées aux jeunes mais aussi aux parents et aux enseignants[65].

Même si les ressources humaines et financières de la Commission, plutôt modestes, limitent pour le moment ses activités de sensibilisation, elle est néanmoins convaincue que de telles activités constituent des outils non négligeables pour protéger les enfants.

Les activités de promotion des organismes publics, tels la Commission, le CPVPC et la CNIL, sont toutefois insuffisantes car elles ne rejoignent que la clientèle qui fréquente leurs sites Web. Dans cette optique, la Commission recommande que la sensibilisation des jeunes soit intégrée aux programmes scolaires.

Que ce soit au primaire ou au secondaire, l'école contribue au développement des enfants. Elle les instruit et les socialise. Elle leur donne des outils pour exercer leur jugement critique, pour agir en citoyen responsable et respectueux des autres. Elle leur permet de réfléchir sur différents sujets économiques, politiques et sociaux.

Il est donc permis de penser que les programmes du primaire et du secondaire pourraient comprendre des thématiques relatives à la protection des renseignements personnels, aux droits et obligations découlant des principes encadrant ce domaine ou encore aux enjeux liés à l'utilisation des TI et du Web 2.0 sur la vie privée des jeunes. Ces thématiques pourraient être expliquées en tenant compte de l'âge des enfants. Et, comme les préoccupations au primaire ne sont pas forcément les mêmes qu'au secondaire, elles pourraient également être enseignées à différents moments du cursus scolaire. L'intégration de telles considérations dans les programmes scolaires aurait enfin l'avantage de sensibiliser en même temps toute une génération.

La Commission scolaire Lester-B.-Pearson a annoncé, en janvier 2011, le lancement d'un programme de citoyenneté numérique.

Ce programme « vise à informer tous les membres de la communauté scolaire, y compris les élèves, les employés et les parents, sur l'utilisation responsable de la technologie. […] Le programme comporte neuf éléments axés sur certains des défis auxquels les utilisateurs de la technologie doivent faire face. […] Ces neufs éléments sont les suivants : l'accès au numérique, le commerce numérique, la communication numérique, la littératie numérique, l'étiquette en ligne, la loi, les droits et les responsabilités en ligne, la santé et le bien-être, la sécurité numérique. »

Source : « Dévoilement du nouveau programme de citoyenneté numérique », (2011) vol. XIV, n°6 *Pearson News* 1.

64. http://www.jeunes.cnil.fr (dernière consultation: 06 juin 2011).
65. http://www.youthprivacy.ca/fr (dernière consultation: 06 juin 2011).

1.2.2. Engagement des entreprises

Cette démarche de sensibilisation et d'éducation doit s'accompagner d'un engagement des entreprises qui collectent, communiquent et utilisent les renseignements personnels de jeunes. L'implication des entreprises peut même être utilisée comme un moyen de rejoindre les jeunes et un avantage concurrentiel.

Extrait de la politique de confidentialité du site Barbie géré par le groupe Mattel

« Mattel Inc, et sa famille de sociétés (« Mattel ») s'engagent à protéger votre vie privée en ligne lorsque vous visitez un site Internet exploité par la société Mattel. Nous enregistrons uniquement les informations que vous ou votre enfant âgé de 13 ans ou plus nous fournissez de votre plein gré. Nous ne demandons et ne conservons aucun renseignement personnel en ligne sur les enfants de moins de 13 ans sans l'accord d'un parent ou d'un tuteur légal, à l'exception des quelques circonstances autorisées par la loi et décrites dans ces informations. »

Source : http://www.fr.barbie.com (section « Éthique de respect de la vie privée ») (dernière consultation: 06 juin 2011).

Les lois de protection des renseignements personnels obligent les entreprises à respecter un certain nombre de principes lors du traitement des renseignements personnels. La Commission veille à l'application de ces principes quelle que soit la nature du support utilisé pour recueillir et conserver ces informations.

Les principes énoncés notamment dans la *Loi sur la protection dans le secteur privé* n'accordent pas un traitement différencié aux jeunes, contrairement aux articles 248 et 249 de la *Loi* québécoise *sur la protection du consommateur*[66] qui, depuis plus de 30 ans, interdi-sent de « faire de la publicité à but commercial destinée à des personnes de moins de treize ans »[67]. Ou encore à la *Children's Online Privacy Protection Act*[68] qui, aux États-Unis, réglemente le traitement des renseignements personnels des enfants de moins de treize ans.

Cette loi américaine, en vigueur depuis avril 2000, a été adoptée à la suite du rapport *Privacy Online : A Report to Congress*[69] de la Federal Trade Commission[70]. Ce rapport recommandait au Congrès de légiférer afin d'encadrer la collecte, la communication et l'utilisation des renseignements personnels à l'ère numérique, des enfants de moins de treize ans. Dès lors, les sites dédiés, exclusivement ou en partie, à cette clientèle doivent publier leur politique de confidentialité dans un langage clair et obtenir le consentement des parents avant la collecte de renseignements personnels.

Sur le plan international, la *Résolution sur la vie privée des enfants en ligne*, adoptée en 2008, exige « des restrictions appropriées en matière de collecte, d'utilisation et de communication de renseignements personnels concernant les enfants lorsqu'il s'agit de publicité en ligne ciblant les enfants ou de publicité comportementale »[71].

Même si de telles mesures doivent être encouragées, il convient néanmoins de constater que les jeunes sont courtisés sur Internet, de façon plus ou moins déguisée, par des entreprises qui leur demandent de fournir toujours plus de renseignements personnels. Ces méthodes favorisent leur profilage.

66. L.R.Q., c. P-40.1.
67. Notons que la problématique de la publicité fait également l'objet de discussions en ce qui concerne notamment la publicité dite ciblée ou comportementale. Concernant ce type de publicité impliquant des mineurs, voir notamment : GROUPE DE TRAVAIL « ARTICLE 29 » SUR LA PROTECTION DES DONNÉES, *Avis 2/2010 sur la publicité comportementale en ligne*, WP 171, 22 juin 2010. Selon les auteurs, « les fournisseurs de réseaux publicitaires devront informer les parents de la collecte et de l'utilisation d'informations concernant leurs enfants et obtenir leur consentement avant de collecter et d'exploiter ces informations à des fins de ciblage comportemental des enfants. Eu égard à ce qui précède, et compte tenu de la vulnérabilité des enfants, le groupe de travail est d'avis que les fournisseurs de réseaux publicitaires ne devraient pas proposer de catégories de centres d'intérêt destinées à diffuser des publicités comportementales ou à influencer des enfants. », p. 20.
68. 15 U.S.C. § 6501 à 6506.
69. FTC 1998, *préc.*, note 28.
70. Concernant le rôle de la Federal Trade Commission, voir *supra*, 1.1.1. Les politiques de confidentialité simplifiées.
71. Précité, note 57.

Les commissaires à la protection des données et de la vie privée incitent « les exploitants de sites Web destinés aux enfants à démontrer leur conscience sociale en adoptant des politiques de confidentialité et des accords d'utilisation clairs, simples et compréhensibles, ainsi qu'en informant les utilisateurs sur les risques relatifs à la protection de la vie privée et à la sécurité et sur les choix que leur offrent les sites Web. »

Source : *Résolution sur la vie privée des enfants en ligne*, Résolution adoptée lors de la 30e Conférence internationale des commissaires à la protection des données et de la vie privée, Strasbourg (France), 17 octobre 2008.

À ce propos, il est à noter que le Conseil de l'Europe a adopté, le 23 novembre 2010, une recommandation visant à encadrer ce procédé. Un des considérants de cette recommandation, d'application générale, se lit comme suit :

> « Considérant que le profilage des enfants peut avoir des conséquences graves pour eux durant toute leur vie et, étant donné qu'ils ne sont pas à même d'exprimer seuls un consentement libre, spécifique et éclairé lors de la collecte de données à caractère personnel à des fins de profilage, il est nécessaire de prendre des mesures spécifiques et appropriées de protection de l'enfance afin de tenir compte de l'intérêt supérieur de l'enfant et du développement de sa personnalité, conformément à la Convention des Nations Unies relative aux droits de l'enfant. »[72]

La Commission appuie cette idée et recommande au législateur d'envisager l'ajout d'une interdiction dans les lois de protection du consommateur ou de protection des renseignements personnels concernant le profilage des jeunes.

Par ailleurs, il convient également de constater que l'accessibilité, la clarté et la compréhension des politiques de confidentialité sont souvent décriées bien qu'elles demeurent un outil informationnel à considérer répondant à l'obligation d'information préalable à l'expression d'un consentement éclairé.

C'est pourquoi, afin de renforcer l'information préalable à l'expression du consentement des personnes concernées, la Commission recommande que soient envisagés la simplification des politiques de confidentialité[73] et le recours à des pictogrammes de protection[74].

D'une part, la simplification permet aux entreprises de présenter un condensé de leurs engagements en matière de protection des renseignements personnels en parallèle avec une politique détaillée de ceux-ci. Ce type de présentation permet aux personnes concernées de rapidement savoir quelles sont les intentions d'un site Web commercial ou d'un réseau social quant au traitement de leurs renseignements personnels. Il permet également aux entreprises d'adapter leurs propos au public cible, à savoir les jeunes.

D'autre part, les pictogrammes de protection permettent aux entreprises de signaler leurs objectifs de confidentialité d'une façon « ludique » et accessible quelle que soit la nature du support envisagé pour recueillir et conserver les renseignements personnels. Ces pictogrammes doivent être compréhensibles par tous et plus particulièrement par les jeunes. Ainsi, la présence d'un tel pictogramme sur un site Internet aurait pour effet d'indiquer aux jeunes que ce site leur est destiné et s'engage à respecter leurs renseignements personnels.

Illustration de pictogrammes visant à interdire le visionnement d'un film selon l'âge

Source : Régie du cinéma (Québec)

72. CONSEIL DE L'EUROPE, *Recommandation CM/Rec(2010)13 du Comité des Ministres aux États membres sur la protection des personnes à l'égard du traitement automatisé des données à caractère personnel dans le cadre du profilage*, 23 novembre 2010. Lors des travaux préparatoires, l'AFAPDP, à titre d'observateur, a eu l'occasion de proposer que soit interdit le profilage à l'égard des enfants, comme souligné par Me Saint-Laurent, ancien président de la Commission et de l'AFAPDP, lors d'un discours prononcé en novembre 2009. Jacques SAINT-LAURENT, « Les droits de l'enfant face au développement des technologies de l'information et de la communication », Allocution prononcée lors du *Séminaire international des droits de l'enfant*, Tunis (Tunisie), 24 novembre 2009.

73. *Supra*, 1.1.1. Les politiques de confidentialité simplifiées.

74. *Supra*, 1.1.2. Les pictogrammes de protection.

Le recours à de tels procédés permettrait à la Commission de vérifier l'engagement des entreprises à l'égard des principes de protection des renseignements personnels. Cela lui permettrait également d'évaluer plus facilement l'information préalable à l'expression d'un consentement, communiquée aux personnes concernées en cas de plainte.

La protection des renseignements personnels des natifs du numérique nécessite, selon la Commission, que des actions soient entreprises en faveur de la sensibilisation, de l'éducation et de l'implication de l'ensemble des acteurs.

Recommandation 5 : La Commission recommande que le réseau de l'éducation développe des programmes scolaires au niveau du primaire et du secondaire visant à éduquer les jeunes aux enjeux des TI et du Web 2.0.

Recommandation 6 : La Commission invite le législateur à s'interroger sur la pertinence de modifier les lois de protection du consommateur ou des renseignements personnels notamment pour interdire le profilage des jeunes dans les environnements électroniques.

1.3. LA DÉCLARATION DES FAILLES DE SÉCURITÉ

Exemples d'incidents portés à la connaissance de la Commission

Perte
- perte des renseignements personnels des clients ou des employés au sein d'un organisme public ou d'une entreprise
- perte de différents supports (disques durs, documents papiers, clés USB) lors de déplacements
- perte de données lors de transferts entre organismes publics ou entreprises

Vol
- vol de différents supports (ordinateurs, chèques) contenant des renseignements personnels

Accès / Divulgation
- divulgation non autorisée de renseignements personnels concernant des clients (dossiers de crédit, carte de crédit)
- accès non autorisé à des renseignements personnels via Internet
- envoi, par la poste ou par courriel, de documents contenant des renseignements personnels au mauvais destinataire
- information visible par la fenêtre de l'enveloppe
- lettres non cachetées

Conservation / Destruction
- mise aux rebuts non sécuritaire de matériel contenant des renseignements personnels
- documents contenant des renseignements personnels mis dans des poubelles publiques

La sécurité est un principe fondamental en matière de protection des renseignements personnels. Les organismes publics et les entreprises doivent respecter ce principe et adopter des mesures de sécurité adaptées au contexte. Au Québec, cette obligation est énoncée dans la *Loi sur l'accès* et dans la *Loi sur la protection dans le secteur privé* qui exigent des « mesures de sécurité propres à assurer la protection des renseignements personnels collectés, utilisés, communiqués, conservés ou détruits et qui sont raisonnables compte tenu, notamment, de leur sensibilité, de la finalité de leur utilisation, de leur quantité, de leur répartition et de leur support »[75]. Cette obligation est également contenue dans la *Loi concernant le cadre juridique des technologies de l'information*[76].

Pour consolider l'obligation d'adopter et de maintenir des mesures de sécurité efficaces et efficientes tout au long du cycle de vie des renseignements personnels, la Commission recommande que celle-ci s'accompagne d'une obligation de déclaration des failles de sécurité à une autorité de protection et, dans certaines circonstances, aux personnes concernées.

1.3.1. Les failles de sécurité

Pour remplir leurs obligations, les organismes publics et les entreprises adoptent des mesures de sécurité organisationnelles, humaines et techniques. Toutefois, comme nous le rappelle fréquemment l'actualité, en matière de sécurité, le « risque zéro » n'existe pas. Les organismes publics et les entreprises ne sont donc pas à l'abri d'incidents pouvant conduire, par exemple, à l'oubli de documents contenant des renseignements personnels dans un lieu public, à l'envoi au mauvais destinataire de correspondances d'affaires, à la conservation non sécuritaire de matériel contenant des renseignements personnels par un dépositaire chargé de les détruire ou carrément à la perte et au vol de documents.

Une faille de sécurité constitue donc un manquement dans la mise en œuvre et l'application des mesures de sécurité[77]. Elle peut entraîner une perte de renseignements personnels ou encore leurs accès, utilisation ou divulgation non autorisés. Elle n'est pas toujours associée aux technologies de l'information (TI) et elle peut provenir d'une simple erreur ou négligence humaine.

Une faille de sécurité est donc un phénomène dont les causes multiples appellent divers moyens de prévention. Un des moyens consiste à procéder à une analyse des risques en tenant compte du support et de la sensibilité des données. Un autre consiste à informer le personnel d'un organisme public ou d'une entreprise des mesures de protection retenues et des risques engendrés par leur non-respect. Tester régulièrement les mesures de sécurité en place et, le cas échéant, procéder aux ajustements nécessaires permet aussi aux organismes publics et aux entreprises de maintenir des mesures de sécurité efficaces et efficientes.

75. *Loi sur l'accès*, art. 63.1; *Loi sur la protection dans le secteur privé*, art. 10.
76. L.R.Q., c. C-1.1, art. 25 et 26.
77. Pour une compilation des failles de sécurité par types, par secteurs d'activités ou encore par données visées, voir notamment : *Datalossdb* (http://datalossdb.org), *Nymity* (http://www.nymity.com), *Dataloss Barometer* (http://www.datalossbarometer.com), *Identity Theft Resource Center* (http://www.idtheftcenter.org). (dernière consultation : 06 juin 2011).

La nécessité de maintenir de telles mesures de sécurité est d'autant plus importante qu'une faille de sécurité est susceptible de conduire à un vol d'identité qui consiste à collecter et à utiliser des renseignements personnels à l'insu et sans l'autorisation de la victime. Ce type de fraude n'est pas sans conséquence. Par exemple, les personnes physiques peuvent être tenues responsables des dettes contractées avec leurs informations[78] (nom, prénom, numéro d'assurance sociale, etc.). Le public peut perdre confiance envers les organismes publics et les entreprises visés par une faille de sécurité impliquant le vol de renseignements personnels. En ce qui concerne les entreprises, cette perte de confiance pourra avoir un impact sur leur réputation, leurs marques de commerce, mais aussi sur leur chiffre d'affaires.

Dès lors, outre les mesures de prévention, les organismes publics et les entreprises doivent réagir rapidement advenant une faille de sécurité. Pour ce faire, il leur est possible de se référer soit aux procédures qu'ils ont développées à l'interne, soit à l'*Aide-mémoire à l'intention des organismes et entreprises – Que faire en cas de perte ou de vol de renseignements personnels?*[79] élaboré par la Commission.

Selon cet *Aide-mémoire*, les organismes publics et les entreprises peuvent, sur une base volontaire, aviser la Commission de la survenance d'une faille de sécurité impliquant des renseignements personnels.

Cette déclaration volontaire des failles de sécurité trouve également application en Ontario, au Manitoba et en Colombie-Britannique, par exemple. En effet, les autorités de protection des renseignements personnels de ces provinces proposent aussi des guides à l'intention des organismes publics et des entreprises[80].

Ces guides, à l'image de l'*Aide-mémoire* de la Commission, précisent qu'en plus de contacter l'autorité de protection et les personnes concernées, il peut être nécessaire, selon le cas, d'aviser la police, les assureurs, les ordres professionnels, les banques et les agences de crédit. Ils précisent quand et comment informer les autorités de protection et les personnes concernées. Ils rappellent l'importance de circonscrire rapidement le problème et de mettre en place des mesures pour éviter qu'une telle situation ne se reproduise.

Déclarations volontaires présentées à la Commission (année financière)

	2008-2009	2009-2010	2010-2011
Secteur privé	7	11	4
Secteur public	1	5	1
TOTAL	8	16	5

À cet effet, la Commission a recueilli diverses données au cours des trois dernières années. Ces données proviennent des déclarations volontaires qui lui ont été présentées ainsi que d'une inspection que la Commission a amorcée auprès des ministères et organismes gouvernementaux afin de,

> « vérifier l'état de la situation quant à la perte et [au] vol de renseignements personnels au sein de ces [organismes]. Plus spécifiquement, cette inspection vise à connaître le nombre d'événements ayant donné lieu à un vol ou une perte de renseignements personnels par

78. « Rappelons que les informations recherchées sont de nature très variées. En effet, le voleur d'identité peut vouloir obtenir des informations d'identification (nom, prénom, âge, sexe, adresse, numéro de téléphone, nom de jeune fille de la mère, numéro d'assurance sociale [NAS], numéro d'identification personnel [NIP], revenu, emploi, situation familiale, lieux de résidence, code utilisateur, pseudonyme, etc.), des habitudes de consommation (magasins fréquentés, relevés de compte, actifs, obligations, etc.), des habitudes de navigation (sites web visités, fréquences des visites, nom des forums, amis sur le net, etc.), des habitudes de vie (loisirs, relations, moyens de déplacement, périodes de congés, etc.), ou encore des données sensibles concernant la carrière, l'employeur, le dossier médical, ou encore le casier judiciaire. », Benoît DUPONT et Esma AIMEUR, « Les multiples facettes du vol d'identité », (2010) vol. LXIII, *Revue internationale de criminologie et de police technique et scientifique*, 177, 179.

79. COMMISSION D'ACCÈS À L'INFORMATION DU QUÉBEC, *Aide-mémoire à l'intention des organismes et des entreprises – Que faire en cas de perte ou de vol de renseignements personnels ?*, Avril 2009, ci-après « Aide-mémoire ».

80. INFORMATION AND PRIVACY COMMISSIONER OF ONTARIO, W*hat to do if a privacy breach occurs: Guidelines for government organizations*, December 2006; OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER FOR BRITISH COLUMBIA, *Breach Notification Assesment Tool*, December 2006 et *Keys Steps in Responding to Privacy Breaches*, June 2008; MANITOBA OMBUDSMAN, *Reporting a Privacy Breach To Manitoba Ombudsman*, March 2007.

organisme au cours des trois dernières années ainsi que les mesures prises pour réagir à ces incidents. De plus, l'inspection vise à savoir s'il existe une politique ou une directive en matière de perte ou de vol de renseignements personnels pour chacun des organismes. »[81]

Cette inspection, dont les suivis sont en cours d'élaboration, a permis de mettre en évidence que des failles de sécurité surviennent à l'occasion au sein des organismes publics. Il ressort également que les façons de réagir à ces incidents varient d'un endroit à l'autre laissant parfois les personnes concernées dans l'ignorance de ce qui menace la sécurité de leurs renseignements personnels.

Pour la Commission, il est essentiel que les organismes publics et les entreprises adoptent une attitude préventive et une démarche curative dans les cas d'incidents impliquant une faille dans la sécurité des renseignements personnels.

1.3.2. L'obligation de déclarer les failles de sécurité

Une étude menée en 2009, pour le compte du Commissariat à la protection de la vie privée du Canada (CPVPC), vient conforter cette proposition car :

> « les répondants s'attendaient à ce que, sous un régime obligatoire, leur entreprise élaborerait une politique de signalement plus structurée, devien-drait plus sensibilisée à l'importance de protéger la vie privée, se préoccuperait davantage de la prévention des incidents et augmenterait la responsabilité à l'égard de la protection des renseignements personnels dans les activités de l'organisation. »[82]

Ainsi, alors que l'obligation de sécurité a un caractère préventif, l'obligation de déclaration des failles de sécurité aurait davantage un caractère curatif. Elle viendrait renforcer l'obligation de sécurité. Ces deux obligations se complèteraient donc.

Cette approche trouve application dans d'autres juridictions. Par exemple aux États-Unis, où la majorité des États ont adopté une législation en ce sens, la Californie s'est donné, en 2002, une loi qui impose aux organismes publics et aux entreprises l'obligation de déclarer aux personnes concernées les failles de sécurité[83]. Depuis ce temps, comme l'indiquent ses rapports annuels[84], le *California Office of Privacy Protection* a préparé des règles de pratique pour encadrer l'obligation de déclaration[85]. De plus, il répond aux demandes des organismes publics et des entreprises quant à l'application de la loi. Il les guide dans les démarches à entreprendre lorsque survient une faille de sécurité pour en limiter les incidences sur la protection des renseignements personnels. Il informe également les personnes dont les renseignements personnels ont ou sont susceptibles d'avoir été visés par une faille de sécurité.

Nombre de demandes d'assistance relatives à une faille de sécurité						
2003-2004	2004-2005	2005-2006	2006-2007	2007-2008	2008-2009	2009-2010
3602 (1)	983	1117 (2)	380 (2)	921 (2)	n/d	181 (2)

(1) Entrée en vigueur de la loi et publication des *Recommended Practices on Notice of Security Breach Involving Personal Information*
(2) Mise à jour des *Recommended practices on Notice of Security Breach Involving Personal Information*

81. COMMISSION D'ACCÈS À L'INFORMATION DU QUÉBEC, *Rapport annuel de gestion 2009-2010*, Québec, Gouvernement du Québec, 2010, p. 36.
82. COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Rapport annuel au Parlement 2009 – Rapport sur la Loi sur la protection des renseignements personnels et sur les documents électroniques*, Ottawa, Ministre des Travaux publics et des Services gouvernementaux Canada, 2010, p. 63.
83. Cal. Civ. Code, §1798.29 et §1798.82. Cette obligation concerne les organismes publics et les entreprises « that owns or licenses computerized data that includes personal information ».
84. http://www.privacy.ca.gov/activity_hightlights.htm (dernière consultation: 06 juin 2011).
85. CALIFORNIA OFFICE OF PRIVACY PROTECTION, *Recommended Practices on Notice of Security Breach Involving Personal Information*, October 2003 (last revised June 2009).

Pour leur part, les États membres de l'Union européenne avaient jusqu'au 25 mai 2011[86] pour transposer dans leurs lé-gislations relatives à la protection des renseignements personnels, une disposition selon laquelle les failles de sécurité doivent être dénoncées à l'autorité nationale compétente et aux personnes concernées[87].

Au Canada, un projet de loi[88] est mort au feuilleton lors de la dissolution du Parlement en mars 2011. Il était prévu qu'une organisation soumise à la *Loi sur la protection des renseignements personnels et sur les documents électroniques*[89] serait tenue de déclarer « toute atteinte importante aux mesures de sécurité qui a trait à des renseignements personnels »[90] au CPVPC. La gravité de l'atteinte serait fonction du degré de sensibilité des renseignements, du nombre d'individus touchés par la faille et de la récurrence du problème. De plus, l'organisation aurait dû aviser la personne concernée si cette atteinte présentait « un risque réel de préjudice grave à son endroit »[91]. L'organisation aurait alors dû tenir compte, notamment, de la sensibilité des renseignements en cause, de la probabilité qu'ils aient été mal utilisés ou qu'ils soient sur le point de l'être.

En Alberta, depuis le 1er mai 2010, en vertu du *Personal Information Protection Act*[92], les organisations[93] doivent déclarer à l'*Office of the Information and Privacy Commissioner* (OIPC) « tout incident impliquant la perte ou l'accès non autorisé ou la divulgation de renseignements personnels »[94]. Cette déclaration doit se faire dès qu'il existe « un risque réel de préjudice important pour un individu en raison de la perte, de l'accès non autorisé ou de la divulgation »[95]. Dès lors, l'OIPC peut recommander à l'organisation d'aviser les personnes concernées par cet évènement. Il est à noter que les organisations conservent, en tout temps, la possibilité d'aviser les personnes concernées de leur propre chef[96].

Un règlement d'application accompagne cette loi[97]. Il précise le contenu et la forme de la déclaration devant parvenir à l'OIPC[98] et aux personnes concernées[99]. Dans les deux cas, la déclaration doit contenir une description de la faille, des renseignements personnels visés et des mesures prises pour en minimiser les conséquences. Elle doit également préciser la date estimée de la faille et le nom de la personne pouvant répondre aux questions concernant cette faille au sein de l'organisation.

86. PARLEMENT EUROPÉEN ET CONSEIL, *Directive 2009/136/CE du Parlement européen et du Conseil du 25 novembre 2009 modifiant la directive 2002/22/CE concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques, la directive 2002/58/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques et le règlement (CE) no 2006/2004 relatif à la coopération entre les autorités nationales chargées de veiller à l'application de la législation en matière de protection des consommateurs*, Journal officiel de l'Union européenne, no L 337 du 18 décembre 2009, p. 11-36, art. 4(1).
87. *Id.*, art. 2.
88. *Loi modifiant la Loi sur la protection des renseignements personnels et les documents électroniques*, projet de loi n° C-29, (dépôt et 1ère lecture à la Chambre des communes – 25 mai 2010), 3e sess., 40e légis. (Can.), ci-après « Projet de loi C-29 ».
89. L.C. 2000, c. 5.
90. *Projet de loi C-29*, *préc.*, note 88, art. 11.
91. *Id.*, art. 11.
92. S.A. 2003, c. P-6.5.
93. Cette notion s'entend de « a corporation, an unincorporated association, a trade union as defined in the Labour Relations Code, a partnership as defined in the Partnership Act, and an individual acting in a commercial capacity, but does not include an individual acting in a personal or domestic capacity », *Id.*, art. 1(1)(i).
94. *Id.*, art. 34.1 (1). (notre traduction)
95. *Id.*, art. 34.1 (1). (notre traduction)
96. *Id.*, art. 37.1 (7).
97. *Personal Information Protection Act Regulation*, Alta, Reg. 366/2003.
98. *Id*, art. 19.
99. *Id.*, art. 19.1.

Par ailleurs, la déclaration destinée à l'OIPC doit mentionner les risques encourus par les personnes concernées et le nombre de personnes affectées par la faille. Cette déclaration doit être faite par écrit.

Cependant, les organismes publics ne sont pas soumis à cette obligation de déclaration des failles de sécurité. Ils peuvent néanmoins aviser volontairement l'OIPC de telles failles, en remplissant un formulaire disponible sur le site Web de cette autorité[100].

Comme on peut le constater, l'obligation de déclarer les failles de sécurité aurait pour effet d'instaurer un dialogue entre les organismes publics et les entreprises, d'une part, et la Commission et les personnes concernées, d'autre part.

1.3.3. Les enjeux liés à la déclaration obligatoire

Que ce soit à l'égard des organismes publics ou des entreprises, la Commission a, entre autres, pour fonctions de surveiller l'application de la loi et de s'assurer du respect de la protection des renseignements personnels. L'obligation de déclarer les failles de sécurité à la Commission s'inscrit dans cet objectif. En effet, une telle déclaration donnerait à la Commission l'opportunité de conseiller et d'accompagner les organismes publics et les entreprises dans le choix des mesures à prendre et d'effectuer un suivi. Cela lui permettrait également de répondre adéquatement aux demandes des médias et aux éventuelles plaintes du public et de développer des documents d'information à l'intention des organismes publics, des entreprises et des personnes concernées adaptés aux situations ayant causé les failles de sécurité. L'obligation de déclarer les failles de sécurité servirait à renforcer la confiance des citoyens envers les organismes publics et les entreprises qui détiennent leurs renseignements personnels et permettrait à la Commission de mieux jouer son rôle de surveillance quant au respect de l'obligation de sécurité des renseignements personnels.

De plus, une intervention opportune en ce sens contribuerait à réduire les retombées économiques négatives liées au vol d'identité.

Il faut bien l'admettre, cette proposition de déclaration à la Commission est le résultat d'une vulnérabilité évidente dans la mise en œuvre et l'application des mesures de sécurité. Il incombe alors aux organismes publics et aux entreprises d'adopter des mécanismes les alertant de la survenance d'une faille de sécurité. De plus, pour éviter qu'une faille ne se reproduise et pour rétablir la confiance du public et des personnes concernées, il leur revient de réaliser des enquêtes pour détecter l'origine de la faille et d'y remédier rapidement. Ils doivent également mettre en place de nouvelles mesures de sécurité et former le personnel en conséquence.

Par ailleurs, la Commission croit préférable que les organismes publics et les entreprises informent eux-mêmes les personnes concernées. Il est important de circonscrire rapidement la faille et d'analyser les informations visées pour éviter d'alarmer à tort ces personnes.

En ce qui a trait aux personnes concernées, la déclaration obligatoire d'une faille de sécurité susceptible d'affecter leurs renseignements personnels leur donnerait l'occasion de prendre certaines mesures pour en minimiser les conséquences. Elles pourraient agir auprès de leurs institutions financières, contacter les agences de crédit, porter plainte à la police et éventuellement, s'adresser à un avocat, à la Commission ou aux tribunaux pour faire valoir leurs droits envers l'organisme public ou l'entreprise. Ces démarches auraient pour but de les protéger de toutes utilisations ultérieures de leurs renseignements personnels.

100. OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER OF ALBERTA, *Breach Report Form*, May 2010 (revised).

En raison des enjeux découlant de la déclaration obligatoire des failles de sécurité pour les différents acteurs, la Commission recommande que les organismes publics et les entreprises soient obligés de déclarer à la Commission toute faille de sécurité présentant un risque pour les renseignements personnels. En fonction des mesures prises pour circonscrire la faille et de la sensibilité des renseignements personnels, la Commission pourra alors ordonner que soient informées les personnes concernées. Cette intervention de la Commission vise à ré-duire les déclarations hâtives et alarmistes. Néanmoins, un organisme public ou une entreprise demeurerait libre en tout temps d'aviser, de son propre chef, les personnes concernées.

La Commission considère que l'obligation de déclarer les failles de sécurité vise à établir une concertation entre les organismes publics, les entreprises, le public et la Commission. Il en va de la confiance des citoyens envers les organismes publics et les entreprises. Cette confiance sera augmentée si la Commission apparaît comme un partenaire dans la gestion de la sécurité des renseignements personnels.

Recommandation 7 : La Commission recommande que la *Loi sur l'accès* et la *Loi sur la protection dans le secteur privé* soient modifiées par l'ajout d'une obligation de lui déclarer les failles de sécurité qui surviennent dans les organismes publics et les entreprises et qui impliquent des renseignements personnels.

Recommandation 8 : La Commission recommande que soient déterminées les conditions et les modalités conduisant à déclarer des failles de sécurité impliquant des renseignements personnels.

Recommandation 9 : La Commission recommande que lui soit confié le pouvoir d'ordonner aux organismes publics et aux entreprises d'aviser, aux conditions qu'elle déterminera, les personnes concernées d'une faille de sécurité impliquant leurs renseignements personnels et de prendre les mesures qu'elle jugera nécessaires pour assurer une protection adéquate de leurs renseignements personnels.

1.4. LA FONCTION DE RESPONSABLE DANS LE SECTEUR PRIVÉ

Bien souvent, dans le secteur privé, le citoyen ne sait pas à quelle personne s'adresser au sein d'une entreprise s'il désire obtenir une copie de son dossier ou s'il veut faire rectifier des renseignements personnels le concernant. De surcroît, lorsque l'entreprise ne répond pas à sa demande ou la rejette et qu'il dépose une demande d'examen de mésentente à la Commission, cette dernière ignore souvent, elle aussi, à quel interlocuteur s'adresser.

Depuis 17 ans, la *Loi sur la protection dans le secteur privé* demande à « toute personne qui exploite une entreprise » de s'assurer du respect des principes rattachés à la protection des renseignements personnels. Si une entreprise est responsable actuellement des renseignements personnels qu'elle a en sa possession ou sous sa garde, rien ne l'oblige toutefois à désigner nommément une personne pour assumer cette responsabilité.

Les avantages liés au fait qu'une personne réponde auprès du public et de la Commission de l'application de la *Loi sur la protection dans le secteur privé* et qu'elle contribue à établir dans l'entreprise une culture de protection des renseignements personnels ne doivent pas être mésestimés. Aussi, la Commission croit nécessaire qu'un responsable de l'accès et de la protection des renseignements personnels soit désigné.

« L'accès aux documents [ou l'accès d'un individu à son dossier personnel] n'implique pas que les citoyens peuvent s'adresser à n'importe qui et que tous les fonctionnaires peuvent satisfaire directement aux demandes. Bien au contraire, l'anarchie et la prolifération des relations réduiraient l'accès et le droit à l'information en empêchant la gestion et la diffusion ordonnées des pièces disponibles et mettraient en danger la protection des dossiers personnels. Il importe aussi que le citoyen sache à qui il doit transmettre sa demande et à qui il peut se plaindre, que les mécanismes d'accès soient cohérents et que le traitement des demandes soit uniforme. »

Source : COMMISSION D'ÉTUDE SUR L'ACCÈS DU CITOYEN À L'INFORMATION GOUVERNEMENTALE ET SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS, *Information et liberté*, Québec, Gouvernement du Québec, 1981, p. 31.

1.4.1. La fonction de responsable dans le secteur public

Dans le secteur public, la fonction de personne responsable de l'accès aux documents et de la protection des renseignements personnels a été instaurée et a démontré son utilité au cours des 29 dernières années.

En effet, la *Loi sur l'accès* désigne d'office la personne ayant la plus haute autorité comme personne responsable pour exercer les fonctions conférées par cette loi[101]. Cette personne peut toutefois en désigner une autre et lui déléguer tout ou partie de ses fonctions. Le cas échéant, un avis de cette délégation doit être transmis à la Commission. Également, le nom du responsable et les coordonnées permettant de communiquer avec lui doivent être accessibles au public sur les sites Internet des organismes visés par le *Règlement sur la diffusion*[102].

La Commission croit qu'un responsable devrait être désigné pour assumer tout ou partie des fonctions conférées par la *Loi sur la protection dans le secteur privé*. Quelques législations canadiennes y pourvoient déjà.

101. *Loi sur l'accès*, art. 8.
102. Précité, note 17, art. 4(1)3°.

1.4.2. La situation à l'échelle canadienne

Au regard de la *Loi sur la protection des renseignements personnels et les documents électroniques*, « une organisation est responsable des renseignements personnels dont elle a la gestion »[103]. Dès lors, elle « doit désigner une ou des personnes qui devront s'assurer du respect des principes énoncés »[104] dans la loi. En outre, « il doit être possible de connaître sur demande l'identité des personnes que l'organisation a désignées »[105] à cette fin.

À cet égard, les dispositions législatives en Alberta[106] et en Colombie-Britannique[107] sont équivalentes à celles de la loi canadienne. Tout comme la *Loi sur la protection dans le secteur privé*, ces trois lois visent tant les entreprises individuelles que les compagnies, les associations, les sociétés et les syndicats.

La loi canadienne et les lois de l'Alberta et de la Colombie-Britannique ont formellement instauré la fonction de responsable dans le secteur privé depuis près de 10 ans. Ces mesures se traduisent dans les entreprises privées par la désignation d'un responsable de la protection des renseignements personnels, d'un ombudsman ou d'un « chef de la vie privée ».

1.4.3. Un rôle essentiel dans les communications avec l'entreprise

Au Québec, une personne qui exploite une entreprise doit, à la demande d'une personne concernée, répondre aux demandes d'accès à des renseignements personnels et aux demandes de rectification qui lui sont faites[108].

La *Loi sur la protection dans le secteur privé* prévoit des dispositions détaillées pour régir ces demandes. De plus, la loi prévoit que « toute personne qui exploite une entreprise (…) doit notamment porter à la connaissance du public l'endroit où ces dossiers sont accessibles et les moyens d'y accéder »[109].

Ainsi, on pourrait croire qu'une personne peut facilement obtenir une copie de son dossier ou le faire rectifier. Or, dans les faits, il n'est pas toujours aisé pour un citoyen de communiquer avec une entreprise pour obtenir ses renseignements personnels ou connaître les mesures mises en place pour en assurer la conservation et la protection.

Comme le requiert la *Loi sur l'accès*, les responsables de l'accès et de la protection des renseignements personnels dans les organismes publics doivent répondre aux demandeurs et les aviser des recours possibles devant la Commission. Dans le secteur privé, les entreprises doivent également répondre aux demandeurs en motivant leur refus et en les informant de leurs recours[110]. Or, il semble que les entreprises font preuve d'un certain laxisme dans le respect de ces obligations. En 2010, la Commission a reçu plus de 250 demandes d'examen de mésentente. La moitié des entreprises avaient notifié leur refus par écrit et, parmi celles-ci, seulement une quarantaine ont informé les personnes concernées des recours possibles devant la Commission.

103. Précité, note 89, art. 5. Voir également l'Annexe 1 de cette loi, plus particulièrement le premier principe dont le texte est reproduit en annexe du présent rapport, *infra*, Annexe 3 – Dispositions législatives et réglementaires étrangères.
104. *Id.*, Annexe 1, art. 4.1.
105. *Id.*, Annexe 1, art. 4.1.2.
106. *Personal Information Protection* Act, *préc.*, note 92, art. 5.
107. *Personal Information Protection* Act, S.B.C., 2003, c. 63, art. 4.
108. *Loi sur la protection dans le secteur privé*, art. 27 et suiv..
109. *Id.*, art. 29.
110. *Id.*, art. 34 « La personne qui refuse d'acquiescer à la demande d'accès ou de rectification d'une personne concernée doit lui notifier par écrit son refus en le motivant et l'informer de ses recours ».

La Commission a également constaté que les fonctions découlant de la *Loi sur la protection dans le secteur privé* sont occupées par diverses personnes au sein des entreprises. Il peut s'agir, par exemple, du dirigeant, du président ou d'un employé du service des ressources humaines.

En fait, la personne qui traite les demandes doit connaître les obligations qui lui incombent et les restrictions qui peuvent être invoquées. Pour répondre adéquatement aux demandes, une personne responsable devrait avoir l'occasion et le devoir d'acquérir des connaissances pour bien assumer ses fonctions.

En somme, la désignation d'un responsable et la possibilité de connaître l'identité de cette personne permettraient aux personnes titulaires des droits d'accès et de rectification d'établir la communication avec l'entreprise pour exercer leurs droits. De plus, la personne désignée s'assurerait de la qualité des réponses transmises aux personnes concernées et à la Commission. Enfin, la désignation d'un responsable serait également utile à la Commission pour assurer le suivi dans le cas d'examen de mésentente.

1.4.4. Un rôle de promoteur de la protection des renseignements personnels dans l'entreprise

À l'instar du secteur public, si une entreprise estime nécessaire de recueillir un renseignement personnel, elle doit veiller à protéger ce renseignement à toutes les étapes du cycle de vie de celui-ci, soit de sa collecte à sa destruction[111]. Or, il semble que les obligations liées à ce devoir demeurent méconnues ou mal appliquées dans certaines entreprises.

Ainsi, l'entreprise doit avoir un intérêt légitime pour constituer un dossier sur une personne[112]. De plus, elle doit recueillir seulement les renseignements personnels nécessaires à l'objet de ce dossier[113]. À cet égard, des personnes témoignent ou dénoncent à la Commission la collecte de renseignements qui ne sont pas nécessaires pour réaliser les fins d'un dossier. Dans le cadre de leurs plaintes, ces personnes reprochent aux entreprises une cueillette qu'elles jugent abusive et arbitraire. Devant une telle situation, un responsable pourrait notamment voir au respect des obligations de l'entreprise en ce qui concerne la collecte de renseignements personnels en révisant les formulaires de vente ou d'adhésion utilisés par l'entreprise. À l'occasion, il pourrait interpeller l'entreprise, son employeur, sur ses façons de faire.

La Commission est également informée que certaines entreprises communiquent des renseignements à des tiers, sans le consentement des personnes concernées. Il peut s'agir d'informations financières, de renseignements relatifs à un dossier d'employé ou de numéros d'identification personnels.

À l'ère numérique, nombre de communications de renseignements personnels s'effectuent ainsi, bien souvent à l'insu des personnes concernées. Pour éviter de telles atteintes à la protection des renseignements personnels, encore faut-il que l'entreprise s'attarde à ces questions et que son personnel y soit sensibilisé. Un responsable pourrait réviser les formulaires de l'entreprise ou s'assurer de leur existence[114].

111. *Id.*, art. 10.
112. *Id.*, art.4.
113. *Id.*, art. 5.
114. *Supra*, 1.1. La protection des renseignements personnels à l'ère numérique.

La Loi sur la protection dans le secteur privé confère également aux entreprises la responsabilité de la protection des renseignements personnels qu'elles détiennent. Ces entreprises confient parfois la destruction de leurs documents confidentiels, hébergent des données sur leur serveur ou traitent les dossiers clients d'une autre entreprise. Dans ces cas, le responsable pourrait veiller à ce que les mandats confiés à l'extérieur de l'entreprise respectent aussi la confidentialité des informations et la sécurité de leur conservation.

La nomination d'un responsable serait également utile pour les employés de l'entreprise qui désirent connaître les meilleures pratiques en matière de protection de renseignements personnels. Ainsi, un employé pourrait plus facilement valider certains de ses comportements ou encore déclarer une faille de sécurité dont il est témoin[115]. Finalement, son rôle l'amènerait à proposer aux autres membres de l'organisation des comportements adéquats en matière de protection des renseignements personnels.

Le responsable servirait de personne-ressource; comme gardien de l'application de la loi, il pourrait développer une expertise à la mesure des besoins de son entreprise.

1.4.5. La désignation du responsable

Selon la loi actuelle, c'est « la personne qui exploite une entreprise » qui doit s'assurer du respect des principes énoncés dans la *Loi sur la protection dans le secteur privé*. Il manque un rouage essentiel dans la mise en application de la loi en la personne d'un responsable désigné.

Dans la *Loi sur l'accès*, le responsable est la personne ayant la plus haute autorité[116]. Chez les ordres professionnels, le président est « responsable des demandes d'accès et de rectification[117]» faites en vertu de la loi. Ces désignations montrent bien l'importance que le législateur attache à la fonction de responsable.

La Commission croit que la *Loi sur la protection dans le secteur privé* devrait prévoir la création de la fonction de responsable. Cependant, la Commission est consciente que les moyens pour assurer le respect de la loi peuvent varier d'une entreprise à l'autre, selon la taille de l'entreprise, la structure ainsi que la quantité et la sensibilité des renseignements personnels traités.

Ainsi, la Commission comprend qu'il peut être difficile de prévoir une application uniforme et sans nuances de ces obligations à toutes les petites et moyennes entreprises. À cet égard, la Commission considère qu'il serait opportun de s'inspirer des dispositions prévues à la *Charte de la langue française*[118] et à la *Loi sur l'équité salariale*[119] afin de moduler l'application de ces dispositions en fonction du nombre d'employés[120]. La création de la fonction de responsable de l'accès et de la protection des renseignements personnels pourrait donc être recommandée aux entreprises comportant un seuil minimal d'employés à être déterminé par le législateur.

Le dirigeant d'une entreprise ou, selon le cas, le conseil d'administration devrait avoir l'opportunité de désigner un membre de son organisation ou de son personnel de direction et lui déléguer tout ou partie de ses fonctions. Le nom du responsable et ses coordonnées devraient être accessibles à la Commission et au public sur le site Internet de l'entreprise ou sur demande.

Cet arrimage du secteur privé aux secteurs public et professionnel est nécessaire pour assurer le respect des droits des personnes et pour renforcer l'application de la *Loi sur la protection dans le secteur privé*.

115. *Supra*, 1.3. La déclaration des failles de sécurité.
116. *Loi sur l'accès*, art. 8.
117. *Code des professions*, L.R.Q., c. C-26, art. 108.5.
118. L.R.Q., ch. C-11.
119. L.R.Q, ch. E-12.001.
120. La *Charte de la langue française* et la *Loi sur l'équité salariale* prévoient trois niveaux de devoirs et obligations selon le nombre d'employés : 50 et moins, plus de 50 mais de moins de 100 et 100 employés ou plus.

Également, cette mise à niveau est rendue essentielle pour assurer la sensibilisation et la responsabilisation en matière de protection des renseignements personnels, particulièrement convoités à l'ère numérique.

D'une part, avec un responsable désigné, les citoyens, la Commission et même les employés de l'entreprise sauront à quelle personne s'adresser pour connaître les pratiques en matière d'accès et de protection de renseignements personnels et, selon le cas, pour faire valoir leurs droits. D'autre part, la désignation d'une personne-ressource imputable va favoriser le développement d'une culture de protection des renseignements personnels au sein des entreprises. À terme, la confiance du public sera renforcée envers le régime et ses partenaires.

Recommandation 10 : La Commission recommande que la *Loi sur la protection dans le secteur privé* prévoit la création de la fonction de responsable de l'accès et de la protection des renseignements personnels.

Recommandation 11 : La Commission recommande que la fonction de responsable dans le secteur privé puisse être déléguée par l'entreprise à une personne œuvrant au sein de l'entreprise.

PARTIE 2 :
L'ACCÈS AUX DOCUMENTS DES ORGANISMES PUBLICS

2.1. LE PASSAGE DE LA TRANSPARENCE AU GOUVERNEMENT OUVERT

Les démocraties modernes, appuyées sur une administration publique compétente et indépendante, produisent quantité de documents à l'usage des décideurs publics. Notre démocratie repose en partie sur le droit d'accès à cette information qui permet aux citoyens de participer au débat public, de s'organiser pour faire appel aux institutions, et ultimement, de juger et choisir ses représentants. La *Loi sur l'accès* reconnaît le droit pour toute personne d'obtenir l'information détenue par l'administration publique.

Cependant, au départ perçu uniquement comme un droit exigible, il fallait, pour avoir accès aux documents publics, entreprendre des démarches parfois longues et fastidieuses pour obtenir à la pièce des renseignements alors même qu'ils étaient souvent de notoriété publique. Ce modèle contraignant ne pouvait continuer à l'ère de l'information continue et instantanée, jumelée au potentiel offert par les technologies de l'information (TI). En ajoutant l'article 16.1 à la *Loi sur l'accès* en 2006, le législateur mettait alors de l'avant le concept de la diffusion obligatoire et automatique de certains documents ou renseignements accessibles en vertu de la loi.

Art. 16.1 de la *Loi sur l'accès*

Un organisme public, à l'exception du Lieutenant-gouverneur, de l'Assemblée nationale et d'une personne qu'elle désigne pour exercer une fonction en relevant, doit diffuser, dans un site Internet, les documents ou renseignements accessibles en vertu de la loi qui sont identifiés par règlement du gouvernement et mettre en œuvre les mesures favorisant l'accès à l'information édictées par ce règlement.

Au Québec, comme ailleurs, l'administration publique a donc de plus en plus tendance à offrir un grand nombre de documents en ligne afin que les citoyens puissent les consulter eux-mêmes.

2.1.1. Le choix de la transparence

Si l'idée de transparence est présente dans la *Loi sur l'accès*, elle l'est également dans d'autres lois. Par exemple, la *Loi sur la transparence et l'éthique en matière de lobbyisme*[121] permet au citoyen de savoir qui cherche à influencer les décideurs publics. Le nouveau *Code d'éthique et de déontologie des membres de l'Assemblée nationale*[122] crée l'obligation pour tous les députés de déposer une déclaration complète de leurs intérêts et de ceux des membres de leur famille immédiate et prévoit la publication d'un sommaire de ces intérêts.

Par ailleurs, dans un souci de modernisation de l'appareil gouvernemental, le législateur a adopté deux lois établissant « des assises juridiques qui permettent d'utiliser les documents technologiques pour réaliser les échanges électroniques en toute sécurité »[123]. Ainsi, la *Loi sur l'administration publique* accorde la priorité à la qualité des services aux citoyens. Pour ce faire, elle instaure « un cadre de gestion axé sur les résultats et sur le respect du principe de transparence »[124]. Quant à elle, la *Loi concernant le cadre juridique des technologies de l'information*[125] fait en sorte que les documents ou renseignements diffusés par l'administration publique aient la même valeur juridique quel que soit le support utilisé.

Ces lois ont permis le déploiement du « gouvernement en ligne » qui entend « rendre les services publics plus accessibles, plus faciles à utiliser, plus efficaces »[126]. Ainsi, plusieurs ministères et organismes publics proposent des services en ligne tels que la possibilité de faire une demande de crédit pour la TVQ ou de prestation d'assurance

121. L.R.Q., c. T-11.011, art. 1.
122. L.R.Q., c. C-23.1.
123. MINISTÈRE DES SERVICES GOUVERNEMENTAUX DU QUÉBEC, « Gouvernement en ligne – Cadre légal », http://www.msg.gouv.qc.ca/gel/cadre_legal.html (dernière consultation: 06 juin 2011).
124. L.R.Q., c. A-6.01, art. 1(1).
125. Précité, note 76.
126. MINISTÈRE DES SERVICES GOUVERNEMENTAUX DU QUÉBEC, « Gouvernement en ligne – Définition », http://www.msg.gouv.qc.ca/gel/index.html (dernière consultation: 06 juin 2011).

« Le développement de l'administration électronique, ce qu'il convient d'appeler le gouvernement en ligne ou e-government, la création de sites Internet, la disponibilité des outils technologiques permettent déjà à l'administration de rendre plus facilement accessibles les renseignements personnels et les documents administratifs. Le gouvernement du Québec est d'ailleurs résolument engagé dans cette voie depuis quelques années. »

André OUIMET, « Accès à l'information : vers une plus grande transparence », (2004) vol. 6, n° 2 *Éthique publique* 23, 25.

Recommandation n°5 du Rapport quinquennal 2002

Afin de faciliter l'accès aux documents détenus par les organismes publics, la Commission propose que chaque organisme public ait l'obligation d'adopter une politique de publication automatique de l'information.

parentale, de planifier financièrement sa retraite, de vérifier si un bien est affecté d'une dette ou encore de consulter le cadastre d'une propriété[127].

Cependant, le gouvernement en ligne évoque bien davantage que la prestation électronique de services. Il tend également à « renforcer l'exercice des droits démocratiques par les citoyens »[128]. Dans une société moderne et ouverte, la qualité de la participation des citoyens à la vie publique repose sur l'information qu'ils reçoivent. Dès lors, la diffusion obligatoire et automatique de certains documents ou renseignements figure parmi ces façons de stimuler la vie démocratique.

Dans cette optique et répondant en cela à l'appel de la Commission, le gouvernement du Québec a fait le choix de la transparence en favorisant l'accès à plusieurs documents et renseignements d'intérêt pu-blic. Ainsi, depuis le 29 novembre 2009, certains organismes publics doivent diffuser de façon proactive quinze catégories de documents et de renseignements énumérés au *Règlement sur la diffusion*[129]. Le gouvernement, le Conseil exécutif, le Conseil du trésor, les ministères et les organismes gouvernementaux sont donc soumis au *Règlement sur la diffusion*. Par contre, le Lieutenant-gouverneur, l'Assemblée nationale, les organismes muni-cipaux, les organismes scolaires, les établissements de santé ou de services sociaux et les ordres professionnels ne le sont pas.

Les organismes publics visés par ce *Règlement sur la diffusion* doivent alors diffuser sur leur site Internet notamment l'organigramme, le plan de classification des documents, les études, rapports de recherche ou statistiques produits par l'organisme dont la diffusion présente un intérêt pour le public, les documents transmis dans le cadre d'une demande d'accès et dont la diffusion présente également un intérêt public ainsi que les renseignements relatifs à certains contrats et la liste des engagements financiers visés par le *Règlement sur la diffusion*[130]. La diffusion de ces renseignements doit se faire avec diligence et être régulièrement mise à jour.

Le *Règlement sur la diffusion* renferme les germes d'un gouvernement ouvert. Toutefois, il restera embryonnaire à moins de continuer à évoluer vers l'ouverture de l'ensemble des organismes publics et de la totalité de leurs données. Actuellement, en principe, les documents de certains organismes publics sont accessibles sur demande ou grâce à la diffusion proactive prévue au Règlement sur la diffusion. Dans un modèle de gouvernement ouvert, l'ouverture des données publiques rejetterait au rang d'exceptions les documents qui ne sont pas librement et directement accessibles en ligne. Également, une plus grande disponibilité des données publiques aurait en toute vraisemblance l'effet de diminuer le nombre de demandes d'accès aux documents que font les citoyens auprès des organismes publics.

Dès lors, la Commission recommande que l'application du Règlement sur la diffusion soit élargie aux organismes publics qui en sont exemptés. Cette étape n'est pas une fin en soi. Il ne s'agit que d'un premier pas vers le concept de gouvernement ouvert. La Commission encourage le gouvernement à s'inscrire dans cette démarche d'ouverture inspirée de la culture d'Internet favorisant la transparence et la participation citoyenne.

127. L'ensemble des services en ligne offerts aux citoyens et aux entreprises est accessible via le portail du Gouvernement du Québec à l'adresse suivante : http://www.gouv.qc.ca/portail/quebec/pgs/commun (dernière consultation: 06 juin 2011).
128. MINISTÈRE DES SERVICES GOUVERNEMENTAUX DU QUÉBEC, « Gouvernement en ligne – Définition », *préc.*, note 126.
129. Précité, note 17.
130. *Id.*, art. 4.

2.1.2. Le concept de gouvernement ouvert : transparence et participation citoyenne

Le *Règlement sur la diffusion* a permis le passage d'une divulgation réactive sur demande à une diffusion proactive de certains documents et renseignements. Cela favorise la transparence. Toutefois, aujourd'hui, le citoyen revendique de nouvelles façons de participer plus directement à la vie démocratique et d'influencer les orientations politiques. Les différentes plateformes de communication permettent de répondre à cette attente et font en sorte que l'on assiste peu à peu à un changement de paradigme.

Ainsi, en plus de tendre vers une plus grande transparence, le concept de « gouvernement ouvert » réfère également à la participation et à la collaboration entre les décideurs publics et la société civile.

Dans un gouvernement ouvert, la transparence présuppose une libération des données publiques. Celle-ci se fait par le biais de portails sur lesquels il est possible de trouver des données brutes, non traitées, ou encore des analyses sur un thème particulier. Il ne s'agit donc plus seulement ici de diffuser de l'information sous forme de produit final, mais d'offrir l'accès à l'ensemble des données qui ont permis de produire cette information. Ces données peuvent être de différentes natures : statistiques, électorales, budgétaires, géographiques ou encore socio-économiques.

De plus, la transparence signifie que les données mises à la disposition du public doivent être publiées dans un format ouvert. Ainsi, quel que soit le type de données, celles-ci doivent être lisibles par les logiciels disponibles.

Par ailleurs, dans un gouvernement ouvert, la participation directe des citoyens à la vie démocratique est favorisée. La participation implique qu'en devenant accessibles, les données publiques peuvent être soumises à l'usage et à l'appréciation de la société civile. Un gouvernement ouvert encourage les citoyens, les entreprises et les organismes sans but lucratif à rendre ces données compréhensibles pour l'ensemble de la population. En effet, parallèlement à la libération des données publiques, des individus ou des organismes sans but lucratif développent des applications informatiques et proposent des sites Web qui contribuent au développement du concept de gouvernement ouvert.

La collaboration, pour sa part, implique des échanges entre les décideurs publics et la société civile. Effectivement, un gouvernement ouvert devient réalité lorsque

> « les particuliers et les groupes concernés se voient offrir l'accès aux mêmes renseignements que ceux utilisés par le gouvernement et la fonction publique pour analyser un enjeu, un programme ou un service donné et où ils sont invités à formuler leurs commentaires ou à suggérer des idées de politique. »[131]

« La transparence est cruciale pour fournir aux citoyens de l'information sur ce que fait le gouvernement afin que ce dernier puisse, à son tour, être appelé à rendre des comptes. Elle encourage les journalistes, les chercheurs, les fonctionnaires et le public à examiner de près la façon dont le gouvernement exerce le pouvoir au nom des citoyens et, ce faisant, l'améliorer. La participation est essentielle en ce sens que le gouvernement doit demander de son propre chef l'expertise de tous les secteurs afin de pouvoir élaborer des politiques en tirant parti de la meilleure information disponible. Enfin, il faut que la collaboration s'installe pour que les fonctionnaires travaillent les uns avec les autres et avec les citoyens pour régler des problèmes nationaux. »

Andréa NEILL, « Libérer l'information - De la divulgation réactive à la divulgation proactive », Discours prononcé devant l'*Association sur l'accès et la protection de l'information*, Québec, 20 avril 2010.

131. Alysia DAVIES et Dara LITHWICK, *Gouvernement 2.0 et accès à l'information – Le point sur la divulgation proactive et le libre accès aux données aux États-Unis et dans d'autres pays*, Publication n° 2010-15-F, Ottawa, Bibliothèque du Parlement, avril 2010, p. 7.

De nos jours, l'utilisation d'Internet facilite les échanges et permet de nourrir la réflexion publique, étant entendu que « le débat public en est enrichi par des contributions plus vastes que celles émanant des seuls experts traditionnels »[132]. Les données publiques ainsi répandues peuvent susciter des initiatives créatrices et stimuler l'économie à titre de nouvelles ressources injectées dans l'économie du savoir.

La résolution conjointe du 1er septembre 2010 des commissaires canadiens de l'accès à l'information et à la protection de la vie privée résume bien les avantages d'un tel modèle :

> « la collaboration avec les citoyens, les entreprises et les organismes non gouvernementaux […] améliore les voies de communication, encourage l'engagement des citoyens, accroît la confiance envers le gouvernement, favorise les opportunités économiques et finalement, conduit à un gouvernement démocratique plus ouvert, transparent et réceptif. »[133]

Un gouvernement ouvert ne repose pas uniquement sur les TI, mais également sur une volonté gouvernementale de libérer les données publiques. Néanmoins, ce nouveau modèle est rendu possible à l'ère des environnements électroniques car la technologie permet de diffuser une quantité phénoménale d'informations en plus de favoriser les échanges.

Cette nouvelle approche de collaboration entre l'État et la société civile représente un changement de culture. Toutefois, faire émerger des alliés extérieurs à l'administration publique en plus d'améliorer l'imputabilité des décideurs publics ne va pas sans risques et défis.

2.1.3. Les enjeux liés à l'ouverture

Dans la mise en œuvre d'un gouvernement ouvert, la protection des renseignements personnels, les droits d'auteurs, la sécurité nationale, la responsabilité éthique et les inégalités numériques entre les individus demeurent des enjeux fréquemment soulevés.

D'une part, il convient de rappeler qu'un « gouvernement ouvert » est tenu de respecter les principes de protection des renseignements personnels. En effet, « l'ouverture de la sphère publique ne doit pas mettre en péril le droit des individus au respect de leur vie privée »[134]. L'ouverture concerne donc les données à caractère public, non les renseignements personnels.

L'État pourrait, dès lors, profiter du changement de culture découlant de l'ouverture des données pour diminuer la masse de renseignements personnels qu'il recueille et qu'il conserve. Ainsi, le risque de perte ou de communication de ces renseignements serait réduit, en plus de diminuer les coûts reliés à leur conservation et de rassurer les citoyens[135].

D'autre part, il faut repenser la gestion des droits d'auteurs dans le contexte d'un gouvernement ouvert où les données sont diffusées sous un format réutilisable et sont présentées comme un bien public.

Par ailleurs, sur un plan plus politique, le déploiement d'un gouvernement ouvert oblige à « trouver un juste équilibre entre la nécessité de prendre en compte des considérations légitimes de sécurité nationale et celle de garantir au public un droit de regard sur l'action gouvernementale [ce qui] a toujours été une tâche délicate, et elle l'est aujourd'hui plus que jamais »[136].

132. Henri OBERDORFF, *La démocratie à l'ère numérique*, Grenoble, Presses Universitaires de Grenoble, 2010, p. 91.
133. *Transparence gouvernementale*, Résolution des commissaires canadiens de l'accès à l'information et à la protection de la vie privée, Whitehorse (Yukon), 1er septembre 2010. *Infra*, Annexe 2 – Résolutions adoptées par les commissaires à la protection des données et de la vie privée et de l'accès à l'information.
134. ORGANISATION DE COOPÉRATION ET DE DÉVELOPPEMENT ÉCONOMIQUES, « La modernisation du secteur public : l'administration ouverte - Synthèse », (2005) *L'Observateur* 1, 6.
135. CENTER FOR TECHNOLOGY POLICY RESEARCH, *Open Government, some next steps for the UK*, May 2010, p. 43. (notre traduction)
136. ORGANISATION DE COOPÉRATION ET DE DÉVELOPPEMENT ÉCONOMIQUES, *préc.*, note 134, p. 3.

En examinant les expériences étrangères, il appert que la notion de « gouvernement ouvert » est compatible avec celle de « sécurité nationale ». Toutefois, les récentes révélations du site *WikiLeaks* rappellent la fragilité de cet équilibre. En effet, même si certaines informations sont considérées comme « secrètes », nul gouvernement n'est à l'abri de fuites.

Cette expérience démontre néanmoins qu'une responsabilité éthique incombe aux personnes et aux groupes qui s'approprient les données publiques afin de les traiter et de les publier sous une forme plus compréhensible et signifiante pour le public. Ils doivent veiller à ne pas dénaturer l'information. Sinon, le gouvernement sera tenté de restreindre l'accès ou de contrôler la réutilisation des données. La responsabilité est donc l'affaire de tous lorsqu'un gouvernement ouvre l'accès à ses données.

Enfin, une des préoccupations quant à l'ouverture concerne l'existence, encore aujourd'hui, d'une fracture numérique se traduisant par une inégalité d'usage et d'accès aux TI au sein de la population.

Partant, malgré des défis importants, la mise en place d'un gouvernement ouvert est désormais une tendance affirmée dans plusieurs pays dont notamment l'Australie, le Royaume-Uni et les États-Unis.

2.1.4. Modèles de gouvernements ouverts à l'étranger

La Commission propose ici un aperçu des initiatives lancées par l'Australie, le Royaume-Uni et les États-Unis qui sont souvent présentées comme modèles. Ces trois pays ont mis en place des stratégies qui visent à améliorer la transparence des activités gouvernementales en intégrant les TI et le Web 2.0. Ils utilisent aussi bien des portails et des blogues que les réseaux sociaux pour atteindre la population. Ces stratégies possèdent certains objectifs communs. Elles visent à donner libre accès aux données utilisées par le gouvernement et la fonction publique; elles tendent à améliorer la communication avec la population et à promouvoir une plus grande implication des citoyens dans la société et dans les affaires de l'État.

Ainsi, en Australie, le gouvernement a créé en juin 2009 un groupe de travail composé d'experts et d'entreprises provenant de différents milieux pour l'aider à réaliser son projet *Government 2.0.* Dans le cadre de ses travaux, le groupe de travail a notamment organisé des événements[137] conviant des experts d'Internet afin de promouvoir la création d'applications conviviales.

Au terme de ce chantier, le groupe de travail a remis son rapport au gouvernement australien[138]. Ensuite, le gouvernement a émis une déclaration par la voix de son ministre des Finances et de la Déréglementation, par laquelle il adhère au concept de gouvernement ouvert fondé sur une culture d'accès garantie par l'appareil gouvernemental et sur la participation citoyenne[139].

La démarche australienne accorde une large accessibilité aux données et à l'information gouvernementales. Elle en permet l'utilisation grâce à des supports technologiques adaptés. À cette fin, le gouvernement a développé le site *data.gov.au* consacré spécialement à la diffusion des données publiques.

Au moment d'écrire ces lignes, il convient de préciser que le gouvernement australien continue d'inviter les citoyens, les associations et les entreprises à développer des sites Web pour vulgariser et partager les données[140].

137. A. DAVIES et D. LITHWICK, *préc.*, note 131. Les auteures précisent que la tenue du concours « MashupAustralia » visait à « faire la démonstration d'une formule d'accès libre aux données de l'Administration » alors que l'événement « GovHack » invitait des « concepteurs Web, développeurs et autres experts techniques à élaborer des applications Web de données de l'Administration », p. 11.

138. GOVERNMENT 2.0 TASKFORCE, *Engage : Getting on with Government 2.0 – Report of the Government 2.0 Taskforce, Canberra, Government 2.0 Taskforce*, December 2009.

139. AUSTRALIAN GOVERNEMENT INFORMATION MANAGEMENT OFFICE, *Government Response to the Report of the Government 2.0 Taskforce*, May 2010. Voir également la déclaration du ministre des finances et de la déréglementation relative au gouvernement ouvert : AUSTRALIAN GOVERNEMENT INFORMATION MANAGEMENT OFFICE, *Declaration of Open Government*, July 16, 2010.

140. Le gouvernement australien, en collaboration avec le gouvernement de la Nouvelle-Zélande, organise un nouveau concours en 2011 pour encourager la réutilisation des données. Pour plus d'informations, visiter la page dédiée à ce concours : http://libraryhack.org (dernière consultation : 06 juin 2011).

Le Royaume-Uni, dans le cadre du projet *Smarter Government*, analyse depuis quelques années avec des membres de la société civile différentes avenues permettant d'offrir de meilleurs services à la population à meilleur coût[141]. Ainsi, « outre les innovations dans le secteur de la prestation électronique de services, il recommande le passage à un modèle de divulgation proactive en ligne des données de l'Administration »[142].

« Comme gouvernement, nous croyons que nous avons besoin d'ouvrir grand les portes des organismes publics pour que les politiciens et les organismes publics rendent compte de leurs actions auprès des citoyens. Nous reconnaissons aussi que cela aidera à optimiser la gestion des dépenses pu-bliques et à atteindre notre objectif de réduire le déficit record. L'accès aux données gouvernementales apportera des bénéfices économiques substantiels en permettant aux entreprises et aux organismes sans but lucratif de créer des applications innovatrices et des sites Web. »

Source: CABINET OFFICE, *The Coalition : our programme for government*, London, HM Government, May 2010, p. 20. (notre traduction)

Pour concrétiser et favoriser cette ouverture, un échéancier de publication d'un ensemble de données a été établi dans le plan d'action global du gouvernement[143]. Comme prévu à l'échéancier, le gouvernement a créé le portail interactif *data.gov.uk*. En présentation, le site Internet précise l'objectif poursuivi par le gouvernement, la nature des données directement accessibles et redirige les intervenants vers un autre site gouvernemental pour de l'information générale sur les services gouvernementaux et la prestation de service en ligne.

En plus des bases de données gouvernementales, le portail héberge des forums de discussions et des blogues. Le gouvernement y sollicite les idées et les opinions des citoyens sur des sujets d'intérêt public. Le site propose aussi des applications informatiques pour faciliter le traitement et le partage des données. Des initiatives développées à l'extérieur du gouvernement prennent ainsi le relais et ont pour but de faire comprendre à la population ou aux groupes intéressés les données libérées sur *data.gov.uk*.

Aux États-Unis, lors de la campagne présidentielle de 2008, Barack Obama déclarait qu'il souhaitait utiliser les technologies disponibles pour créer un nouveau niveau de transparence gouvernementale et permettre ainsi aux citoyens américains de participer au processus décisionnel du gouvernement[144]. Au lendemain de son investiture, il confirmait son engagement, et dans le cadre du projet *Open Government Initiative*, la Maison-Blanche émettait une directive avec des instructions et des échéanciers que les départements et organismes gouvernementaux doivent respecter dans la mise en œuvre des principes de transparence, de participation et de collaboration citoyennes[145].

Le président américain a également transmis une note destinée aux dirigeants des départements et des agences américaines afin qu'ils renouvèlent leurs engagements à l'égard des principes d'accès édictés dans le *Freedom of Information Act* (FOIA)[146]. Par la suite, le Procureur général des États-Unis a transmis des consignes précises à ces mêmes dirigeants pour que le FOIA soit appliqué convenablement[147].

Plusieurs bases de données brutes ont été mises à la disposition des citoyens par le biais du site *Data.gov*. Comme en Australie et au Royaume-Uni, le gouvernement américain encourage les initiatives externes au gouvernement dans le développement d'applications Internet pour traduire ces données brutes et les rendre utiles à la population.

Le gouvernement ouvert poursuit son avancée. La volonté de permettre aux citoyens de s'approprier les données gouvernementales et à tendre vers un gouvernement ouvert s'illustre également dans d'autres pays. Par ailleurs, la tendance à libérer les données est déjà devenue réalité dans

141. CHIEF SECRETARY TO THE TREASURY, *Putting the Frontline First : Smarter Government*, London, HM Government, December 2009. Le Premier ministre, David Cameron, et le vice-premier ministre, Nick Clegg, ont inscrit le concept de gouvernement ouvert dans leur programme commun, CABINET OFFICE, *The Coalition : our programme for government*, London, HM Government, May 2010, p. 20-21.
142. A. DAVIES et D. LITHWICK, *préc.*, note 131, p. 7.
143. CHIEF SECRETARY TO THE TREASURY, *préc.*, note 141, p. 63-65.
144. Tim O'REILLY, « Government as a Platform », dans Daniel LATHROP and Laurel RUMA, *Open Government – Collaboration, Transparency, and Participation in Practice*, Sebastopol (California), O'Reilly Media Inc., 2010, p. 12. (notre traduction)
145. EXECUTIVE OFFICE OF THE PRESIDENT, *Open Government Directive – Memorandum for the Heads of Executive Departments and Agencies*, 8 December 2009.
146. WHITE HOUSE, *Memorandum on Transparency and Open Government – Memorandum for the Heads of Executive Departments and Agencies*, 21 January 2009.
147. OFFICE OF THE ATTORNEY GENERAL, *The Freedom of Information Act* (FOIA) Guidelines, 19 Mars 2009.

des villes comme San Francisco, New York, Londres, Toronto, Vancouver, Ottawa ou encore Edmonton[148].

2.1.5. La situation au Canada

Actuellement, conformément à plusieurs politiques émises par le Conseil du trésor du Canada, les ministères et organismes fédéraux doivent divulguer de façon proactive un certain nombre de données. Il en va ainsi des dépenses de déplacement et des frais de représentation, des contrats de plus de 10 000 $, de la reclassification des postes, de l'octroi de subventions et de contributions supérieures à 25 000 $ ou encore de la constatation d'actes répréhensibles[149]. Les ministères et organismes fédéraux publient cette information dans la section « divulgation proactive » de leur site Internet.

Par ailleurs, des organismes sans but lucratif mettent également à la disposition de la population cette information. Par exemple, sur le site *VisibleGovernment.ca*, plusieurs projets sont en cours afin notamment de rendre accessible le suivi des demandes d'accès à l'information ou les dépenses de voyage. Le site invite également les politiciens à prendre position quant à la transparence gouvernementale via le site *ibelieveinopen.ca*. Il encourage aussi les citoyens à signaler les problèmes rencontrés dans un quartier quant à l'éclairage, à la signalisation ou aux nids de poules via le site *fixmystreet.ca.*

Des citoyens veillent également à la pérennité des données publiques. Par exemple, à la suite de la cessation des activités du Système de coordination des demandes d'accès à l'information (SCDAI), le professeur Michael Geist de la Faculté de droit de l'Université d'Ottawa a développé le site *Cairs.info*[150]. Les demandes d'accès à l'information faites dans les ministères et organismes fédéraux demeurent ainsi accessibles au public malgré la fermeture du SCDAI.

Ces exemples démontrent l'intérêt des citoyens pour la libération des données publiques. Cet intérêt est partagé par la Commissaire à l'information du Canada qui, à la lumière des modèles étrangers, a dégagé certains principes sur lesquels devrait reposer le concept de gouvernement ouvert au Canada. Ces principes peuvent se résumer de la façon suivante :

1. engagement au plus haut niveau de l'appareil gouvernemental;
2. consultation publique;
3. mise à disposition gratuite des données publiques dans un format lisible et compréhensible quelle que soit la technologie utilisée;
4. respect de la vie privée, des droits d'auteurs, des langues officielles et de la sécurité nationale;
5. stratégie devant être diffusée auprès de l'ensemble des ministères et organismes fédéraux[151].

Il l'est également par le Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique de la Chambre des Communes qui a adopté une motion en avril 2010 visant à entreprendre une réflexion sur la transparence gouvernementale. Les auditions d'experts, d'ici et d'ailleurs, devant ce Comité se sont poursuivies jusqu'à la dissolution de la 40e Législature (26 mars 2011).

148. A. DAVIES et D. LITHWICK, *préc.*, note 131; Alysia DAVIES et Dara LITHWICK, *Gouvernement 2.0 et accès à l'information – Le point sur la divulgation proactive et le libre accès aux données au Canada*, Publication n° 2010-14-F, Ottawa, Bibliothèque du Parlement, avril 2010, p. 1; GROUPE DE TRAVAIL SUR LE JOURNALISME ET L'AVENIR DE L'INFORMATION AU QUÉBEC, *L'information au Québec : un intérêt public*, janvier 2011, p. 100.
149. Voir notamment : *Loi sur la protection des fonctionnaires divulgateurs d'actes répréhensibles*, L.C. 2005, c. 46, art. 11 (1)c).
150. Voir notamment : COMITÉ PERMANENT DE L'ACCÈS À L'INFORMATION, DE LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET DE L'ÉTHIQUE, *Rapport 6 - Système de coordination des demandes d'accès à l'information*, Ottawa, Chambre des communes, 39e Législature, 2e Session, 7 mai 2008. Le Comité dénonce également la cessation des activités du SCDAI et « réclame que le gouvernement conservateur remette sur pied cet outil favorisant la transparence et l'imputabilité ».
151. CANADA, *Débat du Sénat*, 3e sess., 40e légis. 22 juin 2010, « Période des questions – La commissaire à l'information », p. 895 (Mme LEGAULT).

Néanmoins, avant la fin des travaux parlementaires, le gouvernement fédéral a émis une « déclaration sur le renforcement du gouvernement ouvert » permettant ainsi « aux Canadiens de consulter l'information publique sous des formats plus conviviaux et lisibles, de se renseigner davantage sur les rouages du gouvernement et de participer plus directement au processus de prise de décisions »[152]. Ainsi, comme indiqué sur le site *Gouvernement ouvert*[153] lancé à cette occasion, le renforcement du gouvernement ouvert s'accompagne de « données ouvertes », d'une « information ouverte » et d'un « dialogue ouvert ». Conséquemment, au titre du « dialogue ouvert », sont mises de l'avant des initiatives pour lesquelles les citoyens peuvent exprimer leurs commentaires au sujet, entre autres, de la réduction de la paperasse, de la vision commune du Canada et des États-Unis concernant la sécurité et la compétitivité économique à l'intérieur du périmètre ou encore sur le surpoids et l'obésité chez les jeunes.

Ces réflexions et initiatives du gouvernement fédéral font écho à celles menées au Québec ou encore dans des provinces comme l'Ontario et la Colombie-Britannique. En Ontario, la Commissaire à l'information et à la vie privée propose d'implanter le concept d'« accès à l'information intégré » *(Access by Design)* au sein de l'appareil gouvernemental afin que les données publiques soient diffusées de façon proactive. Ce concept repose sur sept principes qui peuvent se résumer de la façon suivante : divulgation proactive, intégration du concept dès la conception des programmes gouvernementaux, responsabilité, collaboration, efficacité, accessibilité et qualité de l'information[154]. En Colombie-Britannique, « la divulgation proactive […] est un des éléments d'un modèle de démocratie électronique plus global. Celui-ci comporte, entre autres, la fourniture de données brutes et de documents de politique aux citoyens et leur permet d'utiliser des outils interactifs pour participer au processus d'élaboration de politiques effectif »[155]. Dès lors, la première ministre s'est engagée à soutenir l'ouverture du gouvernement. Par exemple, les citoyens peuvent suivre l'action du gouvernement notamment sur *Twitter*[156], *Facebook*[157], *YouTube*[158] ou encore avoir accès à différents documents publics sur le site du gouvernement de la province.

La situation évolue donc de diverses façons au Canada alors qu'au Québec, où de plus en plus de documents sont disponibles en ligne, le modèle de gouvernement ouvert devrait se développer.

152. CABINET DU PRÉSIDENT DU CONSEIL DU TRÉSOR ET MINISTRE DE LA PORTE D'ENTRÉE DE L'ASIE-PACIFIQUE, *Le renforcement du gouvernement ouvert*, Communiqué, 18 mars 2011.
153. http://www.ouvert.gc.ca (dernière consultation : 06 juin 2011).
154. Ann CAVOUKIAN, *L'accès à l'information intégré- Les sept principes fondamentaux*, avril 2010.
155. Andréa NEILL, *Libérer l'information : de la divulgation réactive à la divulgation proactive*, Discours prononcé devant l'Association sur l'accès et la protection de l'information, Québec, 20 avril 2010.
156. Précité, note 21.
157. Précité, note 20.
158. http://www.youtube.com (dernière consultation : 06 juin 2011).

2.1.6. Une application pour le Québec

Il y a quelques années, le gouvernement du Québec mettait en œuvre l'idée de « gouvernement en ligne » dont les orientations d'administration électronique, de cyberdémocratie et de société de l'information vont dans le sens de la participation citoyenne et de la collaboration entre les différents acteurs sociaux. Sous ces aspects, elles s'inscrivent tout à fait dans l'approche du gouvernement ouvert et elles sont adaptées à cette évolution.

Selon le ministère des Services gouvernementaux du Québec, les composantes du gouvernement en ligne sont :

« - l'Administration électronique vise l'amélioration de l'ensemble des processus administratifs internes et externes du gouvernement. On y trouve les services en ligne qui visent spécifiquement l'amélioration des processus de prestation de services avec le citoyen (particuliers et entreprises) ;

- la Cyberdémocratie vise le développement et l'amélioration des relations avec le citoyen en tant qu'acteur politique ainsi que les relations inter-gouvernementales ;

- la Société de l'information vise le développement et l'amélioration des relations sociales avec l'ensemble des parties prenantes de la société civile : groupes de pression, associations sans but lucratif, etc. »

Source : MINISTÈRE DES SERVICES GOUVERNEMENTAUX, « Le Gouvernement en ligne », http://www.msg.gouv.qc.ca/gel/index.html (dernière consultation: 06 juin 2011)

La démarche entreprise avec le *Règlement sur la diffusion* concrétise dans une certaine mesure cette ouverture. Celui-ci pourrait néanmoins tendre à encore plus d'ouverture.

Au préalable, comme ailleurs, l'amorce du changement doit provenir d'un engagement clair des hautes autorités gouvernementales en faveur d'un modèle plus simple et plus ouvert d'accès à l'information gouvernementale. Le gouvernement doit demeurer responsable de l'encadrement et de la réalisation d'un plan d'action qui maximise l'utilisation des TI et du Web 2.0. Il doit également faire appel à la contribution des citoyens pour développer des outils technologiques qui facilitent l'utilisation et la compréhension des données publiques. La société québécoise possède dans plusieurs champs une expertise remarquable en matière d'innovation et d'usage des environnements électroniques.

Des individus et des groupes communautaires sont déjà à pied d'œuvre, engagés dans un mouvement qu'ils revendiquent comme un espace supplémentaire d'exercice direct pour la démocratie. Ainsi en est-il, par exemple, du groupe *MontréalOuvert* qui entend « promouvoir l'accès ouvert aux données civiques de la région de Montréal »[159] et présenter un *Plan de développement stratégique d'ouverture des données de la Ville de Montréal* à l'automne 2011. Il donne également accès à différentes « ressources » axées sur l'ouverture des données.

Cette ouverture des données publiques est également soutenue par le Groupe de travail sur le journalisme et l'avenir de l'information au Québec qui invite « le gouvernement du Québec [à continuer] d'évoluer vers le modèle *Opendata* en rendant accessibles toutes ses données publiques en formats ouverts sur une plateforme centralisée »[160] et qui recommande « la création d'un comité de travail pour étudier la mise sur pied d'un modèle québécois de gouvernement ouvert ou cybergouvernement (Open Government) qui pourrait se retrouver sur une plateforme appelée *www.data.gouv.qc* »[161]. La Commission estime même qu'il s'agirait d'une évolution naturelle du régime québécois. Mais, tout d'abord, le gouvernement doit réitérer par des gestes concrets son adhésion à une culture de transparence propice à l'avènement d'un gouvernement ouvert.

Partant, les gestes posés pour le soutien d'une culture de la transparence au sein de l'appareil gouvernemental ne doivent pas occulter le fait qu'un débat public doit se tenir rapidement sur un modèle de gouvernement ouvert pour le Québec.

159. MONTRÉAL OUVERT, « À propos », http://montrealouvert.net/a-propos (dernière consultation: 06 juin 2011).
160. GROUPE DE TRAVAIL SUR LE JOURNALISME ET L'AVENIR DE L'INFORMATION AU QUÉBEC, *préc.*, note 14 8, p. 99.
161. *Id.*, p. 100.

Sur le fond et aux fins de discussions, la Commission propose que l'ouverture englobe les données et les documents produits ou reçus par un organisme public dans l'exercice de ses missions de service public. Cela comprendrait notamment :

- tout ce qui présente un intérêt pour la compréhension des missions de l'État et des services offerts par l'Administration;
- tout ce qui permet aux citoyens de comprendre ce qui motive les décisions prises pour les pouvoirs publics; et
- tout ce qui permet d'exercer un suivi des dépenses effectuées par l'État.

Recommandation 12 : La Commission recommande que l'application du *Règlement sur la diffusion* soit élargie aux organismes publics actuellement exemptés.

Recommandation 13 : La Commission recommande que les organismes publics soient assujettis à un régime élargi d'ouverture des données publiques qui permette l'accès libre à l'ensemble de l'information gouvernementale utile aux citoyens.

Recommandation 14 : La Commission recommande qu'un débat public regroupant l'ensemble des partenaires (parlementaires, citoyens, associations, experts) soit instauré afin d'établir un modèle pour l'ouverture du gouvernement québécois fondé sur la participation et la collaboration.

2.2. LE DÉLAI POUR MOTIVER UN REFUS D'ACCÈS À UN RENSEIGNEMENT

La personne qui désire obtenir l'accès à un document détenu par un organisme public doit adresser sa demande au responsable de l'accès aux documents. Selon l'article 47 de la *Loi sur l'accès*, celui-ci doit répondre « avec diligence et au plus tard dans les vingt jours » suivant la réception de la demande; ce délai peut être prolongé « d'une période n'excédant pas dix jours » lorsque le traitement de la demande dans le délai imparti nuirait au déroulement normal des activités de l'organisme. Finalement, l'absence de réponse de sa part, à l'expiration de ce délai, équivaut à un refus.

L'article 50 de la *Loi sur l'accès* prévoit que les organismes doivent « motiver tout refus » de communiquer un renseignement « et indiquer la disposition de la Loi sur laquelle ce refus s'appuie ». À cet égard, la *Loi sur l'accès* prévoit deux catégories de restrictions sur lesquelles les organismes publics peuvent se fonder pour refuser de communiquer un renseignement[162]. Ces restrictions ont un caractère impératif ou facultatif.

Une restriction impérative ne laisse aucune marge de manœuvre; le document ne doit pas être communiqué. Lorsque ces restrictions sont applicables, l'organisme ou la Commission doivent les soulever en tout temps, même lors de l'examen de la demande de révision. Il peut s'agir notamment de renseignements ayant des incidences sur l'administration de la justice et la sécurité publique[163].

D'autres restrictions revêtent pour leur part un caractère facultatif. Il appartient alors à l'organisme de décider de sa propre initiative de rendre le document accessible ou d'en refuser l'accès en indiquant la restriction à l'accès sur laquelle il s'appuie. Il peut s'agir, par exemple, d'un renseignement ayant des incidences sur les décisions administratives ou politiques[164].

Dans la pratique, lorsque l'organisme fait défaut de répondre aux demandes d'accès dans le délai imparti, il lui arrive de soulever plus tard dans le processus de révision devant la Commission, des motifs de refus basés sur des restrictions facultatives. Il se présente également des situations où il répond aux demandes d'accès sur la base de certains motifs, mais ajoute ultérieurement des motifs fondés sur d'autres restrictions facultatives. Dans certains cas, ces motifs sont soulevés le jour même de l'audience.

Pendant les deux premières années qui ont suivi l'entrée en vigueur de la *Loi sur l'accès*, la Commission a fait preuve de souplesse en permettant aux organismes d'invoquer des motifs de refus facultatifs hors délai. La Commission tenait compte de l'inexpérience des organismes dans l'application de leurs nouvelles obligations. Par la suite et jusqu'en 1999, elle a refusé systématiquement, à moins de circonstances exceptionnelles, l'ajout de tels motifs. La Cour du Québec a longtemps souscrit à cette position.

Toutefois, trois décisions de la Cour du Québec rendues de 1999 à 2004 sont venues changer les règles du jeu[165]. Ces décisions ont établi qu'il est possible de soulever des motifs facultatifs de refus en tout temps puisqu'aucune disposition de la *Loi sur l'accès* ne permet à la Commission de déclarer un organisme forclos de le faire. Selon la Cour, la Commission possède une discrétion pour autoriser de tels ajouts et elle se doit d'exercer cette discrétion.

162. Étant donné que la problématique décrite sous ce volet se retrouve également dans l'application de la *Loi sur la protection dans le secteur privé*, le présent texte s'applique aussi à cette Loi avec les ajustements nécessaires. Voir par exemple les articles 27 à 41 de la *Loi sur la protection dans le secteur privé*.

163. Voir par exemple les articles 28 et 28.1 de la *Loi sur l'accès*.

164. Voir par exemple les articles 32 et 37 de la *Loi sur l'accès*.

165. *Ministère de la Sécurité publique c. Joncas*, J.E. 99-1653 (C.Q.); *Ministère de la Justice c. Schulze*, [2000] C.A.I. 413 (C.Q.); *Service Anti-Crime des Assureurs et Assurances générales des Caisses Desjardins c. Ménard*, [2004] C.A.I. 630 (C.Q.).

Cependant, ces décisions ne sont pas unanimes pour ce qui est des conditions à respecter entourant l'exercice de ce pouvoir. Aussi, la jurisprudence de la Commission évolue au cas par cas pour définir les critères pour autoriser des motifs de refus hors délai. Dans les faits, l'organisme sera généralement autorisé par la Commission à invoquer, même tardivement, des motifs facultatifs de refus. Sinon, dans l'état actuel du droit, l'organisme pourrait prétendre que la Commission ne lui a pas donné une occasion valable de présenter ses observations.

N'étant pas avisé à l'avance des motifs de refus soulevés tardivement par l'organisme, le demandeur risque de ne pas être apte à se préparer pour l'audition de son dossier devant la Commission.

En outre, compte tenu des délais de mise au rôle, le demandeur peut parfois attendre plusieurs mois après sa demande d'accès avant de connaître les véritables motifs de refus de l'organisme. S'il doit se présenter devant la Commission qui aura à juger de la pertinence même de ces motifs, c'est faire supporter au demandeur un trop lourd fardeau.

C'est sans compter que des litiges peuvent aboutir devant les juges administratifs alors qu'une réponse valablement motivée aurait pu satisfaire le demandeur. De plus, la situation actuelle entraîne parfois des remises et des délais supplémentaires dans le traitement des dossiers. Enfin, les juges administratifs, tout comme les demandeurs, peuvent se retrouver dans une situation où ils ne sont pas en mesure de se préparer adéquatement.

Les seuls qui sont avantagés par cette situation sont les organismes qui peuvent, à tout moment, même le jour de l'audience, soulever de nouveaux motifs facultatifs de refus à l'accès aux documents. Cela entraîne un déséquilibre entre les parties et n'ajoute certes pas à la transparence nécessaire des organismes publics.

En effet, c'est le principe même de l'accès à l'information qui se trouve compromis. L'idée au départ, en prévoyant un délai maximum de trente jours, était de ne pas imposer aux organismes des contraintes déraisonnables dans le traitement d'une demande d'accès. Par contre, les rédacteurs du Rapport Paré présumaient que

> « la détermination d'une période relativement brève ne [pouvait] qu'inciter les organismes à mettre sur pied des mécanismes de réponse efficaces et surtout à gérer leur stock de documents le plus rigoureusement possible »[166].

Les membres de la Commission Paré estimaient donc que l'établissement d'un délai précis de traitement des demandes d'accès permettrait d'assurer le succès de la réforme en offrant au demandeur une réponse rapide de l'administration. Les trop longs délais ne pourraient-ils pas avoir pour effet de décourager les demandeurs d'accès à l'information ? Sans compter qu'une information longtemps refusée risque de devenir moins utile ou caduque. Dans notre société très médiatisée et branchée, les objectifs poursuivis à l'origine par le régime d'accès à l'information deviennent encore plus justifiés et pressants.

Dans les circonstances, il importe de clarifier les règles applicables au délai permis pour motiver un refus d'accès à l'information sur la base d'une restriction facultative. Il s'agit de rétablir l'équilibre entre les parties et d'assurer la sauvegarde du principe d'accès à l'information et de la transparence des organismes publics.

166. Commission Paré, *préc.*, note 4, p. 34.

La Commission considère que la *Loi sur l'accès* devrait être modifiée afin de préciser que le délai prévu à l'article 47 pour répondre à une demande et motiver un refus sur la base d'une restriction facultative à l'accès est de rigueur et emporte déchéance. Ainsi, l'organisme qui ne respecterait pas le délai, prolongé ou non, prévu par la *Loi sur l'accès* pour soulever une restriction facultative serait forclos de le faire, sauf circonstances exceptionnelles qu'il devra démontrer.

Recommandation 15 : La Commission recommande de modifier la *Loi sur l'accès* afin de préciser que le délai prévu à l'article 47 pour répondre à une demande d'accès et motiver un refus sur la base d'une restriction facultative à l'accès est de rigueur et emporte déchéance.

Recommandation 16 : La Commission recommande qu'un organisme public ne puisse être relevé du défaut d'invoquer un motif de refus facultatif dans le délai de rigueur prévu pour répondre à une demande d'accès que dans des circonstances exceptionnelles, qu'il aurait le fardeau de démontrer à la Commission.

Recommandation 17 : La Commission recommande de modifier la *Loi sur la protection dans le secteur privé* afin de préciser que le délai prévu à l'article 32 pour répondre à une demande d'accès et motiver un refus sur la base d'une restriction facultative à l'accès est de rigueur et emporte déchéance.

Recommandation 18 : La Commission recommande qu'une entreprise ne puisse être relevée du défaut d'invoquer un motif de refus facultatif dans le délai de rigueur prévu pour répondre à une demande d'accès que dans des circonstances exceptionnelles, qu'elle aurait le fardeau de démontrer à la Commission.

2.3. LA REPRÉSENTATION PAR AVOCAT DEVANT LA COMMISSION.

Les demandes de révision ou d'examen de mésentente présentées à la section juridictionnelle de la Commission sont traitées suivant un processus quasi judiciaire. De ce fait, leur traitement doit respecter certaines exigences imposées par la *Loi sur le Barreau*[167] au regard de la représentation par avocat.

Notamment, l'article 128 (1) b) de la *Loi sur le Barreau* prévoit que seuls l'avocat en exercice ou le conseiller en loi peuvent, pour le compte d'autrui, « préparer et rédiger un avis, une requête, une procédure et tout autre document de même nature destiné à servir dans une affaire devant les tribunaux ». De plus, l'article 128 (2) a) accorde à l'avocat en exercice le droit exclusif de « plaider ou d'agir devant tout tribunal » pour le compte d'autrui.

Au cours des deux dernières années, plusieurs organismes publics et entreprises ont soulevé devant la Commission l'irrecevabilité des demandes de révision ou d'examen de mésentente parce qu'elles avaient été faites pour le compte d'une personne morale par un individu qui n'était pas avocat. Cette situation a mené au rejet de certaines demandes et a donné lieu à des décisions contradictoires de la Commission concernant la recevabilité des demandes. Deux décisions de la Commission portant sur la question de la représentation ont été portées en appel devant la Cour du Québec mais aucune décision n'a été rendue au moment de rédiger le présent rapport[168].

Rappelons que la Commission, dans son rapport quinquennal de 1997, demandait une modification à l'article 128 de la *Loi sur le Barreau* afin d'y préciser qu'il n'est pas du ressort exclusif de l'avocat de plaider ou d'agir devant elle comme cette loi le prévoit pour d'autres tribunaux administratifs[169]. La Commission de la culture, chargée d'étudier ce rapport, a choisi de ne pas se prononcer sur cette demande.

Pour sa part, le Groupe de travail sur le journalisme et l'avenir de l'information au Québec, qui a remis son rapport en janvier 2011[170], recommande que les journalistes puissent agir à tous égards devant la Commission même s'ils ne sont pas avocats.

La Commission reconnaît l'apport important des avocats dans notre système juridique. L'avocat joue un rôle essentiel et il serait souhaitable que tous les justiciables puissent bénéficier d'une telle représentation[171].

Recommandations 19 : Devant une telle situation et sous réserve des décisions qui doivent être rendues par la Cour du Québec, la Commission suggère qu'une réflexion soit engagée avec les partenaires impliqués afin d'analyser la pertinence et la nécessité d'assouplir les exigences de la *Loi sur le Barreau* à l'égard des demandes de révision et d'examen de mésentente qui lui sont présentées par des personnes morales.

167. L.R.Q., c. B-1, art. 1 l).

168. La décision finale de la Commission dans le dossier *S. J. c. Infrastructure Québec (Agence des partenariats public-privé)*, 2010 QCCAI 293 a fait l'objet d'un avis d'appel à la Cour du Québec. La décision interlocutoire de la Commission dans le dossier *Hydro-Québec* c. *W. L.*, 2011 QCCAI 29 a fait l'objet d'une requête pour permission d'en appeler qui n'a pas encore été tranchée par la Cour du Québec.

169. Par exemple, les personnes qui se présentent devant la Commission des relations de travail, la Commission des lésions professionnelles et la Régie du logement sont relevées, par la *Loi sur le Barreau*, de l'obligation d'être représentées par avocat, même si elles agissent « pour le compte d'autrui ».

170. Précité, note 148.

171. *Hydro-Québec, c. C. L.*, 2010 QCCAI 297, paragr. 52, citant la Cour suprême dans *Fortin c. Chrétien*, 2001 CSC 45, par. 54.

2.4. L'ASSUJETTISSEMENT DES ORGANISMES DONT LE FONDS SOCIAL FAIT PARTIE DU DOMAINE PUBLIC

Depuis les années 1960, les entreprises publiques ont connu un essor démontrant l'intention nette des différents gouvernements d'assurer à l'État québécois un rôle actif dans l'économie. Cette orientation s'est traduite par la mise sur pied de plusieurs organismes gouvernementaux à vocation économique. Par la suite, ces entreprises ont obtenu du législateur le pouvoir de créer différents types de filiales afin de rester compétitives, d'être flexibles et d'ouvrir de nouveaux marchés dans une économie en expansion mondialisée. Ce pouvoir a été accordé à de nombreuses entreprises publiques dont Hydro-Québec, la Société des alcools, Loto-Québec, la Caisse de dépôt et placement du Québec et, plus récemment, la société Investissement Québec.

À priori, une « entreprise publique doit être distinguée de tout autre organisme par le fait qu'elle est essentiellement affectée à une tâche économique d'exploitation, de production de biens et/ou services, et par extension de gestion commerciale, industrielle ou financière. »[172] Néanmoins, s'appuyant sur le fait que les citoyens du Québec sont les actionnaires et les propriétaires de ce type d'entreprise, le législateur la soumettait dès 1982 à l'empire général de la *Loi sur l'accès*. Ainsi, les « organismes » qui répondent à l'une ou l'autre des conditions du premier alinéa de l'article 4 de cette loi sont considérés comme des « organismes gouvernementaux ». Il s'agit des organismes « dont le gouvernement ou un ministre nomme la majorité des membres », dont le personnel est « nommé suivant la *Loi sur la fonction publique* (c. F-3.1.1) » ou, plus particulièrement pour les fins qui nous intéressent, ceux « dont le fonds social fait partie du domaine de l'État ».

Par le passé, l'interprétation de l'expression « dont le fonds social fait partie du domaine de l'État » a suscité de nombreuses interrogations en ce qui a trait à l'assujettissement de filiales des entreprises publiques à la *Loi sur l'accès*. Les tribunaux considéraient que le fonds social de la filiale avait cessé de faire partie du domaine de l'État pour appartenir en propre à la filiale. De ce fait, ces entités échappaient à la reddition de compte du régime prévu à la *Loi sur l'accès*, même si l'entreprise mère détenait la totalité des actions de sa filiale.

La Cour d'appel du Québec a renversé ce courant jurisprudentiel en 2002 et a mis fin à une saga judiciaire entreprise en 1997 en concluant qu'Hydro-Québec International, filiale dont les actions étaient détenues à 100 % par Hydro-Québec, était assujettie à la *Loi sur l'accès*. Laconiquement mais fermement, la Cour d'appel a fermé la porte à toute échappatoire lorsque l'État détient la totalité du fonds social d'une entreprise, fut-elle une filiale. Le juge Beauregard affirmait :

> « […] quelle que soit la définition qu'on peut, à l'occasion et suivant les circonstances, donner aux mots « fonds social », je suis d'avis que, pour les fins de la Loi, une société à fonds social dont toutes les actions sont détenues par l'État est un organisme dont le fonds social fait partie du domaine public. Et, en l'espèce, toutes les actions de Hydro-Québec International sont détenues par Hydro-Québec, et tous les biens de Hydro-Québec, y compris les actions de celle-ci dans Hydro-Québec International, sont la propriété de la province.
>
> Bref, pour les fins qui nous intéressent, les mots « fonds social qui fait partie du domaine public » […] renvoient […] aux actions détenues par l'État. La Loi trouve application à l'égard des sociétés dont l'État détient les actions. »[173]

172. Patrice GARANT, *Droit administratif*, 6e édition, Cowansville, Édition Yvon Blais, 2010, p. 111.
173. *Pouliot c. Cour du Québec*, 2002, CANLII 41158 (QC C.A.).

On peut tirer deux constats de cette jurisprudence de la Cour d'appel et de la Commission. D'abord que l'expression « fonds social » renvoie à la notion de capital-actions. Ensuite que la disposition ne s'applique qu'aux organismes dont le fonds social est détenu en totalité par l'État.

Par ailleurs, la question de l'application de la *Loi sur l'accès* aux entreprises publiques et à leurs filiales qui ne sont détenues qu'en partie par l'État demeure entière. Cette situation est préoccupante puisque ces organismes, s'ils ne satisfont pas aux autres conditions édictées à l'article 4 ou si leur loi constitutive ne prévoit pas leur assujettissement, échappent à la nécessaire transparence que commande la *Loi sur l'accès*.

Adoptée il y a bientôt trente ans et sans avoir été modifiée sous cet aspect, la *Loi sur l'accès* tient compte d'un mode plus traditionnel d'organisation de l'administration publique. Aujourd'hui, elle doit être revue pour l'adapter aux nouveaux modes de gestion financière et économique de l'appareil gouvernemental comprenant des partenariats, de la sous-traitance et la création de filiales.

En effet, les organismes qui sont issus de ces nouveaux modes de gestion sont bien souvent largement tributaires des fonds publics. Ils disposent même de sommes considérables. En outre, ils peuvent se voir confier des responsabilités traditionnellement dévolues aux organismes publics même s'ils établissent des partenariats avec l'entreprise privée pour ce faire.

L'accès à l'information est indispensable afin de garantir la participation éclairée des citoyens aux grands débats de la société québécoise entourant l'économie et les finances publiques. Dans les dernières années, on a vu croître la préoccupation des citoyens concernant l'utilisation et la gestion des fonds publics.

La Commission a recommandé à plusieurs reprises dans le passé, tant dans ses rapports quinquennaux de 1997[174] et de 2002[175] que dans plusieurs des avis relatifs à différents projets de loi[176], que les organismes dont le financement est largement assuré par l'État soient assujettis à la *Loi sur l'accès*.

Par analogie, l'article 5 de la *Loi sur le vérificateur général*[177] prévoit déjà qu'une « entreprise du gouvernement » est, aux fins de cette Loi :

> « 2° toute société à fonds social, dont plus de 50 % des actions comportant le droit de vote font partie du domaine de l'État ou sont détenues en propriété par un organisme public, par un organisme du gouvernement ou par une entreprise du gouvernement. »

La dernière intervention de la Commission sur le sujet a été réalisée à l'automne 2010 lors de l'étude du *Projet de loi 123 – Loi sur la fusion de la Société générale de financement du Québec et d'Investissement Québec*[178]. La Loi, sanctionnée le 10 décembre 2010, permet à *Investissement Québec* de constituer des filiales[179]. La proposition de la Commission d'assujettir à la *Loi sur l'accès* les filiales dont les actions sont détenues à plus de 50 % par la nouvelle société n'a pas été retenue. Les parlementaires ont toutefois indiqué que le débat entourant cette question devrait se faire

174. Précité, note 13, p. 77-79.

175. Précité, note 15, p. 53-55.

176. Voir notamment : COMMISSION D'ACCÈS À L'INFORMATION DU QUÉBEC, *Lettre concernant le projet de loi no 123 au ministre du Développement économique, de l'Innovation et de l'Exportation et à la Commission des finances publiques de l'Assemblée nationale*, 9 novembre 2010; COMMISSION D'ACCÈS À L'INFORMATION DU QUÉBEC, *Avis sur le Projet de loi no 137, Loi sur les appellations réservées et les termes valorisants – Commission de l'Agriculture, des Pêcheries et de l'Alimentation*, 2006, p. 7 et suiv.; COMMISSION D'ACCÈS À L'INFORMATION DU QUÉBEC, *Mémoire sur le Projet de loi no 61, Loi sur l'Agence des partenariats public-privé du Québec*, 2004, p. 9-11.

177. L.R.Q., c. V-5.01 ; cette analogie est faite d'ailleurs par la Cour d'appel dans *Pouliot c. Cour du Québec, préc.*, note 173, paragr. 8. Voir aussi la *Loi sur Services Québec*, L.R.Q., c. S-6.3, art. 15.

178. 1re session, 39e législature (Qc.).

179. *Loi Investissement Québec*, L.Q., 2010, c. 37, art. 6.

pour l'ensemble des filiales des organismes gouvernementaux dans le cadre des travaux entourant la révision quinquennale de la *Loi sur l'accès* prévue pour 2011[180].

Effectivement, afin d'éviter l'ambiguïté et l'instabilité juridique et pour favoriser une application uniforme du droit, il apparaît préférable de modifier la *Loi sur l'accès*, plutôt que de prévoir cet assujettissement dans les différentes lois sectorielles.

Évidemment, il faut rappeler que l'assujettissement d'un organisme aux obligations de transparence de la *Loi sur l'accès* ne signifie pas pour autant qu'il doive publiquement dévoiler tout ce qui le concerne. En effet, la *Loi sur l'accès* prévoit des restrictions qui permettent, à certaines conditions, de conserver confidentiels des renseignements industriels, financiers, commerciaux, scientifiques ou techniques. Ces outils sont assez souples pour s'adapter à la mission de chaque organisme gouvernemental.

Recommandations 20 : La Commission recommande que soit modifiée la *Loi sur l'accès* afin d'assujettir tous les organismes dont le fonds social est détenu à plus de 50 % par l'État.

180. QUÉBEC, ASSEMBLÉE NATIONALE, *Journal des débats parlementaires de la Commission des finances publiques*, 1re sess., 39e légis., 19 novembre 2010, « Étude détaillée du projet de loi no 123 – *Loi sur la fusion de la Société générale de financement du Québec et d'Investissement Québec* », vol. 41, no 96.

181. *Projet de loi n° 86, préc.*, note 16, art. 84.

182. L'article 85 de la *Loi sur la protection dans le secteur privé* est similaire à l'article de la *Loi sur l'accès*.

2.5. LES POUVOIRS D'ENQUÊTE ET L'IMMUNITÉ DES MEMBRES DE LA SECTION JURIDICTIONNELLE DE LA COMMISSION

Avant que les fonctions de la Commission ne soient scindées en deux sections distinctes – la section de surveillance et la section juridictionnelle – l'article 129 de la *Loi sur l'accès* s'appliquait à l'ensemble des membres de la Commission. Il se retrouvait alors dans la section générale de la loi intitulée « Fonctions et pouvoirs » et il se lisait ainsi :

> ***129.*** *La Commission, ses membres et toute personne qu'elle charge de faire enquête pour l'application de la présente* ***loi*** *sont investis, à cette fin, des pouvoirs et de l'immunité des commissaires nommés en vertu de la Loi sur les commissions d'enquête (chapitre C-37), sauf du pouvoir d'ordonner l'emprisonnement.*

La modification apportée à l'article 129 de la *Loi sur l'accès* en 2006[181] a reconduit, pour les membres de la section de surveillance de la Commission, les pouvoirs et l'immunité des commissaires nommés en vertu de la *Loi sur les commissions d'enquête*. Il se lit maintenant comme suit :

> ***129.*** *La Commission, ses membres et toute personne qu'elle charge de faire enquête pour l'application de la présente* ***section*** *sont investis, à cette fin, des pouvoirs et de l'immunité des commissaires nommés en vertu de la Loi sur les commissions d'enquête (chapitre C-37), sauf du pouvoir d'ordonner l'emprisonnement.*
>
> *Les enquêtes de la Commission sont faites selon un mode non contradictoire.*
>
> *Au terme d'une enquête, la Commission peut, après avoir fourni à l'organisme public l'occasion de présenter ses observations écrites, lui ordonner de prendre les mesures qu'elle juge appropriées*[182].

Comme on le constate, l'article 129 a donc été modifié, en ce qui a trait à la référence à la *Loi sur les commissions d'enquête*, tout simplement en remplaçant le mot ***loi*** par le mot ***section***. Depuis, le premier alinéa de l'article ne réfère plus qu'aux enquêtes menées pour l'application de la section II du chapitre IV de la *Loi sur l'accès* qui concerne la section de surveillance et il n'est pas reproduit à la section III portant sur le volet juridictionnel. Or, cette construction législative a créé une anomalie qui laisse planer de sérieux doutes sur les pouvoirs et l'immunité des commissaires affectés à la section juridictionnelle de la Commission.

Soulignons que les principaux pouvoirs coercitifs accordés par la *Loi sur les commissions d'enquête* sont les suivants :

- afin de découvrir la vérité, s'enquérir des choses dont l'investigation leur a été déférée, par tous moyens légaux qu'ils jugent les meilleurs;
- assister et présider à l'examen des témoins avec tous les pouvoirs d'un juge de la Cour supérieure en ce qui concerne la procédure de cet examen;
- assigner et requérir la comparution de toute personne dont le témoignage peut se rapporter au sujet de l'enquête;
- contraindre toute personne à déposer devant eux les documents qu'ils jugent nécessaires;
- exiger et recevoir le serment ou affirmation ordinaire de toute personne qui rend témoignage;
- et, quiconque refuse de prêter serment, omet ou refuse de répondre suffisamment à toutes les questions qui peuvent lui être faites ou refuse de témoigner commet un outrage au tribunal.

Par contre, la section juridictionnelle de la Commission est dotée des pouvoirs généraux prévus à l'article 141 de la *Loi sur l'accès* qui s'énonce ainsi :

> ***141.*** *La Commission a tous les pouvoirs nécessaires à l'exercice de sa compétence; elle peut rendre toute ordonnance qu'elle estime propre à sauvegarder les droits des parties et décider de toute question de fait ou de droit.*
>
> *Elle peut notamment ordonner à un organisme public de donner communication d'un document ou d'une partie de document, de s'abstenir de le faire, de rectifier, compléter, clarifier, mettre à jour ou effacer tout renseignement personnel ou de cesser un usage ou une communication de renseignements personnels.*

De prime abord, on pourrait penser que cet article comble l'absence de référence expresse à la *Loi sur les commissions d'enquête* pour accorder aux membres de la section juridictionnelle tous les pouvoirs prévus à cette loi. En effet, l'article 141 de la *Loi sur l'accès* est relativement large et accorde à la Commission tous les pouvoirs nécessaires à l'exercice de sa compétence, à savoir, décider des demandes de révision et d'examen de mésentente. Incidemment, cela inclurait les pouvoirs minimaux habituellement dévolus à un tribunal administratif quant à l'administration de la preuve et l'audition des témoins.

Toutefois, le législateur procède habituellement expressément lorsqu'il souhaite accorder des pouvoirs de commissaires enquêteurs à un organisme public. Il réfère alors à la *Loi sur les commissions d'enquête*. C'est la technique de rédaction la plus commune pour accorder de tels pouvoirs comme en témoignent maints exemples[183]. Citons ceux du Tribunal administratif du Québec et de la Commission des lésions professionnelles.

Tribunal administratif du Québec (TAQ)

> ***74.*** *Le Tribunal et ses membres sont investis des pouvoirs de l'immunité des commissaires nommés en vertu de la Loi sur les commissions d'enquête (chapitre C-37), sauf du pouvoir d'ordonner l'emprisonnement.*
>
> *Ils ont en outre tous les pouvoirs nécessaires à l'exercice de leurs fonctions; ils peuvent notamment rendre toutes ordonnances qu'ils estiment propres à sauvegarder les droits des parties.*
>
> *Ils ne peuvent être poursuivis en justice en raison d'un acte accompli de bonne foi dans l'exercice de leurs fonctions.*

Commission des lésions professionnelles (CLP)

> ***378.*** *La Commission des lésions professionnelles et ses commissaires sont investis des pouvoirs et de l'immunité des commissaires nommés en vertu de la Loi sur les commissions d'enquête (chapitre C-37), sauf du pouvoir d'ordonner l'emprisonnement.*
>
> *Ils ont en outre tous les pouvoirs nécessaires à l'exercice de leurs fonctions; ils peuvent notamment rendre toutes ordonnances qu'ils estiment propres à sauvegarder les droits des parties.*
>
> *Ils ne peuvent être poursuivis en justice en raison d'un acte accompli de bonne foi dans l'exercice de leurs fonctions.*

Il est intéressant de noter que le TAQ et la CLP disposent à la fois des pouvoirs de commissaires enquêteurs et d'un pouvoir plus général comme celui conféré à l'article 141 par la *Loi sur l'accès*. De même, la Régie du logement a demandé et obtenu, à l'automne 2010[184], un tel pouvoir général en complément aux pouvoirs de commissaires enquêteurs déjà dévolus aux régisseurs.

183. *Loi sur la justice administrative*, L.R.Q., c. J-3, art. 74 pour le Tribunal administratif du Québec; *Charte des droits et libertés de la personne*, L.R.Q., c. C-12, art. 112 et 113 pour la Commission des droits de la personne et des droits de la jeunesse; *Code du travail*, L.R.Q., c. C-27, art. 120 pour la Commission des relations de travail; *Loi sur les accidents du travail et les maladies professionnelles*, L.R.Q., c. A-3.001, art. 378 pour la Commission des lésions professionnelles; *Loi sur la Régie du logement*, L.R.Q., c. 8.1, art. 9.8 pour la Régie du logement.

184. *Loi modifiant la Loi sur la Régie du logement et diverses lois concernant le domaine municipal*, L.Q., c. 42, art. 26.

En principe, les juges des tribunaux administratifs disposent des pouvoirs coercitifs que la loi leur attribue expressément. Qu'arriverait-il si la compétence des commissaires de la section juridictionnelle de la Commission était remise en cause en ce qui a trait à l'exercice de ces pouvoirs ? La question mérite d'autant plus d'être soulevée quand les autres organismes exerçant des fonctions d'adjudication similaires à celles de la Commission ont reçu expressément les pouvoirs prévus à la *Loi sur les commissions d'enquête*.

En plus de pouvoirs coercitifs d'enquête, la *Loi sur les commissions d'enquête* confère aux membres de la section de surveillance, l'immunité et les privilèges des juges de la Cour supérieure, pour tout acte fait ou omis dans l'exécution de leurs devoirs. L'immunité des juges de la Cour supérieure est considérable puisqu'elle est, en principe, absolue dans l'exercice de leurs fonctions.

La seule immunité qui s'applique aux membres de la section juridictionnelle est celle accordée par l'article 113 de la *Loi sur l'accès* qui s'énonce ainsi :

> **113.** *Un membre de la Commission ou de son personnel ne peut être poursuivi en justice en raison d'un acte officiel accompli de bonne foi dans l'exercice de ses fonctions.*

Ce type de disposition correspond davantage à une immunité relative conditionnée par la bonne foi. Ce type d'immunité est plutôt relié aux activités de nature administrative plutôt qu'à l'exercice des fonctions d'adjudication d'un organisme. C'est ainsi que les membres affectés à la section de surveillance sembleraient mieux dotés au regard de l'immunité que les membres siégeant à la section juridictionnelle. Cela va à contresens. En effet, tout juge ne doit-il pas « être en mesure de travailler en toute indépendance et à l'abri de toute crainte… [et ne pas] être inquiété par des allégations de mauvaise foi, de préjudice ou d'autre chose semblable ? »[185].

Les modifications apportées en 2006 à l'article 129 de la *Loi sur l'accès* visaient à préciser que le processus d'enquête de la section de surveillance de la Commission se fait selon un mode non contradictoire et à tenir compte de la division de la Commission en deux sections distinctes.

Ces modifications ne cherchaient probablement pas à limiter les pouvoirs et l'immunité des membres de la section juridictionnelle. D'une disposition à caractère général, alors que les fonctions juridictionnelle et de surveillance de la Commission étaient unifiées, le premier alinéa de l'article 129 de la *Loi sur l'accès* est demeuré au chapitre de la surveillance, sans qu'une corrélation soit faite avec la section juridictionnelle lorsque la structure de la Commission a été scindée.

Dans ces circonstances, la Commission propose d'accorder aux membres de la section juridictionnelle des pouvoirs et une immunité similaires à leurs collègues de la section de surveillance et à d'autres membres de tribunaux administratifs.

Recommandation 21 : La Commission recommande que la *Loi sur l'accès* et, par concordance, la *Loi sur la protection dans le secteur privé* soient modifiées pour accorder explicitement à tous ses membres les pouvoirs et les immunités des commissaires nommés en vertu de la *Loi sur les commissions d'enquête*.

185. *Sirros v. Moore*, [1975] 1 Q.B. 118, p. 136, cité dans *Morier et Boily* c. Rivard, [1985] 2 R.C.S., 716, paragr. 96.

TABLE DES RECOMMANDATIONS

La protection des renseignements personnels à l'ère numérique

Recommandation 1 : La Commission recommande au législateur d'obliger les organismes publics et les entreprises à adopter des politiques de confidentialité simplifiées présentant, en termes clairs et compréhensibles, une vue d'ensemble de leurs engagements en matière de protection des renseignements personnels.

Recommandation 2 : La Commission recommande au législateur d'imposer aux organismes publics et aux entreprises l'utilisation de pictogrammes de protection informant les citoyens de leurs engagements en matière de protection des renseignements personnels.

Recommandation 3 : La Commission recommande au législateur d'obliger les organismes publics et les entreprises à signaler la présence de mécanismes susceptibles d'identifier ou de localiser une personne physique lors de l'utilisation de leurs produits.

Recommandation 4 : La Commission rappelle aux organismes publics et aux entreprises d'intégrer les principes de protection des renseignements personnels dès la conception de leurs biens et services et de les appliquer tout au long du cycle de vie de ces renseignements.

Les natifs du numérique

Recommandation 5 : La Commission recommande que le réseau de l'éducation développe des programmes scolaires au niveau du primaire et du secondaire visant à éduquer les jeunes aux enjeux des TI et du Web 2.0.

Recommandation 6 : La Commission invite le législateur à s'interroger sur la pertinence de modifier les lois de protection du consommateur ou des renseignements personnels notamment pour interdire le profilage des jeunes dans les environnements électroniques.

La déclaration des failles de sécurité

Recommandation 7 : La Commission recommande que la *Loi sur l'accès et la Loi sur la protection dans le secteur privé* soient modifiées par l'ajout d'une obligation de lui déclarer les failles de sécurité qui surviennent dans les organismes publics et les entreprises et qui impliquent des renseignements personnels.

Recommandation 8 : La Commission recommande que soient déterminées les conditions et les modalités conduisant à déclarer des failles de sécurité impliquant des renseignements personnels.

Recommandation 9 : La Commission recommande que lui soit confié le pouvoir d'ordonner aux organismes publics et aux entreprises d'aviser, aux conditions qu'elle déterminera, les personnes concernées d'une faille de sécurité impliquant leurs renseignements personnels et de prendre les mesures qu'elle jugera nécessaires pour assurer une protection adéquate de leurs renseignements personnels.

La fontion de responsable dans le secteur privé

Recommandation 10 : La Commission recommande que la *Loi sur la protection dans le secteur privé* prévoit la création de la fonction de responsable de l'accès et de la protection des renseignements personnels.

Recommandation 11 : La Commission recommande que la fonction de responsable dans le secteur privé puisse être déléguée par l'entreprise à une personne œuvrant au sein de l'entreprise.

Le passage de la transparence au gouvernement ouvert

Recommandation 12 : La Commission recommande que l'application du *Règlement sur la diffusion* soit élargie aux organismes publics actuellement exemptés.

Recommandation 13 : La Commission recommande que les organismes publics soient assujettis à un régime élargi d'ouverture des données publiques qui permette l'accès libre à l'ensemble de l'information gouvernementale utile aux citoyens.

Recommandation 14 : La Commission recommande qu'un débat public regroupant l'ensemble des partenaires (parlementaires, citoyens, associations, experts) soit instauré afin d'établir un modèle pour l'ouverture du gouvernement québécois fondé sur la participation et la collaboration.

Le délai pour motiver un refus d'accès à un renseignement

Recommandation 15 : La Commission recommande de modifier la *Loi sur l'accès* afin de préciser que le délai prévu à l'article 47 pour répondre à une demande d'accès et motiver un refus sur la base d'une restriction facultative à l'accès est de rigueur et emporte déchéance.

Recommandation 16 : La Commission recommande qu'un organisme public ne puisse être relevé du défaut d'invoquer un motif de refus facultatif dans le délai de rigueur prévu pour répondre à une demande d'accès que dans des circonstances exceptionnelles, qu'il aurait le fardeau de démontrer à la Commission.

Recommandation 17 : La Commission recommande de modifier la *Loi sur la protection dans le secteur privé* afin de préciser que le délai prévu à l'article 32 pour répondre à une demande d'accès et motiver un refus sur la base d'une restriction facultative à l'accès est de rigueur et emporte déchéance.

Recommandation 18 : La Commission recommande qu'une entreprise ne puisse être relevé du défaut d'invoquer un motif de refus facultatif dans le délai de rigueur prévu pour répondre à une demande d'accès que dans des circonstances exceptionnelles, qu'elle aurait le fardeau de démontrer à la Commission.

La représentation par avocat devant la Commission

Recommandations 19 : Devant une telle situation et sous réserve des décisions qui doivent être rendues par la Cour du Québec, la Commission suggère qu'une réflexion soit engagée avec les partenaires impliqués afin d'analyser la pertinence et la nécessité d'assouplir les exigences de la *Loi sur le Barreau* à l'égard des demandes de révision et d'examen de mésentente qui lui sont présentées par des personnes morales.

L'assujettissement des organismes dont le fonds social fait partie du domaine public

Recommandations 20 : La Commission recommande que soit modifiée la *Loi sur l'accès* afin d'assujettir tous les organismes dont le fonds social est détenu à plus de 50 % par l'État.

Les pouvoirs d'enquête et l'immunité des membres de la section juridictionnelle de la Commission

Recommandation 21 : La Commission recommande que la *Loi sur l'accès* et, par concordance, la *Loi sur la protection dans le secteur privé* soient modifiées pour accorder explicitement à tous ses membres les pouvoirs et les immunités des commissaires nommés en vertu de la *Loi sur les commissions d'enquête*.

BIBLIOGRAPHIE

BIBLIOGRAPHIE

Lois et Règlements québécois

Charte de la langue française, L.R.Q., c. C-11.

Charte des droits et libertés de la personne, L.R.Q., c. C-12.

Code civil du Québec, L.R.Q., c. C-1991.

Code d'éthique et de déontologie des membres de l'Assemblée nationale, L.R.Q., c. C-23.1.

Code des professions, L.R.Q., c. C-26.

Code du travail, L.R.Q., c. C-27.

Loi concernant le cadre juridique des technologies de l'information, L.R.Q., c. C-1.1.

Loi Investissement Québec, L.Q., 2010, c. 37.

Loi modifiant la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels et d'autres dispositions législatives, projet de loi n° 86, (sanctionné – 14 juin 2006), 2ème sess., 37e légis. (Qc).

Loi modifiant la Loi sur la Régie du logement et diverses lois concernant le domaine municipal, L.Q., c. 42.

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

Loi sur l'administration publique, L.R.Q., c. A-6.01.

Loi sur la fusion de la Société générale de financement du Québec et d'Investissement Québec, projet de loi n° 123, (sanctionné – 10 décembre 2010) 1ère sess., 39e légis. (Qc).

Loi sur la justice administrative, L.R.Q., c. J-3.

Loi sur la protection des renseignements personnels dans le secteur privé, L.R.Q., chapitre P-39.1.

Loi sur la protection du consommateur, L.R.Q., c. P-40.1.

Loi sur la Régie du logement, L.R.Q., c. 8.1.

Loi sur la transparence et l'éthique en matière de lobbyisme, L.R.Q., c. T-11.011.

Loi sur l'équité salariale, L.R.Q., c. E-12.001.

Loi sur le Barreau, L.R.Q., c. B-1.

Loi sur le vérificateur général, L.R.Q., c. V-5.01.

Loi sur les accidents du travail et les maladies professionnelles, L.R.Q., c. A-3.001.

Loi sur Services Québec, L.R.Q., c. S-6.3.

Règlement sur la diffusion de l'information et sur la protection des renseignements personnels, c. A-2.1, r. 0.2.

Autres textes législatifs

California Civil Code

Children's Online Privacy Protection Act, 15 U.S.C.

Directive 2009/136/CE du Parlement européen et du Conseil du 25 novembre 2009 modifiant la directive 2002/22/CE concernant le service universel et les droits des utilisateurs au regard des réseaux et services de communications électroniques, la directive 2002/58/CE concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques et le règlement (CE) n°2006/2004 relatif à la coopération entre les autorités nationales chargées de veiller à l'application de la législation en matière de protection des consommateurs, Journal officiel de l'Union européenne, n° L 337 du 18 décembre 2009, pp. 11-36.

Loi modifiant la Loi sur la protection des renseignements personnels et les documents électroniques, projet de loi C-29, (dépôt et 1ère lecture – 25 mai 2010), 3e sess., 40e légis. (Can.).

Loi sur la protection des fonctionnaires divulgateurs d'actes répréhensibles, L.C. 2005, c. 46.

Loi sur la protection des renseignements personnels et les documents électroniques, L.C. 2000, ch. 5.

Personal Information Protection Act, S.A. 2003, c. P-6.5.

Personal Information Protection Act, S.B.C., 2003, c. 63.

Personal Information Protection Act Regulation, Alta, Reg. 366/2003.

15 U.S.C. Sec. 45.

Jurisprudences

Association canadienne pour la légitime défense c. Québec (Ministère de la Sécurité publique), 2010 QCCAI 209.

Fortin c. Chrétien, 2001 CSC 45.

Hydro-Québec, c. C. L., 2010 QCCAI 297.

Hydro-Québec c. W. L., 2011 QCCAI 29.

Ministère de la Justice c. Schulze, [2000] C.A.I. 413 (C.Q.)

Ministère de la Sécurité publique c. Joncas, J.E. 99-1653 (C.Q.).

Pouliot c. Cour du Québec, 2002, CANLII 41158 (QC C.A.).

Service Anti-Crime des Assureurs et Assurances générales des Caisses Desjardins c. Ménard, [2004] C.A.I. 630 (C.Q.).

Sirros v. Moore, [1975] 1 Q.B. 118.

S. J. c. Infrastructure Québec (Agence des partenariats public-privé), 2010 QCCAI 293.

Morier et Boily c. Rivard, [1985] 2 R.C.S. 716.

Livres, Ouvrages collectifs et Articles

CHASSIGNEUX, C., *Guide pour l'élaboration d'une politique de confidentialité*, Montréal, Chaire L.R Wilson sur le droit des technologies de l'information et du commerce électronique, 2008.

DAVIES, A. et D. LITHWICK,

- *Gouvernement 2.0 et accès à l'information – Le point sur la divulgation proactive et le libre accès aux données au Canada*, Publication n° 2010-14-F, Ottawa, Bibliothèque du Parlement, avril 2010.
- *Gouvernement 2.0 et accès à l'information – Le point sur la divulgation proactive et le libre accès aux données aux États-Unis et dans d'autres pays*, Publication n° 2010-15-F, Ottawa, Bibliothèque du Parlement, avril 2010.

DORAY, R. et F. CHARRETTE, *Accès à l'information*, vol. 1, Cowansville, Les Éditions Yvon Blais, 2010.

DUPONT, B. et E. AIMEUR, « Les multiples facettes du vol d'identité », (2010) vol. LXIII, *Revue internationale de criminologie et de police technique et scientifique*, 177.

GARANT, P., *Droit administratif,* 6e édition, Cowansville, Édition Yvon Blais, 2010.

GAUTRAIS, V., « Les contrats de cyberconsommation sont presque tous illégaux! », (2005) *Revue du Notariat* 617.

GAUTRAIS, V. et P. TRUDEL, *Circulation des renseignements personnels et Web 2.0*, Montréal, Éditions Thémis, 2010.

LENHART, A., K. PURCELL, A. SMITH and K. ZICKUHR, *Social Media & Mobile Internet Use Among Teens and Young Adults*, February 2010.

LIVINGSTONE, S., K. OLAFSSON and E. STAKSRUD, *Social Networking, Age and Privacy*, April 2011.

NEILL, A., Libérer l'information : de la divulgation réactive à la divulgation proactive, Discours prononcé devant l'*Association sur l'accès et la protection de l'information*, Québec, 20 avril 2010

OBERDORFF, H., *La démocratie à l'ère numérique*, Grenoble, Presses Universitaires de Grenoble, 2010.

O'REILLY, T., « Government as a Platform », dans Daniel LATHROP and Laurel RUMA, *Open Government – Collaboration, Transparency, and Participation in Practice*, Sebastopol (California), O'Reilly Media Inc., 2010.

OUIMET, A., « Accès à l'information : vers une plus grande transparence », (2004) vol. 6, n° 2 *Éthique publique* 23.

ROBERTSON, L., « La fraude d'identité : connaissez-vous ? », dans *Congrès annuel du Barreau du Québec 2009*, Service de la formation continue du Barreau du Québec, 2009.

ROY, R., « Les 12-24 ans : utilisateurs extrêmes d'Internet et des TI », (2009) vol. *7*, n° 1 *Réseau CÉFRIO* 3.

Documents gouvernementaux et autres

ASSOCIATION FRANÇAISE DU MULTIMÉDIA MOBILE, « Indicateurs clés du multimédia mobile et marketing par SMS », Communiqué de presse, 21 juin 2010.

ASSOCIATION SUR L'ACCÈS ET LA PROTECTION DE L'INFORMATION, *Guide pratique sur l'accès et la protection de l'information*, vol. 1, Cowansville, Les Éditions Yvon Blais, 2010.

AUSTRALIAN GOVERNMENT INFORMATION MANAGEMENT OFFICE,

- *Government Response to the Report of the Government 2.0 Taskforce*, May 2010.
- *Declaration of Open Government*, July 16, 2010.

CABINET DU PRÉSIDENT DU CONSEIL DU TRÉSOR ET MINISTRE DE LA PORTE D'ENTRÉE DE L'ASIE-PACIFIQUE, *Le renforcement du gouvernement ouvert*, Communiqué, 18 mars 2011.

CABINET OFFICE, *The Coalition : our programme for government*, London, HM Government, May 2010.

CALIFORNIA OFFICE OF PRIVACY PROTECTION, *Recommended Practices on Notice of Security Breach Involving Personal Information*, October 2003 (last revised June 2009).

CAVOUKIAN, A.,

- « La protection intégrée de la vie privée – Les sept principes fondamentaux », août 2009 (modifié en janvier 2011).
- « L'accès à l'information intégré- Les sept principes fondamentaux », avril 2010.

CENTER FOR TECHNOLOGY POLICY RESEARCH, *Open Government, some next steps for the UK*, London, Center for Technology Policy Research, May 2010.

CENTRE FRANCOPHONE D'INFORMATISATION DES ORGANISATIONS, « Un fort potentiel pour l'Internet mobile au Québec », (2010) vol. 1 n° 3 *NeTendances* 14.

CHIEF SECRETARY TO THE TREASURY, *Putting the Frontline First : Smarter Government*, London, HM Government, December 2009.

COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA,

- *Rapport annuel au Parlement 2009 – Rapport sur la Loi sur la protection des renseignements personnels et sur les documents électroniques*, Ottawa, Ministre des Travaux publics et des Services gouvernementaux Canada, 2010.
- *Ébauche – Rapport sur les consultations de 2010 du Commissariat à la protection de la vie privée du Canada sur le suivi, le profilage et le ciblage en ligne, et l'informatique dans les nuages*, octobre 2010.
- *Rapport sur les consultations de 2010 du Commissariat à la protection de la vie privée du Canada sur le suivi, le profilage et le ciblage en ligne et sur l'infonuagique*, mai 2011.

COMMISSION D'ACCÈS À L'INFORMATION DU QUÉBEC

- *Le consentement des personnes à la communication de renseignements nominatifs les concernant*, Politique adoptée le 6 mars 1985.
- *Une vie privée mieux respectée, un citoyen mieux informé – Rapport sur la mise en œuvre de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels et de la Loi sur la protection des renseignements personnels dans le secteur privé*, Québec, Commission d'accès à l'information du Québec, 1987.
- *Un passé éloquent, un avenir à protéger - Rapport sur la mise en œuvre de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels et de la Loi sur la protection des renseignements personnels dans le secteur privé*, Québec, Commission d'accès à l'information du Québec, 1992.

- *Vie privée et transparence administrative au tournant du siècle, Rapport sur la mise en œuvre de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels et de la Loi sur la protection des renseignements personnels dans le secteur privé*, Québec, Commission d'accès à l'information du Québec, 1997.
- *Inforoute, attention zone scolaire*, 1999.
- *Une réforme de l'accès à l'information : le choix de la transparence, Rapport sur la mise en œuvre de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels et de la Loi sur la protection des renseignements personnels dans le secteur privé*, Québec, Commission d'accès à l'information du Québec, 2002.
- *Mémoire sur le Projet de loi no 61, Loi sur l'Agence des partenariats public-privé du Québec*, 2004.
- *Avis sur le Projet de loi no 137, Loi sur les appellations réservées et les termes valorisants – Commission de l'agriculture, des pêcheries et de l'alimentation*, 23 février 2006.
- *La technologie d'identification par radiofréquence (RFID) doit-on s'en méfier ?*, mai 2006.
- *Rapport annuel de gestion 2008-2009*, Québec, Commission d'accès à l'information du Québec, 2009.
- *Plan stratégique 2009-2012*, Québec, Commission d'accès à l'information du Québec, 2009.
- *Aide-mémoire à l'intention des organismes publics et des entreprises – Que faire en cas de perte ou de vol de renseignements personnels ?*, Avril 2009.
- *Rapport annuel de gestion 2009-2010*, Québec, Commission d'accès à l'information du Québec, 2010.
- *Lettre concernant le projet de loi no 123 au ministre du Développement économique, de l'Innovation et de l'Exportation et à la Commission des finances publiques de l'Assemblée nationale*, 9 novembre 2010.

COMMISSION D'ÉTUDE SUR L'ACCÈS DU CITOYEN À L'INFORMATION GOUVERNEMENTALE ET SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS, *Information et liberté : rapport de la Commission d'étude sur l'accès du citoyen à l'information gouvernementale et sur la protection des renseignements personnels*, Québec, Direction générale des publications gouvernementales, Ministère des communications, 1981.

COMMITTEE ON CYBER-SAFETY, *Cybersafety issues affecting children and young people*, Canberra (Australia), 21 March 2011.

COMITÉ PERMANENT DE L'ACCÈS À L'INFORMATION, DE LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET DE L'ÉTHIQUE, *Rapport 6 - Système de coordination des demandes d'accès à l'information*, Ottawa, Chambre des communes, 39e Législature, 2e Session, 7 mai 2008.

CONSEIL DE L'EUROPE, *Recommandation CM/Rec(2010)13 du Comité des Ministres aux États membres sur la protection des personnes à l'égard du traitement automatisé des données à caractère personnel dans le cadre du profilage*, 23 novembre 2010.

EUROSTAT, « Information society statistics », September 2010.

EXECUTIVE OFFICE OF THE PRESIDENT, *Open Government Directive – Memorandum for the Heads of Executive Departments and Agencies*, 8 December 2009.

FEDERAL TRADE COMMISSION,

- *Online Privacy : A Report to Congress*, June 1998.
- *Self-Regulation and Privacy Online : A Report to Congress*, July 1999.
- *Privacy Online : A Report to Congress*, June 1998.
- *Privacy Online : Fair Information Practices in the Electronic Marketplace – A Report to Congress*, May 2000.
- *Protecting Consumer Privacy in an Era of Rapid Change – Preliminary FTC Staff Report*, December 2010.
- GROUPE DE TRAVAIL « ARTICLE 29 » SUR LA PROTECTION DES DONNÉES,
- *Avis 10/2004 sur « Dispositions davantage harmonisées en matière d'informations*, WP100, 25 novembre 2004.
- *Avis 2/2009 sur la protection des données à caractère personnel de l'enfant (Principes généraux et cas particulier des écoles)*, WP 160, 11 février 2009.
- *Avis 2/2010 sur la publicité comportementale en ligne*, WP 171, 22 juin 2010.

GROUPE DE TRAVAIL DES COMMISSAIRES À LA VIE PRIVÉE ET DES DÉFENSEURS CANADIENS DES ENFANTS ET DES JEUNES, *Il devrait y avoir une loi : les sauts périlleux de la vie privée des enfants au 21e siècle*, Document de réflexion, 19 novembre 2009.

GROUPE DE TRAVAIL SUR LE JOURNALISME ET L'AVENIR DE L'INFORMATION AU QUÉBEC, *L'information au Québec : un intérêt public*, janvier 2011.

GOVERNMENT 2.0 TASKFORCE, *Engage : Getting on with Government 2.0 – Report of the Government 2.0 Taskforce*, Canberra, Governement 2.0 Taskforce, December 2009.

INFORMATION AND PRIVACY COMMISSIONER OF ONTARIO,

- *What to do if a privacy breach occurs: Guidelines for government organizations,* December 2006.
- *Response to the FTC Framework for Protection Consumer Privacy in an Era of Rapid Change*, January 2011.

MANITOBA OMBUDSMAN, *Reporting a Privacy Breach To Manitoba Ombudsman*, March 2007.

OFFICE OF THE ATTORNEY GENERAL, *The Freedom of Information Act (FOIA) Guidelines*, 19 Mars 2009.

OFFICE OF THE PRIVACY COMMISSIONER OF AUTRALIA, *Guide to handling personal information security breaches*, August 2008.

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER FOR BRITISH COLUMBIA,

- *Breach Notification Assesment Tool*, December 2006.
- *Keys Steps in Responding to Privacy Breaches*, June 2008.

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER OF ALBERTA, *Breach Report Form*, May 2010 (revised).

ORGANISATION DE COOPÉRATION ET DE DÉVELOPPEMENT ÉCONOMIQUES, « La modernisation du secteur public : l'administration ouverte - Synthèse », (2005) *L'Observateur* 1.

ORGANISATION DE COOPÉRATION ET DE DÉVELOPPEMENT ÉCONOMIQUES, *Simplifier les notices d'information sur la protection de la vie privée : rapport et recommandations de l'OCDE*, DSTI/ICCP/REG(2006)5/FINAL, 24 juillet 2006.

THE PUBLIC INTEREST ADVOCACY CENTRE, *All in the Data Family : Children's Privacy Online*, september 2008.

Résolution concernant l'accréditation de nouvelles autorités, Résolution adoptée lors de la 24e Conférence internationale des commissaires à la protection des données et de la vie privée, Cardiff (Royaume-Uni), 2002.

Résolution visant l'amélioration des pratiques d'information en matière de protection des données et de la vie privée, Résolution adoptée lors de la 25e Conférence internationale des commissaires à la protection des données et de la vie privée, Sydney (Australie), 12 septembre 2003.

Résolution sur la protection intégrée de la vie privée, Résolution adoptée lors de la 32e Conférence internationale des commissaires à la protection des données et de la vie privée, Jérusalem (Israël), octobre 2010.

Résolution sur la transparence gouvernementale, Résolution des commissaires canadiens de l'accès à l'information et à la protection de la vie privée, Whitehorse (Yukon), 1er septembre 2010.

Résolution sur la vie privée des enfants en ligne, Résolution adoptée lors de la 30e Conférence internationale des commissaires à la protection des données et de la vie privée, Strasbourg (France), 17 octobre 2008.

SAINT-LAURENT, J., « Les droits de l'enfant face au développement des technologies de l'information et de la communication », Allocution prononcée lors du *Séminaire international des droits de l'enfant*, Tunis (Tunisie), 24 novembre 2009.

WHITE HOUSE, *Transparency and Open Government – Memorandum for the Heads of Executive Departments and Agencies*, 21 January 2009.

Sites Web

BARBIE, http://www.fr.barbie.com.

CLUB PENGUIN, http://www.clubpenguin.com/fr.

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, « Espaces Jeunes », http://www.jeunes.cnil.fr.

COMMISARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, « mavie privée. monchoix. mavie », http://www.youthprivacy.ca/fr.

CREATIVE COMMONS, creativecommons.org.

DATA.GOV, « Raw Data Catalog », http://explore.data.gov/catalog/raw.

DATA.GOV.AU, http://data.gov.au.

DATA LOSS BAROMETER, http://www.datalossbarometer.com.

DATALOSSdb, http://datalossdb.org.

FACEBOOK, http://www.facebook.com.

GOUVERNEMENT OUVERT, http://ouvert.gc.ca.

IBM, http://www.ibm.com.

IDENTITY THEFT RESOURCE CENTER, http://www.idtheftcenter.org.

JEUNESSE J'ÉCOUTE, http://jeunessejecoute.ca.

MINISTÈRE DES SERVICES GOUVERNEMENTAUX DU QUÉBEC,

- « Gouvernement en ligne – Cadre légal », http://www.msg.gouv.qc.ca/gel/cadre_legal.html.
- « Gouvernement en ligne – Définition », http://www.msg.gouv.qc.ca/gel/index.html.

MONTRÉAL OUVERT, « À propos », http://montrealouvert.net/a-propos.
MY SPACE, http://myspace.com.
NATIONAL CONFERENCE OF STATE LEGISLATURE, http://www.ncsl.org.
NYMITY, http://www.nymity.com.
RÉSEAU ÉDUCATION-MÉDIAS, http://www.education-medias.ca.
TOGETHERVILLE, http://togetherville.com.
TRUSTE, http://www.truste.com.
TWITTER, http://twitter.com.
WEB AVERTI, http://www.webaverti.ca.
YOUTUBE, http://www.youtube.com.

ANNEXES

ANNEXE 1 : RECOMMANDATIONS DU RAPPORT QUINQUENNAL 2002

RECOMMANDATION N° 1

La Commission recommande donc le maintien de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels. Toutefois, elle recommande que des modifications importantes soient apportées rapidement, particulièrement au chapitre de l'accès à l'information.

RECOMMANDATION N° 2

La Commission invite le législateur à s'interroger sur la pertinence de modifier la Charte des droits et libertés de la personne afin que le droit à l'information puisse jouir d'une protection équivalente à celle des libertés et droits fondamentaux, des droits politiques ou des droits judiciaires.

RECOMMANDATION N° 3

Afin de favoriser une meilleure compréhension des motifs à l'origine d'un refus de communiquer un document, la Commission recommande que l'article 50 de la Loi sur l'accès soit modifié de façon à obliger le responsable de l'accès à indiquer au demandeur, lorsque le contexte s'y prête, quel préjudice la communication du document pourrait engendrer, quel est le processus décisionnel actuellement en cours et à quel moment le document pourra être accessible.

RECOMMANDATION N° 4

La Commission recommande que le ministre des Relations avec les citoyens et de l'Immigration entreprenne, en collaboration avec des responsables de l'accès aux documents, des travaux de réflexion devant mener à l'établissement de directives ou d'outils d'aide à la décision pour soutenir les responsables lorsque ces derniers doivent exercer un pouvoir discrétionnaire conduisant au refus de communiquer un document.

RECOMMANDATION N° 5

Afin de faciliter l'accès aux documents détenus par les organismes publics, la Commission propose que chaque organisme public ait l'obligation d'adopter une politique de publication automatique de l'information.

RECOMMANDATION N° 6

Chaque organisme public devrait avoir l'obligation d'adopter un Plan de publication de l'information. Devrait automatiquement être publié ou diffusé tout document qui serait de la nature de ceux décrits dans ce Plan.

RECOMMANDATION N° 7

La Commission recommande également que les organismes publics aient l'obligation de dresser un Index général des documents. Cet index remplacerait l'actuelle liste de classement tenue en vertu de l'article 16 de la Loi sur l'accès. Il permettrait de connaître quelle information est détenue par chaque organisme.

RECOMMANDATION N° 8

La Commission invite le législateur à examiner la possibilité de rendre accessibles les avis et les recommandations dès que le processus décisionnel est achevé. Cette approche aurait l'avantage d'accorder aux avis et aux recommandations le même traitement que les analyses et, surtout, elle tiendrait compte du désir de plus en plus manifeste du citoyen de participer aux grands débats de la société.

RECOMMANDATION N° 9

La Commission recommande que les responsables de l'accès aux documents aient l'obligation d'évaluer le préjudice qui pourrait vraisemblablement découler de la communication d'un avis ou d'une recommandation. À cet effet, le responsable devrait pouvoir compter sur des outils d'aide à la décision élaborés par le ministre des Relations avec les citoyens et de l'Immigration.

RECOMMANDATION N° 10

La Commission recommande donc aux organismes publics d'évaluer l'ensemble des tâches effectuées par le responsable de l'accès et, en tenant compte des résultats, de consacrer les ressources humaines, financières et matérielles requises.

RECOMMANDATION N° 11

La Commission recommande donc que les responsables de l'accès aux documents puissent avoir la possibilité, dès leur entrée en fonction, de suivre une formation portant sur la Loi sur l'accès. Une formation continue devrait également être offerte aux responsables. Le ministre des Relations avec les citoyens et de l'Immigration devrait être responsable de la mise en œuvre de ces programmes de formation.

Puisque les technologies de l'information sont des outils indispensables à une meilleure diffusion de l'information et à un traitement efficace et rapide des demandes d'accès, la formation dispensée aux responsables de l'accès aux documents devrait également inclure ces sujets.

RECOMMANDATION N° 12

La Commission recommande que la Loi sur l'accès soit modifiée afin de prévoir que le rapport annuel d'un organisme public doit contenir un rapport du responsable de l'accès aux documents concernant ses activités pour l'année écoulée.

RECOMMANDATION N° 13

La Commission recommande que le ministre des Relations avec les citoyens et de l'Immigration puisse assumer un fort leadership auprès d'un réseau de responsables de l'accès aux documents et, qu'à cet égard, il ait entre autres l'obligation de voir à la formation de ces responsables.

RECOMMANDATION N° 14

La Commission recommande que le ministère des Relations avec les citoyens et de l'immigration fasse la promotion de l'utilisation d'outils de suivi communs visant à obtenir toute l'information pertinente sur la gestion des demandes d'accès à des documents.

RECOMMANDATION N° 15

La Commission recommande l'adoption des dispositions concernant les ordres professionnels contenues dans le Projet de loi n° 122.

RECOMMANDATION N° 16

La Commission recommande que soient assujettis tous les organismes dont le financement est largement assuré par l'État.

RECOMMANDATION N° 17

La Commission réitère donc sa recommandation de réviser la définition d'organisme municipal qui apparaît à la Loi sur l'accès afin de prendre en compte la composition du conseil d'administration et la provenance des fonds.

RECOMMANDATION N° 18

Dans un tel contexte, la Commission renouvelle la recommandation formulée dans le Rapport quinquennal de 1997, selon laquelle toute personne devrait avoir un droit d'accès aux renseignements qui concernent un établissement d'enseignement privé visé par le deuxième paragraphe de l'article 6 de la Loi sur l'accès.

RECOMMANDATION N° 19

La Commission propose donc à nouveau la diminution des délais prévus aux articles 30, 33, 35 et 37 de la loi.

RECOMMANDATION N° 20

La Commission propose à nouveau de modifier l'article 30 afin d'y prévoir que le responsable de l'accès ne peut refuser l'accès à une décision ou un décret du Conseil exécutif ou une décision du Conseil du trésor qui datent de plus de vingt ans.

RECOMMANDATION N° 21

La Commission souhaite que le législateur ramène le délai de 25 ans prévu à l'article 33 à un délai de rétention de 15 ans.

RECOMMANDATION N° 22

Le délai de 15 ans prévu à l'article 35 de la loi devrait être réduit à un délai de 10 ans.

RECOMMANDATION N° 23

À défaut de rendre accessibles les avis et les recommandations dès que la décision qui en découle est rendue, la Commission recommande que le délai de rétention de 10 ans prévu à l'article 37 soit ramené à 5 ans.

RECOMMANDATION N° 24

La Commission recommande à nouveau que la requête pour permission d'en appeler soit abolie, sauf lorsque l'appel porte sur une décision finale interlocutoire à laquelle la décision finale ne peut remédier.

RECOMMANDATION N° 25

La Commission recommande à nouveau que soient modifiés les articles 61 de la Loi sur le secteur privé et 147 de la Loi sur l'accès afin d'éviter la présentation de requêtes pour permission d'en appeler tant que la Commission n'a pas entendu l'ensemble de la preuve et rendu une décision finale à ce propos.

RECOMMANDATION N° 26

La Commission recommande à nouveau que la personne qui a déposé une demande de révision ou une demande d'examen de mésentente auprès de la Commission ne puisse pas être condamnée aux dépens par la Cour du Québec si la décision de la Commission est portée en appel par une autre partie.

RECOMMANDATION N° 27

Afin de reconnaître un exercice complet du droit d'accès, un organisme public qui porte en appel une décision rendue par la Commission qui lui est défavorable devrait donc prendre en charge tous les frais judiciaires et extrajudiciaires de la personne physique à qui la Commission a donné raison.

RECOMMANDATION N° 28

La Commission recommande à nouveau d'uniformiser les dispositions pénales de la Loi sur l'accès et de la Loi sur le secteur privé. Les articles 158 à 162 de la Loi sur l'accès devraient être reformulées afin d'assujettir à un régime des responsabilité stricte les infractions qui y sont décrites.

Par ailleurs, le montant des amendes prévu par ces deux lois devrait également être équivalent. De plus, une disposition pénale devrait être ajoutée à la Loi sur le secteur privé afin que puisse être sanctionné le non-respect des ordonnances rendues à la suite d'une enquête.

Finalement, la défense de bonne foi reconnue à l'article 163 devrait céder sa place à une preuve de diligence raisonnable.

RECOMMANDATION N° 29

La Commission recommande que soit ajouté à la Loi sur l'accès une disposition qui stipulerait que l'intérêt de l'enfant doit prévaloir lorsqu'une personne y ayant droit demande accès au dossier de cet enfant.

RECOMMANDATION N° 30

La Commission recommande que le législateur clarifie la Loi sur l'accès et la Loi sur le secteur privé afin qu'il soit interdit de refuser à une personne l'accès à un renseignement qui concerne son état de santé, à moins que cette communication ne risque vraisemblablement de créer un préjudice grave pour sa santé et que les lois, règlements et Code de déontologie des ordres professionnels soient adaptés en conséquence.

RECOMMANDATION N° 31

La Commission recommande que soient modifiées la Loi sur l'accès et la Loi sur le secteur privé afin d'y ajouter une disposition qui autoriserait le regroupement de citoyens lors du traitement des plaintes par la Commission.

RECOMMANDATION N° 32

La Commission recommande que la Loi sur la santé et la sécurité du travail soit amendée afin qu'il ne soit plus possible d'interpréter les articles 174 et 176 de cette Loi de façon à empêcher une personne d'exercer son droit à un recours devant la Commission d'accès à l'information pour faire réviser un refus de communiquer des renseignements fournis par des tiers.

RECOMMANDATION N° 33

La Commission devrait être investie du pouvoir d'ordonner la destruction d'un fichier de renseignements personnels en application de la Loi sur le secteur privé.

La Commission devrait être investie du pouvoir d'accorder des dommages-intérêts punitifs si, au terme d'une enquête, elle constate qu'il y a eu violation des droits relatifs à la protection des renseignements personnels reconnus par la Loi sur l'accès ou la Loi sur le secteur privé.

RECOMMANDATION N° 34

Les ministères et organismes doivent appliquer les principes de protection de renseignements personnels dans le développement de leur système d'information.

RECOMMANDATION N° 35

Les ministères et organismes doivent inviter responsables de la protection des renseignements personnels à participer aux travaux de développement de leur système d'information.

RECOMMANDATION N° 36

Les ministères et organismes doivent sensibiliser les concepteurs et les architectes de systèmes d'information aux principes de protection de renseignements personnels.

RECOMMANDATION N° 37

Les organismes publics doivent procéder à une analyse des risques en matière de la protection des renseignements personnels dans les travaux préliminaires de conception de systèmes.

RECOMMANDATION N° 38

Le cadre juridique du dossier patient dans le secteur de la santé doit être actualisé.

RECOMMANDATION N° 39

Sur la base d'objectifs bien définis et d'une solide évaluation, le développement d'un ou plusieurs modèles d'échanges d'information, à l'échelle locale ou régionale, permettrait de bâtir une solution technologique favorisant une meilleure circulation des renseignements de santé des citoyens et répondant ainsi aux besoins des intervenants du secteur de la santé.

RECOMMANDATION N° 40

La Commission demande que le concept de l'étanchéité des fichiers détenus par un organisme public soit clairement reconnu dans la Loi sur l'accès.

RECOMMANDATION N° 41

Une modification devrait être apportée à l'article 125 de la Loi sur l'accès de manière à ce que la Commission puisse accorder une autorisation que si des mesures de sécurité assurent le caractère confidentiel des renseignements personnels.

RECOMMANDATION N° 42

Une modification devrait être apportée à l'article 125 de la Loi sur l'accès de manière à ce que la Commission puisse requérir, à l'égard de certaines demandes, l'avis préalable d'un comité d'éthique.

RECOMMANDATION N° 43

Que l'article 125 de la Loi sur l'accès soit la seule disposition devant régir les demandes d'accès à l'information des chercheurs.

RECOMMANDATION N° 44

Que l'article 125 de la Loi sur l'accès soit modifié de façon à ce que la Commission n'accorde à une personne ou à un organisme l'autorisation de recevoir communication de renseignements nominatifs que sur avis de l'organisme détenteur de ces renseignements.

RECOMMANDATION N° 45

Que l'article 125 de la Loi sur l'accès soit modifié de façon à ce que l'organisme qui communique des renseignements nominatifs soit responsable d'assurer le suivi des conditions fixées par la Commission, de faire rapport annuellement à la Commission et de prévoir la conclusion d'un contrat entre un organisme détenteur et un chercheur.

RECOMMANDATION N° 46

Que la Commission parlementaire de la culture se penche sur la création d'entrepôts de données dédiés à la recherche ou leur réseautage et évalue de l'opportunité de faire des recommandations quant à des modifications législatives visant à encadrer, le cas échéant, ce phénomène en émergence.

RECOMMANDATION N° 47

La Loi sur le secteur privé devrait prévoir qu'un commissaire peut exercer seul les pouvoirs de la Commission d'accès à l'information en matière d'enquête. Une telle modification devrait également être apportée dans la Loi sur l'accès qui renferme la même lacune.

Dans le même ordre d'idées, un commissaire devrait être autorisé à exercer seul les pouvoirs qui sont reliés à l'exercice de sa fonction d'adjudication, tels les pouvoirs généraux, les pouvoirs en matière de demande frivole, faite de mauvaise foi ou inutile et les pouvoirs en matière de péremption d'une demande. Devraient donc être modifiés les articles 141, 130.1 et 146.1 de la Loi sur l'accès et les articles 55, 57 et 60 de la Loi sur le secteur privé.

RECOMMANDATION N° 48

La Commission invite donc le législateur à lever toute ambiguïté se rattachant au champ d'application de la Loi sur le secteur privé.

RECOMMANDATION N° 49

La Commission recommande que l'on donne suite aux recommandations formulées par le Conseil de la santé et du bien-être dans son rapport intitulé « La Santé et le bien-être à l'ère de l'information génétique, enjeux individuels et sociaux à gérer. »

RECOMMANDATION N° 50

La Commission recommande donc le maintien de la structure actuelle et qu'elle puisse demeurer un organisme multifonctionnel qui jumelle des fonctions à la fois adjudicative et administrative.

RECOMMANDATION N° 51

La Commission recommande que ses ressources humaines, matérielles et financières puissent être augmentées afin qu'elle puisse pleinement réaliser les mandats que le législateur lui a confiés.

RECOMMANDATION N° 52

Afin de faire face à la demande et de façon à éviter une paralysie qu'entraînerait une absence prolongée d'un membre, la Commission recommande une augmentation du nombre de ses membres.

RECOMMANDATION N° 53

La Commission recommande donc que des mesures soient prises pour s'assurer que la Commission relève de façon fonctionnelle de l'Assemblé nationale et que son budget lui soit octroyé par le bureau de l'Assemblée nationale.

ANNEXE 2 : RÉSOLUTIONS ADOPTÉES PAR LES COMMISSAIRES À LA PROTECTION DES DONNÉES ET DE LA VIE PRIVÉE ET DE L'ACCÈS À L'INFORMATION

Résolution visant l'amélioration des pratiques d'information en matière de protection des données et de la vie privée

Adoptée lors de la 25ème Conférence internationale des commissaires à la protection des données et à la vie privée

Sydney (Australie)

12 septembre 2003

La 25e Conférence des commissaires pour la protection des données et des informations a adopté la résolution suivante :

1. La conférence attire l'attention des organisations, qu'elles soient du secteur public ou du secteur privé, sur l'importance de :

- donner des indications beaucoup plus précises sur la façon dont elles traitent et utilisent les données personnelles,
- généraliser la mise au point de la façon dont ces informations seront communiquées, et, ce faisant, de
- permettre aux personnes concernées de comprendre et d'être conscients de leurs droits et choix, ainsi que des moyens qui sont à leur disposition pour les préserver
- encourager les organisations à rendre leurs pratiques transparentes, ce qui rendrait, ainsi, plus honnête le traitement et l'utilisation qu'elles font des données.

2. La conférence approuve les moyens qui sont proposés pour réaliser ces objectifs et qui sont les suivants :

- développer et utiliser un format succinct de présentation donnant une vue d'ensemble des informations sur les données, qui serait standardisé dans le monde entier, en étant adopté par toutes les organisations, et qui mentionnerait :
  - les informations les plus importantes que la personne concernée doit connaître,
  - celles qu'elle est susceptible de vouloir connaître le plus ;
- utiliser, pour ce faire, un langage simple, direct et sans ambiguïté
- utiliser le langage employé par le site Internet ou un formulaire servant à recueillir les informations
- faire porter la présentation sous format sur un nombre réduit de points qui, selon ce qui est indiqué ci-dessus, devraient suivre et inclure les principes importants concernant la protection des données, tels que l'indication de :
  - qui recueille les informations personnelles et comment il est possible de le contacter (avec, au minimum, le nom de l'organisation et son adresse géographique),
  - quelles informations personnelles l'organisation recueille et par quels moyens,
  - à quelles fins l'organisation recueille ces informations personnelles
  - l'éventuelle transmission de ces informations à d'autres organisations et, si tel est le cas, le type d'organisation et son ou leur nom, en indiquant également à quelles fins,
  - les choix offerts aux personnes concernées pour ce qui relève de leur domaine privé et l'explication de la façon dont elles peuvent les exercer facilement, en particulier, le choix d'accepter ou non que leurs informations soient communiquées

à des tiers, pour des raisons autres mais légales, et celui du type d'information personnelle qu'elles doivent donner afin de pouvoir bénéficier d'un service
  - un résumé indiquant à la personne concernée, quels sont ses droits d'accès, de correction, de blocage ou de suppression,
  - quelle autorité de contrôle indépendante les personnes concernées peuvent approcher de façon à vérifier les informations qui leur sont données,
- l'utilisation de moyens appropriés de façon à permettre aux personnes concernées de trouver facilement des informations supplémentaires, y compris :
  - les informations que toute loi en vigueur exige que les organisations fournissent aux personnes concernées, y compris concernant leurs droits d'accès, de correction, de blocage ou de suppression, et la durée pendant laquelle une organisation peut garder des données personnelles,
  - l'explication complète de l'information résumée dans la présentation sous un format succinct.
  - la déclaration complète faite par l'organisation sur ses pratiques concernant son traitement et son utilisation des informations.

3. La conférence considère que ce type de présentation, sous un format succinct et standardisé, devra être conforme à toutes les lois nationales s'appliquant à ce domaine, et devra s'ajouter, lorsque cela sera nécessaire et également compatible avec elle, à toute notification qu'une organisation est légalement obligée de faire à une personne concernée.

4. La conférence est consciente de l'importance du moment où sont présentées les informations concernant les personnes pour la protection de leurs données et de leur droit au domaine privé. Par exemple, il est particulièrement désirable que les informations leur soient présentées automatiquement au moment précis où elles ont la possibilité de choisir le type d'informations personnelles qu'elles veulent donner et lorsqu'il leur est indiqué que ces informations peuvent être communiquées à des tiers. Dans d'autres cas, il peut être approprié de laisser les personnes concernées chercher à protéger leurs données et les informations sur leur domaine privé au moyen de liens évidents. La conférence connaît le travail important qu'a effectué le groupe de travail sur la protection des données de l'UE et, en particulier, son Article 29 concernant la présentation automatique de la protection des données et des informations sur le domaine privé, dans sa *Recommandation 2/2001 sur certaines obligations minimum concernant le recueil de données personnelles en ligne dans l'Union européenne*.

5. La conférence considère que la détermination du moment où la présentation sous un format succinct (qui devrait tenir compte à la fois du milieu « en ligne » ou « hors-ligne ») peut constituer, pour les commissaires pour la protection des données et du droit au domaine privé, une question à laquelle ils peuvent contribuer très utilement par leur travail.

6. La conférence est informée des activités portant sur les mêmes questions, telles que le développement de langages pour ordinateurs permettant de décrire les politiques suivies. Cela va dans le sens, pour le futur, d'une présentation de ces politiques sous format standardisé et succinct.

7. La conférence considère qu'il s'agit là de premiers pas faits pour encourager de meilleures pratiques concernant la façon dont les organisations communiquent, concernant le domaine privé, les informations sur leur traitement et leur utilisation et des données personnelles. La conférence est informée des initiatives qui ont été prises dans ce domaine, pour améliorer la communication entre les organisations et les personnes qui s'adressent à elles. La conférence se réjouit de travailler avec les organisations et les groupes d'intérêt qui ont entrepris ces travaux et elle envisage, elle-même, de contribuer à l'amélioration de la communication entre les organisations et les personnes concernées, au cours de ses futures conférences.

Résolution sur la protection intégrée de la vie privée

Adoptée lors de la 32ème Conférence internationale des commissaires à la protection des données et de la vie privée

Israël (Jérusalem)

27 au 29 octobre 2010

Considérant que les progrès technologiques remettent en question la protection de la vie privée et la capacité des particuliers d'exercer pleinement leur droit d'accès à l'information;

Considérant que les politiques et règlements actuels ne parviennent pas à eux seuls à assurer la pleine protection de la vie privée;

Considérant que l'adoption d'une approche plus rigoureuse s'impose afin de composer avec les effets croissants et systémiques des technologies de l'information et des communications (TIC) et des réseaux de grande envergure;

Considérant qu'il est nécessaire d'intégrer la protection de la vie privée dans la conception, le fonctionnement et la gestion des TIC et des systèmes connexes pendant toute la période de conservation des renseignements afin de protéger pleinement la vie privée;

Considérant la protection intégrée de la vie privée, un concept global pouvant s'appliquer à l'ensemble des activités d'une organisation de bout en bout, y compris à la technologie de l'information, aux pratiques administratives, aux procédés, à la conception matérielle et aux réseaux;

La 32e Conférence internationale des commissaires à la protection des données et de la vie privée, réunie à Jérusalem, décide de prendre les mesures suivantes :

1. Reconnaître la protection intégrée de la vie privée comme étant un élément fondamental de la protection de la vie privée;

2. Favoriser l'adoption des principes fondamentaux de la protection intégrée de la vie privée, tels que ceux qui sont énoncés ci-dessous, comme lignes directrices pour l'intégration de la protection de la vie privée dans les activités des organisations;

3. Inviter les commissaires à la protection des données et à la vie privée à :

a. promouvoir la protection intégrée de la vie privée le plus largement possible, personnellement et par la distribution de documents et d'information;

b. favoriser l'intégration des principes fondamentaux de la protection intégrée de la vie privée dans le libellé des politiques et textes de loi sur la protection de la vie privée dans leur territoire de compétence;

c. favoriser la recherche sur la protection intégrée de la vie privée;

d. envisager de porter la protection intégrée de la vie privée à l'ordre du jour des événements qui auront lieu lors de la Journée internationale de la protection des données (le 28 janvier);

e. rendre compte lors de la 33e Conférence internationale des commissaires à la protection des données et de la vie privée, s'il y a lieu, des activités et initiatives liées à la protection intégrée de la vie privée qui ont été réalisées dans leur territoire de compétence, dans le but de partager des pratiques exemplaires.

La protection intégrée de la vie privée :

Les sept principes fondamentaux

1. Prendre des mesures proactives et non réactives; des mesures préventives et non correctives
2. Assurer la protection implicite de la vie privée
3. Intégrer la protection de la vie privée dans la conception
4. Assurer une fonctionnalité intégrale selon un paradigme à somme positive et non à somme nulle
5. Assurer la sécurité de bout en bout, pendant toute la période de conservation des renseignements
6. Assurer la visibilité et la transparence
7. Respecter la vie privée des utilisateurs

Note explicative

Le droit d'exercer un contrôle sur la collecte, l'utilisation et la divulgation de renseignements qui nous concernent représente l'un des fondements d'une société libre. Les progrès technologiques remettent en cause ce droit et la capacité des particuliers de l'exercer pleinement. Les règlements et politiques ne suffisent plus à protéger la vie privée. Compte tenu de la complexité et de l'interconnectivité croissantes des technologies de l'information, seule l'intégration directe des mesures de protection de la vie privée dans les systèmes et procédés au moment de leur conception saurait suffire.

Le concept de *protection intégrée de la vie privée* a été élaboré comme réponse structurée aux effets systémiques toujours croissants des technologies de l'information et des communications (TIC) et de la mise en place de réseaux de grande envergure. La *protection intégrée de la vie privée* désigne une philosophie et une approche consistant à intégrer la protection de la vie privée dans la conception, le fonctionnement et la gestion des technologies et systèmes d'information, pendant toute la période de conservation des renseignements.

Les principes fondamentaux de la *protection intégrée de la vie privée* décrivent les mesures proactives à prendre pour faire de la protection de la vie privée le mode implicite de fonctionnement de toutes les organisations, tout en assurant une fonctionnalité intégrale; il s'agit d'une approche à la protection de la vie privée qui est à somme positive et non à somme nulle.

Résolution sur la vie privée des enfants en ligne

Adoptée lors de la 30ème Conférence internationale des commissaires à la protection des données et de la vie privée

Strasbourg (France)

15-17 octobre 2008

Partout dans le monde, les jeunes se branchent à Internet depuis leur domicile, leur école et leurs appareils sans fil. Ils utilisent Internet à des fins d'interaction sociale – ils échangent des histoires, des idées, des photos et des vidéos, ils demeurent en contact pendant la journée avec leurs amis par messagerie texte et ils jouent à des jeux en ligne avec d'autres personnes de l'autre bout du monde.

Ce faisant, les jeunes doivent également faire face aux difficultés et aux défis liés à la protection de leurs renseignements personnels en ligne. L'absence de réglementation de nombreux services Internet rend cette tâche ardue. Beaucoup des sites les plus populaires auprès des jeunes recueillent une grande quantité de renseignements personnels à des fins de vente et de marketing.

La quantité de renseignements personnels recueillie et conservée ne fera qu'accroître avec l'augmentation du nombre d'applications et de technologies offertes sur Internet. Aujourd'hui déjà, les jeunes ignorent souvent que leurs renseignements, leurs habitudes et leur comportement en ligne sont surveillés.

Les recherches indiquent que les jeunes (de même que de nombreux adultes) lisent rarement les politiques de confidentialité des sites Web qu'ils visitent, ce qui n'est pas surprenant puisque les politiques de nombreux sites sont rédigées dans une langue spécialisée, technique ou juridique difficile à comprendre pour la majorité des lecteurs.

Bien que plusieurs jeunes reconnaissent les risques liés à leurs activités en ligne, ils ne possèdent pas l'expérience, les connaissances techniques ou les outils nécessaires pour atténuer ces risques. Ils ignorent souvent leurs propres droits juridiques.

Il y a près de 20 ans, en 1989, l'Assemblée générale des Nations Unies a adopté la Convention relative aux droits de l'enfant, qui déclare que les États doivent respecter et protéger les droits de l'enfant, y compris leur droit à la protection de leur vie privée.

Depuis, les commissaires à la protection des données et de la vie privée se soucient de plus en plus des atteintes à la vie privée des enfants en ligne.

En outre, dans sa déclaration sur la protection de la dignité, de la sécurité et de la vie privée des enfants adoptée le 20 février 2008 par le Comité des Ministres du Conseil de l'Europe, ce dernier a déclaré être convaincu de la nécessité d'informer les enfants de la permanence des contenus qu'ils peuvent créer sur l'Internet et des risques qui y sont liés. Il a, en outre, déclaré qu'il convient de veiller à ce qu'aucun historique des contenus générés par des enfants sur l'Internet, susceptible de porter atteinte à leur dignité, à leur sécurité et à leur vie privée, et de les rendre vulnérable, maintenant ou à un stade ultérieur de leur vie, ne soit accessible de façon durable ou permanente, excepté dans le cadre de la lutte contre les infractions.

Parallèlement, les commissaires ont reconnu qu'une approche axée sur l'éducation, en combinaison avec une réglementation sur la protection des données, demeure l'une des méthodes les plus efficaces pour aborder ce problème. Notamment, plusieurs pays ont mis en oeuvre des solutions novatrices axées sur l'éducation pour relever le défi que pose la protection de la vie privée des enfants sur Internet.

Les enfants et les jeunes ont le droit de connaître une expérience en ligne sécuritaire et enrichissante, où ils connaissent et comprennent les intentions des personnes avec qui ils interagissent.

Les commissaires à la protection des données et de la vie privée qui se sont réunis à l'occasion de la 30e Conférence internationale ont résolu de :

- encourager l'élaboration d'approches axées sur l'éducation pour améliorer la situation liée à la protection de la vie privée en ligne, sur les plans national et international;
- s'efforcer de veiller à ce que les enfants et les jeunes du monde entier aient accès à un environnement en ligne sécuritaire qui respecte leur vie privée;
- collaborer avec des partenaires et des intervenants dans son propre pays et à l'étranger, en reconnaissant que la coopération avec les professionnels qui influencent chaque jour la vie des enfants est cruciale;
- travailler entre eux pour échanger des pratiques exemplaires et mettre en oeuvre des activités d'éducation du public afin de sensibiliser davantage les enfants et les jeunes aux risques relatifs à protection de la vie privée inhérents à leurs activités en ligne et aux choix éclairés qu'ils peuvent faire pour contrôler leurs renseignements personnels;
- encourager les éducateurs à reconnaître que la sensibilisation à la protection de la vie privée est un aspect primordial de l'éducation des enfants et qu'il faut l'intégrer à leur programme d'enseignement;
- demander que les autorités adoptent des lois limitant la collecte, l'utilisation et la communication des renseignements personnels des enfants, y compris des dispositions appropriées en cas de non-respect de ces exigences;
- exiger des restrictions appropriées en matière de collecte, d'utilisation et de communication de renseignements personnels concernant les enfants lorsqu'il s'agit de publicité en ligne ciblant les enfants ou de publicité comportementale;
- inciter les exploitants de sites Web destinés aux enfants à démontrer leur conscience sociale en adoptant des politiques de confidentialité et des accords d'utilisation clairs, simples et compréhensibles, ainsi qu'en informant les utilisateurs sur les risques relatifs à la protection de la vie privée et à la sécurité et sur les choix que leur offrent les sites Web.

LE PASSAGE DE LA TRANSPARENCE AU GOUVERNEMENT OUVERT

Résolution sur la transparence gouvernementale

Adoptée par les commissaires canadiens de l'accès à l'information et à la protection de la vie privée

Whitehorse (Yukon)

1er septembre 2010

Contexte

Des appels à une plus grande ouverture et transparence exercent une pression croissante sur les gouvernements afin que ceux-ci changent leurs méthodes traditionnelles et réactionnelles de communication de l'information en méthodes qui favorisent une diffusion automatique. Partout dans le monde, des gouvernements reconnaissent l'importance de communiquer l'information au public de façon transparente et accessible. Ils comprennent que la collaboration avec les citoyens, les entreprises et les organismes non gouvernementaux en vue de multiplier leurs sources d'information améliore les voies de communication, encourage l'engagement des citoyens, accroît la confiance envers le gouvernement, favorise les opportunités économiques et finalement, conduit à un gouvernement démocratique plus ouvert, transparent et réceptif.

Les technologies permettent maintenant aux institutions publiques d'entrer en contact direct avec les citoyens, de dévoiler l'information de façon automatique et de soutenir, par la diffusion de l'information, le contrat social entre le gouvernement et les citoyens.

La transparence des gouvernements s'appuie sur les lois sur l'accès à l'information. Cependant, il faut aller plus loin que le concept à la base de ces lois afin de promouvoir une toute nouvelle vision du rôle du gouvernement et de la participation des citoyens dans celui-ci. Bien que l'accès à l'information permette un droit d'accès à l'information gouvernementale, ces lois sont fondamentalement réactionnelles puisque l'accès n'est accordé que sur demande.

Les commissaires de l'accès à l'information et à la protection de la vie privée encouragent la transparence gouvernementale et promeuvent un changement de paradigme d'une divulgation réactive vers une divulgation proactive, pour arriver en bout de ligne à la transparence gouvernementale.

Voici les principes de base d'une stratégie de transparence gouvernementale :

- **L'engagement des gouvernements** à tous les niveaux afin de promouvoir un changement de culture favorisant la transparence. Les principes devraient être établis par des instruments législatifs et politiques qui comportent des objectifs clairs, déterminent les responsabilités et les obligations de rendre compte, et prévoient des échéanciers précis. Afin de contribuer à la divulgation de l'information de façon automatique, les gouvernements devraient étoffer des programmes qui assurent l'intégration des mécanismes d'accès et de transparence dans les étapes de la conception et la mise en œuvre de tous les nouveaux programmes et services. Ces instruments devraient prendre en considération la protection des renseignements personnels, la confidentialité, la sécurité, les droits d'auteur et toutes autres lois pertinentes.

- La participation du public grâce à une **vaste consultation publique permanente**. Les gouvernements devraient consulter la population pour déterminer quelle information est requise pour obtenir une reddition de comptes. Les consultations devraient constituer la base pour déterminer les priorités concernant la divulgation et l'utilisation de l'information.
- **De l'information complète, accessible et exploitable**. Cela signifie que l'information devrait être diffusée gratuitement ou à coût minime, et comprendre les structures de données pour faciliter la recherche, la compréhension et l'interprétation de l'information. Elle devrait également être présentée dans des formats standards, ouvert et apte à être adapté et réutilisé. Les gouvernements devraient également collaborer avec les citoyens, les entreprises et les organismes non gouvernementaux, les encourager à participer au processus et maximiser l'utilisation des technologies afin de multiplier les accès à l'information.

DANS CE CONTEXTE, LES COMMISSAIRES À L'INFORMATION ET À LA PROTECTION DE LA VIE PRIVÉE DU CANADA (« COMMISSAIRES ») ADOPTENT LES RÉSOLUTIONS SUIVANTES :

1. les commissaires soutiennent et encouragent la transparence des gouvernements et la reddition de comptes qui sont des fondements importants d'une bonne gouvernance et des éléments essentiels pour une démocratie forte et efficace;
2. les commissaires demandent au gouvernement fédéral et à tous les gouvernements provinciaux et territoriaux de reconnaître l'importance de la transparence gouvernementale et de prendre des engagements précis pour rehausser les normes de transparence et la participation du public;
3. les gouvernements devraient établir des mécanismes d'accès et de transparence dès les étapes de la conception et de la mise en œuvre de tous les nouveaux programmes et services afin de faciliter et améliorer la divulgation automatique de l'information.
4. par le moyen de consultations publiques continues, les gouvernements devraient régulièrement cerner les sources de renseignements, et les diffuser de façon automatique, transparente et dans un format exploitable. L'accès du public à l'information devrait être gratuit ou à coût minime;
5. dans la mise en œuvre d'une politique de transparence gouvernementale, les gouvernements fédéral, provinciaux et territoriaux devraient accorder une attention particulière à la protection des renseignements personnels, à la confidentialité, à la sécurité, aux droits d'auteur et à toutes autres lois pertinentes.

ANNEXE 3 : DISPOSITIONS LÉGISLATIVES ET RÉGLEMENTAIRES ÉTRANGÈRES

LA DÉCLARATION DES FAILLES DE SÉCURITÉ

Alberta - Personal Information Protection Act (S.A. 2003, c. P-6.5) et Personal Information Protection Act Regulation (Alta. Reg. 366/2003)

Personal Information Protection Act	Personal Information Protection Act Regulation
34.1 (1) An organization having personal information under its control must, without unreasonable delay, provide notice to the Commissioner of any incident involving the loss of or unauthorized access to or disclosure of the personal information where a reasonable person would consider that there exists a real risk of significant harm to an individual as a result of the loss or unauthorized access or disclosure. (2) A notice to the Commissioner under subsection (1) must include the information prescribed by the regulations.	**19** A notice provided by an organization to the Commissioner under section 34.1(1) of the Act must be in writing and include the following information: (a) a description of the circumstances of the loss or unauthorized access or disclosure; (b) the date on which or time period during which the loss or unauthorized access or disclosure occurred; (c) a description of the personal information involved in the loss or unauthorized access or disclosure; (d) an assessment of the risk of harm to individuals as a result of the loss or unauthorized access or disclosure; (e) an estimate of the number of individuals to whom there is a real risk of significant harm as a result of the loss or unauthorized access or disclosure; (f) a description of any steps the organization has taken to reduce the risk of harm to individuals; (g) a description of any steps the organization has taken to notify individuals of the loss or unauthorized access or disclosure; (h) the name of and contact information for a person who can answer, on behalf of the organization, the Commissioner's questions about the loss or unauthorized access or disclosure.

37.1 (1) Where an organization suffers a loss of or unauthorized access to or disclosure of personal information that the organization is required to provide notice of under section 34.1, the Commissioner may require the organization to notify individuals to whom there is a real risk of significant harm as a result of the loss or unauthorized access or disclosure (a) in a form and manner prescribed by the regulations, and (b) within a time period determined by the Commissioner. (2) If the Commissioner requires an organization to notify individuals under subsection (1), the Commissioner may require the organization to satisfy any terms or conditions that the Commissioner considers appropriate in addition to the requirements under subsection (1). (3) The Commissioner must establish an expedited process for determining whether to require an organization to notify individuals under subsection (1) in circumstances where the real risk of significant harm to an individual as a result of the loss or unauthorized access or disclosure is obvious and immediate. (4) The Commissioner may require an organization to provide any additional information that the Commissioner considers necessary to determine whether to require the organization (a) to notify individuals under subsection (1), or (b) to satisfy terms and conditions under subsection (2). (5) An organization must comply with a requirement (a) to provide additional information under subsection (4), (b) to notify individuals under subsection (1), or (c) to satisfy terms and conditions under subsection (2). (6) The Commissioner has exclusive jurisdiction to require an organization (a) to provide additional information under subsection (4), (b) to notify individuals under subsection (1), or (c) to satisfy terms or conditions under subsection (2). (7) Nothing in this section is to be construed so as to restrict an organization's ability to notify individuals on its own initiative of the loss of or unauthorized access to or disclosure of personal information.	**19.1** (1) Where an organization is required under section 37.1 of the Act to notify an individual to whom there is a real risk of significant harm as a result of a loss of or unauthorized access to or disclosure of personal information, the notification must (a) be given directly to the individual, and (b) include (i) a description of the circumstances of the loss or unauthorized access or disclosure, (ii) the date on which or time period during which the loss or unauthorized access or disclosure occurred, (iii) a description of the personal information involved in the loss or unauthorized access or disclosure, (iv) a description of any steps the organization has taken to reduce the risk of harm, and (v) contact information for a person who can answer, on behalf of the organization, questions about the loss or unauthorized access or disclosure. (2) Notwithstanding subsection (1)(a), where an organization is required to notify an individual under section 37.1 of the Act, the notification may be given to the individual indirectly if the Commissioner determines that direct notification would be unreasonable in the circumstances.

Californie - California Civil Code

1798.29. (a) Any agency that owns or licenses computerized data that includes personal information shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

(b) Any agency that maintains computerized data that includes personal information that the agency does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

(c) The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section shall be made after the law enforcement agency determines that it will not compromise the investigation.

(d) For purposes of this section, "breach of the security of the system" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the agency. Good faith acquisition of personal information by an employee or agent of the agency for the purposes of the agency is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.

(e) For purposes of this section, "personal information" means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:

(1) Social security number.

(2) Driver's license number or California Identification Card number.

(3) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

(4)Medical information.

(5) Health insurance information.

(f) (1) For purposes of this section, "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

(2) For purposes of this section, "medical information" means any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional.

(3) For purposes of this section, "health insurance information" means an individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify athe individual, or any information in an individual's applicaton and claims history, including any appeals records.

(g) For purposes of this section, "notice" may be provided by one of the following methods:

(1) Written notice.

(2) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in Section 7001 of Title 15 of the United States Code.

(3) Substitute notice, if the agency demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars ($250,000), or that the affected class of subject persons to be notified exceeds 500,000, or the agency does not have sufficient contact information. Substitute notice shall consist of all of the following:

(A) E-mail notice when the agency has an e-mail address for the subject persons.

(B) Conspicuous posting of the notice on the agency's Web site page, if the agency maintains one.

(C) Notification to major statewide media.

(h) Notwithstanding subdivision (g), an agency that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this part shall be deemed to be in compliance with the notification requirements of this section if it notifies subject persons in accordance with its policies in the event of a breach of security of the system.

1798.82. (a) Any person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

(b) Any person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

(c) The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section shall be made after the law enforcement agency determines that it will not compromise the investigation.

(d) For purposes of this section, "breach of the security of the system" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business. Good faith acquisition of personal information by an employee or agent of the person or business for the purposes of the person or business is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.

(e) For purposes of this section, "personal information" means an individual's first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:

(1) Social security number.

(2) Driver's license number or California Identification Card number.

(3) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account.

(4)Medical information.

(5) Health insurance information.

(f) (1) For purposes of this section, "personal information" does not include publicly available information that is lawfully made available to the general public from federal, state, or local government records.

(2) For purposes of this section, "medical information" means any information regarding an individual's medical history, mental or physical condition, or medical treatment or diagnosis by a health care professional.

(3) For purposes of this section, "health insurance information" means an individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify athe individual, or any information in an individual's applicaton and claims history, including any appeals records.

(g) For purposes of this section, "notice" may be provided by one of the following methods:

(1) Written notice.

(2) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in Section 7001 of Title 15 of the United States Code.

(3) Substitute notice, if the person or business demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars ($250,000), or that the affected class of subject persons to be notified exceeds 500,000, or the person or business does not have sufficient contact information. Substitute notice shall consist of all of the following:

(A) E-mail notice when the person or business has an e-mail address for the subject persons.

(B) Conspicuous posting of the notice on the Web site page of the person or business, if the person or business maintains one.

(C) Notification to major statewide media.

(h) Notwithstanding subdivision (g), a person or business that maintains its own notification procedures as part of an information security policy for the treatment of personal information and is otherwise consistent with the timing requirements of this part, shall be deemed to be in compliance with the notification requirements of this section if the person or business notifies subject persons in accordance with its policies in the event of a breach of security of the system.

1798.84. (a) Any waiver of a provision of this title is contrary to public policy and is void and unenforceable.

(b) Any customer injured by a violation of this title may institute a civil action to recover damages.

(c) In addition, for a willful, intentional, or reckless violation of Section 1798.83, a customer may recover a civil penalty not to exceed three thousand dollars ($3,000) per violation; otherwise, the customer may recover a civil penalty of up to five hundred dollars ($500) per violation for a violation of Section 1798.83.

(d) Unless the violation is willful, intentional, or reckless, a business that is alleged to have not provided all the information required by subdivision (a) of Section 1798.83, to have provided inaccurate information, failed to provide any of the information required by subdivision (a) of Section 1798.83, or failed to provide information in the time period required by subdivision (b) of Section 1798.83, may assert as a complete defense in any action in law or equity that it thereafter provided regarding the information that was alleged to be untimely, all the information, or accurate information, to all customers who were provided incomplete or inaccurate information, respectively, within 90 days of the date the business knew that it had failed to provide the information, timely information, all the information, or the accurate information, respectively.

(e) Any business that violates, proposes to violate, or has violated this title may be enjoined.

(f) A prevailing plaintiff in any action commenced under Section 1798.83 shall also be entitled to recover his or her reasonable attorney's fees and costs.

(g) The rights and remedies available under this section are cumulative to each other and to any other rights and remedies available under law.

LA FONCTION DE RESPONSABLE DANS LE SECTEUR PRIVÉ

Canada - Loi sur la protection des renseignements personnels et les documents électroniques, L.C. 2000, ch. 5 – Annexe 1

4.1 Premier principe — 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 des principes énoncés ci-dessous.

4.1.1. Il incombe à la ou aux personnes désignées de s'assurer que l'organisation respecte les principes même si d'autres membres de l'organisation peuvent être chargés de la collecte et du traitement quotidiens des renseignements personnels. D'autres membres de l'organisation peuvent aussi être délégués pour agir au nom de la ou des personnes désignées.

4.1.2. Il doit être possible de connaître sur demande l'identité des personnes que l'organisation a désignées pour s'assurer que les principes sont respectés.

4.1.3. Une organisation est responsable des renseignements personnels qu'elle a en sa possession ou sous sa garde, y compris les renseignements confiés à une tierce partie aux fins de traitement. L'organisation doit, par voie contractuelle ou autre, fournir un degré comparable de protection aux renseignements qui sont en cours de traitement par une tierce partie.

4.1.4. Les organisations doivent assurer la mise en œuvre des politiques et des pratiques destinées à donner suite aux principes, y compris :

a) la mise en œuvre des procédures pour protéger les renseignements personnels;

b) la mise en place des procédures pour recevoir les plaintes et les demandes de renseignements et y donner suite;

c) la formation du personnel et la transmission au personnel de l'information relative aux politiques et pratiques de l'organisation; et

d) la rédaction des documents explicatifs concernant leurs politiques et procédures.

Alberta - Personal Information Protection Act, SA 2003, c. P-6.5

5 (1) An organization is responsible for personal information that is in its custody or under its control.

(2) For the purposes of this Act, where an organization engages the services of a person, whether as an agent, by contract or otherwise, the organization is, with respect to those services, responsible for that person's compliance with this Act.

(3) An organization must designate one or more individuals to be responsible for ensuring that the organization complies with this Act.

(4) An individual designated under subsection (3) may delegate to one or more individuals the duties conferred by that designation.

(5) In meeting its responsibilities under this Act, an organization must act in a reasonable manner.

(6) Nothing in subsection (2) is to be construed so as to relieve any person from that person's res-ponsibilities or obligations under this Act.

Colombie-Britanique - Personal Information Protection Act, SBC 2003, c. 63

4 (1) In meeting its responsibilities under this Act, an organization must consider what a reasonable person would consider appropriate in the circumstances.

(2) An organization is responsible for personal information under its control, including personal information that is not in the custody of the organization.

(3) An organization must designate one or more individuals to be responsible for ensuring that the organization complies with this Act.

(4) An individual designated under subsection (3) may delegate to another individual the duty conferred by that designation.

(5) An organization must make available to the public

(a) the position name or title of each individual designated under subsection (3) or delegated under subsection (4), and

(b) contact information for each individual referred to in paragraph (a).