

Les pouvoirs et fonctions de l'ombudsman
dans la *Loi sur la protection des renseignements
personnels et les documents électroniques* :

Une étude d'effectivité

Rapport de recherche

France HOULE et
Lorne SOSSIN

Août 2010

Recherche commanditée par le
Commissariat à la protection
de la vie privée du Canada

Les opinions exprimées dans cette étude sont celles des auteurs de ce rapport et ne reflètent pas nécessairement celles du Commissariat à la protection de la vie privée.

N° de cat. IP54-38/2011F
ISBN 978-1-100-97122-3

© Copyright 2010 France Houle et Lorne Sossin

PRÉFACE

C'est en vertu du par. 58(2) de la *Loi sur la protection des renseignements personnels* que la Commissaire à la protection de la vie privée nous a mandatés pour faire une analyse du droit et des politiques sous-jacentes à la protection des renseignements personnels par le secteur privé.

L'objectif général de ce contrat de recherche est de faire un examen de la structure, du mandat et des pouvoirs qui ont été attribués au Commissariat, tel qu'institué par la *Loi sur la protection des renseignements personnels* et la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE).

Selon les termes de notre contrat, notre perspective analytique consiste à effectuer une étude d'effectivité de la Partie I *Loi sur la protection des renseignements personnels et les documents électroniques*. En effet, le Commissariat souhaite connaître nos vues sur la question générale suivante : est-ce que le modèle de l'ombudsman est un modèle effectif pour réglementer les pratiques relatives à la protection des renseignements personnels par le secteur privé. Plus précisément, il nous a d'abord été demandé d'examiner les politiques publiques sous-jacentes à la genèse de la loi et l'historique du cadre juridique jusqu'à ce jour, d'analyser les fonctions et les pouvoirs attribués au Commissariat à la vie privée ainsi que leur utilisation par les commissaires nommés pour occuper cette charge publique depuis l'adoption de la LPRPDE. L'objectif de ces analyses étant d'évaluer l'impact de cet usage sur l'observance de la loi par les organismes qui y sont assujettis. Ensuite, partant des constats sur les problèmes qui ont été identifiés, il s'agit d'examiner d'autres modèles institutionnels canadiens et étrangers (également créés pour réglementer l'usage des renseignements personnels par des organismes du secteur privé) dans une perspective comparative, et ce, dans le but de faire des propositions de réforme.

Les idées et les analyses contenues dans ce rapport sont présentées dans le but d'alimenter la réflexion sur des voies possibles pour améliorer la protection des renseignements personnels des citoyens, résidents permanents et étrangers vivant et travaillant au Canada ou encore qui font affaires ou consomment les biens et services produits par les grandes, moyennes et petites entreprises canadiennes. Nous espérons que notre réflexion engendrera des débats et interactions entre les gouvernements, les industries, les experts et les consommateurs. Étant donné la complexité de la réglementation fédérale, provinciale et supranationale dans ce secteur d'activités, nos analyses ne peuvent ni constituer, ni prétendre constituer le fin mot de l'histoire sur cette question.

Pour plus d'information sur ce rapport, veuillez contacter :

France Houle

Professeure titulaire
Faculté de droit
Université de Montréal
C.P. 6128, Succ. Centre-ville
Montréal (Québec) H3C 3J7
(514) 343-6870
Courriel : france.houle@umontreal.ca

Lorne Sossin

Professeur titulaire
Faculté de droit
Université de Toronto
39 Queen's Park
Toronto (Ontario) M5S 2C3
(416) 946-8229
Courriel : lorne.sossin@utoronto.ca

REMERCIEMENTS

Les auteurs remercient tout spécialement leurs assistants de recherche : Jeffrey Baggs, Mélissa Blaise, Anne-Catherine Boucher, François Goyer, Kristen Rohr et Nicolas Vermeys ainsi que toutes les personnes qui ont accepté de participer à notre enquête empirique et dont les noms ne peuvent pas être dévoilés, ni leur affiliation institutionnelle puisque nous nous sommes engagés à maintenir leur complet anonymat.

Enfin, nous dédions tout spécialement nos plus sincères remerciements aux membres du personnel du Commissariat à la protection de la vie privée qui nous ont assistés dans la préparation de ce rapport en nous fournissant une grande quantité d'informations et en nous accordant le temps nécessaire pour répondre à nos multiples questions.

TABLE DES MATIÈRES

| | |
|--|------------|
| SOMMAIRE | 1 |
| Objectifs de l'étude..... | 1 |
| Méthodes de recherche | 1 |
| Conclusions générales..... | 2 |
| Contexte..... | 6 |
| Défis | 8 |
| Forces et faiblesses | 9 |
| Conclusions et recommandations spécifiques | 12 |
| RAPPORT DE RECHERCHE | 19 |
| Introduction générale..... | 19 |
| PARTIE I – La LPRPDE : Une loi intégrée dans le droit de la concurrence..... | 23 |
| PARTIE II – Démarches et modes d'évaluation de la compétence du Commissariat à la protection de la vie privée du Canada aux termes de la LPRPDE..... | 122 |
| CONCLUSIONS GÉNÉRALES ET RECOMMANDATIONS..... | 183 |
| TABLES BIBLIOGRAPHIQUES..... | 193 |
| ANNEXE A..... | 213 |
| PARTIE III – SANCTIONS PÉCUNIAIRES..... | 213 |
| ANNEXE B | 217 |
| Régime de sanctions administratives..... | 217 |

SOMMAIRE

Objectifs de l'étude

C'est en avril 2009 que le Commissariat à la protection de la vie privée nous confiait le mandat d'analyser l'effectivité de la Partie I de la *Loi sur la protection des renseignements personnels et les documents électroniques* (la 'LPRPDE'). Plus spécifiquement, il nous fut demandé d'examiner l'effectivité de la structure, du mandat et des pouvoirs qui ont été attribués au Commissaire à la protection de la vie privée, dans le but de répondre à la question générale suivante : est-ce que le modèle de l'ombudsman est un modèle effectif pour réglementer les pratiques relatives à la protection des renseignements personnels par le secteur privé?

Méthodes de recherche

Pour effectuer cette analyse de l'effectivité de la LPRPDE, nous avons fait une revue de la littérature mettant l'accent sur une analyse du discours macro-économique, politique et juridique des acteurs ayant participé à l'élaboration de la loi. Il s'agissait surtout d'examiner les politiques publiques sous-jacentes à la genèse de la loi et à l'historique du cadre juridique jusqu'à ce jour, d'analyser les fonctions et les pouvoirs attribués au Commissariat à la protection de la vie privée ainsi que l'utilisation de ces pouvoirs par les commissaires nommés pour occuper cette charge publique. À cet égard, nous avons été appelé à examiner d'autres modèles institutionnels canadiens et étrangers (également créés pour réglementer l'usage des renseignements personnels par des organismes du secteur privé) dans une perspective comparative. En ce qui a trait à l'examen de l'utilisation des pouvoirs législatifs, nous avons notamment procédé par le moyen d'entretiens conduits auprès d'acteurs privés afin de connaître leur point de vue sur l'effectivité de la LPRPDE.

Conclusions générales

Le modèle d'ombudsman et les activités de conformité en place ont permis d'atteindre d'importants objectifs. Toutefois, à la lumière de ces réalisations, devrions-nous en accomplir davantage et, dans l'affirmative, comment devons-nous procéder? Notre recherche nous permet de croire qu'un changement s'effectue vers l'assurance d'une protection accrue pour les consommateurs et que, pour s'y conformer, il faudra octroyer d'autres pouvoirs précis au CPVP. Toutefois, avant de modifier la LPRPDE, nous pressons le CPVP d'envisager de mener des recherches supplémentaires sur plusieurs sujets. En effet, plusieurs pièces du casse tête manquent pour donner une meilleure idée de l'environnement actuel dans lequel s'applique et devra s'appliquer la LPRPDE. Pour cette raison, nous recommandons de procéder à des recherches approfondies :

- **Recommandation 1 :**

- **Nouvelles questions de recherche**

1. Les défis et enjeux soulevés par le Web 2.0 et harmonisation des systèmes réglementaires nationaux et supranationaux
2. La capacité d'adaptation du modèle de l'ombudsman sous la LPRPDE pour régler efficacement ce nouvel environnement technologique.
3. La capacité d'adaptation du modèle fédératif contemporain (partage des compétences, droits des personnes, coopération fédérale-provinciale) pour répondre à ces nouveaux défis et enjeux. En particulier, examiner les théories relatives à l'interprétation fonctionnelle de la constitution et les possibilités qu'offre le concept de fédéralisme en réseau.

Ceci étant dit, et partant de l'hypothèse selon laquelle un changement s'effectue vers l'assurance d'une protection accrue pour les consommateurs, il faudra répondre à la question de savoir si le CPVP devrait se voir accorder davantage de pouvoirs afin de s'acquitter de plus grandes responsabilités relativement à la protection des consommateurs. Advenant que le CPVP envisage cette possibilité, nous formulons les recommandations qui suivent.

- **Recommandation 2 :**

- **Étendre les limites du modèle d'ombudsman aux petites et moyennes entreprises**

Le modèle d'ombudsman convenait particulièrement bien à la première étape de réglementation de l'industrie, qui suscitait de considérables préoccupations à propos des répercussions de la réglementation sur l'entreprise commerciale. Or, le modèle actuel ne semble pas convenir aussi bien au secteur des petites et moyennes entreprises, où les taux de conformité sont plus faibles et le risque à l'égard des renseignements personnels, plus important. Le CPVP devrait continuer à user de son influence aux termes du modèle d'ombudsman pour parvenir au respect de la LPRPDE, surtout de la part des grandes entreprises (p. ex. les banques, les compagnies d'assurance, les services publics, la technologie de l'information et les médias) et continuer à cibler les petites et moyennes

entreprises à des fins de sensibilisation, d'éducation et de mesures incitatives liées à la conformité.

- **Recommandation 3 :**
Accorder des pouvoirs limités pour ce qui est de rendre des ordonnances

En définitive, nonobstant les importantes réussites du CPVP, les taux de conformité à la LPRPDE demeurent probablement trop faibles, et le risque encouru par les consommateurs eu égard à leurs renseignements personnels détenus par les petites et moyennes entreprises au Canada, probablement trop élevé. Malgré leur importance, les efforts de sensibilisation et d'éducation de même que les mesures incitatives liés à la conformité destinés aux petites et moyennes entreprises peuvent ne pas suffire à atteindre les buts visés. En se fiant à l'expérience des organismes de réglementation provinciaux du Canada ainsi qu'à l'expérience américaine et européenne, la capacité d'imposer une amende et autres possibilités de rendre des ordonnances peuvent entraîner une conformité supplémentaire et constituer un important élément dissuasif malgré un emploi peu fréquent. Les avantages de cette approche paraissent tangibles et les risques, moins inévitables. Le risque, par exemple, a tendance à porter sur la réaction négative attendue de la part des entreprises, des tensions contradictoires accrues, la judiciarisation ainsi qu'à des coûts additionnels et une plus grande complexité tant pour le CPVP que pour les entreprises. L'expérience provinciale avec les organismes de réglementation investis du pouvoir de rendre des ordonnances suggère toutefois une surestimation possible de ces risques.

Bien que nous ne soyons assurément pas les premiers à préconiser de plus grands pouvoirs en matière d'ordonnances, nous ne pensons pas qu'en ce moment, le CPVP a besoin de pouvoirs élargis et envahissants, comme des ordonnances de cessation. À notre avis, le renforcement du pouvoir du CPVP en matière d'ordonnances ne devrait cibler que le genre d'activités d'exécution de la loi appropriées pour les petites et moyennes entreprises (par exemple, les amendes et les sanctions). Ce sont ces secteurs où les taux de conformité semblent les plus faibles et où toutes les données disponibles des organismes provinciaux chargés de surveiller le respect de la loi suggèrent que seule la menace de sanctions qui influent sur la rentabilité peut mener à un changement dans le comportement des entreprises et, en définitive, dans la culture entrepreneuriale. Même si le pouvoir de rendre des ordonnances peut ne pas s'avérer aussi nécessaire dans le secteur des grandes entreprises, où le CPVP a déjà réalisé des progrès en ce qui a trait à l'amélioration de la conformité, il pourrait avoir des effets bénéfiques dans ce contexte également. Le pouvoir de rendre des ordonnances peut renforcer l'importance des politiques en matière de protection de la vie privée par l'entremise de ces secteurs ainsi qu'améliorer l'image des agents de vérification de la conformité. De plus, l'expérience positive issue de la collaboration, de la consultation et de l'engagement de ce secteur avec le CPVP a permis de jeter les importantes bases d'un savoir, d'une confiance et d'une crédibilité institutionnels sur lesquelles miser si le CPVP recevait d'autres outils de réglementation.

Les pouvoirs supplémentaires décrits feront probablement en sorte que le CPVP devienne un organisme de réglementation plus efficient et efficace

en vertu de la portée de la LPRPDE. Le fait d'énoncer à nouveau les quatre critères établis par Bennett et Raab et dont il a été question à la partie 2 permet de constater les améliorations éventuelles suivantes.

- 1) **Économie** (p. ex. le coût correspondant à l'instauration d'un régime réglementaire). Le passage à un modèle hybride peut réduire le besoin de la séparation existante des activités du CPVP en deux sphères distinctes, l'une se rapportant à la LPRPDE et l'autre à la *Loi sur la protection des renseignements personnels*. Des dépenses supplémentaires associées au modèle hybride pourraient s'ajouter, mais en tant qu'approche générale, rien ne justifie un changement important dans le budget ou la dotation du CPVP advenant l'adoption d'un modèle hybride.
- 2) **Efficience** (p. ex. le coût du régime mesuré par rapport à ses résultats). Le passage à un modèle hybride mènerait sans doute à une efficience accrue, surtout dans les secteurs des petites et moyennes entreprises. Une plus vaste incursion dans ces secteurs, typiquement plus sensibles au risque et aux sanctions d'ordre financier, associée à l'effet dissuasif de l'évitement d'une intervention réglementaire a bien des chances d'entraîner des résultats plus importants pour un investissement égal sur le plan des efforts et des ressources. En outre, ce modèle réglerait la situation actuelle où le fait d'entamer des poursuites à la Cour fédérale constitue le seul, et malheureusement inefficace, moyen par lequel le CPVP peut voir une de ses ordonnances exécutée.
- 3) **Efficacité** (p. ex. la mesure dans laquelle les résultats pratiques du régime lui permettent d'atteindre ses objectifs ultimes). Les études du CPVP et de la CIPPIC abordées dans la partie 2 montrent que le taux de non-conformité demeure élevé. Le passage à un modèle hybride est susceptible d'accroître la conformité, particulièrement dans les secteurs des petites et moyennes entreprises (il est impossible de mesurer l'efficacité sans repères et objectifs précis).
- 4) **Équité** (p. ex. la mesure dans laquelle le régime étend la protection de manière équitable dans l'ensemble des groupes sociaux). Bien que les consommateurs semblent apprécier une protection accrue découlant des activités du CPVP s'il s'agit de clients de banques ou de compagnies d'assurance, de médias sociaux ou grand public, ceux des petites et moyennes entreprises bénéficient d'une protection bien moindre. L'adoption d'un modèle hybride améliorerait l'équité et assurerait que la protection des consommateurs ne dépende pas autant de la taille et de la complexité de l'entreprise comme c'est le cas maintenant.

Il serait justifié de renforcer de façon restreinte les pouvoirs réglementaires du CPVP, au moins afin de comprendre ceux d'imposer des amendes pour non-conformité.

- **Recommandation 4 :**
Accorder un pouvoir explicite d'émettre des directives

Des directives claires quant à l'utilisation de ce pouvoir de rendre des ordonnances, et des mesures de protection afin de garantir l'équité aux personnes qui en font l'objet, représenteront des outils essentiels de responsabilisation et, selon nous, elles devraient accompagner le pouvoir de réglementation supplémentaire. L'élaboration de directives fournit aussi l'occasion de consulter les intervenants, d'analyser les pratiques exemplaires d'organismes de réglementation pairs en plus de constituer un contexte au sein duquel les valeurs du CPVP peuvent être clairement communiquées aux personnes assujetties à la portée de la LPRPDE pour le CPVP.

- **Recommandation 5 :**
Envisager d'autres pouvoirs réglementaires créatifs – Programme d'accréditation

Le CPVP pourrait offrir un programme d'accréditation à la suite duquel les entreprises adoptant les « pratiques exemplaires » pourraient recevoir son imprimatur, un peu comme la certification LEED que peuvent obtenir les immeubles appliquant les meilleures pratiques environnementales. De tels systèmes d'accréditation — ou de notation — pourraient alors servir aux gouvernements municipaux et provinciaux à d'autres fins réglementaires ou aux entreprises à des fins commerciales (p. ex. dans le cadre d'une stratégie publicitaire). Une initiative connexe pourrait impliquer la rédaction d'avis destinés au public afin de lui faire savoir si une entreprise respecte un ensemble de normes, ce qui s'apparente à des avis d'inspection de salubrité affichés dans les restaurants et informant le public si l'établissement a passé une inspection avec succès ou non. Ces initiatives d'accréditation ou d'établissement de normes sont rarement fructueuses en soi. Leur succès dépend plutôt d'autres organismes de réglementation et industries qui devraient trouver des mesures incitatives à l'endroit des entreprises afin qu'elles consentent plus d'argent à la conformité. Par exemple, le fait qu'un gouvernement, un organisme ou une grande société accepte de limiter son appel d'offres aux entreprises ayant obtenu une note particulière relativement à la protection de la vie privée, ou qu'un permis ou une subvention donnés d'un gouvernement étaient liés à une note particulière relativement à la protection de la vie privée, pourrait constituer des mesures incitatives efficaces.

Nous ne suggérons pas que le CPVP accrédite, inspecte ou impose des étiquettes sur l'ensemble du secteur privé; toutefois, une initiative pilote au sein d'une industrie précise affichant un faible taux de conformité ou lorsque des membres vulnérables du public sont particulièrement à risque (p. ex. les jeunes qui partagent leurs renseignements personnels en ligne) pourrait fort bien prouver si cette stratégie réglementaire est efficiente et efficace. La création de mesures incitatives et de marchés internes en vue du respect accru de la LPRPDE représente un exemple d'une initiative conforme au modèle d'ombudsman, avec la possibilité d'accroître la conformité en vertu de la LPRPDE, mais exigeant une approche proactive envers le mandat du CPVP.

- **Recommandation 6 :**
Améliorer les mécanismes de reddition de comptes afin d'assurer une planification stratégique à long terme et des repères significatifs

Le CPVP utilise déjà un certain nombre de mécanismes de reddition de comptes efficaces, mais leur incidence est limitée. Il manque à l'actuelle structure de reddition de comptes un sens de la planification stratégique à long terme et de repères significatifs. Bien que le CPVP ne soit pas sous-examiné, il s'avère souvent difficile de relever les critères utilisés par les divers examens en vue de son évaluation. Fait encore plus troublant, les normes par rapport auxquelles le CPVP évalue son propre rendement ne sont pas clairement connues. Même s'il recueille des données et note les tendances dans ses activités, ou le degré de plaintes ou de règlements, le CPVP n'a désigné aucun repère ou cible pouvant servir à évaluer ses activités. La FTC fournit un modèle utile à cet égard. Comme il en a été question dans la partie 2, la FTC publie un plan stratégique quinquennal qui met en lumière un nombre de buts généraux (p. ex. protéger les consommateurs) qui comprennent individuellement un ensemble d'objectifs liés aux mesures de rendement, aux stratégies en vue d'atteindre le but en question ainsi qu'à la méthode d'évaluation.

Enfin, nous recommandons que le CPVP adopte une approche de planification stratégique plus claire en ce qui concerne ses activités en vertu de la LPRPDE, y compris ce qui suit :

- L'établissement de points de référence à des fins de conformité à la LPRPDE;
- La surveillance et le suivi de la conformité sur une base continue, au moins dans les secteurs cibles ou prioritaires comme les petites et moyennes entreprises;
- Des mesures d'évaluation du rendement pour les activités du CPVP à cet égard;
- Une planification stratégique à court, moyen et long terme avec des objectifs établis associés à des échéances précises.

Contexte

Notre mandat de recherche a porté, rappelons-le, sur les fonctions et pouvoirs de l'ombudsman tels qu'ils sont édictés dans la LPRPDE. Il ne s'étend pas à une critique de la portée et des limites des principes contenus dans le Code type sur la protection des renseignements personnels (annexe 1 de la LPRPDE). Le caractère limité de notre étude exclut donc des questions fondamentales et, en particulier, celle relative au passage du Web 1.0 au Web 2.0 qui remettrait en cause, selon des spécialistes, certaines des hypothèses qui sous-tendent les principes qui ont été élaborés dans le cours des années 1990, approuvés par le législateur au début des années 2000 et adoptés dans la LPRPDE.

Tout près de 10 ans se sont écoulées depuis la mise en vigueur de la LPRPDE. Dans ce court laps de temps, des bouleversements majeurs se sont produits avec l'avènement du Web 2.0. Ces changements ont et continueront d'emporter des conséquences importantes, voire même radicales, sur la manière d'accéder, de

traiter et d'utiliser les renseignements personnels. Aussi, toute réflexion future en vue d'assurer la protection des renseignements personnels utilisés par les industries du secteur privé et plus particulièrement dans le cadre des échanges et du commerce électroniques devront inclure ces nouvelles dimensions. Il faut donc lire les conclusions et les recommandations de notre étude en tenant compte des limites importantes que comporte notre mandat de recherche. En effet, en 2010, il apparaît assez évident que les autorités publiques devront tenir compte de ce nouvel environnement technologique lorsque, dans le cadre du processus de révision à venir de la LPRPDE, elles seront appelées à évaluer l'adéquation entre les pouvoirs et fonctions du Commissaire à la protection de la vie privée et la réglementation de l'usage, de la collecte et de la conservation des renseignements personnels par le secteur privé dans le Web 2.0.

Cela dit, il semble bien que l'impact de la LPRPDE ait été positif au cours des dix années d'existence. En ce sens, le recours aux offices d'un ombudsman –plutôt qu'un tribunal administratif, par exemple– ont permis des avancées éducatives non négligeables chez les acteurs privés assujettis à la loi. En effet, malgré les nombreuses embûches sur le plan des idées économiques et politiques en vogue durant les années 1990, privilégiant une approche nettement plus minimaliste en matière d'interventions gouvernementales dans le marché et imposant de ce fait des contraintes juridiques importantes, le recours à l'institution de l'ombudsman a, somme toute, mené à des résultats positifs. En effet, il semblerait qu'il en ait résulté une meilleure prise de conscience chez les acteurs privés (personnes physiques et morales) de l'importance de protéger les renseignements personnels des individus et que ces protections soient appliquées d'une manière plus cohérente et uniforme tant sur le plan interne.

Cependant, est-ce que cette institution possède les instruments nécessaires pour intervenir efficacement dans le contexte contemporain? Évidemment, la réponse à cette question varie selon la perspective normative des uns et des autres. Toutefois, s'il était envisagé de modifier les pouvoirs et fonctions du Commissariat, il faudrait de toute évidence qu'il y ait une bonne compréhension préalable du contexte factuel, mais aussi des discours économique, politique et juridique contemporains. À cet égard, bien que certains obstacles se soient aplanis, ce qui permettrait d'envisager l'attribution de pouvoirs additionnels au Commissariat, l'institution de l'ombudsman n'est pas un vase creux : on ne peut tout y mettre sans profondément dénaturer l'institution. En conséquence, au-delà de l'attribution de certains pouvoirs et fonctions propres à l'institution de l'ombudsman, il serait peut-être préférable d'instituer un autre type d'organisme public, surtout si l'attribution d'autres pouvoirs a pour objectif de permettre l'exercice de contraintes à l'égard des acteurs privés. Sur ce point, on peut observer que lorsqu'il s'agit de réglementer les activités de la société civile (d'une catégorie d'individus ou d'industries), les législateurs canadiens préfèrent normalement créer un organisme décentralisé, qui peut être un tribunal administratif (exerçant seulement une fonction de nature décisionnelle), ou un organisme de régulation économique (exerçant des fonctions réglementaires de nature économique ou sociale, des fonctions administratives et des fonctions de nature décisionnelle). Dans le passé, c'est à cette dernière option que le législateur a recouru pour réglementer des activités commerciales.

Toutefois, il faut préciser que les organismes décentralisés ont traditionnellement eu pour vocation d'exercer une surveillance limitée à certaines activités très spécifiques et de nature particulière plutôt que générale (d'où le caractère spécialisé de ces organismes). Dans le contexte de l'application d'une réglementation à portée générale, telle celle relative à la protection des renseignements personnels, on peut s'interroger sur la faisabilité d'attribuer des pouvoirs généraux de contraintes à un organisme décentralisé fédéral. À tout le moins, il faudrait qu'une analyse des coûts, des avantages et inconvénients, ainsi que des limites juridiques d'une telle approche soit faite.

Défis

Avant d'entreprendre une démarche de réforme législative dans ce vaste champ de la protection des renseignements personnels, plusieurs défis doivent être relevés. Ils ont tous traits à une meilleure connaissance des enjeux contemporains et à l'interaction entre les divers facteurs qui interagissent et qui sont sous-jacents à ces enjeux. Pour nommer les principaux, il faut que les acteurs principaux aient une connaissance et une compréhension partagée des liens entre le développement de l'économie du savoir et la protection des renseignements personnels afin de :

- Mieux comprendre la portée et les limites des principes du Code directeur dans le nouvel environnement technologique du Web 2.0
 - Est-ce que toutes ou parties des obligations sociales des entreprises en cette matière devraient être renforcées, modifiées ou éliminées?
- Mieux évaluer les risques de ce nouvel environnement et mieux connaître les besoins des citoyens et consommateurs en matière de protection des renseignements personnels.
 - Peut-on observer des changements générationnels importants relatifs à l'attitude générale quant aux attentes en matière de protection des renseignements personnels? Si oui, de quelle nature et comment affectent-ils les postulats sous-jacents à la LPRPDE?
- Créer les outils méthodologiques afin de mieux comprendre et évaluer les systèmes normatifs nationaux (fédéral et provinciaux) et supranationaux.
 - Quelles sont les forces et les faiblesses de ces systèmes, non pas chacun en soi, mais les uns par rapport aux autres? Est-il possible ou souhaitable de les rendre plus harmonieux? Si oui, comment?

Nous ne faisons que soulever que quelque unes des questions qui nous apparaissent centrales lors de débats futurs. En effet, les réponses à ces questions auront des répercussions sur l'attribution de pouvoirs et de fonctions à l'institution publique qui sera en charge de la mise en œuvre de la LPRPDE. Ces quelques éléments de réflexions suffisent pour suggérer qu'une étude préalable approfondie, impliquant une vaste consultation auprès de toutes les parties prenantes, devrait être faite. Sur le plan de la gouvernance publique, l'enjeu est de s'assurer que toutes les parties prenantes partagent une plus grande compréhension commune des enjeux actuels. En somme, il s'agit d'établir de plus larges consensus sur la définition de ces enjeux puisque de ceux-ci

découleront des voies d'action plus claires afin d'identifier des solutions relatives aux instruments de l'action administrative, ainsi qu'aux fonctions et pouvoirs attribués à l'institution chargée d'appliquer la loi.

Forces et faiblesses

Notre revue de la littérature nous a permis d'identifier les principales forces et faiblesses suivantes dans la LPRPDE.

Les forces identifiées sont celles liées aux attributions de pouvoirs relatives à l'éducation du public, à la recherche, ainsi qu'aux enquêtes et vérifications. Sur les pouvoirs d'enquête et de vérification, plusieurs intervenants sont d'avis qu'il s'agit de l'une des fonctions les plus importantes que puisse effectuer un commissaire à la protection de la vie privée. Le principal avantage étant que le commissaire peut ainsi encourager l'autoréglementation par les acteurs assujettis par la loi. Les principales faiblesses identifiées par les critiques ont porté sur des questions de forme, le processus consultatif, et de fond : le choix du modèle de l'ombudsman plutôt que celui du tribunal administratif, l'absence du pouvoir d'émettre des ordonnances, la non-divulcation des résultats des enquêtes portant sur les plaintes et l'accès à la Cour fédérale.

- **Le processus consultatif**

Au moment de l'élaboration des politiques et de l'étude du projet de loi, les critiques ont fait valoir que trop peu de discussions publiques avaient été menées afin de dégager de plus larges consensus sur les pouvoirs qui devaient être attribués au Commissaire à la vie privée. Plusieurs sont d'avis que les perspectives des entreprises privées ont largement dominé les débats et, par conséquent, le choix des politiques publiques. De fait, l'examen de la littérature disponible montre que les préoccupations des citoyens, notamment examinées sous l'angle de la protection des consommateurs, sont peu présentes dans les débats de cette époque ce qui est paradoxal compte tenu que l'enjeu de ces débats portait sur la question fondamentale de la protection des renseignements personnels. Ainsi, il en ressort un sentiment général chez les critiques que la protection des renseignements personnels était à l'arrière-plan du projet de loi ; ce dernier se voulait d'abord un instrument servant à promouvoir le commerce électronique. Selon eux, le gouvernement (lors de l'élaboration de la politique) et le Parlement (lors de l'étude du projet de loi) auraient posé des postulats desquels ils n'auraient pas dérogé. Des principaux postulats il faut entre autres retenir celui selon lequel il fallait doter l'autorité publique qui serait chargée d'appliquer la loi d'instruments de politiques qui soient les plus légers, simples, flexibles, efficaces et effectifs possibles.

- **Les questions de fond**

En raison d'un processus de consultation insuffisant, les critiques estiment qu'il n'y a pas eu de véritables débats sur des questions de fond, telles celles de savoir si un pouvoir de rendre des jugements exécutoires et sans appel devait être attribué à l'autorité publique et, le cas échéant, si un tribunal spécialisé devrait être créé. En effet, certains intervenants estimaient que les pouvoirs attribués

au commissaire, à titre d'ombudsman, seraient insuffisants pour garantir la mise en œuvre effective de la loi. Une revue des débats parlementaires montre en effet que peu de voix discordantes se sont fait entendre. Le commissaire à la protection de la vie privée de l'époque a occupé une large place dans ces débats, alors qu'il était fortement opposé à toute discussion sur l'idée d'attribuer des pouvoirs contraignants au Commissariat. Il préférerait fonctionner à la manière d'un médiateur et d'utiliser son pouvoir de persuasion et de négociation afin de régler les plaintes à l'amiable. Il était également d'avis que la bonne approche aux problèmes relatifs à la protection de la vie privée était celle qui passait par un processus d'éducation, de discussion et d'examen du système de gestion de l'information d'une entreprise contre laquelle un individu se plaint, de sorte qu'il soit possible d'en identifier les failles et d'y apporter des correctifs systémiques.

Après l'adoption de la LPRPDE, les critiques relatives aux effets de ces choix législatifs devinrent plus précises. Ce qui suit est un très bref résumé de trois critiques formulées par les auteurs et relatives aux pouvoirs et fonctions de l'ombudsman ainsi que des réponses qui ont été données à ces critiques par la Commissaire à la protection de la vie privée.

1) Le modèle de l'ombudsman comparé à celui du tribunal administratif – critique du système de résolution des plaintes

Critique des auteurs. Ils mettent en doute l'efficacité du mécanisme de résolution des plaintes. En outre, ils estiment que les coûts impliqués, les délais et l'incertitude engendrés par ce mécanisme sont devenus des considérations déterminantes pour les parties qui désirent déposer une plainte. Un des problèmes qu'ils croient être à la source de cette ineffectivité est que le Commissariat rend uniquement publique de courts sommaires de ses enquêtes. En effet, cela a pour effet d'empêcher que les plaintes puissent servir de précédent et, par conséquent, de moyen efficace pour informer et guider les parties à l'avenir.

Réponse de la Commissaire. Le Commissariat n'est pas un tribunal administratif et, par conséquent, il ne devrait pas être évalué selon les mêmes critères. La commissaire à la protection de la vie privée agit comme un tiers neutre qui a le mandat de communiquer ouvertement avec les deux parties aux prises dans une affaire. Le commissaire doit travailler activement avec les parties pour résoudre le conflit afin d'en arriver à une solution juste. Son rôle est aussi pédagogique puisqu'elle doit tenter d'influencer la culture de protection de la vie privée à l'intérieur d'une entreprise n'agissant pas en conformité avec la loi. Le modèle axé sur les plaintes donne la possibilité aux individus d'être actifs à l'égard de la protection de leurs renseignements personnels et aux entreprises d'être conscientes de leurs pratiques de gestion des renseignements personnels qu'elles détiennent. La Commissaire ajoute qu'il ne faut pas faire abstraction du fait qu'elle peut toujours prendre l'initiative d'une plainte en vertu de la loi, lorsqu'il existe des motifs raisonnables de le faire. Enfin, elle estime que ses vastes pouvoirs d'enquête constituent en quelque sorte le contrepoids à l'absence du pouvoir d'émettre des ordonnances. En effet, lors d'une enquête, le rôle de la Commissaire est d'extraire tous les faits et toutes les considérations utiles et

nécessaires pour trouver une solution durable. Les solutions qui émergent sont utiles non seulement pour résoudre la plainte immédiate, mais également pour encourager des transformations systémiques vers une culture durable de respect de la vie privée. À son avis, le processus contradictoire qui s'imposerait, si elle était dotée du pouvoir d'émettre des ordonnances, ne lui permettrait pas de résoudre des conflits de d'une manière qui serait *a priori* et nécessairement plus efficace.

2) Divulgence des résultats d'enquêtes de plaintes et transparence

Critique des auteurs. Il y a manque de transparence quant aux initiatives du commissaire pour assurer la conformité avec la loi, notamment dans le refus de dévoiler les noms des entreprises qui ont fait l'objet de plaintes. Faute de conséquence à tout constat de non-conformité, il n'y a pas d'incitatif suffisant pour encourager les entreprises en défaut à changer leurs comportements. De plus, le manque de transparence priverait le public et les autres entreprises de connaissances très utiles sur les pratiques exemplaires qui auraient été proposées par le Commissariat à l'entreprise visée par la plainte d'un individu. Enfin, le manque de transparence résulte aussi en une difficulté d'évaluer si le système réglementaire fonctionne adéquatement.

Réponse de la Commissaire. La nature et la finalité de l'institution de l'ombudsman n'est pas compatible avec l'idée selon laquelle la Commissaire devrait divulguer plus d'information sur le traitement et le résultat des plaintes dans le but de dégager des précédents. Le modèle de l'ombudsman n'est pas destiné à créer des précédents normatifs qui lieront dans l'avenir les parties qui se trouveront dans des situations similaires. Les parties impliquées dans une plainte doivent pouvoir participer dans le processus en sachant que leurs situations personnelles seront prises en compte, tout en étant confiantes qu'elles peuvent participer dans la négociation de la solution qui sera retenue. Si les parties savaient dès le départ qu'une solution prédéterminée leur serait imposée, le processus de conciliation échouerait. En revanche, la commissaire, en demeurant toujours consciente de son obligation de confidentialité, a le pouvoir de divulguer les détails d'une plainte si ceux-ci sont d'intérêt public, tel qu'édicte au paragraphe 20(2) de la LPRPDE.

3) L'accès à la Cour fédérale

Critique des auteurs. L'accessibilité au recours devant la Cour fédérale doit être mise en doute, compte tenu des coûts que cette procédure engendre (en plus des coûts de la procédure de plainte devant le Commissariat). Le processus en deux étapes est long et coûteux : il est susceptible de décourager les plaintes, de réduire le nombre d'affaires qui pourraient être entendues par la Cour fédérale et qui lui permettraient d'interpréter la loi et d'étoffer la jurisprudence sur les principes sous-jacents à la protection des renseignements personnels. Ces coûts doivent aussi tenir compte de l'incertitude qu'engendre la procédure devant la Cour fédérale. En effet et d'une part, jusqu'à ce que certaines questions d'interprétation soient traitées par la Cour fédérale ou par la Cour d'appel fédérale, les plaignants ne sont pas en mesure d'évaluer les chances de succès d'un leur plainte. D'autre part, le Commissaire ne peut pas être certain qu'il a

adopté la bonne approche normative pour régler une affaire et il peut en résulter de la confusion chez les entreprises quant à la nature et à l'étendue de leurs obligations de protection. Par ailleurs, certains soulignent le manque d'expertise de la Cour sur les questions relatives à la protection des renseignements personnels, ce qui n'en fait pas le meilleur forum pour régler ce genre de litige. Enfin, ils estiment que puisque c'est à la Cour fédérale qu'il reviendrait de définir les dispositions de la loi, le rôle du commissaire serait marginal malgré son expertise en protection des renseignements personnels. Qui plus est, les décisions de la Cour pourraient aussi avoir pour effet de miner l'autorité du commissaire auprès des entreprises.

Réponse de la Commissaire. L'intervention de la Cour fédérale ne désavantage pas sérieusement les plaignants. Faire cette affirmation revient à négliger le fait que la commissaire peut, directement et au nom du plaignant, saisir la Cour fédérale d'une affaire. De plus, puisque la commissaire n'a pas de pouvoirs décisionnels exécutoires, elle a beaucoup de latitude pour assister et conseiller un plaignant qui veut directement saisir la Cour de sa plainte. L'ombudsman a été choisi comme modèle de mise en application de la LPRPDE avec l'intention d'éviter, lorsque cela est possible, le besoin de s'adresser à une cour et d'ainsi pouvoir proposer une réparation de manière informelle et peu coûteuse. La commissaire peut arriver à trouver une solution efficace et satisfaisante pour les parties à l'extérieur des tribunaux, ce qui allège le fardeau des plaignants.

*
* *

C'est donc dans ce contexte général où des critiques récurrentes étaient formulées à l'égard du modèle de l'ombudsman et des pouvoirs et fonctions que ce modèle inspire que nous avons effectué nos recherches et nos analyses en amont et en aval de l'adoption et la mise en œuvre de la loi.

Conclusions et recommandations spécifiques

Dans la partie I, nous avons analysé les idées économique, politique et juridique qui ont dominé le discours sous-jacent à l'élaboration de la LPRPDE ainsi que celles qui émergent dans le contexte contemporain afin de faire ressortir le plus clairement possible les points de convergence et de divergence entre les principaux éléments de ces discours passé et actuel.

Le discours économique

- Il favorise toujours l'imposition d'un minimum de contraintes aux entreprises dans le but de garantir l'accès aux marchés nationaux et internationaux.
 - Cependant, la réflexion sur le rôle de la réglementation sociale (catégorie à laquelle fait partie la LPRPDE) a progressé vers une plus grande sensibilité à l'égard de la protection des consommateurs.

- En effet, que l'État ait pour objectif de protéger ses citoyens (consommateurs) contre les abus de pouvoir des entreprises est conçu comme étant un rôle contemporain tout à fait légitime.
- L'idée de protection du consommateur doit être pensée au niveau intranational, mais aussi au niveau supranational puisque les États doivent, dans la mesure du possible, harmoniser leurs réglementations sociales de manière à garantir une protection efficace contre les échanges d'information entre les États.
- Ce dernier objectif est d'autant plus important que les développements technologiques du Web 2.0 laissent présager la nécessité d'une telle harmonisation : la loi doit s'insérer dans un réseau de normes pour être effective. Lorsqu'on tient compte de ces nouveaux développements technologiques, l'idée de consolider le Système d'intégrité sur les plans national et international prend tout son sens. À cet égard, des recherches additionnelles et ciblées sur les répercussions de ces changements technologiques sur la capacité des organismes publics à mettre en œuvre leur mission de protection des renseignements personnels seraient essentielles à la réflexion sur l'effectivité de la LPRPDE.

Le discours politico-administratif

- Bien que le discours politico-administratif sur l'organisation et les pouvoirs des organismes publics chargés de mettre en œuvre les lois n'ait pas changé de façon radicale, le dogmatisme des idées qui prévalaient durant les années 1980 et qui militaient contre la mise sur pied de nouveaux organismes publics semble s'être estompé. Ceci est particulièrement vrai lorsqu'on recense le nombre d'organismes parlementaires de surveillance des activités de l'administration qui ont été créés pour les fins de consolider notre Système national d'intégrité. En effet, on peut noter un réel engouement des politiciens pour ces organismes de surveillance depuis les quatre dernières années.
 - Il serait utile de mieux comprendre les fondements et les limites des compétences qui peuvent être attribuées à ce type d'organisme, surtout lorsqu'ils sont appelés à agir dans le secteur privé. Cette réflexion sera particulièrement pertinente dans le contexte où le législateur envisagerait d'ajouter des pouvoirs (tels des pouvoirs de nature réglementaire et pénale) au Commissariat, pouvoirs qui ne sont pas normalement associés à ceux d'un ombudsman que celui-ci relève ou non du Parlement.
- Enfin, il apparaît que le remplacement du Commissariat par un organisme faisant partie de la catégorie des organismes décentralisés et, plus précisément, par un organisme de régulation sociale ('sociale' et non 'économique' puisque la LPRPDE est une réglementation sociale et non économique) et doté de pouvoirs de nature administrative (tels le pouvoir d'enquête), décisionnel (tels le pouvoir d'émettre des ordonnances et d'infliger des peines) et réglementaire pourrait être une option envisageable.

Le contexte juridique

- Il faut noter l'élévation du droit à la protection des renseignements personnels au statut de norme quasiconstitutionnelle. Ce statut militerait en faveur d'offrir de meilleures protections aux citoyens et consommateurs relativement à l'usage de leurs renseignements personnels.
 - Il faut aussi mentionner l'importance de sauvegarder l'autonomie des individus et des décisions qu'ils prennent relativement à l'usage de leurs renseignements personnels. Veulent-ils plus de protection? Peut-on observer des tendances distinctes selon les générations en cause? Est-ce que le Commissariat pourrait être conçu non seulement comme un lieu où on éduque le public, mais aussi comme un lieu où *on apprend du public*? À cet égard, serait-il indiqué pourvoir le Commissariat de fonds (et des pouvoirs) nécessaires pour tenir périodiquement des fora de citoyens, dont le but serait de mieux comprendre leurs attentes en plus de celles exprimées par l'industrie et des groupes d'intérêts?
- Il faut également prendre note de la construction du droit administratif global relatif à la protection des renseignements personnels depuis plus de 20 ans. Celle-ci se poursuit et se complexifie. À cet égard, on peut mentionner plusieurs initiatives : Initiative espagnole et Projet Gallway ayant des visées harmonisatrice ainsi que le GPEN visant une meilleure exécution des normes, l'initiative de l'Agence mondiale anti-dopage relative à la protection des renseignements personnels des athlètes, et, finalement, le cadre normatif de l'APEC avec ses projets Pathfinders et le Cross-Boarder Privacy Rules System. Toutes ces initiatives sont riches d'enseignements pour réfléchir aux options de réformes.
 - Des recherches additionnelles seraient nécessaire afin de mieux comprendre quelles sont les forces et les faiblesses de notre système canadien de protection des renseignements au regard de ce réseau de normes faisant partie du droit administratif global.
 - Il pourrait aussi être utile d'envisager l'attribution de pouvoirs au Commissariat afin qu'il puisse clairement participer aux débats à l'échelle supranationale et peut-être même constituer un comité de coopération (composé du Commissaire fédéral et des commissaires provinciaux, de fonctionnaires fédéraux et provinciaux, de représentants d'industries (petites, moyennes et grandes), de groupes d'intérêts (notamment de protection des consommateurs) et de citoyens. Il s'agirait en quelque sorte de créer une délégation canadienne (sous forme d'un conseil consultatif) ayant suffisamment d'autorité pour discuter des questions relatives à la protection des renseignements personnels et qui pourrait intervenir sur la création des normes et mécanismes du droit administratif global dans ce domaine.
- Il faut souligner que les problèmes constitutionnels soulevés par l'adoption de la LPRPDE en 2000 ne sont toujours pas résolus. S'il était envisagé d'attribuer des pouvoirs d'ordonnance au Commissaire et que ceux-ci pouvaient être appliqués à toutes les entreprises canadiennes, cela susciterait des débats fédéraux-provinciaux houleux. À cet égard, il est essentiel d'exercer une vigile juridique à l'égard des débats des cours de

justice, notamment sur la validité des processus d'harmonisation. Sur ce point, le Renvoi à la Cour suprême relatif à la création d'un organisme de réglementation fédérale relatif aux valeurs mobilières est à suivre. Les motifs de la Cour pourraient vraisemblablement aller dans la direction d'une interprétation plus fonctionnelle du partage des compétences législatives, ce qui ouvrirait la voie à la mise en œuvre d'une forme de fédéralisme en réseau, incluant toutes les entités de la fédération (fédérale, provinciales et municipales). À titre d'exemple, une interprétation fonctionnelle pourrait mener les entités de la fédération à conclure une ou des ententes fédérale-provinciales (et municipales) afin d'assurer une meilleure exécution de la loi compte-tenu des problèmes contemporains. Par ailleurs, il serait également utile de se pencher sur la possibilité de créer un secrétariat fédéral, au sein du Commissariat, et ayant pour fonction de coordonner la réflexion et la recherche à tous les niveaux de gouvernements (incluant les gouvernements municipaux). Ces travaux auraient des visées réformatrices et auraient pour objectifs de fournir les données et les analyses nécessaires pour trouver les meilleures solutions et pratiques administratives pour régler les problèmes soulevés liés aux nouvelles utilisations des technologies de l'information contemporaines.

- S'agissant de l'attribution d'éventuels pouvoirs de nature pénale, il faut souligner que, pour l'heure, et au sein du gouvernement fédéral, il semble bien que seul le CRTC (un organisme de régulation économique) en soit pourvu.
 - Au Québec, le Tribunal des droits de la personne peut octroyer des dommages-intérêts punitifs aux personnes physiques et morales violant sciemment la Charte des droits et libertés de la personne. Il est utile de noter à cet égard que le Tribunal des droits de la personne se penche sur la violation de droits de nature quasi-constitutionnelle. En effet, puisque la protection des renseignements personnels a vraisemblablement acquis ce statut juridique, des analogies pourraient être faites pour justifier l'attribution de tels pouvoirs au Commissariat.

Dans la Partie II, nous avons exploré en détail le milieu opérationnel du CPVP relatif à la LPRPDE. En vue de souligner les critères d'évaluation appropriés, nous avons exploré les perspectives empiriques, comparatives et normatives du modèle d'ombudsman du CPVP.

- **D'un point de vue empirique**
 - Un examen des extraits du CPVP fondé sur les données uniquement n'est pas satisfaisant. Le fait que le nombre de demandes ou de plaintes ait augmenté ou diminué ne révèle pas si le modèle du CPVP visant à assurer la conformité à la LPRPDE fonctionne bien.
 - Les données à elles seules peuvent appuyer les arguments relatifs à l'efficacité ou à l'inefficacité du CPVP. Les données qualitatives sur les évaluations des intervenants et universitaires quant au CPVP peuvent enrichir les données quantitatives.
 - La perception commune à l'effet que le modèle du CPVP est beaucoup plus efficace au sein des industries établies comme celle des banques ou de l'assurance qu'au sein des petites entreprises,

où les renseignements personnels risquent d'être vulnérables, est particulièrement frappante.

- **D'un point de vue comparatif**
 - L'évaluation actuelle de la LPRPDE et du CPVP peut être améliorée par l'intégration des leçons susceptibles d'être tirées d'autres administrations canadiennes (notamment le Québec, l'Alberta et la Colombie-Britannique.) de même que des États-Unis et du Royaume-Uni.
 - Au sein des autres administrations canadiennes, par exemple, nous avons remarqué que l'expérience du Québec démontrait que l'indépendance et l'impartialité, à titre de normes du droit administratif de base, offraient les fondements sur lesquels reposent la conception institutionnelle et la recherche d'un modèle optimal. Les exemples de l'Alberta et de la Colombie-Britannique montrent que le modèle d'ombudsman peut coexister avec d'autres mesures d'exécution et de conformité et les compléter, y compris les pouvoirs de rendre des ordonnances.
 - Les exemples des États-Unis comme la FCC et la FTC sont le reflet de la transition des règlements spéciaux politisés vers des règlements stratégiques fondés sur des données probantes. Cette approche envers la réglementation met l'accent sur la planification, l'établissement de points de référence et l'évaluation du rendement.
 - En Europe, nous avons observé que le juridisme de coopération représentait un cadre pratique afin de comprendre la façon dont un plus grand rôle pour l'État et un plus grand rôle pour le marché pouvaient constituer des objectifs complémentaires pour un organisme de réglementation. L'exemple européen, comme celui d'autres organismes canadiens de réglementation en matière de protection de la vie privée, suggère un mélange complexe et complémentaire des modèles d'ombudsman et du pouvoir de rendre des ordonnances.
- **D'un point de vue normatif**
 - Le choix des critères d'évaluation est une expression de certaines valeurs particulières. Par exemple, le fait que Bennett et Raab donnent priorité à l'économie, à l'efficacité, à l'efficacité et à l'équité, qui sont liées à la sphère de la protection de la vie privée, donne à penser que la mesure de la justice distributive dans la réglementation en matière de protection de la vie privée (qui offre la meilleure protection des données?) est tout aussi importante que le fait de veiller à ce que l'industrie respecte la loi.

Qu'il soit analysé du point de vue empirique, comparatif ou normatif, nous sommes d'avis qu'il y a des éléments qui confirment que le modèle d'ombudsman du CPVP est un succès, ce qui a eu une incidence concrète et importante sur les objectifs énoncés dans la LPRPDE, et d'autres qui donnent à penser que le CPVP est restreint dans la réalisation de son mandat en vertu de la LPRPDE. Nombreux sont ceux qui appuient l'argument selon lequel une transition vers une LPRPDE orientée vers la protection des consommateurs ou un effort afin de veiller au respect de la LPRPDE par les petites entreprises nécessitent l'obtention de plus grands pouvoirs de rendre des ordonnances afin de compléter les responsabilités d'ombudsman actuelles.

RAPPORT DE RECHERCHE

INTRODUCTION GÉNÉRALE

L'évaluation de l'effectivité des législations adoptées par nos élus est un objet de préoccupation grandissant pour des pays du monde entier. Depuis environ une trentaine d'années, les États-Unis, le Canada, l'Australie, la Nouvelle-Zélande, les pays membres de l'Union européenne y compris l'Angleterre (pour ne mentionner que ceux-là) ont affecté des ressources humaines et financières importantes à la mise en œuvre de ce projet évaluatif. Maintenant mieux connus par des expressions telles que « réglementation intelligente » au Canada, « *smart regulation* » aux États-Unis, « *better regulation* » en Angleterre ou « réglementation de qualité » dans l'Union européenne, ce vaste projet a influé sur la conception des systèmes réglementaires ainsi que l'élaboration et l'exécution des réglementations prescrites par ces États. Au niveau du gouvernement fédéral canadien, ce projet a pris une forme plus structurée et plus définitive avec l'approbation par le Cabinet de la *Directive sur la rationalisation de la réglementation*¹.

Ce projet de rationalisation de la réglementation implique donc un processus évaluatif continu, allant de la naissance à la mort des lois et règlements prescrits par les autorités étatiques. À cet égard, plusieurs lois édictées dans les 10 ou 15 dernières années comprennent fréquemment des dispositions législatives

1 Au Canada, le concept de réglementation intelligente a été formellement adopté par le Cabinet fédéral en 2007 : Canada, Gouvernement du Canada, *Directive du Cabinet sur la rationalisation de la réglementation*, Ottawa, Sa Majesté la Reine du chef du Canada, 2007, 16 p. La Directive est disponible en format électronique sur le site du gouvernement du Canada : <http://www.tbs-sct.gc.ca/ri-qr/directive/directive00-fra.asp> (dernière visite le 23 août 2008). Cette Directive est entrée en vigueur le 1^{er} avril 2007.

exigeant qu'un examen quinquennal soit fait. Cet examen vise à vérifier si, et dans quelle mesure, les objectifs législatifs ont été atteints et, dans la négative, s'il serait souhaitable de modifier la législation afin d'arriver à ce but.

Une telle disposition a été insérée dans la Partie I de la *Loi sur la protection des renseignements personnels et les documents électroniques*² (LPRPDE). Le premier examen a eu lieu en 2006; le second se déroulera en 2011. C'est en vue de ce deuxième examen qu'il nous a été demandé de rédiger ce rapport de recherche. Le projet spécifique qui nous a été confié porte sur une évaluation de l'effectivité de l'institution de l'ombudsman, à titre d'autorité administrative en charge de la mise en œuvre de la LPRPDE. La question générale qui nous a été posée est la suivante : Est-ce que ce modèle peut protéger les renseignements personnels des individus détenus par le secteur privé? Possède-t-elle des pouvoirs suffisants et adaptés pour relever les défis contemporains soulevés dans la fédération canadienne, mais aussi à l'échelle mondiale?

Pour répondre à ces questions, nous nous sommes engagés dans un processus d'évaluation dans le but de mesurer les succès et les insuccès dans l'exécution de la *Loi*. Toutefois, le mandat ne vise pas à prendre des mesures quantitatives de ces succès et insuccès (mesurer l'*efficience*), mais à procéder à une évaluation qualitative (qui peut être une étude d'*efficacité* ou d'*effectivité*). Avant de préciser plus avant les termes de ce mandat, précisons ce qu'il faut entendre par *efficience*, en distinguant ce concept de celui d'*efficacité* et d'*effectivité*.

- ***Cadre analytique***

Le concept d'efficience provient de la science économique³. Un système est qualifié d'efficace sur le plan économique lorsque « l'allocation des ressources rares entre les différents producteurs et leur utilisation conduisent à un ensemble de biens produits tel qu'il n'existe pas d'autres ensemble comportant plus de chacun des biens produits⁴ ». L'idée générale sous-jacente au concept d'efficience est que rien de plus ne peut être réalisé compte tenu des ressources disponibles (on dira alors que le système est optimal). Un système économique est jugé plus efficace qu'un autre s'il peut fournir des biens et des services à la société sans que plus de ressources en travail et en capital ne soient utilisées.

2 *Loi sur la protection des renseignements personnels et les documents électroniques*, L.C. 2000, chap. 5, art. 29(1).

3 Claude Jessua, Christian Labrousse et Daniel Vitry (dir.), *Dictionnaire des sciences économiques*, Paris, PUF, 2001, p. 345. Dans ce dictionnaire, les auteurs utilisent le terme *efficacité* plutôt qu'*efficience*. Toutefois, dans ce rapport, nous utiliserons le terme *efficience* économique, afin d'éviter les confusions entre les concepts utilisés dans les deux disciplines.

4 *Id.*, p. 345.

En revanche, l'efficacité et l'effectivité sont deux concepts qui appartiennent à la sociologie du droit⁵. L'efficacité est un concept évaluatif de la *mise en œuvre* des normes juridiques. Une loi est qualifiée d'efficace lorsqu'elle atteint l'effet désiré (voulu ou recherché) par le législateur. À tout le moins, il doit s'agir d'un effet qui se situe dans la direction souhaitée par le législateur et non pas en contradiction avec elle⁶. Dans son acception dominante, l'efficacité du droit désigne la mesure, en termes d'écart, entre la norme juridique et le comportement qu'elle est censée régir⁷. En somme, les études d'efficacité jettent uniquement un regard en aval de la loi. C'est pour cette raison que ce type d'évaluation est une méthode critiquée par certains chercheurs qui la trouve trop réductrice et qu'ils y ont substituée celle plus large d'effectivité⁸.

Tout comme l'efficacité, l'effectivité est aussi un concept évaluatif de la norme juridique, mais porte un regard non seulement sur sa mise en œuvre, mais aussi sur son processus de production et de réception chez les acteurs sociaux. Afin de mieux capter la richesse d'un phénomène juridique dans toutes ses dimensions matérielles et temporelles, les études d'effectivité permettent l'évaluation de tous les effets susceptibles d'être engendrés par un phénomène juridique. Les études d'effectivité peuvent porter sur tout ou partie du cycle de vie d'un phénomène juridique de son émergence à son déclin, puis à sa fin. Donc, le concept effectivité comprend celui d'efficacité, mais il ne se limite pas à l'examen des seuls effets désirés, voulus ou recherchés par le législateur, mais s'étend aussi aux autres effets d'une loi. Par cette évaluation, les chercheurs examinent tant ce qui se passe en amont qu'en aval de la loi afin de comprendre et d'expliquer les multiples effets d'une loi, au-delà de ceux explicitement inscrits dans une loi. Par exemple, dans le contexte de la LPRPDE, nous nous intéressons non seulement à déterminer si les renseignements personnels sont mieux protégés en raison de cette loi, mais nous nous intéressons aussi aux autres effets que pourrait avoir la culture de la protection des renseignements personnels, tels que la professionnalisation d'agents de protection de la vie privée dans les grandes entreprises, ou l'amélioration de la conformité par l'entremise de l'information fournie à l'échelon municipal pour soutenir le lancement de petites entreprises.

- **Termes du mandat**

Ce bref tour d'horizon de ces trois concepts évaluatifs permet de circonscrire plus clairement le mandat de recherche qui nous a été confié. Il s'agit, en effet, d'évaluer l'effectivité de la LPRPDE. Toutefois, il ne s'agit pas de faire une

5 Pierre Lascoumes et Évelyne Serverin, « Théories et pratiques de l'effectivité du droit », (1986) 2 *Droit et Soc.* 101.

6 Guy Rocher, « L'effectivité du droit », dans Andrée Lajoie, Roderick A. MacDonald, Richard Janda et Guy Rocher (dir.), *Théories et émergence du droit : pluralisme, surdétermination et effectivité*, Montréal, Éditions Thémis, 1998, p. 133-149.

7 Luzius Mader, *L'évaluation législative. Pour une étude empirique des effets de la législation*, Lausanne, Payot, 1985, p. 57.

8 P. Lascoumes et É. Serverin, *supra*, note 5.

étude d'effectivité complète comportant une analyse de tous les effets voulus et non voulus, immédiats et différés, concrets ou symboliques de la production, réception et mise en œuvre de cette loi. Notre mandat est plus modeste dans ses visées. Il comporte deux volets principaux, soit l'étude de l'effectivité souhaitée et de l'effectivité observée. Ces deux volets forment l'ossature de ce rapport

Plus précisément, il nous a d'abord été demandé d'examiner le contexte d'émergence de la *Loi*, y compris les politiques publiques sous-jacentes à la genèse de la *Loi* et l'historique du cadre juridique jusqu'à ce jour, ainsi que le contexte actuel. L'objectif étant ici d'identifier des changements importants qui se sont produits depuis que la *Loi* est en vigueur et qui permettent d'identifier de nouvelles pistes de recherche portant sur des avenues possibles de modifications aux politiques publiques sous-jacentes à la *Loi*. Ensuite, il nous a été demandé d'examiner les fonctions et les pouvoirs attribués au Commissariat à la protection de la vie privée (l'ombudsman) ainsi que leur utilisation par les commissaires nommés pour occuper cette charge publique depuis l'adoption de la *Loi*. L'objectif de ces analyses étant d'évaluer l'impact de ce modèle sur l'observance de la *Loi* par les organismes qui y sont assujettis. Enfin, il nous a été demandé d'examiner d'autres modèles institutionnels canadiens et étrangers (également créés pour réglementer l'usage des renseignements personnels par des organismes du secteur privé) dans une perspective comparative, et ce, dans le but d'identifier s'il existe ailleurs des pratiques qui seraient mieux adaptées au contexte actuel.

- *Limites de la recherche*

Deux limites importantes de cette recherche doivent être soulignées d'emblée. D'une part, les auteurs de ce rapport ne sont pas des spécialistes des lois relatives à la protection des renseignements personnels. En tant que professeurs de droit administratif, les auteurs possèdent une expertise notamment sur les systèmes réglementaires, l'organisation, les fonctions et pouvoirs des organismes composant l'administration publique. C'est dans cette optique qu'il faut lire ce rapport et comprendre le mandat qui nous a été confié. En effet, la commissaire à la protection de la vie privée a retenu nos services parce que sa préoccupation principale porte sur la question de savoir si l'institution de l'ombudsman est un modèle adéquat pour garantir une application effective de la LPRPDE. D'autre part, notre mandat de recherche a pour objet une analyse de ce que le législateur a fait (posture descriptive) et non de ce qu'il aurait dû accomplir (posture normative) ou ce qu'il devrait accomplir (posture prescriptive). De plus, il s'agit d'une recherche de type exploratoire et l'objectif principal est d'identifier des lacunes dans les connaissances. En conséquence, il ne s'agit pas ici de formuler des conclusions généralisables, mais simplement d'identifier des propositions ou des hypothèses de recherches futures ainsi que des pistes de réformes législatives.

- *Plan du rapport*

Ce rapport est divisé en deux parties. La première partie porte sur l'effectivité souhaitée par différents acteurs étatiques et sociaux impliqués dans l'élaboration de cette nouvelle politique publique visant la protection des renseignements

personnels dans le secteur privé. Ces discussions ayant mené à l'adoption de la LPRPDE se sont déroulées dans un contexte économique, politique et juridique propre aux années 1990. En 2010, ce contexte a changé. Dans l'optique de situer des problèmes plus actuels et afin d'orienter les discussions futures lors de la prochaine ronde de l'examen parlementaire de l'effectivité de la LPRPDE, nous aborderons également dans cette première partie quelques thèmes émergeant dans le contexte contemporain. Dans la deuxième partie, il s'agit plutôt de faire un bilan évaluatif de l'effectivité observée de la *Loi*. Passant tout d'abord par une description des choix qui ont été faits par le législateur dans la LPRPDE, nous proposons ensuite une étude comparative d'autres modèles institutionnels existant au Canada et ailleurs pour terminer sur un examen de certaines questions entourant l'évaluation du Commissariat à la protection de la vie privée.

PARTIE I – La LPRPDE : Une loi intégrée dans le droit de la concurrence

L'effectivité souhaitée d'une loi se retrace par l'analyse du contexte d'émergence de celle-ci en vue de décrire les multiples questions et problèmes dont le législateur a dû tenir compte avant même de proposer le nouveau projet de loi. Nous procéderons par un examen du discours des acteurs publics et privés sur les contraintes économiques, politiques et juridiques qui ont influencé les orientations de la future politique publique qui deviendra la LPRPDE. Parce que l'effectivité souhaitée s'intéresse à des événements qui sont survenus dans le passé, la méthode la plus efficace pour faire l'analyse du discours des acteurs publics et privés qui ont participé au processus est celle de l'examen de la documentation disponible et pertinente à cette époque. Cependant, puisque notre objectif est également d'identifier des pistes de recherches futures relatives à la LPRPDE, il importe aussi de vérifier si, et dans quelle mesure, ces contraintes que nous avons déjà identifiées dans le contexte d'émergence de la loi sont les mêmes dans le contexte contemporain. Dans le cas contraire, les autorités gouvernementales devront s'interroger sur l'influence que ces nouvelles contraintes pourraient exercer sur toute proposition de réforme envisagée.

Section 1. Le contexte général d'émergence de la LPRPDE

Bien qu'une loi fédérale sur la protection des renseignements qui s'appliquerait au secteur privé fût revendiquée depuis la fin des années 1980⁹, ce n'est qu'en 1996 que le ministre d'Industrie Canada promet une loi-cadre sur la protection des renseignements personnels. Au mois d'avril 1997, le Comité permanent sur les droits de la personne et des personnes handicapées dépose un rapport intitulé *La vie privée : où se situe la frontière*¹⁰. Le Comité propose de

9 Nancy Holmes, *Les lois fédérales du Canada sur la protection de la vie privée*, Ottawa, Bibliothèque du Parlement, Service d'information et de recherche parlementaires, 2008, p. 2.

10 Canada, Parlement, Comité permanent sur les droits de la personne, *La vie privée : où se situe la frontière*, Ottawa, Services et Approvisionnements Canada, 1997.

remplacer la *Loi sur la protection des renseignements personnels* par une autre loi qui s'appliquerait au Parlement et à toutes les agences gouvernementales, ainsi qu'au secteur privé relevant de la compétence fédérale. Au mois de janvier 1998, les ministères de l'Industrie et de la Justice publient un document de travail intitulé *La protection des renseignements personnels — Pour une économie et une société de l'information au Canada*.

Outre ces documents, il existe très peu d'articles savants discutant spécifiquement de l'organisation et du fonctionnement du futur cadre juridique. La documentation disponible fut essentiellement produite par ou pour le gouvernement. En effet, certains experts sur la vie privée ont rédigé, à la demande d'Industrie Canada, des études en préparation de l'élaboration d'un cadre juridique relatif à la protection des renseignements personnels dans le secteur privé. Les études les plus influentes qui ont été écrites pour le gouvernement sont celles de Lawson¹¹ et Bennett (notamment celle sur les mécanismes de mise en œuvre de la loi¹²). Mais le document le plus important est le document de travail produit à la demande des ministères de l'Industrie et de la Justice par le Groupe de travail sur le commerce électronique¹³. Par un avis publié dans la *Gazette du Canada*, le gouvernement a sollicité des commentaires sur ce document de travail. Les mémoires devaient être déposés au plus tard le 27 mars 1998¹⁴.

En somme, les discussions entourant une future politique publique relative à la protection des renseignements personnels dans le secteur privé ont commencé il y a environ une vingtaine d'années au Canada. À cette époque, c'est-à-dire autour de la fin des années 1980¹⁵, trois facteurs principaux ont eu un impact fondamental sur l'énoncé de politique publique du gouvernement du Canada et qui allait servir à élaborer le futur projet de loi.

Premièrement, l'énorme potentiel économique d'Internet ouvrait une nouvelle page de l'histoire économique mondiale, celle de l'ère de l'information et de l'économie du savoir. Étant donné ce potentiel économique dont les

11 Ian Lawson, *Protection de la vie privée et l'autoroute de l'information : les options du Canada en matière de réglementation*, Ottawa, Industrie Canada, 1995.

12 Colin Bennett, *Regulating Privacy in Canada: An Analysis of Oversight and Enforcement in the Private Sector*, Ottawa, Industrie Canada, 1996.

13 Gouvernement du Canada, ministères de l'Industrie et de la Justice, Groupe de travail sur le commerce électronique, *La protection des renseignements personnels. Pour une économie et une société de l'information au Canada*, Services de distribution, Direction générale des communications, 1998, 30 p.

14 *Gazette du Canada*, partie I, vol. 132, n° 4 — Le 24 janvier 1998, avis n° IPPB-002-98 — Publication d'un document de discussion sur la protection des renseignements personnels sur le marché.

15 Canada, Parlement, Chambre des communes, Comité permanent de la justice et du Solliciteur général, *Une question à deux volets : comment améliorer le droit d'accès à l'information tout en renforçant les mesures de la protection des renseignements personnels, Accès et renseignements personnels : les prochaines étapes*, Ottawa, Gouvernement du Canada, 1987, 63 p.

ramifications étaient encore partiellement maîtrisées, il était difficile pour un gouvernement de poser des contraintes trop importantes dans ce nouvel environnement sans être en mesure d'expliquer les justifications économiques sous-jacentes à celles-ci. Une intervention musclée prématurée aurait été considérée comme posant le risque de nuire au développement des entreprises canadiennes. Cette préoccupation s'inscrivait dans le courant d'idées économiques dominantes de l'époque dont certaines feront l'objet d'un premier développement.

Ces idées économiques ont eu une influence déterminante sur le plan politique. Tout en mettant un terme à la domination des idées fondatrices de l'État providence, les théories économiques qui se sont progressivement imposées à partir des années 1970 ont également ouvert une nouvelle ère de la gouvernance publique. Au début des années 1980, les programmes réglementaires n'étaient plus vus comme des instruments efficaces pour remédier aux défaillances du marché : ils étaient dorénavant conçus comme étant pathogènes en soi. Il fallait donc éviter de créer de nouveaux programmes réglementaires dans la mesure du possible, mais si cela devenait indispensable, il fallait tenir compte d'un nouvel ensemble de valeurs et de principes. Le deuxième développement sera consacré à cette question.

Enfin, le contexte juridique national et international concourait aussi en faveur de certaines orientations dans le futur projet de loi. En effet, les connaissances du moment sur le partage des compétences entre les gouvernements fédéral, provinciaux et territoriaux militaient en faveur d'une intervention prudente du gouvernement fédéral dans le domaine de la protection des renseignements personnels. Par ailleurs, il y avait déjà émergence d'une démarche normative portant sur la protection des données personnelles tant à l'intérieur qu'à l'extérieur du Canada et, étant donné le nouvel impératif politique de coordination des actions et d'harmonisation des normes, les pressions en faveur d'une législation compatible avec les objectifs commerciaux étaient fortes. Nous en discuterons en troisième lieu.

1.1 Le contexte économique : Au carrefour de modèles économiques

Une économie de marché suppose la propriété privée des moyens de production et un système régulateur qui assure la coordination du marché. Le mécanisme des prix et l'action de la concurrence constitue les deux éléments-clés du mécanisme de coordination¹⁶. En conséquence et selon la théorie économique classique¹⁷, l'État ne doit pas directement intervenir dans le fonctionnement des lois du marché dans le but de réguler la demande.

16 *Dictionnaire des sciences économiques, supra*, note 3, p. 544.

17 Adam Smith, *Recherche sur la nature et les causes de la richesse des nations*, (trad. G. Garnier), vol. 2, Paris, Flammarion, 1991; Pierre Rosanvallon, *Le libéralisme économique : histoire de l'idée de marché*, Paris, Seuil, 1989, 237 p.

Dans les années 1930, Keynes a contesté le bien-fondé de cette idée issue de la théorie économique classique. Le modèle keynésien, qui a été appliqué dans les États occidentaux incluant le Canada entre 1945 et 1974 a été, comme on le sait, sévèrement critiqué à la suite des deux chocs pétroliers qui ont secoué l'économie durant les années 1970. Ce sont ces critiques qui ont marqué un retour aux fondements de la théorie de l'économie classique pour plusieurs chercheurs qui se sont regroupés sous la bannière l'École néoclassique. Ceux-ci ont fortement influencé les politiques économiques des États, notamment celles des pays membres de l'OCDE à partir des années 1970. Au Canada, cette tendance devient plus prégnante au début des années 1980 et elle est toujours présente de nos jours. Cependant, certaines prises de position des théoriciens néoclassiques et relatives aux interventions limitées de l'État dans l'économie ont été modifiées au début des années 1990 par la théorie de la croissance économique endogène. Cette théorie a été particulièrement influente en raison des nouveaux défis que posait la mise en place de l'économie du savoir.

C'est donc au carrefour des courants théoriques économiques établis et émergents que débute la réflexion sur la protection des renseignements personnels notamment au sein de l'OCDE, des États-Unis, de la communauté européenne et du Canada. Au moins trois idées économiques principales ressortent de la documentation. D'abord, il est reconnu qu'il existe une tension entre la libre circulation de l'information et la propriété des renseignements personnels. Ensuite, les règles générales du droit de la concurrence semblaient inefficaces pour contrer l'usage abusif des renseignements personnels. Finalement, il devait y avoir un équilibre entre la libre concurrence et la protection des consommateurs afin de favoriser l'établissement d'un environnement propice à l'innovation technologique. C'est donc dans l'esprit de faire converger les idées d'une saine concurrence dans le cours du développement de la nouvelle économie du savoir qu'il est possible de comprendre les choix économiques qui ont présidé à l'élaboration de la LPRPDE.

1.1.1 La libre circulation de l'information et propriété des renseignements personnels

Au début des années 1950, l'École néoclassique devient la principale école de pensée aux États-Unis. Son influence grandit considérablement durant les années soixante-dix et au-delà des frontières américaines¹⁸, si bien qu'elle forme le cœur des programmes de grands partis politiques aux États-Unis, en Europe (notamment en Angleterre), en Australie, Nouvelle-Zélande ainsi qu'au Canada au début des années 1980.

Le modèle économique des néoclassiques est celui de l'économie de l'offre. Selon ce modèle, la manière la plus effective de soutenir la croissance

18 Bernard Guerrien, *L'Économie néo-classique*, Paris, La Découverte, 1989, 128 p.

économique est d'aider les entreprises à produire davantage de biens et services, de les inciter à entrer sur de nouveaux marchés et de lever le plus possible les freins fiscaux et réglementaires qui entravent leur développement. Selon cette optique, les interventions étatiques sont jugées légitimes lorsqu'elles ont pour objectif de réglementer les pratiques qui faussent le libre jeu de la concurrence. Toute réglementation visant des pratiques économiques n'étant pas décrétées anticoncurrentielles par le droit de la concurrence était en général fortement contestée parce qu'elle était jugée inefficace sur le plan économique. Les théoriciens estimaient que cette réglementation produisait des coûts élevés, ce qui signifie qu'elle n'offrait pas la combinaison optimale des facteurs de production recherchée pour atteindre l'efficacité économique. Cette réflexion a exercé une influence déterminante sur la mise en œuvre des politiques de dérèglementation.

Au Canada, c'est surtout la réglementation économique qui a été la cible d'attaques vigoureuses des économistes et des gens d'affaires. Cependant, la réglementation sociale, catégorie dans laquelle la LPRPDE s'inscrit (la LPRPDE n'a pas pour objet de poser des barrières à l'entrée dans un marché, mais plutôt de protéger les consommateurs), n'a pas été autant affectée par cette vague de dérèglementation qu'elle ne l'a été aux États-Unis. C'est entre autres ce qui explique que la création d'une telle politique publique d'envergure fédérale ait pu être envisagée au Canada alors qu'une telle loi générale n'a pas encore vu le jour aux États-Unis¹⁹. Conséquemment, la question se pose à savoir : Quelle est la fonction économique d'une loi telle que la LPRPDE?

Les documents gouvernementaux des années 1990 laissent penser qu'un double objectif était dans la mire des autorités étatiques : favoriser la circulation de l'information tout en protégeant la propriété des renseignements personnels appartenant aux consommateurs. Dans le document produit en 1998 par le Groupe de travail sur le commerce électronique (le « Groupe de travail ») formé conjointement par Industrie et Justice Canada²⁰, ces paramètres constituent le cadre des discussions sur les contours de la future politique publique. Sur l'objectif de la circulation de l'information, on peut lire : « Il faut également [...] des règles permettant aux particuliers, aux institutions et aux entreprises d'échanger facilement des renseignements [...] il faut éviter de créer un "paradis des données" ou d'obstacles à la libre circulation de l'information²¹. » Sur l'objectif de protéger les renseignements personnels, le document précise qu'il s'agit de protéger le « droit de chacun à décider quand, comment et dans quelle mesure il souhaite partager avec autrui des renseignements personnels²² ».

19 Paul M. Schwartz, « Privacy and Preemption », (2009) 118 Yale L. J. 902, 912. L'auteur explique que les États-Unis ont plutôt adopté une approche sectorielle et n'ont pas adopté une loi générale couvrant le secteur privé.

20 Groupe de travail sur le commerce électronique, *supra*, note 13.

21 *Id.*, p. 2 et 14.

22 *Id.*, p. 5.

Par ailleurs, dans ce document on fait également valoir le rôle des renseignements personnels dans l'économie : il « devient de plus en plus pressant de recueillir et d'utiliser comme jamais auparavant des renseignements personnels ». Mais on invoque du même souffle l'instauration d'un « système équitable où l'usage abusif de renseignements personnels ne pourra conférer un avantage concurrentiel²³ ».

1.1.2 L'usage abusif des renseignements personnels

Dans un autre document produit pour Industrie Canada, l'avocat Rick Shields énumère les différentes formes de renseignements personnels accessibles au public et explique comment ces seules sources, prises ensemble, sont un terrain fertile pour des organismes privés leur permettant de compiler des renseignements personnels sur les habitants d'un territoire²⁴. On savait déjà à l'époque que certaines compagnies privées possédaient de très grandes quantités de renseignements personnels sur leurs clients. On n'a qu'à penser aux banques, aux compagnies d'assurance, de télécommunications, de transport, etc. Plusieurs craintes ont été formulées par les entreprises et les consommateurs à l'égard de l'usage potentiellement abusif de ces renseignements. Une des craintes formulées par les entreprises était que cette possession puissent engendrer des pratiques anticoncurrentielles qui auraient favorisé, par exemple, l'abus de position dominante par ces organismes privés détenteurs de banques de données contenant les renseignements personnels.

C'est dans ce contexte que des questions ont été soulevées sur l'efficacité des règles générales du droit de la concurrence pour contrer ces pratiques. En effet, le droit de la concurrence met en place la structure juridique de base par laquelle les comportements ayant pour conséquence de créer des déséquilibres dans le marché sont interdits. Le droit de la concurrence des années 1990 était donc construit autour de telles interdictions et celles-ci tombaient dans le champ du droit criminel. Or, comme on le sait, le standard de preuve requis en matière criminelle est très élevé, d'où la difficulté d'assurer la conformité à ce droit par les acteurs économiques. Bien que ce constat ait été fait à l'égard de nombreux secteurs de l'activité économique, les insuffisances du droit de la concurrence pour réguler le jeu de la libre concurrence dans l'espace informationnel et dématérialisé du commerce électronique apparaissait encore plus criant aux yeux des experts. En effet, contrairement à l'économie industrielle où l'appropriation des ressources et la production de biens dominant, le développement de l'économie du savoir est lié à l'appropriation des connaissances et à la production continue d'innovation. Contrairement aux ressources et aux biens, le savoir est considéré comme un *bien non rare* : il est présent en quantité suffisante (pour satisfaire nos besoins et nos désirs) et il possède la particularité

23 *Id.*, p. 6.

24 Rick Shields, *Les renseignements personnels accessibles au public et la Loi sur la protection des renseignements personnels et les documents électroniques* du Canada, Ottawa, 12 octobre 2000 (document écrit pour le compte de McCarthy Tétrault et portant le numéro DMS-Ottawa #5574162/v.2).

d'être partageable. En conséquence, la concurrence à l'égard du savoir est très forte, ce qui affecte beaucoup l'efficacité des interdictions posées par le droit de la concurrence.

C'est de ce premier constat qu'il faut comprendre l'importance de certains régimes réglementaires ayant pour objet de protéger des niches économiques très précises tout en donnant des garanties juridiques suffisantes pour prévenir les situations anticoncurrentielles et maintenir l'équilibre concurrentiel dans un secteur d'activités économiques. Dans une économie du savoir, des lois telles que celles relatives à la protection de la propriété intellectuelle, du droit d'auteur et également des renseignements personnels jouent ce rôle. Elles pallient en quelque sorte aux insuffisances du droit de la concurrence à protéger efficacement les conditions d'échange de l'information couramment utilisée dans le monde de l'économie du savoir. La LPRPDE et ces autres lois étaient estimées essentielles pour construire l'infrastructure juridique de base pour une mise en place harmonieuse de l'économie du savoir.

En somme, c'est par une compréhension des limites du droit de la concurrence et par l'ajout de compléments juridiques infrastructurels à ce droit, dans le but de favoriser la croissance de l'économie du savoir, qu'il convient de comprendre la réglementation des usages des renseignements personnels par la LPRPDE. Comme plusieurs commentateurs de la loi l'ont souligné (et certains dénoncés), l'aspect dominant de la LPRPDE n'est pas la protection du droit à la vie privée des citoyens. En effet, et comme nous venons de le voir, il s'agit, d'une part, de réglementer les conduites commerciales afin de favoriser l'échange et le commerce des renseignements personnels tout en prévenant les abus dans l'usage des renseignements personnels et nuisibles au jeu de la libre concurrence. D'autre part, il s'agit de protéger les consommateurs tout en suscitant un climat de confiance chez ces derniers de manière à créer un environnement propice à l'innovation technologique.

1.1.3 La création d'un environnement propice à l'innovation technologique

Créer un environnement favorable à l'innovation technologique est une préoccupation qui prendra progressivement plus d'importance à partir des années 1990 et, avec elle, les théories économiques préconisant les interventions étatiques à cet égard auront graduellement plus d'emprise dans le discours gouvernemental. À partir des années 1990, l'orthodoxie néoclassique commence à céder sa place à des points de vue de théoriciens défendant des modèles d'économie mixte. Ceux-ci acceptent que certains secteurs économiques puissent être plus ou moins réglementés par l'État selon le contexte concurrentiel dans lequel les échanges commerciaux évoluent. Puisque le commerce électronique est vu par plusieurs comme la voie d'avenir en matière d'échanges commerciaux, la sécurité des transactions devient la question de l'heure. En effet, si le Canada vise le développement de ces nouvelles technologies, il faut que les consommateurs aient confiance dans ces nouveaux systèmes d'échanges commerciaux. Comme l'affirme le Groupe de travail : « Puisque plus de la moitié des Canadiens sont d'avis que l'inforoute réduit la vie privée au Canada, il est essentiel à la croissance de l'économie

de l'information canadienne que les consommateurs aient confiance dans le système. [...] une loi qui définit un ensemble de règles communes pour la protection des renseignements personnels aidera à renforcer cette confiance [...]»²⁵. » Dans ce contexte, la réglementation sociale favorisant l'innovation technologique est une action étatique jugée légitime.

À l'intérieur du modèle économique général néoclassique, différentes théories spécifiques à caractère plus interventionnistes — que celles ayant fleuries durant les années 1980 — prendront formes. L'une de ces théories économiques porte sur la croissance endogène. Cette théorie propose un modèle d'économie mixte selon lequel un accent important est mis sur les interventions étatiques dans l'économie en vue d'accroître l'innovation technologique (incluant le commerce électronique) et, de là, soutenir la croissance économique. C'est d'abord Solow qui, dans les années 1950, avait établi la primauté du développement technologique comme facteur explicatif de la croissance économique soutenue durant les Trente glorieuses. Romer a apporté une contribution à la théorie de Solow en montrant que le progrès technique, aussi appelée innovation²⁶, constituait une variable endogène, c'est-à-dire qu'il était le fruit d'actions intentionnelles de la part des acteurs économiques. Cette démonstration a eu des répercussions très importantes sur le renouvellement du rôle de l'État dans l'économie depuis les années 1990. Sur un plan général, ce renouvellement a facilité le passage du paradigme de la réglementation pathogène à celui de la réglementation intelligente dont nous reparlerons dans la section suivante. Mais pour le moment qu'il suffise de dire que lorsque le gouvernement désire mettre en œuvre le modèle économique de la croissance endogène, il doit prendre pour acquis que les actions intentionnelles des acteurs économiques — visant notamment à augmenter le capital technologique et le stock de connaissances — favorisent le développement de l'économie du savoir et, partant, la croissance économique²⁷.

Ces préoccupations économiques étaient bel et bien présentes lors des discussions entourant la LPRPDE. En effet, dans la section du document produit par le Groupe de travail, expliquant pourquoi la protection des renseignements personnels qui existait à l'époque n'était plus suffisante, on peut lire :

De nouvelles technologies, la collecte croissante de données dans le secteur privé, l'évolution des tendances du marché et le nouveau marché mondial qui s'ouvre au commerce électronique, voilà autant d'éléments qui contribuent au rôle de plus en plus important de l'information dans

25 Groupe de travail sur le commerce électronique, *supra*, note 13, p. 6.

26 Sur le concept d'innovation, voir le *Dictionnaire des sciences économiques*, *supra*, note 3, p. 474-476.

27 Pierre-Yves Hénin et Pierre Ralle, « Les nouvelles théories de la croissance. Quelques apports pour la politique économique », *Revue économique – Hors série* 82, 82-86.

l'économie mondiale. Dans cette nouvelle économie mondiale, l'information est un bien précieux qui peut être porteur d'emplois, de prospérité et d'un meilleur service à la clientèle. Si l'on y ajoute d'autres facteurs clés, il devient de plus en plus pressant de recueillir et d'utiliser comme jamais auparavant des renseignements personnels²⁸.

Ainsi, en permettant les échanges et le commerce des renseignements personnels, la future LPRPDE occuperait une place dans la stratégie économique du Canada où le développement de l'économie du savoir, l'équilibre concurrentiel et la protection des renseignements personnels seraient conçus comme des éléments d'une politique qui seraient inextricablement liés.

1.2 Le contexte politique : L'impact des théories relatives à l'organisation étatique

C'est à partir des critiques des économistes néoclassiques des programmes réglementaires qu'un examen méticuleux du fonctionnement et de l'organisation de l'administration publique est entrepris par des chercheurs provenant des sciences économique et administrative et s'intéressant à la science politique. Dès la fin des années 1960, les théoriciens de l'École de Chicago, notamment ceux rassemblés sous la bannière de la théorie du *Public Choice*²⁹ ont contribué de façon significative à la compréhension du processus décisionnel par l'administration publique. Ces travaux ont entre autres mené à une réflexion fondamentale sur l'organisation des institutions administratives. Ils ont aussi inspiré les travaux des théoriciens provenant de la science administrative. Ces derniers ont notamment proposé une nouvelle philosophie de gestion aux gouvernements qu'ils ont nommé le Nouveau Management Public.

Cette philosophie de gestion a eu un impact sur le fonctionnement des organismes administratifs puisque les théoriciens de cette école ont préconisé l'adoption du modèle d'organisation du marché par l'administration publique. Au Canada, les gouvernements fédéral et provinciaux y ont adhéré à partir des années 1980 afin de moderniser leur administration publique. L'influence de ces deux courants théoriques sur l'organisation et le fonctionnement de l'administration publique est importante, car ils ont mené les gouvernements à repenser leurs rapports entre les organismes publics et privés tant sur le choix des institutions étatiques à créer pour surveiller l'application des programmes réglementaires qu'à l'égard du choix des instruments d'intervention étatique.

28 Groupe de travail sur le commerce électronique, *supra*, note 13, p. 6.

29 Le texte fondateur de la théorie du *Public Choice* est celui écrit James M. Buchanan et Gordon Tullock, *The Calculus of Consent*, Ann Arbor, University of Michigan Press, 1962, 361 p.

1.2.1 Le choix de l'institution étatique

Dans les documents gouvernementaux relatifs à la future LPRPDE, la question de savoir quel pourrait être le modèle institutionnel le plus adéquat pour garantir une application efficace de la LPRPDE n'a pas fait l'objet d'une discussion. L'ombudsman en poste de l'époque, le commissaire à la protection de la vie privée Phillips, émit l'avis que son bureau, le Commissariat à la protection de la vie privée et établi sous la *Loi sur les renseignements personnels*, pouvait se charger de l'application de la nouvelle loi, mais ses justifications pour soutenir un tel choix étaient peu développées. Cette absence ou quasi-absence de débats sur l'institution chargée de l'application de la loi étonne puisque plusieurs raisons auraient pu être avancées au soutien de ce choix et qui auraient été considérées convaincantes à cette époque.

La première raison et la plus évidente est celle liée au contexte de la crise des finances publiques. À partir des 1980, les politiciens n'étaient pas enclins à proposer la création d'un organisme public additionnel. L'heure était plutôt à la réduction et à la réorganisation de l'administration publique en vue de diminuer les dépenses publiques. Néanmoins, lorsqu'on envisageait la création d'un nouveau programme réglementaire, il fallait bien qu'un organisme public fut chargé d'en assurer la surveillance, ce qui impliquait forcément une dépense publique additionnelle. Du point de vue du politicien qui doit défendre un tel dossier, il est plus facile de dissimuler la dépense en ajoutant une compétence additionnelle à un organisme déjà existant qu'en créant un tout nouvel organisme public. Comme le commissaire à la protection de la vie privée de l'époque le faisait valoir dans son mémoire répondant au document produit par le Groupe de travail : « Ce qui est tout aussi important dans cette approche (accroître le champ de compétence du commissaire), c'est d'éviter la prolifération de la bureaucratie ainsi que les coûts excessifs et inutiles³⁰. » [traduction]

Outre ces considérations financières, deux autres raisons ont milité en faveur des choix qui ont été faits lors de l'élaboration de la LPRPDE. D'une part, des discussions importantes se déroulaient sur des questions telles que l'application uniforme du droit, l'évitement des chevauchements des règles de droit ainsi qu'à leur multiplication, notamment dans un système fédéral. Le commissaire Phillips était conscient de celles-ci puisqu'il a écrit que le modèle d'ombudsman « offre les avantages de la sensibilité à des problèmes organisationnels particuliers combinés à un engagement à l'égard de l'application uniforme des principes de protection de la vie privée³¹ » [traduction].

D'autre part, une autre idée importante qui influençait le discours public portait sur la critique du concept d'intérêt public. Les théoriciens du *Public Choice* étaient d'avis qu'il n'existait pas véritablement de distinction entre l'intérêt public

30 Groupe de travail sur le commerce électronique, *supra*, note 13, p. 8.

31 *Ibid.*

et l'intérêt privé dans la mesure où ils argumentaient que l'intérêt public n'était en somme que l'agrégat des intérêts privés. De ce point de vue, le rôle de l'État devait être repensé. Il ne s'agissait plus pour l'État de diriger la société civile, mais d'arbitrer les intérêts en jeu et d'équilibrer l'action publique en conséquence. Dans les années 1990, il était en quelque sorte relativement aisé pour un gouvernement d'adopter cette posture théorique dans la mesure où ce rôle d'arbitre de l'État avait été reconnu par la Cour suprême en 1992 dans l'affaire *Nova Scotia Pharmaceutical Society*³². Vu sous cet angle, le discours du commissaire Phillips était aussi, à cet égard, dans l'air du temps puisqu'il faisait valoir que le modèle d'ombudsman était adapté au contexte moderne. En effet, en reposant sur la consultation, la conciliation et la négociation, l'ombudsman pouvait, entre autres, être « [...] cognizant of the complexities of business [...] » et être plus sensible aux problèmes organisationnels particuliers du secteur privé³³.

C'est à la suite d'une réflexion portant sur l'ensemble de ces préoccupations que de nouvelles idées organisationnelles ont émergé, notamment celle d'attribuer des compétences transversales à certains organismes de l'administration publique.

1.2.1.1 L'attribution de compétences transversales

La théorie du *Public Choice* est une théorie économique qui examine des problèmes qui font normalement partie du champ d'étude de la science politique. C'est avec les travaux de Niskanen dans les années 1970 que l'étude du comportement des fonctionnaires et du fonctionnement de la bureaucratie, en particulier, s'est clairement distinguée comme champ spécifique de la théorie du *Public Choice*³⁴. Un premier problème mis au jour par les théoriciens du *Public Choice* portait sur le cloisonnement des compétences des organismes. C'est dans ce cadre de réflexion qu'il y a eu une remise en question du modèle d'organisation vertical et hiérarchique de l'administration publique. Selon eux, lorsque chaque organisme gouvernemental se voit attribuer un domaine d'action sociale et économique spécifique et exclusif, cela ne favorise pas la communication et la coordination entre les organismes faisant partie de la même administration publique (fédérale, par exemple) et ceux faisant partie d'autres administrations publiques (provinciales ou celles d'autres États). Ce que les théoriciens du *Public Choice* ont constaté est qu'une telle organisation en silo engendre une concurrence malsaine entre les organismes étatiques dans la mesure où les administrateurs publics ont tendance à créer plus de normes réglementaires en vue de maximiser leur budget et leur champ de compétence.

C'est à partir de cette critique qu'une idée dominante s'est imposée durant cette époque à savoir que le secteur public était inefficace : l'administration publique

32 *R. c. Nova Scotia Pharmaceutical Society*, 1992, 2 R.C.S. 606, à la p. 46 de la version pdf disponible sur LexUM : <http://scc.lexum.umontreal.ca/fr/1992/1992rcs2-606/1992rcs2-606.pdf> (dernière visite : le 12 juillet 2009).

33 Groupe de travail sur le commerce électronique, *supra*, note 13, p. 8.

34 William Niskanen, *Bureaucracy and Representative Government*, Chicago, Aldine Atherton, 1971, 241 p.

est trop rigide dans son fonctionnement, trop centralisée dans son organisation, trop coûteuse, trop centrée sur son propre développement et incapable d'innover. L'objectif du triple-E (Économie, Efficacité, Efficience) s'impose en nouveau credo des politiciens³⁵. Ces réflexions ont mené vers la formulation de quelques idées sur les fondements des nouveaux organismes administratifs de l'avenir. En effet, souplesse et décentralisation plus poussée devenaient des concepts centraux d'organisation et ayant notamment mené à la prolifération d'un organisme d'un nouveau genre dans l'administration publique canadienne : les agences. Ce qui est intéressant avec ce nouveau type d'organisme est le lien de parenté entre l'agence et l'ombudsman, comme le constate Daniel Mockle³⁶. De plus, l'auteur précise que la prolifération de ce modèle en droit administratif canadien contemporain est « l'expression structurelle des exigences du Nouveau management public³⁷ » puisqu'en effet le modèle de l'agence présente au moins cinq caractéristiques : 1. la définition claire des missions de l'agence; 2. la large décentralisation des responsabilités et des moyens; 3. le rôle central de l'usage; 4. l'évaluation des résultats concrets des activités de l'agence; 5. des fonctions limitées à l'exécution et de la loi³⁸. À cette liste de caractéristiques, nous en ajoutons une sixième, soit l'attribution fréquente de compétences transversales à ces organismes.

En l'espèce, il s'agit bien sûr de la protection des renseignements dans les secteurs public (*Loi sur la protection des renseignements personnels*) et privé (LPRPDE). Dans ce dernier cas, le secteur privé comprend autant les organismes privés sous compétence fédérale que provinciales ou territoriales³⁹. On peut donc constater que le domaine de la protection des renseignements personnels a clairement vocation d'un programme réglementaire d'application transversale. Dans ce contexte, la question relative à la capacité d'une institution publique d'agir de manière la plus impartiale possible compte tenu du devoir d'équilibrer les intérêts de toutes les parties prenantes devient centrale.

1.2.1.2 L'équilibre entre les intérêts des parties prenantes

Un deuxième problème qui a été identifié par les théoriciens du *Public Choice* est celui relatif à la mise en œuvre du principe de l'intérêt public. Comme nous le mentionnions plus haut, les théoriciens du *Public Choice* estimaient que l'idée selon laquelle l'intérêt public était un concept distinct de l'intérêt privé était

35 Paolo Urlio, « La gestion publique au service du marché », dans Marc Hufty (dir.), *La pensée comptable : État, néolibéralisme, nouvelle gestion publique*, Paris et Genève, PUF et Les nouveaux Cahiers de l'IUED, 1998, p. 91-124.

36 Daniel Mockle, *La gouvernance, l'État et le droit*, Éd. Bruylant, 2007, p. 233.

37 *Id.*, p. 232.

38 *Id.*, p. 233.

39 *Loi sur la protection des renseignements personnels et les documents électroniques*, *supra*, note 2, art. 23 et suivants. Sur cette question on peut lire : Canada, commissaire à la protection de la vie privée, *Rapport au Parlement relativement aux lois provinciales essentiellement similaires*, Ottawa, Travaux publics et Services gouvernementaux, 2002. Cette publication est disponible sur le site du Commissariat : www.priv.gc.ca (dernière visite : 10 juillet 2009).

fausse. Ils ont donc postulé que tant les acteurs privés que publics sont motivés par la maximisation de leurs intérêts personnels (le revenu, le pouvoir, l'altruisme, etc.⁴⁰). Par conséquent, en faisant la démonstration que les autorités publiques n'agissaient que pour optimiser leur bien-être, les théoriciens du *Public Choice* démontraient du même souffle que l'intérêt général n'était en somme que l'agrégat des intérêts privés⁴¹. Pour éviter que ces autorités agissent de manière inéquitable et partielle, il fallait rendre visible les mécanismes administratifs qui avaient pour effet de neutraliser ou de contrecarrer la mise en œuvre équitable et impartiale des programmes réglementaires. Au moins deux mécanismes ont été pointés du doigt : 1) la rigidité de la réglementation qu'il fallait alors remplacer par une réglementation plus souple; 2) un processus qui permit une plus grande ouverture informationnelle de sorte que toutes les parties prenantes puissent faire valoir leur point de vue sur l'élaboration et l'application de la loi. Dans le document de travail sur le commerce électronique, le Groupe de travail insiste sur l'adoption de normes souples pour la protection des renseignements personnels : « La nouvelle loi canadienne doit [...] fournir des directives souples mais efficaces pour la protection de droits exécutoires et des règles du jeu équitables sur le marché⁴². » Plus loin, le Groupe de travail préconise l'adoption de la norme approuvée par l'Association canadienne de normalisation (le Code type CSA) parce qu'elle « présente plusieurs avantages en tant que point de départ pour la loi » notamment parce qu'elle « offre une certaine souplesse⁴³ ». Quant au commissaire, il ne s'opposait pas à l'adoption de cette norme bien qu'il proposa des améliorations sur plusieurs aspects⁴⁴.

Sur le thème de l'ouverture informationnelle, les théoriciens du *Public Choice* étaient d'avis que les informations détenues par les autorités publiques au moment de la prise de décision étaient nécessairement partielles, compte tenu que leur conception de l'intérêt public était forgée par la seule compréhension des fonctionnaires de cet intérêt public. Lorsqu'on comprend le concept d'intérêt public comme étant constitué d'un agrégat d'intérêts privés, on voit immédiatement l'importance que revêt l'idée, chez les théoriciens du *Public Choice*, d'inclure toutes les parties prenantes aux discussions entourant soit l'élaboration ou l'application de la loi (ou les deux). Pour ces théoriciens, il

40 Sur ce point, ces théoriciens feraient ressortir que c'est la raison pour laquelle le commissaire Phillips a proposé que le Commissariat à la protection de la vie privée soit également en charge de l'application de la nouvelle loi.

41 Ejan Mackaay et Stéphane Rousseau, *Analyse économique du droit*, 2^e éd., Montréal, Éditions Thémis, 2008, paragr. 144 : « Les choix collectifs de la société doivent être analysés comme résultant de la composition des choix individuels. »

42 Groupe de travail sur le commerce électronique, *supra*, note 13, p. 13.

43 *Id.*, p. 16.

44 Bruce Phillips, commissaire à la protection de la vie privée du Canada, *Response to the Government of Canada, Discussion Paper : « The Protection of Personal Information: Building Canada's Information Economy Society »*, Ottawa, Commissariat à la protection de la vie privée du Canada, 1998, annexe 1 [Ci-après appelé « Mémoire du commissaire Phillips »].

importait que soient mis en œuvre des mécanismes adéquats afin de combler les lacunes informationnelles des organismes publics. Ces mécanismes seraient en quelque sorte garants d'une plus grande équité procédurale.

Replacée dans le contexte de la réflexion sur la future LPRPDE, cette préoccupation était également très présente. En effet, l'adoption de la norme de l'Association canadienne de normalisation était également fondée sur le fait qu'elle recueillait « le consensus des principaux intervenants du secteur privé, des organisations de consommateurs et autres groupes d'intérêt public, ainsi que celui d'organismes publics⁴⁵ ». Il était donc important que les normes de fond applicable aux organismes privés reflètent leurs intérêts. Il était également important que les mécanismes d'application de la loi permettent aussi la plus grande ouverture informationnelle possible. À cet égard, la solution était de favoriser des mécanismes d'enquête suffisamment larges et englobant afin que le commissaire ait en main le maximum d'information pertinente avant de formuler des recommandations ou de procéder à la conciliation ou à la médiation d'une plainte déposée par un consommateur. De plus, et toujours dans le but de permettre des discussions franches et complètes entre le commissaire et l'organisme privé faisant l'objet de la plainte, la confidentialité du processus d'enquête fut envisagé puis adoptée dans la LPRPDE.

1.2.2 Le choix des instruments d'intervention

Selon le Nouveau management public, le secteur public partage des traits communs avec le secteur privé. En raison de ces ressemblances, certains outils de gestion employés par le secteur privé peuvent être utilisés par le secteur public. L'un de ces outils est l'étude coût-efficacité qui demande qu'un rapport soit établi entre le coût et l'efficacité d'un instrument d'intervention étatique afin de déterminer l'outil le plus efficace sur le plan économique. À partir des années 1980, lorsque sont identifiés de nouveaux problèmes sociaux et économiques qui appellent une intervention étatique, on demande à l'État de réfléchir aux solutions de rechange à la réglementation classique (le règlement)⁴⁶. À partir des années 1990, cette réflexion s'organise autour du concept de la réglementation intelligente. C'est à la suite de ces débats que les pays de l'OCDE se sont entendus sur l'objectif de produire une réglementation « meilleure », « de qualité » ou « intelligente »⁴⁷. C'est dans ce contexte que la coopération entre l'État et ses partenaires publics et privés est au cœur de la stratégie sur la réforme réglementaire et repose en grande partie sur l'harmonisation des normes. De son côté, la responsabilité implique entre

45 Groupe de travail sur le commerce électronique, *supra*, note 13, p. 16.

46 Sur le thème du choix des instruments d'intervention de l'État, voir entre autres : Lester M. Salamon (éd.), *The Tools of Government: A Guide to the New Governance*, Oxford, Oxford University Press, 2002, 669 p.; Pearl F. Eliadis, Margaret M. Hill et Michael P. Howlett, *Designing Government: from Instruments to Governance*, Montréal, McGill-Queen's University Press, 2005, 454 p.

47 Sur l'adoption du concept de la réglementation intelligente par le Canada, voir note 1.

autres que les acteurs gouvernés par l'État puissent exercer leur libre-arbitre. Il s'agit alors de favoriser les approches réglementaires allant dans le sens d'une plus grande responsabilisation des acteurs sociaux et économique

1.2.2.1 La coopération entre les acteurs publics et privés

Repenser la qualité de la réglementation et la gestion du processus réglementaire implique un changement du rôle de l'État. Avec la fin de l'ère de l'État providence, l'État n'est plus autant appelé à diriger les acteurs sociaux et économiques, mais à faciliter le commerce ou à s'allier à ses partenaires de la société civile. C'est dans ce contexte que les acteurs publics (États nationaux et étrangers) et privés recherchent une plus grande coopération entre eux⁴⁸. Au cœur de ce vaste projet, deux objectifs sont visés : harmoniser les normes et changer la culture organisationnelle.

C'est la globalisation du commerce qui impose cet impératif d'harmonisation des normes qu'elles soient d'origine étatique ou autre. Il faut éviter la « tyrannie des différences⁴⁹ » normatives qui posent des entraves jugées inutiles au commerce intérieur et international. À cette époque, l'industrie a orchestré un discours qui a eu beaucoup de poids auprès des gouvernements : les entreprises canadiennes doivent pouvoir accéder aux marchés au moindre coût. Il s'ensuit que toute réglementation leur imposant des exigences supérieures à celles de leurs concurrents a pour effet de diminuer leur capacité de faire la concurrence. Cette préoccupation ressort clairement du document produit par le Groupe de travail sur le commerce électronique : « Assurer la protection efficace des renseignements personnels peut s'avérer essentiel pour que le Canada reste concurrentiel à l'échelle internationale dans l'économie de l'information mondiale⁵⁰. » Dans sa *Politique de réglementation de 1992*, le gouvernement fédéral demande explicitement à son administration publique de prouver que « des mesures ont été prises pour faire en sorte que les programmes de réglementation gênent le moins possible la compétitivité du Canada » et que le « fardeau de la réglementation, imposé aux Canadiens a été minimisé grâce à des méthodes comme la coopération avec d'autres gouvernements⁵¹ ». L'objectif de renforcer la coopération aux niveaux national et international en harmonisant les normes devient, dès lors, un impératif de gestion administrative

48 Québec, ministère du conseil exécutif, *La Réglementation par objectifs, Propositions du Groupe de travail Justice – Secrétariat à l'allègement réglementaire*, Québec, ministère du Conseil exécutif, 2001, p. 5, accessible en ligne : http://www.mce.gouv.qc.ca/allègement/documents/reglementation_objectifs.pdf (dernière visite : 14 juillet 2009).

49 L'expression a été utilisée par le Comité consultatif externe sur la réglementation intelligente dans son document : *La réglementation intelligente. Une stratégie réglementaire pour le Canada, supra*, note 47.

50 Groupe de travail sur le commerce électronique, *supra*, note 13, p. 8.

51 Canada, Secrétariat du Conseil du Trésor, *Politique de réglementation*, Ottawa, Conseil du Trésor du Canada, 1992, p. 4 et 5.

fédérale⁵². Cet impératif est également énoncé dans le document produit par le Groupe de travail sur le commerce électronique :

Si l'on veut que tous les Canadiens bénéficient d'une véritable protection globale de leur vie privée, les gouvernements fédéral, provinciaux et territoriaux devront travailler en étroite coopération pour donner lieu à une approche harmonisée dans l'ensemble du pays. Cela est essentiel pour le commerce interprovincial autant que pour le commerce international⁵³.

Le commissaire Phillips était aussi en accord avec l'objectif d'harmonisation des normes⁵⁴. De plus, la réflexion trouvait écho chez d'autres regroupements de la société civile, tels la Conférence sur l'harmonisation des lois au Canada. En effet, cette dernière avait commencé à réfléchir à la question de la protection uniforme des données dans le secteur privée dès 1995⁵⁵. La Conférence avait aussi rédigé un projet de loi en 1998⁵⁶. En conséquence, un consensus fort existait déjà sur cette question au moment des discussions entourant la future LPRPDE.

Cependant, pour atteindre cet objectif de coopération par l'harmonisation des normes, il apparaissait primordial de changer la culture organisationnelle entre les acteurs publics et privés. Il fallait créer un environnement où règnerait un esprit de collaboration entre les gouvernements, l'industrie, les ONG et les citoyens intéressés ou affectés par les mesures réglementaires envisagées. À cet égard, divers mécanismes pouvaient, en effet, faciliter le dialogue entre les acteurs politiques, économiques et sociaux : la consultation, la négociation, la conciliation et la médiation sont de ceux-là. Dans le document du Groupe de travail, la discussion sur les mécanismes de mise en œuvre de la future loi font notamment une large place au règlement amiable des disputes entre les consommateurs et l'industrie⁵⁷. Les préférences du commissaire Phillips allaient également dans ce sens⁵⁸. Par ailleurs, bien

52 En 2007, ces exigences deviendront encore plus précises et plus impératives avec la *Directive du Cabinet sur la rationalisation de la réglementation*, *supra*, note 47.

53 Groupe de travail sur le commerce électronique, *supra*, note 13, p. 14.

54 Mémoire du commissaire Phillips, *supra*, note 44, p. 13.

55 Voir les comptes rendus des réunions annuelles de la Conférence (1995 Québec, QC, Annexe M : *Protection de la vie privée dans le secteur privé*) disponibles à l'adresse suivante : <http://www.ulcc.ca/fr/poam2/index.cfm?sec=1995&sub=1995ac> (dernière visite : 13 juillet 2009).

56 Voir les comptes rendus des réunions annuelles de la Conférence (1998 Halifax, N.-É., Annexe A : *Loi uniforme sur le commerce électronique*) disponibles à l'adresse suivante : <http://www.ulcc.ca/fr/poam2/index.cfm?sec=1998&sub=1998ja> (dernière visite : 13 juillet 2009).

57 Groupe de travail sur le commerce électronique, *supra*, note 13, p. 24.

58 Mémoire du commissaire Phillips, *supra*, note 44, p. 11.

que le Groupe de travail ait laissé la porte ouverte en ce qui concernait la possibilité de créer un tribunal administratif, cette possibilité n'a été mentionnée qu'en passant et n'a pas occupé une place réellement importante dans les débats⁵⁹. Le commissaire Phillips était silencieux sur la question, mais le simple fait qu'il fut d'avis que le Commissariat devait être chargé de l'application de la nouvelle loi constituait un rejet implicite de l'option du tribunal administratif. D'ailleurs, il écrivait que la surveillance devait s'exercer de la manière la moins coercitive possible : « Le commissaire à la protection de la vie privée appuie et met en pratique le point de vue selon lequel une surveillance réussie passe essentiellement par la consultation, la conciliation et la négociation et recourt le moins possible à la coercition et à la menace⁶⁰. » [traduction]

1.2.2.2 La responsabilisation des acteurs gouvernés par l'État

Le thème de la responsabilisation des acteurs économiques et sociaux provient d'une réflexion plus large sur l'exercice de l'autorité étatique et la liberté des citoyens qui a entre autres été lancée par Hayek en 1944 avec la publication de son ouvrage-phare : *La route de la servitude*⁶¹. La thèse centrale d'Hayek est que la socialisation de l'économie⁶² et l'intervention massive de l'État sur le marché débouchent sur la suppression des libertés individuelles. Cette critique, acceptée par les théoriciens du *Public Choice*, influencera fortement la façon de réglementer à partir des années 1980-1990. Du modèle de la réglementation des moyens, les États expérimenteront plus avec des solutions de rechange, telles la réglementation des objectifs, l'autoréglementation ou encore l'absence et l'abstention réglementaire. Ces nouvelles expérimentations ont surtout éclos dans les secteurs économiques, car ce sont les industries qui ont critiqué la réglementation des moyens en dénonçant ses effets néfastes sur leur capacité à prendre des décisions économiquement efficaces, c'est-à-dire des décisions leur permettant de mener une véritable concurrence sur les marchés. Elles ont argumenté que le manque de souplesse de la réglementation des moyens nuisait à leur capacité de concurrencer parce qu'elle empêchait l'innovation technologique⁶³.

Plus près d'ici, Rod MacDonald, qui était alors président de la Commission du droit du Canada, avait, lors d'une conférence organisée par les juristes de l'État et tenue en l'an 2000, préconisé une approche de la gouvernance publique

59 Groupe de travail sur le commerce électronique, *supra*, note 13, p. 25.

60 Mémoire du commissaire Phillips, *supra*, note 44, p. 8.

61 Friedrich A. von Hayek, *La route de la servitude*, (trad. de G. Blumberg de *The Road to Serfdom*), 2^e éd., Paris, PUF, 1985, p. 24-29. Hayek a publié cet ouvrage en 1944.

62 La socialisation de l'économie est un concept lié à la notion de justice sociale ou encore de justice distributive : *Dictionnaire des sciences économiques*, *supra*, note 3, p. 496-498.

63 *La Réglementation par objectifs*, *supra*, note 48.

et privée axée sur le respect du libre-arbitre des individus et la recherche d'un nouvel équilibre juridique maximisant la liberté d'action des citoyens. Il avait proposé que l'État abandonne « autant que possible l'idée que le droit est un mécanisme de contrôle social régissant une population qui n'a pas la capacité d'agir de façon équitable et juste envers autrui en l'absence de balises rigides (droit régulateur) ». Selon cet auteur, il fallait remplacer le droit régulateur par un droit favorisant l'interaction humaine, « et qui pose les jalons qui nous indiquent nos valeurs et qui nous incitent à les respecter⁶⁴ ».

C'est dans ce contexte intellectuel que l'État aura dorénavant tendance à proposer des programmes réglementaires souples (*soft law*) plutôt que rigide (*hard law*) lorsque le contexte s'y prête⁶⁵. Ainsi, lorsque les discussions sur la future LPRPDE ont commencé, la souplesse réglementaire faisait déjà partie des postulats sous-jacents à la création de nouvelles politiques publiques. C'est ce qui explique que la possibilité de réglementer les moyens plutôt que les objectifs n'aient même pas fait partie de la discussion dans le document produit par le Groupe de travail sur le commerce électronique. Dans ce document, seuls des objectifs à atteindre par les organismes privés sont proposés. Par ailleurs, le document fait aussi une large place à l'autoréglementation. Le Groupe discute en détail du contenu de normes volontaires déjà approuvées par l'Association canadienne de la normalisation (le Code type CSA) ou encore de la possibilité de laisser chaque secteur industriel le soin d'adopter son propre code sectoriel. Lorsque ce type de réglementation est adopté (la réglementation par objectifs et l'autoréglementation), l'autorité publique chargée de son application se voit forcément conférer une plus grande marge d'appréciation relative à la portée de la norme et à l'évaluation des comportements qui seront jugés conformes ou non conformes⁶⁶.

1.3 Le contexte juridique : Les contraintes normatives internes et externes

En proposant de légiférer sur la protection des renseignements personnels, le gouvernement fédéral voulait remédier à deux problèmes qui se posaient de manière assez urgente. En effet, d'une part, l'Union européenne avait adopté une directive en vertu de laquelle elle s'autorisait à imposer une barrière non tarifaire à tout organisme privé, canadien ou d'une autre nationalité, dont le commerce impliquait l'échange de renseignements personnels, s'il n'y avait pas de régime de protection des renseignements personnels sur le territoire

64 Roderick A. MacDonald, « La réforme du droit et ses organismes », *Actes de la XIV^e Conférence des juristes de l'État*, Cowansville, Les Éditions Yvon Blais Inc., 2000, p. 377 à 397.

65 Sur la mutation des rôles de l'État : Charles-Albert Morand, *Le droit néo-moderne des politiques publiques*, Paris, L.G.D.J., 1998, p. 71 et s.

66 *R. c. Nova Scotia Pharmaceutical Society*, [1992] 2 R.C.S. 606.

étatique d'assise de l'entreprise en question et qui fut jugé adéquat par l'Union européenne⁶⁷.

Afin d'éviter l'imposition d'une telle barrière, le Canada devait instaurer un régime de protection et, pour se conformer aux exigences européennes, le régime devait établir des normes d'application uniforme à tous les organismes faisant l'échange de tels renseignements que ce soit sur les plans intraprovincial, interprovincial ou international. Le gouvernement fédéral estimait ne pas avoir le temps d'attendre que toutes les provinces et territoires aient agi avant que les effets de la directive européenne n'affectent le commerce entre les entreprises canadiennes et européennes. Il a donc décidé d'instituer un régime national. D'autre part, même si les provinces et territoires avaient agi rapidement, la crainte était qu'ils mettent en œuvre des régimes disparates et, que, ce faisant, certaines provinces ou territoires tentent de s'avantager sur le plan concurrentiel au détriment des autres partenaires de la fédération canadienne. C'est pour éviter ces deux maux que le gouvernement fédéral a décidé de mettre en marche un processus d'élaboration de la future LPRPDE. De toute évidence, même si ces objectifs étaient louables, un doute planait quant à l'autorité constitutionnelle du gouvernement fédéral de légiférer sur cette question.

En effet, tant les gouvernements fédéral que provinciaux pouvaient revendiquer une compétence législative sur la protection des renseignements personnels en vertu des articles 91 et 92 de la *Loi constitutionnelle de 1867*⁶⁸. Les gouvernements provinciaux pouvaient notamment recourir à leur compétence sur la propriété (des renseignements personnels) et les droits civils (le droit au respect à la vie privée) [art. 92.13] ainsi que toutes les matières d'une nature purement locale ou privée dans la province [art. 92.16]; cette dernière compétence permettant à une législature « [...] dans les limites de ses compétences législatives, [de] régler dans la province, une entreprise ou activité donnée⁶⁹ ». De son côté, le gouvernement fédéral pouvait invoquer sa compétence sur la réglementation générale des échanges et du commerce en s'appuyant sur l'art. 91.2. Toutefois, ce fondement était plus incertain, car les portées et limites de cette compétence fédérale restaient à préciser. Les paramètres d'application de l'art. 91.2 étaient encore assez flous.

Dans ce troisième développement, nous décrivons dans un premier temps les principales normativités internationales et nationales fixant des balises à la

67 Parlement européen et Conseil de l'Europe, *Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données*, J.O. L 281, 23 novembre 1995, p. 31-50. Accessible en ligne : http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexplus!prod!DocNumber&lg=fr&type_doc=Directive&an_doc=1995&nu_doc=46 (dernière visite : 22 juillet 2009).

68 *Loi constitutionnelle de 1867*, 30 & 31 Vict., chap. 3 (R.-U.).

69 *Canadian Indemnity Co. et al. c. Procureur général de la Colombie-Britannique*, 1977, 2 R.C.S. 504, 512 et 519; *Procureur général (Québec) c. Kellogg's Co. of Canada et al.*, 1978, 2 R.C.S. 211, 225.

réflexion qui s'engageait sur la future LPRPDE dans les années 1990⁷⁰. Dans un deuxième temps, nous explorons l'état du droit constitutionnel durant ces années de discussions afin de faire ressortir les paramètres à l'intérieur desquels le Parlement fédéral devait manœuvrer pour garantir que sa future loi puisse reposer sur des fondements constitutionnels qui soient les plus solides possible. Il faut noter ici que notre objectif n'est pas de donner une opinion juridique sur le partage des compétences, mais de tout simplement faire état de quelques difficultés qui se soulevaient durant cette période.

1.3.1 L'émergence d'une normativité relative à la protection des renseignements personnels

C'est au début des années 1980 qu'une prise de conscience internationale émergeait à l'égard du caractère potentiellement très intrusif des nouvelles technologies d'information et de communications dans la vie privée des individus. Cette prise de conscience s'est également étendue aux individus qui, soit à titre de consommateurs, de clients ou de patients, ont réclamé un plus grand respect de leur vie privée. C'est d'abord l'OCDE puis l'Union européenne qui a émis des directives relatives à la protection des renseignements personnels. Comme nous le verrons dans le premier développement, ces directives ont eu un effet domino, lequel a éventuellement débouché sur une proposition du gouvernement fédéral de légiférer sur cette question.

Les entreprises canadiennes et le Québec n'avaient cependant pas attendu que le gouvernement fédéral agisse et avaient déjà mis en place des normativités à géométrie variable (contenu et contrainte). La possibilité que plusieurs régimes régionaux ou sectoriels fussent mis en place n'était pas perçue d'un bon œil par tous. On peut notamment imaginer que les grandes entreprises sous réglementation fédérale étaient du nombre de celles qui souhaitaient que des normes nationales fussent adoptées. L'idée de créer des normes minimales nationales dans ce secteur d'activités faisait surface. Dans le deuxième développement, nous décrirons brièvement le contenu des normes édictées par le Québec et celles de l'Association canadienne de normalisation pour illustrer les disparités normatives entre les deux régimes et les contraintes qu'elles engendraient pour les entreprises œuvrant dans plusieurs provinces canadiennes, y compris le Québec.

1.3.1.1 Le développement d'une normativité extraterritoriale

C'est le 23 septembre 1980 que l'OCDE adoptait le tout premier document international sur la vie privée et les renseignements personnels. Les *Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données*

70 Groupe de travail sur le commerce électronique, *supra*, note 13, p. 8.

*de caractère personnel*⁷¹ comprennent des recommandations sur les aspects importants que devait couvrir un système réglementaire protégeant la vie privée. Cette directive se voulait un effort afin de concilier les différents concepts afférant à la notion de la vie privée que l'on retrouvait alors dans les pays membres de l'OCDE⁷². Elle était conçue de manière à encourager le respect de la vie privée ainsi qu'une prise de conscience à l'égard des problèmes soulevés par les échanges et le commerce des renseignements personnels des individus⁷³.

Les Lignes directrices de l'OCDE sont importantes car elles ont constitué le fondement de plusieurs lois ayant pour but de protéger les renseignements personnels. En particulier, Bennett rapporte qu'un bon nombre d'États européens ont adopté des lois basées sur les huit principes énoncés dans la partie 2 de l'annexe des lignes directrices de l'OCDE⁷⁴. Ces huit principes fondamentaux sont les suivants : 1) la limitation en matière de collecte; 2) la qualité des données; 3) la spécification des finalités; 4) la limitation de l'utilisation; 5) les garanties de sécurité; 6) la transparence; 7) la limitation en matière de collecte; 8) la qualité des données⁷⁵. Selon l'article 6 des Lignes directrices de l'OCDE, ces huit principes fondamentaux constituent des normes minimales⁷⁶. De plus, l'OCDE n'a fait que recommander aux pays membres de se conformer à ces normes. Le manquement à celles-ci ne comportait pas de sanction de nature juridique. L'OCDE misait sur la valeur morale de ses directives : si un pays membre refusait de s'y conformer ou de les incorporer dans son droit interne, ceci pouvait nuire à la réputation de son pays, mais surtout à celle des entreprises nationales. Selon Becker, cette pression morale a été suffisante pour insuffler le désir aux membres de travailler dans un esprit de coopération⁷⁷. Ces directives furent également utiles aux ressortissants d'un pays membre qui purent y recourir pour exercer des pressions internes auprès de leur gouvernement afin qu'il offrit une protection adéquate.

71 Organisation de coopération et de développement économiques (OCDE), *Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel*, adoptée le 23 septembre 1980. Accessible en ligne : http://www.oecd.org/document/57/0,3343,fr_2649_34255_1815225_1_1_1_1,00.html (dernière visite : 22 juillet 2009).

72 Richard Becker, « Recent Developments: Transborder Data Flows: Personal Data », 1981, 22 *Harv. Int'l. L. J.* 241, 246.

73 *Id.*, 244.

74 Colin Bennett et Charles Raab, *The Governance of Privacy: Policy Instruments in Global Perspective*, Aldershot, Ashgate, 2003, p. 75.

75 Voir annexe A pour un contenu plus détaillé de ces principes.

76 *Id.* (annexe A), art. 6.

77 R. Becker, *supra*, note 72, p. 247.

En 1985, l'OCDE a confirmé son engagement à protéger les renseignements personnels en approuvant la *Déclaration sur les flux transfrontières de données*⁷⁸. Les pays membres ont en effet déclaré que, « [c]onsidérant les importants progrès qui ont été atteints dans le domaine de la protection de la vie privée aux niveaux national et international », qu'il était de leur intention de continuer leur travail afin d'améliorer le respect de la vie privée et la protection des renseignements personnels. Treize ans plus tard, soit en 1998, les pays membres ont réaffirmé leur engagement à se conformer aux lignes directrices approuvées en 1980 ainsi qu'aux *Lignes directrices de l'OCDE régissant la politique de cryptographie* (1997) et de celles incluses dans la *Declaration on the Protection of Privacy on Global Networks*⁷⁹. Malgré tous ces énoncés d'intention, le contenu des obligations spécifiques imposées aux États membres restait tout de même assez vague. La seule obligation qui semblait plus contraignante que les autres portait sur l'engagement des États membres à évaluer leur progrès dans un délai de deux ans suivant la déclaration⁸⁰.

Au terme de cette brève revue des efforts consentis par l'OCDE afin de développer une normativité sur la protection des renseignements personnels, il faut conclure que le fait saillant digne de mention est celui où les États membres sont arrivés à un consensus sur les huit principes fondamentaux contenus dans les lignes directrices de 1980⁸¹. Ces principes n'ont pas eu d'effet direct sur les autorités canadiennes, mais ils ont en revanche stimulé la discussion des acteurs économiques, sociaux et politiques.

C'est en 1995 que de véritables pressions commencent à s'exercer sur les autorités canadiennes. En approuvant la *Directive sur la protection des données*⁸², l'Union européenne sonnait le glas à une approche de droit mou. En effet, c'est cette directive qui a contribué à l'adoption du principe du « safe Harbour » aux

78 Organisation de coopération et de développement économiques (OCDE), *Déclaration sur les flux transfrontières de données*, 11 avril 1985. Accessible en ligne : http://www.oecd.org/document/32/0,3343,fr_2649_34255_1888160_1_1_1_1,00.html (dernière visite : 23 juillet 2009).

79 Organisation de coopération et de développement économiques (OCDE), *Declaration on the Protection of Privacy on Global Networks*, 19 octobre 1998. Accessible en ligne : <http://www.oecd.org/dataoecd/39/13/1840065.pdf> (dernière visite : 23 juillet 2009).

80 *Id.*, voir le dernier paragraphe de la déclaration.

81 C. Bennett et C. Raab, *supra*, note 74, p. 74.

82 *Directive relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données*, *supra*, note 67.

États-Unis⁸³ et à l'adoption des lois canadiennes et australiennes⁸⁴. La majorité des normes issues de la directive s'applique seulement aux pays membres de l'Union, créant des obligations relatives à la protection de la vie privée lors d'échanges de renseignements personnels⁸⁵. Cependant, l'article de la directive — qui a été déterminant pour les pays étrangers comme le Canada — est l'article 25 du chapitre IV (transfert de données à caractère personnel vers des pays tiers) qui confère le pouvoir aux États membres de l'Union de refuser l'échange des données avec les pays qui n'offrent pas de « protection adéquate⁸⁶ ».

Les caractéristiques que doit comporter un « régime adéquat » ne sont pas précisées dans la directive et pour en circonscrire la portée, la Commission européenne a produit un rapport en 1998 dans lequel elle propose une méthode d'évaluation pour déterminer si un régime confère un niveau de protection adéquat⁸⁷. Selon la Commission, le régime d'un pays tiers doit revêtir une similitude fonctionnelle avec ceux des pays membres de l'Union pour être déclaré adéquat⁸⁸. En outre, la Commission insiste sur le fait qu'il ne s'agit pas d'imposer les mécanismes européens : ils ne constituent pas les seuls modèles adéquats de protection des renseignements personnels. Au contraire, la Commission dit vouloir éviter l'impérialisme normatif. À cette fin, la Commission précise qu'un régime d'un pays tiers sera jugé adéquat s'il a pour effet d'offrir la même protection effective que les régimes européens. En d'autres termes, la démonstration selon laquelle la mise en œuvre des principes énoncés dans la Directive donne les résultats escomptés est suffisante⁸⁹. L'Union européenne évalue l'effectivité des régimes sur deux niveaux. Au niveau général, un régime adéquat favorise l'avancement des connaissances portant sur les principes de base qui doivent sous-tendre la protection des renseignements

83 C. Bennett et C. Raab, *supra*, note 74, p. 132. Le *Safe Harbour* comporte sept principes visant la protection des renseignements personnels. C'est une liste de normes volontaires élaborées par les entreprises. Lorsqu'elles s'enregistrent auprès du département du Commerce, elles donnent les renseignements qu'elles ont reçus sur les Européens afin qu'ils puissent avoir la possibilité de vérifier l'exactitude des renseignements. Ils ont également la possibilité d'exercer un recours contre les entreprises qui violent les principes.

84 C. Bennett et C. Raab, *supra*, note 74, p. 166.

85 *Directive relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, supra*, note 67, art. 34.

86 *Id.*, art. 25.1. Le texte de l'article 25 est reproduit dans l'Annexe B.

87 Commission européenne, Direction générale du marché intérieur et services, *Preparation of a methodology for evaluating the adequacy of the level of protection of individuals with regard to the processing of personal data: annex to the annual report 1998 (XV D/5047/98) of the working party established by article 29 of directive 95/46/EC*, Luxembourg, Office des publications officielles de la communauté européenne, 1998.

88 *Id.*, art. 7.

89 *Id.*, art. 12. Ces principes sont : 1) Le principe de participation individuelle; 2) Le principe de l'objectif final; 3) Le principe de proportionnalité; 4) Le principe de qualité.

personnels. Au niveau spécifique, le système doit permettre la résolution des plaintes des individus faisant valoir une violation de leur droit à la protection de leurs renseignements personnels⁹⁰. Elle ajoute que les plaintes doivent être entendues par une autorité indépendante et que des mesures sécuritaires appropriées soient mises en place afin de prévenir la transmission ou l'accès non voulu par une entreprise aux renseignements personnels qu'elle détient sur des individus.

1.3.1.2 Le développement d'une normativité intraterritoriale

Au moment où le gouvernement fédéral réfléchit à son projet de loi sur la protection des renseignements personnels dans le secteur privé, deux initiatives importantes avaient déjà vu le jour au Canada : celle du Québec et celle de l'Association canadienne de la normalisation. Donc, dès la moitié de la décennie 1990, il y avait émergence d'une normativité canadienne qui faisait planer la crainte qu'un patchwork de lois provinciales et territoriales, mais aussi sectorielles, se réalise, ce qui aurait pu engendrer des disparités normatives importantes minant l'équilibre concurrentiel entre les différents acteurs économiques⁹¹. C'est d'ailleurs un des arguments que le ministre Manley a fait valoir lorsqu'il a présenté son projet de loi :

À l'heure actuelle, les renseignements personnels sont des marchandises que l'on peut acheter, vendre et échanger. Il existe aujourd'hui au Canada ce que le commissaire fédéral à la protection de la vie privée a appelé un « ensemble disparate » de lois, de règlements et de codes. Actuellement, les renseignements personnels traversent toutes les frontières, qu'elles soient provinciales, territoriales ou nationales. La plupart des industries ne sont assujetties à aucune règle concernant la collecte, l'utilisation et la communication des renseignements personnels. Seul le Québec a une loi générale s'appliquant au secteur privé dans les limites de son territoire⁹².

90 *Id.*, art. 16. Sur un plan plus technique, la Commission suggère dans son rapport que l'analyse porte sur trois facteurs. Un régime adéquat doit inclure : 1) Un mécanisme explicite de protection (telle une loi); 2) Un mécanisme de contrôle; 3) Un mécanisme prévoyant un recours à la suite duquel des sanctions peuvent être imposées après qu'il y ait eu constat d'une violation des normes régissant la protection des renseignements personnels.

91 Colin Bennett, *Regulating Privacy in Canada: An Analysis of Oversight and Enforcement in the Private Sector*, Ottawa, Industrie Canada, 1996, p. 6.

92 Gouvernement du Canada, ministre de l'Industrie, « Notes pour une Allocution : L'honorable John Manley, ministre de l'Industrie, devant le comité sénatorial chargé d'étudier le projet de loi C-6 », Ottawa, 2 décembre 1999. Accessible en ligne : <http://www.ic.gc.ca/eic/site/ecic-ceac.nsf/fra/gv00217.html> (dernière visite : 23 juillet 2009).

Dans cette section, nous comparons les contenus du *Code type sur la protection des renseignements personnels*⁹³ approuvé par l'Association en 1996 et de la *Loi sur la protection des renseignements personnels dans le secteur privé*⁹⁴ adoptée en 1994 par l'Assemblée nationale du Québec, afin de faire ressortir quelques disparités importantes qui existaient déjà au moment des discussions du gouvernement fédéral entourant la future LPRPDE.

Le Code type a été établi deux ans après que la province de Québec eut adopté sa propre loi et qui assujettissait toutes les entreprises faisant l'échange et le commerce de renseignements personnels. L'inspiration de la loi québécoise prend sa source dans les articles 35 à 41 du *Code civil du Québec* qui ont consacré le principe du respect de la vie privée. Le Code type et la loi québécoise tirent aussi leur inspiration des Lignes directrices établies par l'OCDE en 1981. Le Code type est un code volontaire établissant un standard minimum de protection des renseignements personnels. Le Code énonce dix principes⁹⁵, alors que la loi québécoise ne prescrit aucun principe comme tel, mais édicte néanmoins des normes relatives à tous les principes contenues dans le Code type. Pour illustrer les disparités entre ces deux systèmes normatifs, nous comparerons ci-après les contenus des deux textes et relatifs à deux principes du Code.

Sur le principe de la responsabilité (1^{er} principe), il est expliqué dans le Code type qu'un organisme est responsable des renseignements personnels qu'il gère. Il doit désigner une ou des personnes qui devront s'assurer du respect des neuf autres principes énoncés dans le Code type. Dans la loi québécoise, le législateur édicte qu'un organisme doit désigner une personne responsable des renseignements personnels, et ce, même si d'autres personnes utilisent ces renseignements dans l'organisme⁹⁶. De plus, l'identité de la personne responsable doit être divulguée si une demande est faite en ce sens par un membre du public⁹⁷. La loi québécoise prévoit également que les agents responsables des renseignements personnels dans un organisme doivent être enregistrés auprès du gouvernement⁹⁸. On peut donc constater que les obligations dans la loi québécoise sont plus lourdes que celles contenues dans le

93 Association canadienne de normalisation (CSA), *Code type sur la protection des renseignements personnels*, CAN/CSA-Q830-96, Rexdale, CSA, 1996 [ci-après « Code type »].

94 *Loi sur la protection des renseignements personnels dans le secteur privé*, L.R.Q., chap. P-39.1 [ci-après « Loi québécoise »].

95 1) La responsabilité; 2) La détermination des fins de la collecte de renseignements; 3) Le consentement; 4) La limitation de la collecte; 5) L'utilisation, la communication et la conservation des renseignements; 6) L'exactitude des renseignements; 7) Les mesures de sécurité; 8) La transparence; 9) L'accès aux renseignements personnels et 10) La possibilité de porter plainte contre le non-respect des principes.

96 Code type, *supra*, note 93, art. 4.1.1.

97 *Id.*, art. 4.1.2.

98 Loi québécoise, *supra*, note 94, art. 70.

Code type au chapitre de la mise en œuvre du principe de la responsabilité, ce qui facilite l'accès aux données par les personnes concernées.

Sur le consentement de l'individu à ce que ses renseignements personnels fassent l'objet d'une collecte (3^e principe), le Code type explique que l'individu doit être informé de la collecte, de l'utilisation ou de la communication de renseignements personnels qui le concerne. Il doit également y consentir, à moins qu'il ne soit pas possible de le faire. Le Code type suggère aussi qu'il est possible d'obtenir un consentement implicite⁹⁹. Dans la loi québécoise, il y a plusieurs articles qui portent sur le consentement. Alors que le Code type semble être plus intéressé par des questions de méthode d'obtention de renseignements personnels¹⁰⁰, les articles 6 et 9 de la loi québécoise forment la base d'une obligation prescrivant que les renseignements personnels ne peuvent pas être collectés sans le consentement valide d'une personne. L'article 13 de la loi québécoise édicte que les renseignements personnels ne peuvent pas être transmis à un tiers sans le consentement valide de la personne intéressée. C'est donc à l'égard de la qualité du consentement donné qu'il y a une différence notable entre le Code type et la loi québécoise¹⁰¹. Si l'on compare avec le Code type, les exigences de la loi québécoise sont plus élevées. Dans le Code, il est question de compréhension raisonnable¹⁰², du niveau de consentement qui varie avec la sensibilité des renseignements¹⁰³ et du consentement implicite « lorsque les renseignements sont moins sensibles¹⁰⁴ ». On peut ainsi constater que le degré de consentement requis des individus est clairement plus élevé dans la loi québécoise que celui exigé dans le Code type.

Cette comparaison entre deux normes contenues dans le Code type et la loi québécoise montre qu'en effet il y avait déjà des distinctions importantes entre les deux régimes normatifs qui existaient lors des discussions sur la future LPRPDE. Ce constat explique en partie la raison pour laquelle le gouvernement fédéral a voulu s'interposer pour assurer un certain degré d'harmonisation entre les régimes juridiques et quasi-juridiques existants et à venir. Toutefois, cette initiative n'était pas sans soulever plusieurs questions sur la validité constitutionnelle d'une telle initiative fédérale.

99 Code type, *supra*, note 93, art. 4.3.6.

100 *Id.*, articles 4.3.4 et 4.3.7. L'article 14 prescrit : « 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. Ce consentement ne vaut que pour la durée nécessaire à la réalisation des fins pour lesquelles il a été demandé. Un consentement qui n'est pas donné conformément au premier alinéa est sans effet. »

101 Loi québécoise, *supra*, note 94, art. 14.

102 Code type, *supra*, note 93, art. 4.3.2.

103 *Id.*, art. 4.3.4 et 4.3.6.

104 *Id.*, art. 4.3.6.

1.3.2 La compétence fédérale sur les échanges et le commerce

L'analyse de la validité constitutionnelle d'une loi ou d'une disposition sous l'angle du partage des compétences établi par la *Loi constitutionnelle de 1867* comporte deux volets. Dans un premier temps, il faut rechercher le caractère véritable de la loi ou de la disposition attaquée afin de déterminer à quelle rubrique de compétence cette caractéristique se rapporte le plus¹⁰⁵. Pour déterminer le caractère véritable d'une loi ou d'une disposition, il faut faire un examen de l'objet et de l'effet de la loi ou de la disposition législative contestée¹⁰⁶. L'objectif de ce premier volet de l'analyse est de déterminer si la loi ou la disposition attaquée relève de la compétence de l'ordre de gouvernement qui l'a adoptée¹⁰⁷.

Si on jette un regard sur les articles 3 et 4 de la LPRPDE, on constate que l'objet porte sur les échanges de renseignements personnels : de façon prépondérante sur les échanges commerciaux par tous organismes privés; de façon accessoire, sur les échanges non-commerciaux effectués dans le cadre d'une relation employeur-employé dans une entreprise fédérale¹⁰⁸. Quant aux usages non-commerciaux du secteur public, ils sont couverts par la *Loi sur la protection des renseignements personnels* adoptée par le Parlement fédéral¹⁰⁹. Le trait dominant de la LPRPDE est donc l'échange et le commerce des renseignements personnels. Or, l'échange et le commerce des renseignements personnels est du ressort exclusif des provinces. En effet, la compétence législative des provinces de légiférer l'usage et la protection des renseignements personnels par le secteur privé agissant à l'intérieur de la province, que ce soit en vertu de la compétence sur la propriété et les droits civils [incluant les protections relatives au respect de la vie privée] (92.13)¹¹⁰ ou la santé (92.16), n'a jamais été remise en question sur le plan constitutionnel¹¹¹. D'ailleurs, le

105 Renvoi relatif à la *Loi sur l'assurance-emploi* (Can.), art. 22 et 23, 2005, 2 R.C.S. 669, paragr. 8.

106 Renvoi relatif à la *Loi sur les armes à feu* (Can.), 2000, 1 R.C.S. 783, paragr. 16; *Reference re Validity of Section 5 (a) Dairy Industry Act*, 1949, S.C.R. 1.

107 Renvoi relatif à la *Loi sur l'assurance-emploi* (Can.), art. 22 et 23, *supra*, note 105, paragr. 8; Renvoi relatif au mariage entre personnes du même sexe, 2004, 3 R.C.S. 698, paragr. 13; Renvoi relatif à la *Loi sur les armes à feu* (Can.), *supra*, note 106, paragr. 15; Renvoi fait par le gouvernement du Québec en vertu de la *Loi sur les renvois à la Cour d'appel*, L.R.Q., chap. R-23, relativement à la constitutionnalité des articles 8 à 19, 40 à 53, 60, 61 et 68 de la *Loi sur la procréation assistée*, L.C. 2004, chap. 2 (Dans l'affaire du), 2008 QCCA 1167, paragr. 49.

108 *Loi sur la protection des renseignements personnels et les documents électroniques*, *supra*, note 2, art. 3.

109 *Loi sur la protection des renseignements personnels*, L.R.C. 1985, chap. P-21.

110 Sur ce point, il est intéressant de noter l'article 1 de la *Loi sur la protection des renseignements personnels dans le secteur privé*, *supra*, note 94.

111 *Canadian Indemnity Co. et al.*, *supra*, note 69, 519; *Kellogg's Co. of Canada et al.*, *supra*, note 69, 225.

Ministre Manley a explicitement reconnu ce fait dans son allocution portant sur la présentation du projet de loi C-6 (LPRPDE) :

Cependant, les pouvoirs en matière de commerce reposent sur l'activité commerciale même, et le gouvernement du Canada a besoin que les provinces passent à l'action, car elles sont les seules à avoir compétence relativement à certains des renseignements les plus confidentiels que les Canadiens veulent voir protégés, y compris la plupart des dossiers relatifs à la santé, à l'éducation et à l'emploi¹¹².

Quant à l'effet de la loi, un des problèmes majeurs qu'elle soulève est relatif à sa portée qui s'étend aux échanges et au commerce intraprovincial, ce qui constitue également un empiètement clair sur les compétences provinciales exclusives. Seules les provinces peuvent légiférer sur des matières locales [art. 92(16)].

En conséquence, par l'entremise de la LPRPDE, le gouvernement fédéral aborde des enjeux faisant partie de deux compétences provinciales exclusives. Cependant, comme la Cour suprême le réitère fréquemment, les champs de compétence ne sont pas statiques : leur contenu s'ajuste en fonction de l'évolution de la société canadienne de manière que « le pacte confédératif puisse répondre aux réalités nouvelles¹¹³ ». En revanche, l'interprétation évolutive ne doit pas justifier un empiètement par un ordre de gouvernement sur le champ de compétence exclusif de l'autre. C'est pour cette raison que la Cour fixe des limites à leur évolution, en raison de « certains principes liés à l'essence même du fédéralisme canadien, notamment quant au partage des compétences entre le fédéral et les provinces¹¹⁴ ».

C'est donc dans l'esprit de maintenir un équilibre entre ces principes interprétatifs et dans les relations fédérale-provinciales que la Cour suprême annonçait l'existence d'un deuxième volet à la compétence fédérale sur la réglementation des échanges et du commerce dans l'affaire *City National*

112 Gouvernement du Canada, ministre de l'Industrie, « Notes pour une allocution : L'honorable John Manley, ministre de l'Industrie, devant le comité sénatorial chargé d'étudier le projet de loi C-6 », *supra*, note 92.

113 Renvoi relatif à la *Loi sur l'assurance-emploi* (Can.), art. 22 et 23, *supra*, note 105, paragr. 9; Renvoi fait par le gouvernement du Québec en vertu de la *Loi sur les renvois à la Cour d'appel*, L.R.Q., chap. R-23, relativement à la constitutionnalité des articles 8 à 19, 40 à 53, 60, 61 et 68 de la *Loi sur la procréation assistée*, *supra*, note 107, paragr. 54.

114 Renvoi fait par le gouvernement du Québec en vertu de la *Loi sur les renvois à la Cour d'appel*, L.R.Q., chap. R-23, relativement à la constitutionnalité des articles 8 à 19, 40 à 53, 60, 61 et 68 de la *Loi sur la procréation assistée*, *supra*, note 107, paragr. 57; Renvoi relatif à la sécession du Québec, [1998] 2 R.C.S. 217, paragr. 43 et suiv.

*Leasing*¹¹⁵ et basée sur l'affaire *Parsons*¹¹⁶. Depuis lors, on sait que l'art. 91(2) comporte deux volets : 1) la compétence en matière d'échanges et de commerce internationaux et interprovinciaux, et 2) la compétence générale en matière d'échanges et de commerce touchant le Canada dans son ensemble¹¹⁷.

En l'espèce, lorsque le gouvernement a présenté son projet de loi, il était explicite qu'il entendait s'appuyer sur sa compétence générale en matière de réglementation des échanges et du commerce. En effet, le ministre de l'Industrie de l'époque dit dans son allocution :

Le projet de loi C-6 atteste le leadership du gouvernement. Il s'appuie sur les pouvoirs en matière de commerce pour créer un cadre de protection des renseignements personnels d'un bout à l'autre du pays, cadre qui vise à harmoniser la préparation de toutes les lois provinciales sur la protection des renseignements personnels dans le secteur privé¹¹⁸.

Cependant, le Parlement fédéral ne peut valablement s'appuyer sur cette compétence que s'il franchit deux étapes avec succès : 1) Démontrer que la loi est valide (ou que la disposition contestée fait partie d'un régime législatif valide); 2) Démontrer que la disposition contestée s'intègre suffisamment dans ce régime législatif. Or, les orientations relatives à la politique publique que le gouvernement fédéral s'apprêtait à présenter au Parlement posaient problème à l'une et l'autre étape de la démonstration.

1.3.2.1 L'existence d'un régime législatif valide

Comme la Cour suprême l'écrivait dans l'arrêt *City National Leasing*, la détermination de la validité de la loi fédérale : « [...] comportera normalement l'identification d'un système de réglementation et la vérification de sa conformité aux conditions formulées dans les arrêts *Vapor Canada* et *Transports Nationaux du Canada*¹¹⁹ ». Ces conditions correspondent aux trois premiers des cinq critères énoncés dans *City National Leasing*. Ces critères ont pour

115 *General Motors of Canada Ltd. c. City National Leasing*, 1989, 1 R.C.S. 641. Accessible en ligne en version PDF sur le site LexUM : <http://scc.lexum.umontreal.ca/fr/1989/1989rcs1-641/1989rcs1-641.pdf> (dernière visite : 23 juillet 2009).

116 *Id.*, p. 19 de la version PDF; *Citizens' Insurance Company of Canada c. Parsons*, 1881, 7 App. Cas. 96.

117 *Id.*, p. 20 de la version PDF.

118 Allocution du ministre Manley, *supra*, note 112.

119 *General Motors of Canada Ltd. c. City National Leasing*, *supra*, note 115, p. 35 de la version PDF.

fonction d'établir « correctement l'équilibre à atteindre entre les paragr. 91(2) et 92(13)¹²⁰ ». Ces trois premiers critères sont :

1. La mesure législative contestée doit s'inscrire dans un système général de réglementation;
2. Le système doit faire l'objet d'une surveillance constante par un organisme de réglementation;
3. La mesure législative doit porter sur le commerce dans son ensemble plutôt que sur un secteur en particulier;

En l'espèce, le gouvernement fédéral avait annoncé que son objectif avec la future LPRPDE était d'établir un système général de réglementation (critère 1)¹²¹. Il avait de plus annoncé que le système ferait l'objet d'une surveillance par un organisme de réglementation, soit le commissaire à la protection de la vie privée (critère 2)¹²². Ces deux critères étaient donc satisfaits et ce n'était donc pas à l'égard de ces facteurs que la future loi aurait posé problème, mais sur le troisième : la loi devait porter sur le commerce *dans son ensemble* plutôt que sur un secteur en particulier. Or, le but du gouvernement fédéral était de réglementer l'usage et le commerce des renseignements personnels, c'est-à-dire un secteur particulier ou un objet particulier du commerce¹²³ et non le commerce en général (comme le fait la *Loi sur la concurrence*, par exemple¹²⁴)¹²⁵. Il s'agissait donc d'une faiblesse constitutionnelle qui ne pouvait pas être ignorée. C'est sans doute pour cette raison, du moins en partie, que le gouvernement fédéral a choisi, pour contrer les attaques des provinces, de prévoir que la LPRPDE s'appliquerait aux échanges à l'intérieur d'une province seulement jusqu'au moment où cette province adopterait sa propre loi. Comme l'expliquait le ministre Manley : « Après son entrée en vigueur, ce projet de loi s'appliquera jusqu'à ce que les provinces fassent le nécessaire pour protéger les renseignements personnels dans leur territoire. Il continuera de s'appliquer là où ces renseignements ne seront pas protégés et il vaudra à l'égard d des données personnelles¹²⁶. » C'est donc dans l'espoir que les provinces et territoires adopteraient des lois protégeant les renseignements

120 *Id.*, p. 23 de la version PDF. En 1998, le test prévoyait encore l'analyse de cinq facteurs selon une méthode divisée en trois étapes. Pour des formulations plus simples, voir : *Bande Kitkatla c. Colombie-Britannique (ministre des Petites et moyennes entreprises, du Tourisme et de la Culture)*, 2002, 2 R.C.S. 146, paragr. 58; *Kirkbi AG c. Gestions Ritvik Inc.*, 2005, 3 R.C.S. 302, paragr. 20.

121 Josh Nisker, « PIPEDA: A Constitutional Analysis », 85 R. du B. Can. 317, a fait une brève analyse des critères aux pages 331 et s. de son texte.

122 *Id.*

123 Colin McNairn et Alexander Scott, *A guide to the Personal Information Protection and Electronic Documents Act*, Markham, LexisNexis Canada Inc., Ontario, 2007, p. 14.

124 Comme dans l'arrêt *City National Leasing*, *supra*, note 115.

125 J. Nisker, *supra*, note 121. D'ailleurs, comme nous l'avons déjà mentionné, le ministre Manley a fait le même constat dans son allocution, *supra*, note 112.

126 Allocution du ministre Manley, *supra*, note 112.

personnels dans le secteur privé que le gouvernement misait pour garantir la validité constitutionnelle de sa loi à plus long terme. Aujourd'hui, toutefois, nous sommes loin de ce but.

Ces obstacles qui se posaient à la validité constitutionnelle n'étaient pas les seuls puisqu'il fallait aussi franchir le second volet du test. Même en posant l'hypothèse selon laquelle la loi était valide (1^{er} volet), il restait néanmoins à déterminer, comme la Cour suprême l'enseigne dans sa méthode, si la « disposition contestée est suffisamment intégrée au système pour pouvoir être maintenue en raison de ce rapport ». C'est à ce stade que le cinquième critère énoncé dans l'affaire *City National Leasing* est particulièrement pertinent : « L'omission d'inclure une seule ou plusieurs provinces ou localités dans le système législatif compromettrait l'application de ce système dans d'autres parties du pays¹²⁷ ». Pour analyser ce problème, la Cour suprême a posé le test suivant dans l'affaire *City National Leasing* :

Cela exige de la cour qu'elle examine la gravité de l'empiètement sur les pouvoirs provinciaux pour décider du critère qu'il convient d'appliquer à un tel rapport. Si la disposition respecte ce critère d'intégration, elle est conforme à la compétence du Parlement en tant qu'exercice de son pouvoir général en matière d'échanges et de commerce. Si la disposition n'est pas suffisamment intégrée au système de réglementation, elle ne peut être maintenue en vertu du deuxième aspect du paragr. 91(2)¹²⁸.

En somme, il s'agit de déterminer s'il existe un lien rationnel et fonctionnel entre la loi déclarée valide et la disposition contestée. Selon la Cour, plus l'empiètement est grave plus la norme de concordance (ou le lien rationnel et fonctionnel) sera rigide; plus l'empiètement est bénin plus cette norme sera souple.

1.3.2.2 L'intégration des dispositions contestées au régime législatif

La détermination de la norme de concordance appropriée est un exercice dont les résultats sont peu prévisibles, car la jurisprudence de la Cour suprême est floue sur cette question. En effet, la Cour accorde un pouvoir discrétionnaire important aux juges :

Le même critère ne sera pas approprié dans toutes les circonstances. Pour parvenir à la norme appropriée, la cour doit considérer dans quelle mesure la disposition empiète sur les pouvoirs de la province. La jurisprudence

127 *General Motors of Canada Ltd. c. City National Leasing*, *supra*, note 115, p. 26 de la version PDF.

128 *Id.*, aux pages 35-36 de la version PDF.

que je vais examiner plus bas indique que, dans certaines circonstances, un critère plus strict est de rigueur alors que dans d'autres un critère moins rigoureux est acceptable. Par exemple, si la disposition contestée n'empiète sur les pouvoirs de la province que d'une façon négligeable, un rapport "fonctionnel" peut alors suffire pour justifier la disposition. D'autre part, si la disposition contestée empiète considérablement sur les pouvoirs de la province, un critère plus strict est alors indiqué. La meilleure méthode consiste à examiner minutieusement le critère approprié dans chaque cas¹²⁹.

Ainsi, l'identification de la norme de concordance, servant à établir un rapport de validité constitutionnel entre la loi déclarée valide et la disposition contestée, dépendra d'une évaluation a priori du degré d'empiètement sur les compétences provinciales exclusives. À cet égard, il est important de noter que la Cour a demandé aux juges d'exercer une retenue judiciaire quand ils proposent des critères rigides qui auront pour effet d'invalider de telles mesures législatives. En effet, elle explique :

En déterminant le critère approprié, il faut se rappeler que, dans un régime fédéral, il est certain que, dans la poursuite d'objectifs réguliers, la mesure législative de chaque palier de gouvernement aura parfois des répercussions sur le domaine de compétence d'un autre palier du gouvernement; il faut s'attendre à ce qu'il y ait chevauchement de mesures législatives et il faut s'y adapter dans un État fédéral¹³⁰.

En l'espèce, l'un des mécanismes les plus contestables que le gouvernement fédéral a inséré dans sa loi est celui par lequel il s'autorise à contraindre les provinces à adopter des normes minimales de protection. En effet, comme on le sait, la LPRPDE s'applique à tous les organismes privés qu'ils fassent l'échange et le commerce de renseignements personnels aux niveaux intra ou extra provincial ou international. Or, pour « récupérer sa compétence » sur les échanges et le commerce intraprovinciaux, une province doit adopter une loi essentiellement similaire à la loi fédérale. L'évaluation du caractère essentiellement similaire de la loi provinciale est effectuée par le commissaire à la protection de la vie privée¹³¹, mais c'est le gouverneur en conseil qui doit officiellement reconnaître ce fait par décret¹³². Le contenu des protections

129 *General Motors of Canada Ltd. c. City National Leasing*, *supra*, note 115, p. 32 de la version PDF. Nos italiques.

130 *Id.*, p. 33 de la version PDF.

131 *Loi sur la protection des renseignements personnels et les documents électroniques*, *supra*, note 2, art. 23 (1).

132 *Id.*, art. 26(2).

ainsi que les procédures font partie de l'examen effectué par le commissaire¹³³. Ce n'est qu'une fois cette procédure complétée que la LPRPDE cesse d'avoir des effets sur les échanges et le commerce des renseignements personnels intraprovinciaux et que la loi provinciale prend le relais¹³⁴.

C'est bien par un mécanisme d'harmonisation des lois que le gouvernement impose ses normes nationales aux provinces. Tant en 1998 qu'aujourd'hui la question est de savoir si ce type de mécanisme (ou tout autre mécanisme d'harmonisation ayant pour but l'établissement de normes nationales) est valide. Sur ce point, il est fort possible que nous ayons une réponse à cette question dans quelques années. En effet, le Procureur général du Québec a déposé une demande de renvoi auprès de la Cour d'appel du Québec contestant la validité de la LPRPDE en 2006. La Cour n'a pas pu se pencher sur la question, car le dossier n'est pas en état d'être entendu. En effet, le Procureur général du Québec n'a pas encore déposé ses arguments puisqu'il attend que la Cour suprême du Canada se prononce dans une autre affaire dans laquelle un mécanisme similaire d'harmonisation entre les normes provinciales et nationales est également discuté¹³⁵.

* *
*

Dans cette section, notre objectif était d'identifier quelques facteurs économiques, politiques et juridiques qui ont influencé l'adoption des politiques législatives contenues dans la LPRPDE. Comme on a pu le constater, la LPRPDE vise de multiples objectifs qui ne sont peut-être pas tous conciliables, mais qui, comme dans le cas de toutes les lois, représentent la somme des compromis qui ont dû être faits pour rendre son adoption possible.

Comprendre les idées passées qui ont eu des effets substantiels sur les orientations législatives qui ont finalement été retenues dans la LPRPDE il y a dix ans importe grandement dans un processus évaluatif. En effet, lorsqu'on évalue l'effectivité d'une loi, il faut déterminer si les postulats sous-jacents aux choix législatifs passés tiennent toujours la route. Dans la négative, il devient crucial d'identifier les points de rupture dans le temps pour comprendre les

133 Canada, commissaire à la protection de la vie privée du Canada, *Rapport au Parlement relativement aux lois provinciales essentiellement similaires*, Ottawa, ministère des Travaux publics et Services gouvernementaux, 2002, p. 2. Cette publication est accessible sur le site Web du Commissariat : www.priv.gc.ca (dernière visite : 24 juillet 2009).

134 *Id.*

135 Le mécanisme en cause est celui prévu à l'article 68(1) de la *Loi concernant la procréation assistée et la recherche connexe*, L.C. 2004, chap. 2. Renvoi fait par le gouvernement du Québec en vertu de la *Loi sur les renvois à la Cour d'appel*, L.R.Q., chap. R-23, relativement à la constitutionnalité des articles 8 à 19, 40 à 53, 60, 61 et 68 de la *Loi sur la procréation assistée*, *supra*, note 107, paragr. 34. L'affaire a été entendue le 25 avril 2009 devant la Cour suprême. Le numéro du dossier est le 32750.

événements à la source des problèmes identifiés. À cet égard, les évaluations quantitatives peuvent être utiles. Toutefois, elles sont souvent axées sur l'analyse de parties plutôt que du tout. C'est pourquoi, il ne faut pas négliger les études qualitatives. Évidemment, autant les chiffres que les faits ne disent pas tout, mais lorsqu'ils convergent dans la même direction, les analyses quantitatives et qualitatives fournissent de puissants indicateurs de pistes de réforme. Dans la deuxième section, il s'agit d'identifier ce qui, dans le contexte contemporain, a changé sur le plan factuel et qui pourrait influencer le choix et l'adoption de nouvelles orientations législatives. Une fois cette analyse complétée, nous serons en mesure d'indiquer de nouvelles pistes de recherche afin de faire progresser l'évaluation de l'effectivité de la LPRPDE vers des objets plus spécifiques.

Section 2. Les nouvelles préoccupations contemporaines

Dans l'optique où la LPRPDE nécessiterait des modifications, les ponts entre le passé et l'avenir doivent être bâtis : Qu'est-ce qui a changé dans le contexte économique, politique et juridique depuis l'adoption de la LPRPDE? Existe-t-il des ouvertures ou des contraintes nouvelles faisant en sorte que les discussions sur de possibles réformes de la loi puissent se faire à partir d'autres postulats? Dans cette section, nous proposons quelques pistes de réflexion.

Le premier changement d'importance est sans conteste celui de l'environnement technologique que la LPRPDE est appelée à régir. Un second point d'importance est celui des transformations dans l'organisation de l'État fédéral et dont il faut tenir compte pour mieux comprendre quelle place peut occuper un ombudsman, tel que la commissaire à la protection de la vie privée, dans la surveillance d'activités privées. Enfin, l'évolution des contextes juridiques national et supranational sont aussi des facteurs incontournables qui doivent être examinés lorsque la réflexion s'inscrit dans un objectif de réforme.

2.1 Sur le plan technologique : L'émergence du Web 2.0¹³⁶

Quelles sont les mutations et innovations liées au réseau Internet subséquentes à l'adoption de la LPRPDE? Dans cette section, nous décrivons les utilisations du réseau ayant d'importantes conséquences sur la gestion et la protection des renseignements personnels non envisagées par le législateur lors de la rédaction de la LPRPDE. Bien que ces utilisations soient multiples, elles découlent toutes du même phénomène, à savoir : l'émergence du Web 2.0.

136 Les auteurs remercient tout spécialement M^e Nicolas Vermeys, LL.D., pour l'aide très précieuse qu'il nous a apportée dans la rédaction de cette section du rapport. M^e Vermeys est le coordonnateur des travaux sur la cyberjustice du Centre de recherche en droit public de l'Université de Montréal. Sur la question de la protection des renseignements personnels et le Web 2.0, on peut aussi lire le tout nouvel ouvrage des professeurs Vincent Gautrais, Pierre Trudel, *Circulation des renseignements personnels et le Web 2.0*, Montréal, Les Éditions Thémis, 2010, 231 p.

L'expression « Web 2.0 » est attribuée à Tim O'Reilly¹³⁷, président de O'Reilly Media¹³⁸. Apparue pour la première fois en 2004¹³⁹, cette notion désigne notamment la tendance, observée chez certaines entreprises présentes sur le Web, à publier un contenu généré par les utilisateurs (UGC « User generated content ») plutôt que de recourir au modèle d'affaires traditionnel de mise en ligne de contenus médiatiques propriétaires. Pour reprendre les propos de M. O'Reilly, le Web 2.0 reposerait sur les sept principes suivants :

- Des services, pas un package logiciel, avec des possibilités d'économie d'échelle;
- Un contrôle sur des sources de données uniques, difficiles à recréer, et dont la richesse s'accroît à mesure que les gens les utilisent;
- Considérer les utilisateurs comme des co-développeurs;
- Tirer partie de l'intelligence collective;
- Toucher le marché jusque dans sa périphérie à travers la mise en place de services « prêts à consommer »;
- Libérer le logiciel du seul PC;
- Offrir de la souplesse dans les interfaces utilisateurs, les modèles de développements et les modèles d'affaires.

Bref, le Web 2.0 ne représente pas une réingénierie du réseau, mais bien un modèle d'affaires basé sur l'apport collectif et la convergence des services, lequel serait mieux adapté aux nouvelles réalités d'Internet, comme le démontrent les Wikipedia¹⁴⁰, Youtube¹⁴¹ et Myspace¹⁴² de ce monde.

137 Voir Tim O'Reilly, « What is Web 2.0: Design Patterns and Business Models for the Next Generation of Software », 2005, disponible à l'adresse : <http://oreilly.com/pub/a/web2/archive/what-is-web-20.html?page=1>. Une version française intitulée « Qu'est-ce que le web 2.0 : modèles de conception et d'affaires pour la prochaine génération de logiciels », 2006, est disponible à l'adresse : <http://www.eutech-ssii.com/ressources/1> (dernière visite : 23 mars 2010).

138 *Id.*

139 *Id.*

140 www.wikipedia.org : « Wikipedia est une encyclopédie en ligne universelle et multilingue. Elle est en cours de rédaction collaborative sur Internet avec la technologie wiki. Wikipédia a pour principe d'offrir un contenu libre, neutre et non inédit. »

141 www.youtube.com : « YouTube est le numéro un de la vidéo en ligne et le site le plus consulté par les internautes du monde entier souhaitant regarder et partager des vidéos personnelles. Grâce à YouTube, vous pouvez aisément envoyer et partager des vidéos sur le site fr.youtube.com et sur Internet, via des sites Web, votre mobile, des blogs et des e-mails. »

142 www.myspace.com : « MySpace est une communauté en ligne qui te permet de rencontrer les amis de tes amis. Crée une communauté privée sur MySpace et partage des photos, des blogs et des centres d'intérêt avec ton réseau sans cesse plus grand d'amis communs. Découvre qui connaît qui et comment. Vérifie si seulement six personnes te séparent de Tom Cruise;-) »

Nous sommes donc aujourd'hui confrontés à des relations mutualistes, voire symbiotiques, entre les différents fournisseurs de services, ainsi qu'entre les fournisseurs de service et les utilisateurs, relations qui ne sont pas sans incidences sur les notions de vie privée et de protection des renseignements personnels. En effet, une plus grande contribution de contenu de la part des internautes implique le risque que soient dévoilés, volontairement ou par mégarde, un certain nombre de renseignements personnels. Par ailleurs, la convergence des services emmène une circulation accrue, voire un partage non autorisé, des renseignements visant les utilisateurs de ces services.

Afin de mieux circonscrire les différentes problématiques liées à la protection des renseignements personnels dans le contexte du Web 2.0, nous avons regroupé celles-ci en trois sous-sections : 1) l'émergence des sites de réseautage personnel; 2) le perfectionnement et la polyvalence accrue des moteurs de recherche; et 3) la convergence des outils et services Webs. Notons toutefois que, vu cette convergence, une telle division s'avère artificielle et ne vise qu'à faciliter la lecture du présent rapport. Elle ne saurait constituer une classification « officialisable » des conséquences du Web 2.0 sur les notions de vie privée et de protection des renseignements personnels.

2.1.1 Les sites de réseautage personnel

Les sites de réseautage personnel peuvent être définis comme étant l'« [é] tablissement d'un réseau de relations interpersonnelles sur Internet, qui permet aux utilisateurs de constituer et d'élargir leur cercle de connaissances par l'intermédiaire d'amis, et d'amis des amis, qui constituent le réseau¹⁴³ ». Ces sites, dont les plus notoires sont Facebook¹⁴⁴ et Myspace¹⁴⁵, représentent probablement l'élément du Web 2.0 qui suscite le plus de craintes en matière de protection des renseignements personnels. Un rapport préparé par le Commissariat à la protection de la vie privée intitulé « *La vie privée sur les sites de réseau social : Analyse comparative de six sites* »¹⁴⁶ s'est d'ailleurs penché sur les principales problématiques liées à ces sites. Sans répéter le contenu de ce rapport, il importe de souligner que ces problématiques sont dues à trois composantes : a) l'exploitation des renseignements personnels des internautes par les sites; b) l'exploitation des renseignements personnels des internautes par des tiers; et c) la diffusion illicite des renseignements personnels de tiers par un internaute.

143 www.granddictionnaire.com.

144 <http://www.facebook.com>.

145 <http://www.myspace.com>.

146 Voir Commissariat à la protection de la vie privée du Canada, *La vie privée sur les sites de réseau social : Analyse comparative de six sites*. Ottawa, Commissariat à la protection de la vie privée du Canada, 2009, disponible à l'adresse : http://www.priv.gc.ca/information/pub/sub_comp_200901_f.cfm (dernière visite : 23 mars 2010).

2.1.1.1 L'exploitation des renseignements personnels des internautes

La principale crainte liée aux sites de réseautage personnel découle de l'utilisation des informations recueillies par ces sites. Par exemple, malgré le fait que Facebook ait accepté de répondre aux préoccupations de la commissaire à la protection de la vie privée quant à l'utilisation des renseignements personnels détenus par l'entreprise sur ses abonnés¹⁴⁷, la Politique de confidentialité du site, laquelle a été mise à jour le 9 décembre 2009¹⁴⁸, permet toujours au service d'épier les agissements de ses utilisateurs et de collecter de l'information à l'insu de ceux-ci, notamment via les comptes de tierces parties ou d'autres sites, ce qui s'avère contraire aux exigences de la LPRPDE (art. 4.3 de l'Annexe 1 à la *Loi*). Cette information est par la suite utilisée à des fins statistiques, publicitaires et commerciales qui semblent dépasser les « attentes raisonnables » (art. 4.3.5 de l'Annexe 1 de la LPRPDE) de certains internautes.

Par ailleurs, la « Déclaration des droits et responsabilités » du site¹⁴⁹ prévoit l'accord d'« une licence non-exclusive, transférable, sous-licenciable, sans redevance et mondiale pour l'utilisation des contenus de propriété intellectuelle que vous publiez sur Facebook ou en relation à Facebook ». Comme toute image ou tout écrit contenant des renseignements personnels peut être juridiquement qualifié de « propriété intellectuelle », cette licence semble outrepasser les limites fixées par la LPRPDE (art. 4.5 de l'Annexe 1) relatives à l'utilisation des données.

2.1.1.2 L'exploitation des renseignements personnels des internautes par des tiers

L'exploitation des renseignements personnels des internautes par des tiers n'est pas due à une quelconque intention maléfique des sites de réseautage personnel, mais bien à une insouciance ou une inconscience des internautes. En effet, il semble que les internautes publicisent eux-mêmes une quantité de renseignements personnels les visant sans craindre les conséquences qu'une telle transparence pourrait entraîner¹⁵⁰. Comme l'a démontré un article publié dans le bimestriel français « Le Tigre »¹⁵¹ en janvier 2009, la quantité d'information rendue disponible sur de tels sites est parfois alarmante :

147 *Id.*

148 Voir : <http://www.facebook.com/policy.php>.

149 <http://www.facebook.com/terms.php?ref=pf>.

150 Une trop grande divulgation de renseignements personnels via tels sites pourrait accroître les risques de vol d'identité. Il importe toutefois de souligner que les risques de vol d'identité sont tout aussi élevés lorsque l'on dispose de renseignements personnels dans nos ordures ménagères ou dans le recyclage. Voir http://www.cisc.gc.ca/annual_reports/annual_report_2008/feature_focus_2008_f.html.

151 <http://www.le-tigre.net/Marc-L.html> (dernière visite : 23 mars 2010).

Bon anniversaire, Marc. Le 5 décembre 2008, tu fêteras tes vingt-neuf ans. Tu permets qu'on se tutoie, Marc? Tu ne me connais pas, c'est vrai. Mais moi, je te connais très bien. C'est sur toi qu'est tombée la (mal)chance d'être le premier portrait Google du *Tigre*. Une rubrique toute simple : on prend un anonyme et on raconte sa vie grâce à toutes les traces qu'il a laissées, volontairement ou non sur Internet. Comment ça, un message se cache derrière l'idée de cette rubrique ? Évidemment : l'idée qu'on ne fait pas vraiment attention aux informations privées disponibles sur Internet, et que, une fois synthétisées, elles prennent soudain un relief inquiétant. [...] »

L'article poursuit en précisant que, à l'aide du profil Facebook de Marc, le journaliste fut en mesure de connaître plusieurs détails sur sa vie privée. Évidemment, la vie privée d'un individu lui appartient et il revient à chacun de décider ce qu'il désire publiciser. Il importe donc de ne pas adopter une attitude paternaliste et d'imposer une pudeur collective par voie législative ou autre. Cependant, bien qu'une majorité de sites de réseautage personnel offrent une option permettant de limiter l'accès à son profil, cette option n'est pas toujours activée par défaut, malgré ce que pourraient en croire les utilisateurs¹⁵². Il s'agit donc d'informer et d'éduquer les internautes sur les conséquences de la mise en ligne de renseignements personnels, notamment quant à la perpétuité relative de ces données une fois qu'elles sont versées sur le réseau.

Il importe de préciser que la cueillette de telles informations par un tiers est proscrite par le troisième principe de l'Annexe 1 de la LPRPDE relatif au consentement, notamment à l'article 4.3.1 qui prévoit qu'« [i]l faut obtenir le consentement de la personne concernée avant de recueillir des renseignements personnels à son sujet et d'utiliser ou de communiquer les renseignements recueillis ». Cependant, une entreprise pourrait argumenter qu'un internaute ayant un profil public sur Facebook doit raisonnablement s'attendre à ce que cette information soit recueillie par des tiers (art. 4.3.5 de l'Annexe 1 de la LPRPDE) et qu'un consentement implicite lié à l'utilisation de Facebook existe à cet effet (art. 4.3.7d) de l'Annexe 1 de la LPRPDE).

2.1.1.3 La diffusion illicite des renseignements personnels de tiers par un internaute

Les réseaux sociaux facilitent, pour ne pas dire encouragent, la diffusion illicite des renseignements personnels de tiers. Par exemple, une annonce télévisée de l'entreprise Rogers diffusée en 2008 ventait la possibilité, pour un jeune, de photographier son ami, puis de transmettre ladite image directement dans son album Facebook ou de la partager avec des tiers. Or, une telle publication de

152 Voir *La vie privée sur les sites de réseau social : Analyse comparative de six sites, supra, note 146*.

l'image d'un individu sans obtenir son autorisation préalable est contraire aux enseignements de la Cour suprême¹⁵³.

Bien qu'il ne s'agisse pas de sites de réseautage personnel à proprement parler, les sites permettant de partager des images, tels Flickr¹⁵⁴, ou des vidéos, tels Youtube¹⁵⁵ participent à cette banalisation de la vie privée. Encore une fois, il n'est pas question de porter de jugement de valeur sur la volonté des internautes de partager leur image avec des tiers. Il s'agit simplement de s'assurer que les conséquences d'un tel partage sont bien comprises par ceux-ci. Par ailleurs, tout comme les sites de réseautage personnel, ces sites se réservent certains droits de rediffusion et de réutilisation des contenus affichés par les utilisateurs, ce qui pourrait avoir des conséquences néfastes quant à un éventuel « droit à l'oubli numérique¹⁵⁶ ». Par exemple, les modalités d'utilisation de Youtube prévoient que :

En soumettant des présentations d'utilisateurs à YouTube, vous lui octroyez une licence mondiale, non exclusive, sans droits d'auteur, transférable et pouvant donner lieu à l'octroi d'une sous-licence afin d'utiliser, de reproduire, de distribuer, de préparer des produits dérivés, de présenter et de produire les présentations d'utilisateurs en lien avec le site Web de YouTube et les activités de YouTube (ainsi que de ses successeurs et associés), ce qui comprend, sans s'y limiter, la promotion et la redistribution d'une partie ou de l'ensemble du site Web de YouTube (et les produits dérivés) dans tous les formats médiatiques et par l'entremise de toutes les formes de médias¹⁵⁷. [traduction]

Indirectement, ceci implique que les renseignements personnels contenus dans les vidéos téléversées sur Youtube pourront être exploités par l'entreprise à des fins non prévus par l'internaute. Ceci est d'autant plus problématique lorsque le contenu téléversé contient des renseignements visant un tiers n'ayant pas consenti à une telle diffusion (par exemple un ami participant à la vidéo).

153 Voir *Aubry c. Éditions Vice-Versa inc.*, 1998, 1 R.C.S. 591.

154 <http://www.flickr.com/>.

155 <http://www.youtube.com>.

156 Une proposition de loi afin qu'un tel droit soit reconnu a été déposée en France le 6 novembre 2009. Voir : <http://www.senat.fr/leg/pp109-093.html>. Notons que la notion de « droit à l'oubli » est reconnue par la jurisprudence québécoise. Voir *Bombardier c. Bouchard*, 1996, CanLII 6356 (QC C.A.).

157 <http://www.youtube.com/t/terms> [en anglais seulement].

2.1.2 Le perfectionnement et la polyvalence accrue des moteurs de recherche

À l'époque de l'adoption de la LPRPDE, une majorité de moteurs de recherche répertoriaient les sites Web en fonction de leurs balises méta (*meta tags*), soit des « [b]alise HTML insérée dans l'en-tête d'une page Web, après le titre, qui permet de décrire le contenu de la page afin de la référencer correctement et plus facilement dans les moteurs de recherche¹⁵⁸ ». Concrètement, il s'agit de mots clés que l'on retrouve dans le code HTML d'une page et qui sont censés en décrire le contenu. Les gestionnaires de sites exerçaient donc un certain contrôle sur leur classement selon les balises sélectionnées. Cependant, bien qu'un choix judicieux dans les mots clés employés pour répertorier une page Web aide toujours dans sa classification¹⁵⁹, les outils de recherche modernes utilisent un amalgame de critères pour répertorier des sites. D'ailleurs, Google, lequel est responsable de 65 % des recherches effectuées sur le Web¹⁶⁰, n'utilise pas les balises méta comme critère de classification¹⁶¹. En effet :

Les moteurs de recherche modernes utilisent maintenant des algorithmes complexes et des centaines de critères de cotation différents pour produire leurs résultats. Parmi les sources de données se trouvent la boucle de commande générée par la fréquence des termes de recherche, le nombre de clics d'utilisateurs sur les résultats de recherche et notre propre historique de recherche et de navigation personnel. Par exemple, si une majorité d'utilisateurs cliquent sur le cinquième élément d'une page de résultats de recherche plus souvent que sur le premier, les algorithmes de Google prennent cette action comme un signal que le cinquième résultat est peut-être meilleur que le premier, et ajustera éventuellement les résultats en conséquence¹⁶². [traduction]

C'est donc dire que des renseignements personnels autrefois perdus dans le cyberspace deviennent maintenant facilement accessibles. Qui plus est, l'ajout d'outils de recherche par image tels Google images¹⁶³ permet d'associer un

158 www.granddictionnaire.com.

159 Voir notamment *Netbored c. Avery Holdings Inc.*, 2005 CF 1405 (CanLII), paragr. 4.

160 « comScore Releases June 2009 U.S. Search Engine Rankings », 2009, disponible à l'adresse : http://www.comscore.com/Press_Events/Press_Releases/2009/7/comScore_Releases_June_2009_U.S._Search_Engine_Rankings.

161 Voir : <http://googlewebmastercentral.blogspot.com/2009/09/google-does-not-use-keywords-meta-tag.html>.

162 Tim O'Reilly et John Battelle, « Web Squared: Web 2.0 Five Years On », 2009, disponible à l'adresse : <http://www.web2summit.com/web2009/public/schedule/detail/10194>.

163 <http://images.google.ca/>.

nom à un visage en quelques clics, opération rendue d'autant plus facile par la présence de profils publics sur les différents sites de réseautage personnel. Certains moteurs de recherche permettent également la recherche d'adresses. C'est le cas, notamment, de Googlemaps¹⁶⁴ et de Yahoo! maps¹⁶⁵.

Le moteur Googlemaps a récemment fait couler beaucoup d'encre suite à l'ajout du service « Google Street View », un concept permettant d'explorer « les photos de rues de villes du monde entier grâce aux fonctions de zoom, de rotation et de déplacement¹⁶⁶ ». Depuis son implantation canadienne, le site a permis l'accès à des images d'un citoyen montréalais sortant d'un Sexshop de la rue Ste-Catherine¹⁶⁷, ou encore de deux étudiantes de l'Université d'Ottawa prenant un bain de soleil¹⁶⁸. Bien que le service ait « mis au point une technologie très sophistiquée permettant de rendre flous des visages et des plaques d'immatriculation¹⁶⁹ », il demeure que cette technologie n'est pas infaillible. Qui plus est, même lorsqu'un visage est brouillé, il peut être possible d'identifier l'individu en utilisant d'autres critères tels son positionnement géographique, son apparence et sa tenue vestimentaire¹⁷⁰. Or, bien qu'il soit possible de demander le retrait d'une image¹⁷¹, il demeure que cette technologie va à l'encontre de la position adoptée par la Cour suprême dans *Aubry c. Éditions Vice-versa*¹⁷² selon laquelle « un photographe [doit] obtenir le consentement de toutes les personnes qu'il photographie dans des lieux publics avant de publier leur photographie¹⁷³ ». Cette incohérence devra donc éventuellement être corrigée, soit par voie législative, soit par la fermeture du service.

2.1.3 La convergence des outils et services Web

Comme l'explique Tim O'Reilly :

Quand les composants de base deviennent abondants, il est possible de créer de la valeur en les assemblant de manière nouvelle ou plus efficace. Tout comme la révolution du PC a apporté de nombreuses opportunités d'innovation dans l'assemblage du hardware et a permis à des sociétés comme

164 <http://maps.google.ca/>.

165 <http://ca.maps.yahoo.com/>.

166 Voir : <http://maps.google.ca/help/maps/streetview/>.

167 Voir : <http://www.infinet.net/techno/nouvelles/archives/2009/10/20091008-073509.html>.

168 Ian Kerr, « Soft Surveillance, Hard Consent », conférence prononcée le 1^{er} décembre 2009 à l'Université de Montréal.

169 <http://maps.google.ca/help/maps/streetview/privacy.html>.

170 I. Kerr, *supra*, note 168.

171 <http://maps.google.ca/help/maps/streetview/privacy.html>.

172 *Aubry c. Éditions Vice-Versa inc.*, *supra*, note 153.

173 *Id.*, paragr. 65

Dell faisant une science de cet assemblage de vaincre des sociétés dont le modèle d'affaires reposait sur l'innovation dans la production de composants, nous pensons que le Web 2.0 apportera des opportunités pour des sociétés d'entrer dans la compétition simplement en intégrant et en assemblant des services fournis par d'autres¹⁷⁴.

Ce principe d'« innovation par l'assemblage¹⁷⁵ » implique un certain partage d'informations entre services au cœur d'une même entreprise, voire même entre entreprises distinctes. Par exemple, la barre d'outils du navigateur Firefox incorpore une fenêtre de recherche Google, alors que Facebook permet d'incorporer des vidéos issues du site Youtube. Dans certains cas, des tiers viendront réunir les contenus de fournisseurs distincts pour offrir un service nouveau. C'est le cas, par exemple, du site <http://www.housingmaps.com/>, lequel combine les informations de [Craigslist.com](http://www.craigslist.com/) et de [Googlemaps.com](http://www.google.com/maps) pour permettre une recherche de logement par région géographique¹⁷⁶.

Or, cette collaboration entre différents services implique nécessairement un partage important de données concernant lesdits services mais également concernant les utilisateurs. C'est pourquoi le « Centre de confidentialité » de Google¹⁷⁷ prévient les internautes que « nous proposons certains de nos services sur ou par l'intermédiaire d'autres sites Web. Les informations personnelles que vous fournissez à ces sites peuvent être transmises à Google pour vous permettre de bénéficier du service proposé ». Google est d'ailleurs l'exemple typique de la convergence des services puisque les Règles de confidentialité de Google « s'appliquent à l'ensemble des produits, services et sites Web proposés par Google Inc., ses filiales ou ses sociétés affiliées, à l'exception de DoubleClick et de Postini¹⁷⁸ », ce qui inclut Gmail, Googlemaps, Youtube, Blogger, etc.¹⁷⁹.

Dans le même ordre d'idée, la « Politique de confidentialité de Facebook » prévoit que « [n]ous pouvons proposer des services conjointement avec d'autres sociétés, telles que le service de petites annonces sur Facebook Marketplace. Si vous utilisez ces services, nous sommes en droit de partager vos informations dans le cadre de ce service [...] ». Si un tel partage s'avère nécessaire à l'établissement de passerelles entre services et, donc, à la convivialité générale du Web, il demeure qu'il est contraire aux principes de *détermination des fins de la collecte des renseignements*, de *consentement* et de *limitation de l'utilisation, de la communication et de la conservation* énoncés aux articles 4.2, 4.3 et 4.5 de l'Annexe 1 de la LPRPDE.

174 Voir T. O'Reilly, *supra*, note 137.

175 *Id.*

176 *Id.*

177 <http://www.google.ca/intl/fr/privacypolicy.html>.

178 Voir : <http://www.google.fr/privacypolicy.html>.

179 Voir : <http://www.google.fr/options/>.

Selon les experts, la tendance actuelle pointe vers la création éventuelle d'une « base de données d'identités à l'échelle du réseau¹⁸⁰ » (projet déjà entamé par Google)¹⁸¹, et donc d'un plus grand partage des renseignements personnels des utilisateurs du Web. Cette tendance n'est pas sans rappeler la notion d'« informatique dans les nuages » ou « infonuagique » (cloud computing), laquelle réfère à un « [m]odèle informatique qui, par l'entremise de serveurs distants interconnectés par Internet, permet un accès réseau, à la demande, à un bassin partagé de ressources informatiques configurables, externalisées et non localisables, qui sont proposées sous forme de services, évolutifs, adaptables dynamiquement et facturés à l'utilisation¹⁸² ». Ainsi :

Toute information stockée localement dans un ordinateur pourrait être stockée dans un nuage, y compris les courriels, les documents de traitement de texte, les feuilles de calcul, les vidéos, les dossiers de santé, les photographies, les renseignements fiscaux ou autres renseignements financiers, les plans d'affaires, les présentations PowerPoint, les renseignements comptables, les campagnes de publicité, les numéros de vente, les calendriers des rendez-vous, carnets d'adresses et plus. Tout le contenu du dispositif de stockage d'un utilisateur peut être stocké chez un ou plusieurs fournisseurs de services informatiques dans les nuages¹⁸³.
[traduction]

Or, le fait que cette information soit disponible dans un « nuage » implique qu'elle peut être entreposée sur différents sites offrant des niveaux de sécurité variables, ainsi que dans différents États dont la législation relative à la protection des renseignements personnels n'est pas équivalente aux lois canadiennes¹⁸⁴. Par ailleurs, le fournisseur de service possède un accès à *tous* les renseignements visant un utilisateur, informations qu'il peut, selon le contexte, choisir de partager avec d'autres entreprises¹⁸⁵. Évidemment, si les renseignements personnels versés dans le nuage sont contrôlés par la personne qu'ils identifient, la problématique n'est pas la même que lorsque l'information est versée dans le nuage par un tiers.

* *
*

180 Voir T. O'Reilly, *supra*, note 137.

181 *Id.*

182 Voir : <http://www.granddictionnaire.com>.

183 Voir World Privacy Forum, « Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing », 2009, disponible à l'adresse : <http://www.worldprivacyforum.org/cloudprivacy.html>. [en anglais seulement]

184 *Id.*

185 *Id.*

En somme, il importe de souligner que le fait d'isoler Internet comme étant un simple réseau informatique représente une vision périmée de la technologie. Les téléphones intelligents, AppleTV et la technologie VoIP (Voice over IP) ne sont qu'une série d'exemples qui démontrent que l'interconnectivité et le jumelage des médias nous forcent à redéfinir notre conception de ceux-ci :

... de plus en plus d'appareils pourront être connectés à la nouvelle plate-forme que constitue le web. Quelles applications deviendront possibles quand nos téléphones et nos voitures ne se contenteront plus d'utiliser des données mais en émettront¹⁸⁶?

En matière de gestion et de protection des renseignements personnels les conséquences de ce changement de paradigme sont nombreuses. L'émission de données concernant notre positionnement, nos activités et notre routine, lesquels constituent tous des renseignements personnels au sens de l'article 2 de la LPRPDE, implique une circulation constante de renseignements nous concernant et donc un besoin accru de sécurité pour l'ensemble de ces communications (article 4.7 de l'Annexe 1 de la LPRPDE). Cette multiplication exponentielle des renseignements nous concernant nécessite par ailleurs une prise de conscience collective du fait que les avantages offerts par cette technologie sont difficilement conciliables avec les exigences législatives actuelles relatives à la collecte, la conservation et la destruction de l'information (articles 4.2 et 4.5 de l'Annexe 1 de la LPRPDE).

2.2 Sur le plan organisationnel : L'émergence d'autres types d'institutions étatiques

Avec l'avènement de l'État providence, la branche exécutive a, comme on le sait, pris une expansion considérable non seulement par la création de multiples nouveaux ministères, mais aussi par la création de très nombreux organismes décentralisés (les tribunaux administratifs, les commissions administratives et les organismes de régulation économique).

Durant les années 1970-1980, les gouvernements remettent en cause l'efficacité et l'efficience de l'État providence, ce qui mènera à des réorganisations importantes de services et au démantèlement de plusieurs organismes décentralisés. Toutefois, ce qui est particulièrement notable dans ce réaménagement est l'émergence d'un autre type d'organisme : les organismes de surveillance des activités de l'administration. Ce type d'organisme n'était pas complètement inconnu des législateurs avant les années 1970, mais à partir de cette décennie, d'autres seront créés.

Les organismes de surveillance des activités de l'administration se distinguent par plusieurs traits qui, pour certains auteurs, annoncent la mise en place d'un

186 Voir T. O'Reilly, *supra*, note 137.

système national d'intégrité, ne s'insérant pas, sur le plan organisationnel, dans l'organisation gouvernementale, mais plutôt dans l'organisation parlementaire. Dans un premier temps, nous explorons les origines intellectuelles du concept de système d'intégrité. À cet égard, il faut noter que ce nouveau système d'intégrité est conçu comme un mécanisme de surveillance des activités gouvernementales dans leur ensemble et non pour surveiller les activités du secteur privé. Or, la commissaire à la protection de la vie privée surveille tant les activités publiques (*Loi sur la protection des renseignements personnels*) que privés (la LPRPDE).

Vu la recrudescence dans la création de ce type d'organismes au sein de l'État fédéral, il faut s'interroger sur la cohérence du choix initial d'attribuer la compétence d'appliquer la LPRPDE au commissaire à la protection de la vie privée eu égard aux transformations dans l'organisation de l'État fédéral. C'est sur cette question que nous nous pencherons dans un deuxième temps.

2.2.1 Le système national d'intégrité

Dans un article publié en 1999, le professeur Bruce Ackerman défend ce qu'il appelle la « branche de l'intégrité¹⁸⁷ ». Ce chercheur américain propose formellement l'implantation d'une telle branche dans le système politique républicain des États-Unis. Selon l'auteur, les organismes qui en feraient partie agiraient comme « chien de garde constitutionnel ».

Le professeur Ackerman estime que cette branche doit fonctionner de manière distincte des trois autres branches de l'État (judiciaire, exécutive et législative). Son rôle serait exclusivement centré sur la surveillance et le contrôle des risques de corruptions. À maintes reprises dans son texte, il fait valoir que la réflexion suggérée doit s'affranchir de la conception traditionnelle des trois branches étatiques¹⁸⁸. Il propose donc la construction d'une nouvelle doctrine de la séparation des pouvoirs et encourage ainsi les rédacteurs des constitutions modernes à considérer l'intégration d'une branche de l'intégrité. La principale justification de l'auteur pour soutenir la création d'une branche de l'intégrité est que, selon lui, il n'est pas possible de faire confiance aux politiciens lorsqu'il s'agit de traiter sérieusement du problème de la corruption¹⁸⁹.

La création d'une « branche de l'intégrité » a intéressé d'autres juristes. Le juge Spigelman a proposé son implantation dans le système parlementaire australien et la contribution du juge Spigelman porte notamment sur l'élargissement des compétences de ces organismes faisant partie de ce système d'intégrité.

187 Bruce Ackerman, « The New Separation of Powers » (1999-2000) 113 *Harvard Law Review* 633, 694-696; Voir aussi un article antérieur de Bruce Topperwien, « Separation of Powers and the Status of Administrative Review », (1999) 20 *Australian Institute of Administrative Law Forum* 32.

188 B. Ackerman, *supra*, note 187, 691.

189 *Id.* 694.

2.2.1.1 L'élargissement des compétences des organismes publics

L'idée d'Ackerman a intéressé les juristes provenant d'un système parlementaire comme le nôtre. En effet, quelques années après la publication du texte d'Ackerman, l'honorable juge en chef James Spigelman d'Australie¹⁹⁰ se prononce en faveur de la création d'une « branche de l'intégrité » en Australie. Il transpose ainsi l'idée d'Ackerman dans un système parlementaire de type britannique :

Le Parlement en tant qu'institution fait plus que légiférer : il joue un rôle important en vue de veiller à ce que les pouvoirs conférés aux autorités exécutives et aux juges soient utilisés de manière appropriée, étant donné le pouvoir du Parlement de renvoyer les fonctionnaires judiciaires. La fonction d'intégrité du Parlement est au cœur de la légitimité de notre processus gouvernemental¹⁹¹.
[traduction]

Le juge précise que les compétences d'une telle branche ne devraient pas se limiter aux problèmes de corruption (comme le fait Ackerman) puisqu'il estime qu'une compétence aussi étroitement conçue ne serait pas suffisante en elle-même pour comprendre tous les abus de pouvoirs. Il va donc plus loin en ajoutant que la raison d'être de cette branche doit être élargie pour inclure le respect de la « primauté du droit » et de la « moralité au droit ». Précisons ici que ces deux idées mises de l'avant par le juge, ne sont pas nouvelles puisque le philosophe Lon Fuller les avait déjà exposées dans ses écrits¹⁹².

La branche de l'intégrité devrait avoir pour fonction de surveiller les institutions publiques afin qu'elles ne s'écartent ni des fonctions pour lesquelles elles ont été créées, ni des valeurs publiques auxquelles elles sont tenues de se conformer¹⁹³ :

À titre de courte définition, la branche de l'intégrité de la fonction d'un gouvernement doit veiller à ce que chaque institution gouvernementale exerce les pouvoirs qui lui sont

190 L'honorable juge en chef James Spigelman, « The Integrity Branch of Government – The First Lecture in the 2004 National Lecture Series » discours présenté dans le cadre du *National Lecture Series of the Australian Institute of Administrative Law*, Sydney, 29 avril 2004, disponible en ligne à l'adresse suivante : http://www.lawlink.nsw.gov.au/lawlink/supreme_court/ll_sc.nsf/pages/SCO_speech_spigelman_290404 (dernière visite : 14 décembre 2009). Le juge a publié toute une série de discours sur le même sujet et qui sont accessibles en ligne.

191 L'honorable juge en chef James Spigelman, « The Integrity Branch of Government », *Quadrant*, vol. XLVIII, n° 7, juillet-août 2004, p. 51.

192 On peut lire notamment : Lon L. FULLER, « Positivism and Fidelity to Law — A Reply to Professor Hart », (1958) 71:4 *Harvard Law Review* 630.

193 L'honorable juge en chef Spigelman, *supra*, note 190, p. 52.

conférés de la manière attendue aux fins pour lesquelles ces pouvoirs ont été conférés, et non à d'autres fins. [traduction]

Dans son analyse, le juge Spigelman met l'accent sur l'intégrité institutionnelle plutôt que l'intégrité personnelle tout en constatant que cette dernière est directement reliée à la première. D'une part, il explique que l'intégrité personnelle peut être décrite en termes de qualités personnelles telles que l'honnêteté, l'absence de corruption, la conduite éthique et la conformité aux bons usages. D'autre part, il indique que l'intégrité institutionnelle se décompose en trois principaux éléments : la conduite de toute institution gouvernementale devant donc 1) être autorisée par la loi, 2) être fidèle à la raison d'intérêt public pour laquelle un pouvoir lui a été conféré ou une obligation imposée, et 3) respecter les valeurs auxquelles elle doit obéir¹⁹⁴.

À partir de nombreux exemples, il constate que plusieurs institutions déjà existantes à l'intérieur des trois branches déjà reconnues constituent déjà collectivement un système d'intégrité, mais insiste sur les limites du *statut quo* sur le plan organisationnel¹⁹⁵. En effet, il faut souligner les limites d'un tel système lorsque les organismes qui en font partie ne sont pas suffisamment indépendants à l'égard du gouvernement dont ils sont censés surveiller les actes. Enfin, il considère que la littérature traditionnelle en droit administratif fait déjà état de nombreux thèmes analysant le système d'intégrité, mais qu'il y a lieu d'en suggérer un nouvel assemblage unifié¹⁹⁶. Sur ce point, l'examen du « système d'intégrité » canadien au niveau fédéral montre qu'il existe déjà une grande cohérence sur le plan de l'organisation institutionnelle de ce type d'organisme.

2.2.1.2 La cohérence institutionnelle du système fédéral d'intégrité

Au sein de l'État fédéral canadien, il existe déjà une douzaine d'organismes publics dotés de compétences distinctes, mais toutes en lien avec une idée élargie d'intégrité telle que proposée par le juge Spigelman, et chargés de surveiller les activités gouvernementales qu'elles soient le fruit d'organismes centraux ou décentralisés.

Comme nous le mentionnions en introduction, la création de ce type d'organisme n'est pas complètement nouvelle. En effet, le premier à voir le jour

194 L'honorable juge en chef James Spigelman, « Judicial Review and the Integrity Branch of Government » discours présenté lors du *World Jurist Association Congress*, Shanghai, 8 septembre 2005, disponible en ligne à l'adresse suivante : http://www.lawlink.nsw.gov.au/lawlink/supreme_court/ll_sc.nsf/pages/SCO_spigelman080905 (dernière visite : 14 décembre 2009). Voir aussi : John McMillan, « The Ombudsman and the Rule of Law », 2005, 44 *Australian Institute of Administrative Law Forum* 1; Anita Stumcke et Anne Tran, « The Commonwealth Ombudsman: an Integrity Branch of Government? », 2007, 32 :4 *Alternative Law Journal* 233.

195 L'honorable juge en chef Spigelman, *supra*, note 190, p. 51.

196 *Id.*, p. 57.

et le plus ancien est sans conteste celui du Bureau Vérificateur général né en 1908. Viendra ensuite le Bureau du Directeur des élections en 1920. Toutefois, pendant une période de cinquante ans, aucun autre nouvel organisme de ce type n'a vu le jour. Ce n'est qu'à partir des années 1970 qu'ils font de nouveau leur apparition sur la scène fédérale. En 1970, c'est le Commissariat aux langues officielles qui est créé. En 1983, deux autres commissariats seront créés : le Commissariat à la protection de la vie privée et le Commissariat à l'information. À partir des années 2000, un réel engouement se pointe puisque cinq nouveaux organismes de ce type sont créés : le Directeur parlementaire du budget (2006), le commissaire aux nominations publiques (création en 2006, mais le titulaire du poste n'a pas encore été nommé¹⁹⁷) le Commissariat aux conflits d'intérêts et à l'éthique (Chambre des Communes et Sénat) (2007), le Commissariat à l'intégrité du secteur public (2007) et le Commissariat au lobbying (2008). Enfin, il faut souligner la reconnaissance par le Parlement de l'importance de deux autres commissariats, soit le Commissariat des droits de la personne et le Commissariat de la fonction publique. Ces deux organismes existaient depuis longtemps, mais ce n'est que depuis quelques années que leurs présidents se sont vus reconnaître le statut du haut fonctionnaire du Parlement¹⁹⁸. En somme, notre Système national d'intégrité regroupe des organismes chargés de vérifier une administration du gouvernement fédéral qui soit la plus intègre possible :

- De la gestion des comptes publics et du budget, du système électoral, du système d'accès à l'information ainsi que celui relatif à l'embauche des fonctionnaires et des titulaires de charge publique (dans ce dernier cas, personne n'a encore été nommé à ce poste);
- De la protection du droit à l'intégrité des personnes (protection des renseignements personnels et droits humains);
- Dans la surveillance des mesures pour contrer la corruption des titulaires de charges publiques et des fonctionnaires.

Notre Système national d'intégrité montre un haut niveau de cohérence sur au moins deux plans. Tout d'abord, il y a une très grande cohérence quant au haut degré d'indépendance reconnu à ces organismes afin qu'ils puissent exécuter leur mission à l'abri des pressions gouvernementales. Ensuite, ces organismes sont des agents du Parlement qui ne font pas partie de l'autorité exécutive.

Sur le degré d'indépendance, il importe de noter que les lois constitutives de ces organismes comportent des distinctions très nettes avec celles constituant des organismes décentralisés, tels les tribunaux administratifs. Un des traits distinctifs très significatif est le fait que les présidents de ces organismes sont nommés selon une procédure qui requiert le concours des parlementaires. Généralement, tant la Chambre des communes que le Sénat doivent être consultés par le Gouvernement sur la personne que ce dernier entend nommer

197 *Loi sur les traitements*, L.R.C. 1985, chap. S-3, art. 1.1, loi modifiée par l'art. 227 de la *Loi fédérale sur la responsabilité*, L.C. 2006, chap. 9, art. 109 et s.

198 <http://www2.parl.gc.ca/Parlinfo/compilations/OfficersAndOfficials/OfficersOfParliament.aspx?Language=F>

et recevoir l'approbation des deux chambres¹⁹⁹. Cette procédure de nomination contraste avec celles qui est utilisée pour nommer des membres au sein d'organismes décentralisés (tels que des tribunaux administratifs) puisque la nomination de ces derniers ne requiert que le concours du Gouvernement. Quant à la révocation des mandats des membres nommés au sein des organismes faisant partie du Système national d'intégrité, elle requiert également le concours des deux chambres, ce qui n'est pas le cas pour la révocation des membres des organismes décentralisés.

Sur le rattachement de ces organismes au Parlement, deux points doivent être soulignés. Tout d'abord, tous les présidents de ces organismes sont maintenant reconnus comme de hauts fonctionnaires du Parlement (évidemment, ce statut est en lien avec les procédures spéciales devant être suivies pour nommer ou révoquer ces présidents). L'expression haut fonctionnaire du Parlement désigne plusieurs postes de personnes qui jouent des rôles clés dans l'exercice des fonctions parlementaires :

1. les sénateurs et les députés qui sont nommés à certains postes reliés au Parlement;
2. les greffiers à la procédure et les cadres supérieurs du Sénat, de la Chambre des communes et de la Bibliothèque du Parlement;
3. les fonctionnaires indépendants chargés de la surveillance, relevant du Parlement²⁰⁰.

199 Il est important de noter, toutefois, que les procédures de nomination de ces hauts fonctionnaires du Parlement ne sont pas uniformes. Cependant et sauf pour le commissaire canadien des droits de la personne, tous les présidents de ces organismes sont nommés selon une procédure impliquant l'approbation par au moins la Chambre des communes. Par exemple, le Vérificateur général est nommé par le gouverneur en conseil par commission sous le grand sceau, après consultation du chef de chacun des partis reconnus au Sénat et à la Chambre des communes et approbation par résolution du Sénat et de la Chambre des communes : *Loi sur le vérificateur général*, L.R.C. 1985, chap. A-17, art. 3 (1); une procédure similaire est employée pour la nomination du commissaire aux langues officielles : *Loi sur les langues officielles*, L.R.C. 1985, chap. 31 (4^e suppl.), art. 49 (1); pour la commissaire à la protection de la vie privée : *Loi sur la protection des renseignements personnels*, L.R.C. 1985, chap. P-21, art. 53 (1); le commissaire à l'information : *Loi sur l'accès à l'information*, L.R.C. 1985, chap. A-1, art. 54(1); le commissaire aux conflits d'intérêts et à l'éthique, *Loi sur le Parlement du Canada*, L.R.C. 1985, chap. P-1, art. 81 (1); le commissaire au lobbying : *Loi sur le lobbying*, L.R.C. 1985, chap. 44 (4^e suppl.), art. 4.1 (1); le commissaire de la fonction publique : *Loi sur l'emploi dans la fonction publique*, L.C. 2003, chap. 22, art. 4(5); quant au Directeur général des élections, il est nommé par résolution de la Chambre des communes : *Loi électorale du Canada*, L.C. 2000, chap. 9, art. 13. Finalement, le commissaire des droits de la personne est nommé par le gouverneur en conseil, mais son mandat ne peut être révoqué que par le gouverneur en conseil sur adresse du Sénat et de la Chambre des communes : *Loi canadienne sur les droits de la personne*, L.R.C. 1985, chap. H-6, art. 26 (1) et (4).

200 *Id.*

C'est à cette dernière catégorie qu'appartiennent les présidents des organismes que nous avons énumérés, et incluant celui du Commissariat à la protection de la vie privée qui nous intéresse plus particulièrement. La désignation de haut fonctionnaire du Parlement est utilisée pour :

... insister ainsi sur le fait que ces personnes assument des responsabilités pour le Parlement et en relèvent, et pour les distinguer des autres fonctionnaires du Parlement. L'expression est également employée pour souligner leur indépendance par rapport au gouvernement en place. Ils assument les responsabilités que leur confère la loi et font directement rapport au Sénat ou à la Chambre des communes ou encore aux deux Chambres, habituellement par l'intermédiaire des présidents de ces dernières. Les personnes nommées à ces fonctions travaillent pour le compte du Parlement²⁰¹. (Nos soulignés).

Enfin, pour marquer leurs fonctions, qu'ils doivent exercer de façon indépendante par rapport à l'organe exécutif, les hauts fonctionnaires de ces organismes de surveillance rendent compte de leurs activités annuelles directement devant le Parlement (et non à un ministre comme c'est le cas pour les organismes décentralisés). De plus, ils peuvent saisir le Parlement (et les médias par le fait même) de tout problème qu'ils estiment urgent en tout temps. Ce pouvoir extraordinaire est fondamental puisque, par celui-ci, les présidents peuvent réellement contribuer au fonctionnement effectif du système parlementaire. Comme on le sait, le fonctionnement adéquat du Parlement est tributaire d'un ensemble de coutumes et de conventions constitutionnellement qui ne sont efficaces que si le Gouvernement les respecte. Aussi, dans la tradition parlementaire, les hauts fonctionnaires du Parlement occupent des « postes de responsabilité indépendants créés pour aider le Parlement à tenir les ministres et la bureaucratie responsables de leurs actions et pour protéger les diverses catégories de droits des Canadiens ou encore pour exécuter certaines fonctions indépendantes du pouvoir exécutif ». C'est pour cette raison que les titulaires de ces postes relèvent du Parlement plutôt que du gouvernement (ou d'un ministre en particulier).

Cependant, cette cohérence institutionnelle est imparfaite. En effet, l'idée d'instituer un Système national d'intégrité vise à rendre possible l'exercice d'une surveillance continue des activités gouvernementales dans certains secteurs bien ciblés. Aussi, d'en attribuer la mission à des organismes rattachés au Parlement est sensée sur le plan de l'organisation étatique. D'ailleurs, dans la *Loi fédérale sur la responsabilité* ces charges publiques sont énumérées dans la Partie II de la loi qui est intitulée : Appui au Parlement²⁰². Toutefois, deux de ces « organismes parlementaires de surveillance » dont celui qui nous intéresse

201 *Id.*

202 *Loi fédérale sur la responsabilité, supra*, note 197, art. 109 et s.

— le Commissariat à la protection de la vie privée (l'autre étant la Commission canadienne des droits de la personne) — ont également pour mission de surveiller l'activité du secteur privé dans leur domaine de compétence. La question qui se pose ici est de savoir si ce choix du législateur devrait être remis en question.

2.2.2 La surveillance des activités du secteur privé

Était-il cohérent sur le plan institutionnel d'attribuer à la commissaire à la protection de la vie privée la responsabilité de surveiller des activités autres que gouvernementales? Dans un premier temps, nous examinons deux arguments : l'un favorable; l'autre défavorable. Dans un deuxième temps, nous passerons en revue les catégories d'organismes décentralisés afin d'apporter un éclairage sur le type d'organisme qui pourrait se charger de l'application de la LPRPDE dans l'éventualité où la commissaire à la protection de la vie privée en était délesté

2.2.2.1 Des arguments relatifs au maintien de la compétence du Commissariat sur la LPRPDE

La question de savoir si l'application de la LPRPDE devrait ou non demeurer sous la compétence du Commissariat à la protection de la vie privée fait l'objet de débats. Bien sûr, plusieurs réponses pourraient être apportées à cette question selon la perspective théorique que l'on adopte. Notre objectif ici n'est pas d'épuiser tous les arguments possibles, mais simplement d'en examiner quelques-uns, dans l'optique de stimuler les discussions.

Ainsi, on pourrait être d'avis que le Commissariat devrait demeurer en charge de surveiller l'application de la LPRPDE. Des arguments pragmatiques peuvent être soulevés pour appuyer ce choix. On pourrait d'abord faire valoir *l'expertise institutionnelle*. En effet, il est indéniable que le Commissariat a acquis une expérience considérable depuis qu'il est en charge de surveiller la LPRPDE. De plus, il est incontestable que son expérience antérieure dans l'application de la *Loi sur les renseignements personnels* lui a été d'une aide précieuse pour appliquer la LPRPDE. Ensuite, on pourrait aussi faire valoir l'indivisibilité de l'objet légiféré. La protection des renseignements personnels que ce soit par le secteur public ou le secteur privé soulève des problèmes similaires. Enfin, on pourrait aussi soulever l'argument du risque d'incohérence normative. Si deux organismes distincts sont chargés de surveiller la protection des renseignements personnels dans chacun des secteurs d'activités, des solutions incompatibles pourraient s'ensuivre.

En revanche, si l'on conçoit le rôle de l'ombudsman parlementaire, tel le Commissariat à la protection de la vie privée, comme une institution qui agit à titre de bras droit du Parlement (pour appuyer l'activité parlementaire comme il en est fait mention dans la partie II de la *Loi fédérale sur la responsabilité*), il apparaît incohérent qu'il soit chargé de surveiller des activités qui ne relèvent pas de la fonction parlementaire. En effet, le Parlement est en quelque sorte l'organe de surveillance des activités gouvernementales par excellence. Il est au sommet de la pyramide. Lorsque le Commissariat à la protection de la vie privée surveille l'application de la *Loi sur la protection des renseignements*

personnels, il seconde clairement le Parlement dans l'exécution d'une tâche que ce dernier ne peut pas lui-même effectuer (faute de temps et d'expertise), mais qui relève néanmoins clairement de sa mission institutionnelle. Toutefois, lorsqu'on demande au Commissariat de surveiller si le secteur privé protège les renseignements personnels comme il se doit, le lien entre cette mission privée et la mission publique du Parlement échappe à l'entendement. Ainsi, la division des tâches entre deux organismes distincts apparaîtrait plus cohérente sur le plan de l'organisation des fonctions et pouvoirs des institutions étatiques.

Toutefois, quelque soit les arguments qui aient pu servir dans le passé pour justifier l'extension du mandat de la commissaire à la protection de la vie privée ou qui pourraient être utilisés dans le présent ou dans l'avenir, il faudrait néanmoins que ceux-ci fasse l'objet d'un examen en profondeur, d'autant plus que ce type de question n'a pas été abordée en droit canadien. En effet, même s'il existait de véritables objections à l'attribution d'une compétence relative à la protection des renseignements personnels à deux organismes distincts, il faudrait examiner toutes les pistes de solutions afin d'éviter les solutions faciles. Dans les traditions parlementaire et juridique de *common law*, les institutions sont trop souvent créées au fur et à mesure que se présente les problèmes. Les solutions sont proposées sans qu'il ait sérieusement été tenu compte de facteurs tels la cohérence institutionnelle de l'État, ce qui rend d'ailleurs tout processus de réforme sur grande échelle extrêmement difficile à réaliser.

Dans l'esprit d'une future réforme, il nous semble que cette question ne devrait pas être laissée de côté. Avant de passer à l'action législative, il serait très utile, sinon nécessaire, de bien distinguer entre ce qui est faisable et désirable surtout si l'objectif ultime est de développer un véritable système national d'intégrité. Par exemple, il serait difficile de concilier l'idée qu'au sein d'un même organisme — le Commissariat à la protection de la vie privée — puisse cohabiter dans le corps d'une même personne, soit d'un ombudsman chargé d'appliquer la *Loi sur la protection des renseignements personnels* et d'un décideur chargé de statuer sur des violations de la loi et d'ordonner des peines en vertu de la LPRPDE, sans que la légitimité dans la différence de traitement ne soit continuellement remise en cause minant ainsi à long terme la crédibilité de l'institution. Ceci est d'autant plus vrai si les violations à la loi qui seraient commises par le gouvernement et par le secteur privé étaient essentiellement de même nature.

Une première solution serait de traiter les violations à la loi de la même manière qu'elles soient commises par le secteur public ou privé et de fusionner les deux régimes législatifs en un seul et de pourvoir le Commissariat avec les ressources financières et humaines pour mettre en œuvre ce nouveau mandat. Toutefois, cette solution laisse présager un lot de difficultés additionnelles. En effet, les ressources qui devraient être investies pour que soit mis en œuvre ce nouveau mandat à l'échelle du Canada pourraient atteindre des proportions élephanques. Une deuxième solution serait de créer deux organismes distincts. Par exemple, si au terme de processus de réflexion entourant des modifications à la LRPRDE la conclusion fut qu'il faille attribuer des pouvoirs de nature pénale à l'organisme public chargé de sa mise en œuvre, ne serait-il pas préférable que cet organisme soit détaché du Commissariat à la protection de la vie privée? Cette solution aurait l'avantage d'être plus cohérente sur le

plan institutionnel. En effet, dans l'organisation actuelle de nos administrations publiques canadienne, la tâche de surveiller les activités du secteur privé revient normalement aux organismes décentralisés.

2.2.2.2 Les catégories d'organismes décentralisés

Afin de situer le débat, il est utile de faire un rappel sur les trois grandes catégories d'organismes décentralisés.

- **Les commissions administratives**

Ces commissions se distinguent des autres catégories du fait qu'elles n'exercent souvent qu'un type de fonctions : des fonctions administratives (telles l'inspection, l'enquête, la surveillance des prix, l'information et l'éducation du public, etc.). Accessoirement, elles peuvent aussi exercer quelques fonctions de nature décisionnelle. Le pouvoir le plus fréquent qui leur est attribué à cet égard est celui de statuer sur des plaintes. Souvent les fonctions des commissions administratives et des organismes parlementaires de surveillance des activités gouvernementales sont les mêmes. Ce qui les distinguent sont les sujets et entités surveillés (privés ou publics). Dans le cas de la mise en œuvre de la LPRPDE, il n'y aurait pas de plus-value à l'idée de créer une commission administrative distincte du Commissariat, mais qui auraient essentiellement les mêmes pouvoirs que ceux qui sont actuellement attribués au Commissariat. Cette avenue n'est donc pas particulièrement intéressante ni sur le plan de l'effectivité, ni sur celui de l'efficacité.

- **Les tribunaux administratifs**

Entendu au sens strict, les tribunaux administratifs n'exercent qu'une seule fonction : celle de rendre des décisions individuelles (par exemple : la CISR, le Tribunal des pensions; le Tribunal des vétérans). La possibilité que la surveillance de la LPRPDE soit attribuée à un tribunal administratif au sens utilisé ici n'a pas été, du moins à notre connaissance, sérieusement considérée. Bien sûr, il serait toujours possible de créer deux organismes intégrés (une commission et un tribunal) à l'image de la structure qui a été créée pour la mise en œuvre de la *Loi canadienne sur les droits de la personne* (Commission des droits de la personne et Tribunal des droits de la personne). Mais cette avenue amènerait un lot de difficultés accrues (certaines d'entre elles de nature constitutionnelle). En effet, les portées et limites de la LPRPDE auraient à être radicalement repensées dans ce contexte.

- **Les organismes de régulation (économique ou sociale)**

Ces organismes se distinguent du fait qu'ils exercent trois fonctions : des fonctions administratives (comme les commissions administratives), des fonctions décisionnelles (comme les tribunaux administratifs) et, enfin, des fonctions réglementaires. La fonction réglementaire est la fonction qui justifie le classement d'un organisme sous la catégorie « organisme de régulation ». Voici des exemples faisant partie de la catégorie : organisme de régulation *économique* :

la Commission canadienne des grains²⁰³, le CRTC²⁰⁴, l'Office national de l'énergie²⁰⁵. Dans la catégorie d'organisme de régulation *sociale*, on peut citer le Conseil des relations industrielles²⁰⁶.

Si l'application de la LPRPDE devait être attribuée à un organisme décentralisé, c'est sans aucun doute celui de l'organisme de régulation *sociale* qui pourrait être le plus intéressant puisqu'il permettrait de réfléchir à la protection des renseignements personnels sur un plan beaucoup plus englobant. En effet, puisque tous les pouvoirs peuvent lui être attribués, il peut agir de façon similaire à ombudsman (à qui l'on confère principalement des fonctions administratives tout comme aux commissions administratives), à un tribunal administratif (dans l'optique où l'on souhaiterait lui attribuer des pouvoirs d'émettre des ordonnances) et à l'organisme de régulation sociale (en ce qu'il pourrait exercer des pouvoirs de nature réglementaires (sous la forme de politique ou de règlement).

Enfin, l'intérêt de ce type d'organisme est qu'il peut enquêter et constater les violations à la loi ou aux textes réglementaires qu'il prescrit. De plus, il est intéressant de noter qu'en droit administratif fédéral (mais aussi provincial notamment au Québec avec la création de l'Autorité des marchés financiers ou encore au niveau du gouvernement fédéral avec le projet de création d'une autorité canadienne des valeurs mobilières), on peut noter l'émergence du pouvoir de sanctionner les manquements à la loi.

2.2.2.3 Le choix du type d'organisme décentralisé

Bien que l'état de connaissances sur les missions, pouvoirs et fonctions des organismes décentralisés soit assez limité surtout en droit administratif fédéral, il est utile de dire qu'il n'existe pas à notre connaissance d'organismes décentralisés de la catégorie 1 (commissions administratives) et 2 (tribunaux administratifs) à qui le Parlement a conféré des pouvoirs d'imposer des peines (sous forme d'amende) sur constat de *violations de la loi* par un employé d'un tel organisme. La seule exception que nous avons trouvée à ce principe dans le droit fédéral se trouve dans la *Loi sur l'équité en matière d'emploi*²⁰⁷. Le mécanisme fonctionne comme suit : sur constat de violation de la loi, le ministre peut expédier un avis de sanction pécuniaire (qui constitue une violation de la loi et non une infraction au sens du Code criminel, art. 35(3)). L'employeur peut contester cet avis devant le Tribunal des droits de la personne. Il s'agit donc

203 *Loi sur les grains du Canada*, L.R.C. 1985, chap. G-10.

204 *Loi sur le conseil de la radiodiffusion et des télécommunications canadiennes*, L.R.C. 1985, chap. C-22.

205 *Loi sur l'Office national de l'énergie*, L.R.C. 1985, chap. N-7.

206 Le Conseil canadien des relations de travail est institué par le *Code canadien du travail*, L.R.C. 1985, chap. L-2.

207 *Loi sur l'équité en matière d'emploi*, L.C. 1995, chap. 44, partie III (sanctions pécuniaires), art. 35 et s.

d'une procédure suivant laquelle un tribunal administratif est impliqué dans le processus de sanction, mais seulement après que le ministre ait d'abord constaté la violation de la loi et ait décidé d'imposer une sanction pécuniaire. Nous sommes donc encore loin d'un mécanisme de sanction directement administré par un organisme décentralisé dont il a pu lui-même se saisir (voir annexe A pour lire les dispositions législatives).

Toutefois, soulignons que le Tribunal des droits de la personne du Québec a le pouvoir en vertu de l'art. 49, al. 2, de la *Charte des droits et libertés de la personne* d'octroyer des dommages-intérêts punitifs en cas d'atteinte illicite et intentionnelle à un droit quasi constitutionnel protégé par cette Charte²⁰⁸. Il est intéressant de constater l'existence de ce pouvoir dans le contexte d'exécution d'une loi de nature quasi constitutionnelle, car comme nous le mentionnerons plus loin, il est possible que la protection des renseignements personnels ait maintenant atteint le rang d'un droit quasi constitutionnel.

Normalement, les régimes punitifs qu'on retrouve dans les lois constitutives — que ces deux types d'organismes sont chargés d'appliquer — sont administrés par des juges sur constat d'*infractions* contenues dans ces lois. Le terme « infraction » dans une loi déclenche la procédure de mise en accusation (normalement sur procédure sommaire). Les protections du droit criminel s'appliquent dès lors et ce sont les juges des cours de justice qui doivent faire une déclaration de culpabilité et imposer une peine.

Par contre, il existe des attributions de pouvoirs de nature pénale faites au bénéfice d'organismes de régulation économique ou sociale (3^e catégorie). En effet, de telles dévolutions de pouvoirs ne sont pas méconnues en droit administratif fédéral. Par exemple, en 2005, le Parlement a adopté une modification à la *Loi sur les télécommunications* autorisant le CRTC à imposer des sanctions administratives (voir annexe B pour lire les dispositions législatives). Il serait intéressant de mieux connaître les justifications sous-jacentes à ce changement législatif qui constitue un tournant, du moins dans la législation fédérale, sur le rôle punitif que des organismes décentralisés, tels un organisme de régulation économique comme le CRTC, peuvent jouer dans le processus de surveillance des lois publiques. En effet, l'attribution de pouvoirs de nature pénale à des organismes décentralisés est une idée relativement récente en droit administratif fédéral, mais qui ne semble pas encore imprégner le droit fédéral à grande échelle. Aussi, des recherches plus poussées devraient être faites sur cette question pour mieux comprendre l'émergence de ce

208 *Charte des droits et libertés de la personne*, L.R.Q., chap. C-12, art. 49.

phénomène²⁰⁹. Pour l'heure, de justifications juridiques pourraient être offertes pour soutenir l'attribution de ce type de pouvoirs et fondées sur l'émergence d'autres valeurs et systèmes normatifs.

2.3 Sur le plan juridique : L'émergence d'autres valeurs et systèmes normatifs

Depuis l'adoption de la LPRPDE, les développements des nouvelles technologies de l'information ont révolutionné et continuent de révolutionner l'accès aux connaissances. Leurs utilisations possibles ne cessent de croître, ce qui soulève la question des limites, notamment légales et éthiques, qui devraient être posées à leur application.

Toutes ces transformations changent profondément notre conception du monde et la question fondamentale qui se pose est de savoir s'il existe toujours une adéquation entre les modèles antérieurs de vie bonne avec ces nouvelles réalités. Plusieurs estiment que ces transformations exigent que l'État canadien intervienne pour offrir plus de protection; d'autres sont d'opinion contraire²¹⁰.

Dans cette section, nous examinons les changements qui sont en train de s'opérer dans la sphère juridique et résultants, du moins en partie, de ces avancées technologiques et affectant l'effectivité du droit à la protection des renseignements personnels. Ces changements sont intéressants puisqu'ils rendent possibles des modifications importantes au design des systèmes normatifs en place, notamment dans le but d'offrir des protections accrues aux citoyens à l'égard de leurs renseignements personnels.

Dans un premier temps, nous nous penchons d'abord sur l'évolution d'idées en droit constitutionnel canadien qui, si elles étaient pleinement mise en œuvre, changeraient profondément la conception du design législatif relatif à la protection des renseignements personnels. Dans un deuxième temps, nous nous penchons sur l'émergence de nouveaux systèmes normatifs supranationaux (appelés droit administratif global) relatifs à la protection de ces renseignements personnels. Ces systèmes normatifs sont apparus en raison des problèmes que posent l'utilisation des nouvelles technologies d'information et dans le but d'offrir une protection plus efficace à l'encontre des usages abusifs des renseignements personnels. En effet, le constat ayant été fait qu'il était difficile d'offrir un degré de protection adéquat en agissant juridiquement exclusivement sur le plan national. La construction de ce droit administratif global a rendu

209 Anne-Marie Boisvert, Hélène Dumont et Alexandre Stylios, « En marge de l'affaire Norbourg : les enjeux substantifs et punitifs suscités par le double aspect, réglementaire et criminel, de certains comportements frauduleux dans le domaine des valeurs mobilières », disponible en ligne sur le site Papyrus de l'Université de Montréal à l'adresse suivante : <http://hdl.handle.net/1866/2913>. Il s'agit d'une prépublication. Le texte final sera publié dans : « **Dérives et évolutions du droit pénal** », *Les Cahiers de droit* – numéro spécial à paraître en 2010.

210 Gautrais et Trudel, *supra* note 136.

possible l'émergence d'un vaste réseau de normes et d'institutions connectées entre elles par l'objet « protection des renseignements personnels²¹¹».

2.3.1 L'évolution du droit constitutionnel

Le droit constitutionnel canadien est en pleine mutation, tant sur le plan organisationnel, que celui des droits reconnus aux individus que du partage des compétences. Nous avons discuté plus haut des changements sur le plan de l'organisation par la création d'un système national d'intégrité (on pourrait aussi souligner les mutations dans le paysage judiciaire par le questionnement fondamental sur les garanties d'indépendance qui devraient être reconnues aux juges administratifs, etc.). Dans cette section, nous nous penchons plus particulièrement sur les mutations du droit constitutionnel eu égard aux droits fondamentaux des personnes et eu égard au partage des compétences législatives.

Sur le premier point, la discussion sera orientée vers la question du statut hiérarchique du droit à la protection des renseignements personnels. La question est la suivante : si le droit à la protection des renseignements personnels possède un statut plus élevé qu'un simple droit civil, est-ce que ce statut pourrait servir à donner un ancrage constitutionnel plus solide aux interventions du gouvernement fédéral dans ce domaine et, par conséquent, à la LPRPDE? Comme chacun le sait, les deux paliers de gouvernements ont l'obligation de protéger un droit fondamental, ce qui a forcément des effets sur l'étendue d'une compétence législative existante, même si, par ailleurs, cela ne peut pas avoir pour effet de le modifier²¹². En effet, bien souvent, les compétences législatives à l'égard d'un droit fondamental ne peuvent pas être exclusives à un palier de gouvernement, sans quoi les protections risquent d'être totalement ou partiellement ineffectives. C'est donc dans ce contexte que le fondement du droit à la protection des renseignements personnels revêt une importance particulière.

Par ailleurs, cette discussion serait vaine si une autre mutation du droit constitutionnel n'était pas signalée. En effet, il faut souligner le passage d'une interprétation formelle à une interprétation fonctionnelle du partage des compétences. Bien que cette nouvelle théorie interprétative n'ait pas été

211 Key Centre for Ethics, Law, Justice and Governance, Griffith University et Transparency International Australia, *Chaos or Coherence? Strengths, Opportunities and Challenges for Australia's Integrity Systems: National Integrity Systems Assessment (NISA) Final Report*, 2005, accessible en ligne à l'adresse suivante : <http://www.griffith.edu.au/arts-languages-criminology/key-centre-ethics-law-justice-governance/research/integrity-anti-corruption/projects/?a=37155> (dernière visite : 20 janvier 2010).

212 En principe, la *Charte* n'a pas d'incidence sur le partage des compétences, mais ce présupposé est douteux. Néanmoins, la Cour suprême soutient que l'adoption de la *Charte* canadienne n'a pas eu pour effet de modifier le fédéralisme et les règles du partage des compétences: *R. c. Turpin*, 1989, 1 R.C.S. 1296.

officiellement avalisée par la Cour suprême (à cet égard, il faudra surveiller le jugement de la Cour sur le renvoi relatif au projet de loi fédérale sur les valeurs mobilières), des théoriciens canadiens cherchent à la mettre en valeur, du moins dans certains domaines où le partage des compétences est flou (l'interaction entre les art. 91.2 (compétence fédérale sur les échanges et le commerce) et 92.13 (compétence provinciale sur la propriété et les droits civils) ou explicitement partagée (pouvoirs concurrents dans les domaines de l'immigration et de l'agriculture).

2.3.1.1 La protection des renseignements personnels : droit de nature quasiconstitutionnelle

Les droits de la personne se divisent en deux catégories : les droits fondamentaux et les droits civils (de nature sociale et économique). Les droits civils sont protégés par le droit privé et, à cet égard, il est clair et incontestable que la protection des renseignements personnels, à titre de composante du droit au respect à la vie privée est un droit civil protégé par le droit civil québécois²¹³ et par la *common law* des autres provinces canadiennes. Cependant, il semble bien que le statut de ce droit ait muté, possiblement durant les années 1990. De simple droit civil, il aurait acquis un statut plus élevé, c'est-à-dire le statut de droit fondamental de la personne.

Au Canada, les droits et libertés fondamentaux sont protégés par des textes de nature constitutionnelle et quasiconstitutionnelle. Sur les protections de nature constitutionnelles, il faut signaler d'entrée de jeu que la *Charte canadienne des droits et libertés* ne contient pas de disposition spécifique sur le droit à la vie privée de chaque individu. Toutefois, la Cour suprême avait reconnu, dès la fin des années 1990, que ce droit était inclus dans la section sur les garanties juridiques et plus précisément dans les articles 7 et 8 de la Charte²¹⁴. Cependant, on sait que ces articles sont d'application limitée²¹⁵. En revanche, le serait-il par des règles de nature quasiconstitutionnelle? Avant d'entrer dans ce débat, il faut souligner d'emblée que l'utilisation de l'expression lois à caractère quasiconstitutionnel signifie qu'il s'agit de lois étroitement liées aux valeurs et aux droits prévus par la Constitution. Toutefois, le statut de loi

213 *Code civil du Québec*, Titre deuxième, Chapitre troisième : Du respect de la réputation et de la vie privée, aux articles 35 à 41.

214 Art. 7 de la *Charte* : *R. c. O'Connor*, 1995, 4 R.C.S. 411, *Cheskes c. Ontario*, 2007, CanLII 38387 (ON S.C.); art. 8 : *Hunter c. Southam*, 1984, 2 R.C.S. 145.

215 *Dagg c. Canada (ministre des Finances)*, 1997, 2 R.C.S. 403, paragr. 65-66. En vertu de l'article 7, une loi peut porter atteinte au droit à la vie, la liberté ou la sécurité de la personne dans la mesure où cette atteinte est conforme aux principes de justice fondamentale. Quant à l'article 8, il permet au législateur de faire des lois relatives aux fouilles et aux perquisitions, mais dans la mesure où celles-ci ne sont pas abusives. Or, une loi relative à la protection des renseignements personnels n'interpelle ni l'application de l'article 7 ni celle de l'article 8. Qui plus est, les protections garanties par la *Charte canadienne des droits et libertés* ne s'appliquent pas au secteur privé. En conséquence, le droit au respect de la vie privée des personnes par les entreprises privées ne peut pas être fondé sur la *Charte canadienne*.

quasiconstitutionnelle n'a pas pour effet de modifier l'approche traditionnelle d'interprétation des lois. Il n'est qu'un indicateur à considérer dans leur interprétation, mais n'est pas déterminant en soi. Cette précision étant apportée, il faut souligner que le droit fédéral a évolué en faveur d'une reconnaissance du caractère quasiconstitutionnel en faveur des lois ayant pour objet de protéger les renseignements personnels.

Tout d'abord, la *Loi canadienne sur les droits de la personne* a été reconnue comme ayant un statut quasiconstitutionnel²¹⁶. Bien qu'elle n'ait jamais comporté de disposition relative au respect de la vie privée, la partie IV de la *Loi canadienne sur les droits de la personne* contenait des garanties légales relatives à la confidentialité des renseignements personnels. Cette partie a été abrogée en 1983²¹⁷ et elle a été remplacée par la *Loi sur la protection des renseignements personnels*²¹⁸. C'est en raison de cette histoire législative de la *Loi sur la protection des renseignements personnels* que le juge Noël de la Cour fédérale a décidé dans *Canada (commissaire à la protection de la vie privée) c. Canada (Conseil des relations du travail)* que cette loi revêtait également, de par ses origines, un caractère quasiconstitutionnel²¹⁹.

En somme, la *Loi sur la protection des renseignements personnels* est reconnue comme étant une loi fondamentale du système juridique canadien. Elle fait partie de cette catégorie privilégiée de lois qui « expriment “certains objectifs fondamentaux de notre société” et qui doivent être interprétées “de manière à promouvoir les considérations de politique générale qui (les) sous-tendent”²²⁰ ». Elle rappelle à quel point la protection de la vie privée est nécessaire au maintien d'une société libre et démocratique²²¹ comme le souligne le juge La Forest : « le statut privilégié et fondamental du droit à la vie privée dans notre culture sociale et juridique » (paragr. 69). Ainsi, si la *Loi sur la protection des renseignements personnels* possède ce statut, peut-on aussi qualifier la LPRPDE de loi à caractère quasiconstitutionnel ? Puisque les objets de ces deux lois sont semblables, la conclusion contraire pourrait paraître insolite même si, par ailleurs, leur portée ou leurs effets diffèrent. C'est d'ailleurs l'interprétation qui a été retenue par la Cour fédérale dans l'affaire *Eastmond* dans laquelle le juge écrivait : « Je n'hésite pas à classer la LPRPDE parmi les lois fondamentales du Canada, tout comme la Cour suprême du Canada a jugé

216 *Loi canadienne sur les droits de la personne*, S.C. 1976-1977, chap. 33.

217 L.C. 1980-1981-1982-1983, chap. 111 (ann. IV, art. 3).

218 L.C. 1980-1981-1982-1983, chap. 111, ann. II.

219 [1996] 3 C.F. 609, 652.

220 *Lavigne c. Canada (Commissariat aux langues officielles)*, 2002, 2 R.C.S. 773, paragr. 24. Voir aussi : *Canada (Procureur général) c. Viola*, 1991, 1 C.F. 373, 386 (Cour d'appel fédérale); *Rogers c. Canada (Service correctionnel)*, 2001, 2 C.F. 586, 602-603 (Cour fédérale).

221 *Dagg c. Canada (ministre des Finances)*, *supra*, note 215; *R. c. Dymont*, 1988, 2 R.C.S. 417, 427; voir aussi Joel Feinberg, « Autonomy, Sovereignty, and Privacy: Moral Ideals in the Constitution? », 1982, 58 *Notre Dame L. Rev.* 445.

que la *Loi sur la protection des renseignements personnels* bénéficiait d'un statut quasi constitutionnel [...]»²²².

Cette interprétation du juge s'insère de manière cohérente dans l'évolution du droit interne canadien, mais elle pose aussi la question du partage des compétences législatives dans ce domaine. En effet, pour offrir des protections efficaces aux citoyens d'un bout à l'autre du pays, il faut des interventions concertées par tous les ordres de gouvernements (fédéral, provincial et municipal) de façon à mettre à contribution leurs forces (par ex : les ressources financières du gouvernement fédéral, la compréhension des provinces des spécificités régionales et la proximité des municipalités avec les entreprises et les citoyens). La gouvernance publique sur un mode vertical ou en silo offre des perspectives trop limitées pour résoudre des problèmes tels ceux relatifs à la protection des renseignements personnels. D'ailleurs ce constat a été fait, du moins en partie, puisque la LPRPDE –comme nous l'avons expliqué plus haut– ne constitue pas un modèle législatif reflétant une interprétation strictement formelle du partage des compétences, mais un modèle hybride empreint de formalisme et de fonctionnalisme.

La question qui se pose aujourd'hui est de savoir si le modèle hybride de la LPRPDE est adapté aux réalités nouvelles et peut, par conséquent, offrir les protections jugées nécessaires pour faire face aux avancées technologiques et leurs multiples utilisations. Ce changement de paradigme, que nous postulons pour les fins de l'analyse, dont on mesure mieux les effets aujourd'hui (notamment sur nos modes de vie ainsi que sur nos valeurs et croyances), sert de toile de fond dans le développement qui suit afin de mieux comprendre l'évolution du fédéralisme canadien. En effet, celui-ci se dirigerait déjà, du moins par le modèle hybride retenu dans le domaine de la protection des renseignements personnels, vers une interprétation fonctionnelle plus poussée du partage des compétences législatives.

2.3.1.2 L'interprétation fonctionnelle du partage des compétences législatives

Portrait de son époque, par les tensions politiques et la réalité économique qu'il reflète, l'*Acte d'Amérique du Nord britannique* en 1867 a engendré une longue tradition d'interprétation du partage des compétences provinciales et fédérales sur un axe vertical. Dans un souci de respect « de l'esprit du fédéralisme », on classa les compétences en ménageant l'un et l'autre des gouvernements, évitant autant que faire se peut les chevauchements ou le flou juridique sur une matière législative. Cependant, la question se pose : est-ce que cette approche du fédéralisme, à la fois méthode interprétative et projet politique, permet de résoudre des problèmes aussi complexes que ceux portant sur la protection des renseignements personnels et le flux transfrontière des données?

222 *Eastmond c. Canadien Pacifique Ltée et commissaire à la protection de la vie privée du Canada*, 2004, C.F. 852, paragr. 100.

Selon certains auteurs, cette approche formaliste-dominante du constitutionnalisme canadien répond mal à la nouvelle économie du savoir. Le Canada, afin de mieux performer à l'échelle internationale, devrait se diriger vers une approche interprétative militant pour de plus grands chevauchements entre ses ordres de gouvernements. Ces chevauchements seraient l'occasion de mettre en place un « fédéralisme en réseau » (*networked federalism*) plus en lien avec les schémas organisationnels contemporains. Non pas source d'inefficacité ou de tensions, les réseaux bien développés seraient plutôt des lieux propices à l'innovation et à la coopération entre tous les paliers de gouvernements : fédéral, provinciaux et municipaux. C'est pour mettre à profit l'apport des municipalités que cette approche interprétative a été tout particulièrement développée.

La conjugaison de la globalisation et de la révolution de l'information, nous dit Thomas J. Courchene²²³, a entraîné la mise en place d'une économie basée sur le savoir (*knowledge-based economy*). Créativité, pragmatisme, accessibilité de l'information et souplesse des organisations constituent les mots d'ordre de ce nouvel ordre global. Fondée sur les services plutôt que sur l'exploitation des ressources naturelles, l'économie du savoir (ou postindustrielle) s'organise autour de ville-régions globales (*global city-region*) jouant le rôle des moteurs économiques de leur environnement. En effet, le cœur de l'économie se trouve dans ces grandes villes puisqu'elles sont les seules à offrir une densité suffisante de ressources humaines, principale ressource du secteur tertiaire. Se faisant compétition à l'échelle mondiale pour attirer les meilleurs éléments de cette « classe créative », leur pouvoir d'attraction devient le principal avantage comparatif d'une nation aux yeux des investisseurs et des entreprises transnationales. Au Canada, nos grandes villes ne possèdent aucun statut constitutionnel et souffrent d'un manque chronique de moyens financiers. De plus, leur statut de « créatures des provinces » limite les interventions du fédéral à leur endroit. Ces facteurs réduisent d'autant leur capacité à tirer leur épingle du jeu face aux autres grandes métropoles, particulièrement face à leurs principales concurrentes américaines ou européennes. Ce design constitutionnel, conjugué à une forte culture « territoriale » des différents paliers gouvernementaux au Canada, constituerait donc une menace à notre prospérité selon Courchene et Stein.

L'importance stratégique des villes dans une économie tertiaire illustre bien l'importance d'une plus grande coopération entre les différents paliers de gouvernements. Le fédéralisme canadien, nous dit Stein, a besoin « d'être moins défini, pas plus ; moins concerné par les droits de juridiction, pas plus ; et plus axé sur les résultats, sur ce qu'on doit accomplir, et comment y arriver. »²²⁴

223 Thomas J. COURCHENE, « Global Future for Canada's Global Cities », dans *Transitions : fiscal and Political Federalism in an Era of Change*, Kingston, McGill-Queen's University Press, 2009, p. 263

224 Janice Gross STEIN, « Networked Federalism », dans *Transitions : fiscal and Political Federalism in an Era of Change*, Kingston, McGill-Queen's University Press, 2009, p. 347

Plus précisément, cette absence des municipalités aux tables les plus importantes serait contraire au phénomène de la « glocalisation ». La glocalisation consiste en un double mouvement. Dans un premier temps, la démocratisation des technologies de l'information ont rendus les citoyens plus conscients de l'environnement qui les entourent et désireux d'y participer. Le principal point d'entrée politique devient alors le niveau local, d'autant plus que les villes deviennent, nous l'avons dit, de véritables cité-État au sein du nouvel ordre mondial. Dans un deuxième temps, la rapidité avec laquelle fonctionne une économie du savoir, et l'absence de distance sur laquelle elle se fonde, contribue à la fixation de standards internationaux et nationaux. Alors que certains pouvoirs se déplaçaient vers le bas dans le premier mouvement, d'autres pouvoirs se déplacent maintenant vers le haut. Dans le contexte canadien, ce phénomène est très clairement visible dans les domaines des valeurs mobilières et de la protection de la vie privée (deux débats découlant d'ailleurs de l'interprétation des mêmes articles de la constitution).

Ce double mouvement démontre bien, selon les partisans d'une approche constitutionnelle plus fonctionnelle, l'inévitable interdépendance entre les différents paliers de gouvernements. Ils seraient donc futiles, voir contre-productif, de tenter de désenchevêtrer les compétences de tous et chacun. Au contraire, la rapidité avec laquelle fonctionne cette nouvelle dynamique appelle les autorités à développer des mécanismes plus efficaces, aussi rapides que cette dernière. Le fédéralisme en réseau serait, selon ses partisans, le modèle organisationnel le plus apte à répondre à ces défis.

A. Le fédéralisme en réseau

Qu'est-ce que le fédéralisme en réseau ? Comment peut-il mieux répondre à la nouvelle réalité économique ? Un réseau se distingue d'un système hiérarchique en ce qu'il n'est pas en forme pyramidale, mais plutôt composé de liens et de points correspondants à des contacts entretenus par des acteurs de différentes organisations travaillant dans le même domaine. Particulièrement efficace pour transmettre une grande quantité d'informations, un réseau permet aux acteurs de communiquer leurs renseignements, idées, etc. sans blocages. En effet, l'absence de réponse par un des points du réseau n'empêche pas l'information de continuer à circuler, contrairement à un système hiérarchisé où la transmission est en « écluses ». Un réseau propose donc plusieurs points d'entrée et un foisonnement de contributions.

Une organisation en réseau est fortement décentralisée et ne se préoccupe pas d'avoir le monopole sur son champ de compétence et de pratique. Au contraire, un réseau entretient une culture de coopération et de circulation de l'information afin de multiplier les points d'entrées ouverts aux usagers du réseau (citoyens, entreprises ou membres du réseau). Cette multiplication des points d'entrée permet d'accéder quasi-instantanément à l'information recherchée. La rapidité d'accès à une information harmonisée constitue le principal avantage d'un réseau pour ses utilisateurs ; par le fait même, un avantage comparatif pour l'État l'adoptant.

L'organisation en réseau semble déjà avoir fait ses preuves dans le secteur privé et parapublic où les acteurs sont davantage contraints de s'adapter à leur environnement. Elle est en outre, selon Ronfeldt dans son historiographie des organisations, la forme la plus évoluée de schéma organisationnel²²⁵. Les Canadiens auraient, en somme, tout à gagner à s'imprégner de ce modèle fortement adapté à l'environnement contemporain. Concrètement, le fédéralisme en réseau canadien se traduirait, par exemple, par l'ouverture de secrétariats dans les différentes agences gouvernementales et les différents ministères. Désirables dans les domaines où il existe de l'enchevêtrement²²⁶, ces secrétariats seraient des points de partage d'informations ainsi que de coordination dans l'élaboration des législations et leur application. Les universitaires et les experts du secteur privé ou parapublic seraient aussi intégrés à ce réseau, toujours dans un but de multiplier les contributions à la résolution de problèmes de plus en plus complexes.

Enfin, les nombreux débats entourant l'interprétation des articles 91.2 et 92.13 de la constitution devraient être abordés d'une manière complètement différente. Une approche « en silo » de ces compétences (valeurs mobilières, protection de la vie privée, etc.) céderait sa place à une approche moins linéaire, fonctionnant « sur plusieurs axes ». Plutôt que d'investir des sommes considérables d'énergie dans des débats juridiques, les gouvernements, incluant les gouvernements municipaux, aborderaient ces débats dans un esprit de coopération.

B. Une posture interprétative ne nécessitant pas d'amendements constitutionnels

La mise en place d'un fédéralisme en réseau ne passe pas par des amendements constitutionnels ou des changements institutionnels importants. Au contraire, les débats entourant les articles 91.2 et 92.13 démontrent la présence du flou constitutionnel nécessaire à la mise en place de réseaux dans certains domaines stratégiques. Ainsi, ironiquement, l'une des pommes de discorde constitutionnelles de plusieurs générations nous apparaît aujourd'hui comme une porte d'entrée prédestinée. Il faut, selon les partisans du fédéralisme en réseau, embrasser ce '*legal messiness*' et en tirer profit. La mise en place d'un fédéralisme en réseau est donc plus affaire d'organisation administrative que d'amendements constitutionnels. Il s'agit en fait d'une posture interprétative modelant graduellement nos pratiques.

Bien que cette approche soit parfois déjà observable (constatons, par exemple, la coopération entre la Commissaire canadienne à la protection de la vie privée et son homologue de la Colombie-Britannique), certains obstacles semblent s'opposer à sa généralisation. Ces obstacles sont avant tout culturels, selon les

225 D.F. RONFELDT, *Tribes, Institutions, Markets, Networks : A Framework about Societal Evolution*. 1996, Santa Monica, CA : Rand.

226 Certaines compétences clairement définies, tel que la défense nationale, ne sont pas propices à la mise en place d'un fédéralisme en réseau. Voir STEIN, *supra* note 224, 360.

auteurs, et concernent, d'une part, les fonctionnaires et, d'autre part, les élites politiques.

D'une part, Stein déplore la méfiance que se portent les fonctionnaires des différents paliers de gouvernements, rappelant que les réseaux les plus performants sont ceux fondés sur une bonne cohésion sociale. Les liens de confiance et d'amitiés entre les fonctionnaires, les experts et les universitaires seraient essentiels à une plus grande coopération entre nos institutions. Or, depuis les coupes fédérales des années 1990, nous dit Stein, et probablement depuis plus longtemps dans le cas du Québec, les fonctionnaires provinciaux se montrent très méfiants à l'égard de leurs homologues fédéraux²²⁷. Cette méfiance constitue un frein au partage des informations, des valeurs et des objectifs communs essentiels à la mise en place d'un fédéralisme en réseau.

D'autre part, Stein croit que la vision des relations intergouvernementales de notre élite politique constitue le plus grand obstacle à une approche fonctionnelle de la constitution²²⁸. En effet, la politique canadienne reposerait depuis trop longtemps sur une logique d'affrontement entre les gouvernements, les principales conversations canadiennes s'articulant autour de questions de compétences. Nos leaders devront, nous dit Stein, se distancer de cette culture de territorialité et de contrôle et s'approprier un discours de résolution de problèmes et d'innovation²²⁹. Ce lâcher-prise constitue le plus grand défi de nos élites politiques au XXI^e siècle et serait essentiel au maintien de notre compétitivité. Nos élites doivent apprendre à naviguer dans un système fédératif moins défini et moins linéaire et plus focalisé sur la recherche de solutions.

En somme, le fédéralisme en réseau constituerait l'approche constitutionnelle la mieux adaptée au XXI^e siècle selon ses partisans. Selon Stein, « a global economy rewards those who move sideways as well as up and down along the grid, with a large tolerance for fluid structures that give a quick response »²³⁰. Cette façon d'aborder l'interprétation du partage des compétences pourrait permettre de répondre plus rapidement aux problèmes contemporains mais aussi aux crises mondiales qui se succèdent. L'une de ces crises a été celle qui a été déclenchée par les événements du 11 septembre 2001. La menace terroriste pesant sur l'Occident depuis cette date a entraîné dans son sillage la refonte de plusieurs législations d'ici et d'ailleurs portant sur la sécurité nationale. Les États-Unis ont été particulièrement actifs sur ce front par le renforcement de leurs systèmes juridiques dans le domaine de la sécurité nationale. La *US Patriot*

227 Voir STEIN, *supra* note 224, 364.

228 *Id.*, 365.

229 *Id.*, 365.

230 *Id.*, 348.

Act est un bon exemple à cet égard²³¹ puisque cette loi a engendré des points de tension très forts entre les besoins de sécurité des États-Unis et les besoins de protection des renseignements personnels des citoyens et, en particulier, de nos entreprises et citoyens canadiens. Cet exemple illustre bien la complexité des problèmes (juridiques, mais aussi politiques et diplomatiques) contemporains dans ce domaine d'intervention étatique et l'utilité d'ouvrir la réflexion sur le fédéralisme en réseau.

2.3.1.3 Sécurité nationale et protection des renseignements personnels : points de tensions

La *US Patriot Act* a été adoptée à la suite des événements de septembre 2001 afin de donner davantage de pouvoir d'enquête aux agences gouvernementales chargées de la lutte contre le terrorisme. Cette législation modifie le *Foreign Intelligence Surveillance Act (FISA)* et permet, entre autres, au FBI d'obtenir plus facilement des données personnelles détenues par une entreprise américaine. Bien qu'il fut possible pour le gouvernement américain d'obtenir des renseignements personnels sur les citoyens canadiens avant 2001, la *US Patriot Act* a assoupli la procédure pour obtenir un mandat et a élargi la définition de terrorisme (l'étendant, entre autres, au terrorisme domestique).

Cette nouvelle conceptualisation de la lutte au terrorisme s'est traduite, de manière générale, par un abaissement des critères d'enquête. En effet, les garanties procédurales criminelles ont cédé leur place, à travers les différentes législations, à une nouvelle catégorie de garanties procédurales, plus souples, créée spécifiquement pour servir la lutte anti-terrorisme, créant ainsi des ouvertures plus grandes pour le transfert des données personnelles. Ces mouvements transfrontières de données personnelles constituent un bon exemple des limites de la LPRPDE face aux législations en matière de sécurité nationale. Dans un premier temps, nous examinerons quelques problèmes juridiques entre les applications de la *US Patriot Act* et de la LPRPDE.

Par ailleurs, ce début de XXI^e siècle fut, comme nous l'avons déjà mentionné, marqué par l'explosion des échanges en ligne et, surtout, par l'accumulation par le secteur privé d'une importante quantité de renseignements personnels sur leur clientèle. De vastes banques de données ont ainsi été créées, capables de reconstituer les habitudes quotidiennes d'un citoyen (notamment les citoyens canadiens) en un seul clic. La *US Patriot Act*, à titre d'innovations légales post-11 septembre, conjugué à ce nouveau modèle économique fondé sur l'accumulation de renseignements personnels, ont facilité l'émergence d'une surveillance accrue des agences gouvernementales dont les actions soulèvent

231 *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001*, Pub. L. No. 107-56, 272, Stat. 218, en ligne : <http://www.govtrack.us/congress/billtext.xpd?bill=h107-3162&version=enr> (consulté le 13 juillet 2010), ci-après nommé la «*US Patriot Act*».

des problèmes éthiques. Ces problèmes éthiques feront l'objet d'un deuxième développement

A. Quelques problèmes juridiques entre les applications de la *US Patriot Act* et la *LPRPDE*

Les mécanismes mis en place par la *LPRPDE* afin d'encadrer le transfert de données sensibles à des tiers parties semblent inefficaces au regard de l'application de dispositions législatives contenues dans la *US Patriot Act*. À titre d'exemple, le FBI peut, par un simple ordre secret de la *FISA Court*, contraindre une compagnie américaine à lui céder des informations à caractère personnel. Ce mandat est plus facile à obtenir qu'auparavant, la *US Patriot Act* ayant abaissé les critères pour son obtention²³², ce qui a eu pour effet de neutraliser l'application du concept interdisant « d'aller à la pêche » en matière de fouille et de saisie.

En conséquence, le gouvernement américain peut obtenir des renseignements personnels de citoyens canadiens par l'entremise d'une compagnie américaine ayant une filiale au Canada ou d'une compagnie canadienne transférant ses renseignements personnels à une organisation américaine tiers. Bien qu'il ne s'agisse pas d'une nouvelle réalité –le *FISA* datant de 1978– la *US Patriot Act* a étendu la portée des pouvoirs des agences américaines et facilité leur utilisation. Le secret entourant maintenant la divulgation de données aux autorités américaines vient en outre compliquer l'application de la *LPRPDE*.

Les entreprises visées par une ordonnance secrète obtenue grâce à la *US Patriot Act* sont légalement tenues au secret²³³. De plus, ces ordonnances peuvent avoir des effets extraterritoriaux. Ainsi, une entreprise américaine recevant un tel ordre de la *FISA Court* pourrait remettre au FBI des renseignements contenus dans une banque de données hébergée par sa filiale canadienne à laquelle elle a accès sans en informer cette dernière. En effet, afin de se conformer à la loi américaine, l'entreprise n'avertirait pas sa partenaire canadienne ni, bien entendue, le citoyen canadien dont elle divulgue les renseignements personnels. Ce type d'intrusion dans la vie privée des Canadiens est qualifié par Heather Black, commissaire-adjointe à la protection de la vie privée, de menace à notre souveraineté nationale et de violation de la *LPRPDE*²³⁴. Il est cependant difficile de sanctionner ces contraventions à la loi puisque ces initiatives secrètes passent entre les mailles d'un système fondé sur les plaintes des consommateurs. Le secret entourant les actions gouvernementales en matière de sécurité nationale constitue donc un obstacle à l'application de la *LPRPDE*.

232 *Id.*, le texte du *FISA* se lit maintenant : « [...] that a *significant purpose of the surveillance is to obtain foreing information* [...] » alors que l'ancien texte avait comme critère « *the purpose* ».

233 *Id.*, art. 215.

234 H. BLACK, *11th Annual Meeting on Regulatory Compliance for Financial Institutions*, 2005, en ligne : http://www.priv.gc.ca/speech/2005/sp-d_051118_hb_e.cfm (consulté le 12 juillet 2010)

La LPRPDE semble aussi souffrir d'un déficit d'efficacité face aux législations de sécurité nationale dans les situations où des données sont transférées volontairement à l'étranger. En effet, le mécanisme mis en place pour assurer la protection des données transférées sur un autre territoire, soit un système de clauses contractuelles faisant reposer la responsabilité sur l'entreprise canadienne, ne semble pas efficace ici.

Le Principe 1 de la loi canadienne relatif à la reddition de compte prévoit qu'une compagnie canadienne demeure responsable de la sécurité des renseignements personnels qu'elle transfère à des tiers, particulièrement lorsqu'ils sont situés sur un autre territoire. La LPRPDE ne pouvant être appliquée à l'étranger, cette obligation constitue la pierre angulaire du régime canadien d'encadrement des transferts internationaux de données. Or, afin de répondre à cette obligation, les entreprises canadiennes lient leurs partenaires étrangers à des clauses contractuelles garantissant certains mécanismes de protection des données. Bien que ces clauses puissent être efficaces à l'intérieur du secteur privé, elles ne peuvent empêcher les autorités compétentes d'ordonner à l'entreprise américaine la divulgation des renseignements personnels. En effet, l'entreprise américaine est tenue de respecter la *US Patriot Act*.

Les effets de la LPRPDE s'arrêtent donc aux frontières canadiennes. Une fois les données de citoyens canadiens transférées aux États-Unis, l'État canadien ne peut leur offrir aucune protection, si ce n'est ce système de stipulations contractuelles sanctionnant les entreprises qui sont assujetties à sa compétence. Or, une stipulation contractuelle ne peut empêcher une ordonnance de divulgation habilitée par une législation visant la sécurité nationale.

Cependant, comme le rappelle la commissaire-adjointe à la protection de la vie privée, une entreprise située en sol canadien se doit de respecter d'abord et avant tout la législation canadienne²³⁵. Il existe donc certaines obligations fixées par la LPRPDE susceptibles de mieux protéger la vie privée des Canadiens face à des autorités étrangères aux pratiques envahissantes.

En effet, dans le cas du premier scénario, le secret entourant les démarches des autorités américaines ne devraient pas empêcher le respect de la loi canadienne. Le Principe 7 de la LPRPDE prévoit que les entreprises canadiennes doivent mettre en place des mécanismes de sécurité appropriés et proportionnels au degré de sensibilité des informations détenues. Ces mécanismes technologiques, organisationnels ou physiques doivent protéger les informations d'accès non-autorisés. Il va s'en dire qu'une filiale étrangère tentant d'accéder secrètement à une banque de données d'origine canadienne et située sur le sol canadien afin de divulguer des informations aux autorités la régissant entre dans cette catégorie. À cet égard, l'arrêt *BC Government and Services Employees' Union c. British*

235 *Id.*

*Columbia (Minister of Health Services)*²³⁶ suggère quatre mesures pour mieux prévenir ce genre d'intrusion étrangère. Premièrement, une entreprise devrait restreindre et contrôler les accès électroniques à ses employés. Deuxièmement, les obligations de confidentialité devraient être assorties de clauses pénales substantielles. Troisièmement, les sonneurs d'alarme (*whistle blowers*) devraient être protégés. Enfin, les employés devraient recevoir une formation en ce qui a trait à leurs responsabilités légales.

Quant à l'inefficacité d'une clause contractuelle eu égard à une réquisition découlant d'une loi régissant la sécurité nationale, il est utile de référer à l'affaire CIBC pour éclairer le débat. En 2004, CIBC Visa a informé ses détenteurs de carte de crédit d'un changement dans sa politique d'utilisation. En faisant maintenant affaire avec un nouveau fournisseur de service établi aux États-Unis, l'entreprise avertissait ses clients que leurs informations pourraient être divulguées aux autorités américaines. Ce changement de politique suscitant plusieurs plaintes de consommateurs à la Commissaire canadienne à la protection de la vie privée, cette dernière a enquêté sur la conformité des pratiques de l'entreprise avec la LPRPDE. L'analyse du contrat a révélé que toutes les mesures appropriées avaient été prises par CIBC, la compagnie sous-traitante s'étant engagée par contrat à mettre des mécanismes de protection des données en place. Puisque de telles clauses n'empêcheraient pas une éventuelle divulgation des renseignements aux autorités compétentes, la Commissaire canadienne a jugé que CIBC avait agi correctement en avertissant ses clients de la possibilité d'un tel scénario. En effet, par cette mesure, l'entreprise s'est conformée au Principe 4.8 de la LPRPDE énonçant qu'une organisation doit informer ses clients sur les pratiques de gestion de leurs renseignements personnels²³⁷.

Enfin, la commissaire-adjointe rappelle que les entreprises devraient être plus proactives en ce qui attrait à leur connaissance des renseignements personnels transférés à l'étranger. En effet, la facilité avec laquelle les données sensibles voyagent aujourd'hui, plusieurs entreprises ignorent l'entière portée des mouvements de données qu'ils réalisent. Une meilleure connaissance de leurs pratiques permettrait pourtant à ces organisations de mettre en place des mécanismes corporatifs plus efficaces et plus en accord avec la LPRPDE²³⁸.

Mais au-delà des solutions à la pièce, cet exemple fait ressortir la complexité des problèmes contemporains liés à la protection des renseignements, ici examinés sous la lunette d'un équilibre entre ce droit et la question de la sécurité nationale. En prenant pour point de départ que le droit à la protection des renseignements personnels possède un statut de droit de

236 *B.C. Govt. Serv. Empl. Union v. British Columbia (Minister of Health Services)*, (2005) B.C.S.C. 446, en ligne : <http://www.canlii.org/en/bc/bcsc/doc/2005/2005bcsc446/2005bcsc446.html> (consulté le 15 juillet 2010)

237 BLACK, *supra* note 234, p. 6.

238 *Id.*, p. 7.

nature constitutionnelle, il faut souligner l'importance au Canada de régler cette tension «dans le respect des impératifs à la fois de la sécurité et d'une gouvernance constitutionnelle responsable»²³⁹. La mise en œuvre du fédéralisme en réseau pourrait, à cet égard, fournir des pistes intéressantes et innovantes, notamment en ce qui a trait au rôle d'éducation que pourrait jouer les divers paliers de gouvernement (incluant les gouvernements municipaux). Renforcer ce rôle gouvernemental pourrait également avoir des effets particulièrement bénéfiques lorsqu'on examine les problèmes éthiques, tels que ceux découlant de la lutte anti-terrorisme conjuguée à l'accumulation de renseignements personnels par le secteur privé.

B. Quelques problèmes éthiques découlant de la lutte anti-terrorisme conjuguée à l'accumulation de renseignements personnels par le secteur privé

Gunasekara identifie trois problèmes éthiques découlant de la nouvelle conceptualisation légale de la lutte anti-terrorisme conjuguée à l'accumulation de renseignements personnels par le secteur privé²⁴⁰. D'abord, l'auteur souligne que la tendance des gouvernements à faire du secteur privé leur «partenaire» dans l'application des lois entre en conflit avec le droit à la vie privée des citoyens. En effet, les citoyens transmettent leurs renseignements personnels au secteur privé dans l'objectif d'obtenir un service. Or, ces renseignements, d'abord transmis pour atteindre cet objectif, sont ensuite divulgués à des agences gouvernementales qui ont pour mandat d'assurer le maintien de l'ordre et du bon gouvernement. Ces pratiques de cooptation du secteur privé, élaborées et appliquées à l'insu des citoyens, constituent, selon la Commissaire à la vie privée, des violations des « pratiques équitables les plus fondamentales en matière de renseignements »²⁴¹.

Ce partenariat avec le secteur privé, capable de fournir aux agences gouvernementales une quantité substantielle de renseignements sur une personne, devient d'autant plus préoccupant en raison de l'apparition de nouvelles technologies intrusives. Parmi celles-ci, notons la technique de « forage de banques de données » (*data mining*). Cette technique consiste à appliquer sur des banques de données des modèles statistiques cherchant des

239 *Charkaoui c. Canada (Citoyenneté et Immigration)*, [2007] 1 R.C.S. 350, par. 1 : « L'une des responsabilités les plus fondamentales d'un gouvernement est d'assurer la sécurité de ses citoyens. Pour y parvenir, il peut arriver qu'il doive agir sur la foi de renseignements qu'il ne peut divulguer ou détenir des personnes qui constituent une menace pour la sécurité nationale. En revanche, dans une démocratie constitutionnelle, le gouvernement doit agir de manière responsable, en conformité avec la Constitution et les droits et libertés qu'elle garantit. Ces deux propositions illustrent une tension inhérente au système de gouvernance démocratique moderne. Cette tension ne peut être réglée que dans le respect des impératifs à la fois de la sécurité et d'une gouvernance constitutionnelle responsable.

240 G. GUNASEKARA, « The « Final » Privacy Frontier ? Regulating Trans-Border Data Flows », (2007) 17 *Inter. J. Law & d Information Technology* 147.

241 CANADA, COMMISSARIAT CANADIEN À LA PROTECTION DE LA VIE PRIVÉE. *Rapport annuel au Parlement 2003 2004*, 2004, p.29, en ligne : http://www.priv.gc.ca/information/ar/200304/200304_f.pdf (consulté le 14 juillet 2010).

corrélations entre différentes habitudes de consommation afin d'en tirer une liste de terroristes potentiels. Ainsi, grâce à des données détaillant l'utilisation quotidienne d'une carte de crédit, l'achats de billets d'avions ou la location de voitures, ces modèles statistiques « ajoutent » au profil du citoyen des renseignements relatifs à ses habitudes futures probables. Le plus important projet de forage de banques de données aura été le *Terrorism Information Awareness* (TIA) mis sur pied en 2002 par le Pentagone. Ce projet avait pour objectif de créer une immense banque de données à l'aide des informations rassemblées par le secteur privé. Cette banque aurait ensuite permis d'identifier des modèles associés à la planification d'attaques terroristes²⁴². Bien que ce programme n'existe plus, plusieurs agences américaines font encore des recherches de ce type, recherches qui seraient impossibles sans la cooptation du secteur privé.

Gunasekara soulève aussi la confusion croissante entre les standards législatifs applicables dans les matières criminelles et les standards développés dans le cadre de la lutte anti-terrorisme, moins contraignants. Au-delà des craintes de certains pénalistes de voir ces nouveaux standards s'étendre aux crimes « ordinaires »²⁴³, on peut s'inquiéter de voir les puissants outils conférés aux agences de sécurité servir à des enquêtes criminelles ordinaires. Ainsi, les renseignements personnels obtenus sans les garanties traditionnelles serviraient à des enquêtes portant sur des crimes n'étant pas directement reliés au terrorisme²⁴⁴.

Enfin, Gunasekara nous met en garde contre la récupération par le secteur privé de certains outils technologiques utilisés par les agences gouvernementales dans le cadre de la lutte anti-terrorisme²⁴⁵. Nous rappelant les origines de l'Internet, du GPS ou du four à micro-ondes, l'auteur souligne que l'innovation technologique militaire a souvent servi de laboratoire de recherche et de développement de l'économie de consommation. Ainsi, Gunasekara s'inquiète du jour où de puissants logiciels de forage de banques de données aboutiront entre les mains du secteur privé, tel celui des assurances, par exemple. Dans

242 GUNASEKARA, *supra* note 240, 158.

243 Par exemple, le concept de facilitation, type d'infraction préliminaire créé pour la lutte au terrorisme, s'est déjà étendu à la pédophilie en droit canadien. Voir au sujet de ce concept la relation entre les articles 83.19 (terrorisme) et 172.1 (agression sexuelle sur un mineur facilitée par une communication internet) du Code criminel.

244 Pour en savoir plus sur l'étendu de ces pouvoirs en matière de surveillance, de fouille et de perquisition et de leur implication sur la protection de la vie privée des citoyens, le lecteur peut consulter avec intérêt un rapport de 2009 de la Commissaire à la protection de la vie privée comparant les législations anti-terrorisme canadienne, britannique, française et américaine : CANADA, COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Surveillance, Search or Seizure Powers Extended by Recent Legislation in Canada, Britain, France and the United States*, 2009, en ligne : http://www.priv.gc.ca/parl/2009/parl_bg_090507_e.pdf (consulté le 13 juillet 2010).

245 GUNASEKARA, *supra* note 240, 163.

les faits, ces pratiques sont déjà courantes; quiconque possède un compte sur un réseau social tel que Facebook aura déjà remarqué comment les publicités sur ces pages s'adaptent particulièrement bien à ses besoins. Les promesses de ces outils du secteur public sont en somme de véritables chants de sirènes aux oreilles du secteur privé. L'application stricte des normes de protection de la vie privée à leur endroit doit donc constituer une priorité, conclut Gunasekara, afin d'éviter qu'ils ne deviennent un « Cheval de Troie que l'on admit dans la Cité au prix de notre liberté ».

* *
*

Pour résumer ces développements portant sur le droit constitutionnel, il importe de souligner l'importante activité intellectuelle déployée par les institutions universitaires, judiciaires et gouvernementales (notamment le Commissariat à la protection de la vie privée). Les résultats de cette activité intellectuelle sert de socle à l'innovation juridique ayant pour but de résoudre les problèmes contemporains liés aux nouvelles technologies de l'information qui ouvrent encore plus grandes les portes au transfert des données personnelles détenues par les entreprises entre elles, mais aussi entre les entreprises et les gouvernements. L'élévation du droit à la protection des renseignements au statut de norme quasiconstitutionnelle est salutaire lorsqu'il s'agit d'offrir de plus grandes protections aux citoyens et consommateurs. De même, l'évolution du fédéralisme vers une interprétation plus fonctionnelle de notre constitution pourrait permettre dans l'avenir de mettre en œuvre une forme de fédéralisme de réseau.

Bien sûr, ces changements juridiques sont encore à l'état embryonnaire et bien qu'à première vue ils apparaissent offrir des solutions séduisantes, celles-ci doivent néanmoins être soumises à une évaluation critique. En effet, il s'agit de mieux comprendre les conséquences à plus terme de ces orientations théoriques tant sur le fédéralisme canadien que sur les droits et les libertés des citoyens. Cependant, il faut noter un fort mouvement vers l'élaboration de systèmes normatifs aux visées protectrices. C'est ainsi qu'on peut observer, depuis quelques années, la construction d'un droit administration global relatif à la protection des renseignements personnels.

2.3.2 La construction d'un droit administratif global relatif à la protection des renseignements personnels

Le droit administratif global représente un nouveau champ du droit, qui fait l'objet d'une théorisation plus systématique depuis 2005²⁴⁶. C'est en partant de l'observation selon laquelle la gouvernance mondiale peut être comprise comme s'il s'agissait de réglementation et d'administration que les chercheurs ont constaté l'émergence d'un espace administratif global dans lequel la dichotomie

246 Voir le site de la Faculté de droit de l'Université de New York sur le Global Administrative Law : http://www.iilj.org/global_adlaw.

stricte entre le droit interne et international s'efface²⁴⁷. Ce champ est décrit par le vocable « global » plutôt qu'international afin de refléter l'imbrication des réglementations interne et internationale²⁴⁸.

Le droit administratif global comprend les mécanismes, principes et pratiques ainsi que les codes sociaux s'y rattachant et son étude inclut celle des institutions réglementaires intergouvernementales formelles, des réseaux réglementaires intergouvernementaux informels ainsi que les arrangements relatifs à la coordination des systèmes réglementaires, des institutions réglementaires nationales agissant par référence à un régime intergouvernemental international, etc.²⁴⁹

Dans cette partie, nous décrivons brièvement quelques réseaux normatifs relatifs à la protection des renseignements personnels qui se sont construits depuis les dix dernières années. Ces réseaux constituent des objets de recherche riches d'enseignements tant pour accroître la compréhension du droit administratif global que pour inspirer des réformes législatives.

Le premier système est composé de plusieurs réseaux de normes et illustre bien la création de mécanismes d'harmonisation et de coordination ayant des visées générales. Les objectifs du deuxième système sont similaires au premier, mais il a une vocation plus particulière. En effet, il s'agira, lors de ce deuxième développement, de décrire le réseau de normes émanant de l'Agence mondiale anti-dopage. Enfin, le troisième système, celui provenant de l'APEC et instituant un cadre législatif duquel ont découlé les projets Pathfinders ainsi que le Cross-Border Privacy Rules System et instituant un système original d'accréditation.

2.3.2.1 La création de mécanismes d'harmonisation et de coordination de portée générale

Bien qu'il n'existe pas encore de grande convention internationale portant sur le flux des données transfrontières et la protection des renseignements personnels, le réseau de normes supranationales s'appuie grandement sur les directives de l'OCDE. Ces directives demeurent le texte de base sur lequel il existe un consensus international sur la protection des données. Cette remarque importe puisque la question du flux des données transfrontières et la protection des renseignements personnels est encore largement conçue comme une question portant principalement sur l'échange et le commerce. À preuve, les accords de libre-échange qui incorporent des stipulations relatives à la protection

247 Nico KRISCH et Benedict KINGSBURY, « Introduction: Global Governance and Global Administrative Law in the International Legal Order » (2006) 17:1 E.J.I.L. 1-13, 1.

248 *Id.*, 5.

249 Benedict KINGSBURY, Nico KRISCH et Richard B. STEWART, « The Emergence of Global Administrative Law » (2005) 68:15 Law and Contemporary Problems 15, 17.

des renseignements personnels. À titre d'exemples canadiens, on peut citer ALENA²⁵⁰, et plus récemment, l'Accord de libre-échange entre le Canada et le Pérou²⁵¹ et celui entre le Canada et la Jordanie²⁵². Il faut aussi mentionner l'Accord entre le Canada et la Communauté européenne sur les dossiers des passagers²⁵³. Cet accord fait référence à la *Directive sur la protection des données*²⁵⁴. Par ailleurs, et ce qui est plus intéressant, c'est le développement d'une pluralité d'ententes de type « droit mou/soft law ». Ces ententes portent sur des travaux préparatoires réalisés en vue de négocier de futurs accords. Nous décrivons ici brièvement quelques initiatives : l'initiative espagnole, le cadre de l'APEC et le projet Galway sur la responsabilité. La fonction principale de ces initiatives est de favoriser une élaboration de principes harmonisateurs de protection des renseignements personnels entre les États. Enfin, l'initiative la plus récente, celle relative à la création d'un *Global Privacy Enforcement Network*, met plutôt l'accent sur l'exécution efficace des normes de protection.

250 *Accord de libre-échange nord-américain entre le gouvernement du Canada, le gouvernement des États-Unis mexicains et le gouvernement des États-Unis d'Amérique*, 17 décembre 1992, 1994, R.T. Can. n° 2, entré en vigueur le 1^{er} janvier 1994, accessible en ligne à l'adresse suivante : http://www.international.gc.ca/trade-agreements-accords-commerciaux/agr-acc/nafta-alena/texte/index.aspx?lang=fra&menu_id=50&menu=r (dernière visite : 20 mars 2010). L'article 2105 discute les renseignements personnels mais c'est encore une exception d'une obligation de divulgation plutôt qu'une garantie/protection pour les renseignements personnels.

251 *Accord de libre-échange entre le Canada et la République du Pérou*, 29 mai 2008, entré en vigueur le 1^{er} août 2009, à l'art. 1507, accessible en ligne à l'adresse suivante : <http://www.international.gc.ca/trade-agreements-accords-commerciaux/agr-acc/peru-perou/peru-toc-perou-tdm.aspx?lang=fra> (dernière visite : 20 mars 2010).

252 *Accord de libre-échange entre le Canada et le Royaume hachémite de Jordanie*, 28 juin 2009, art. 15.4, accessible en ligne à l'adresse suivante : <http://www.international.gc.ca/trade-agreements-accords-commerciaux/agr-acc/jordan-jordanie/agreement-toc-tdm-accord.aspx?lang=fra> (dernière visite : 20 mars 2010)

253 *Accord entre la Communauté européenne et le gouvernement du Canada sur le traitement des données relatives aux informations préalables sur les voyageurs et aux dossiers passagers*, 3 octobre 2005, *Journal officiel de l'Union européenne* L 82/15 21.3.2006, entré en vigueur le 22 mars 2006, accessible en ligne à l'adresse suivante : http://www.canadainternational.gc.ca/eu-ue/assets/pdfs/031005PNR_fra.pdf (dernière visite : 20 mars 2010). Au préambule : « Vu la décision pertinente de la Commission, prise en application de l'article 25, paragraphe 6, de la directive 95/46/CE (ci-après dénommée "la décision"), en vertu de laquelle l'autorité canadienne compétente concernée est considérée assurer un niveau de protection adéquat des données IPV/DP transférées depuis la Communauté européenne (ci-après dénommée "la Communauté") et concernant les vols de passagers à destination du Canada, conformément aux engagements concernés, annexés à la décision en question. »

254 *Directive relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données*, *supra*, note 67.

A. L'élaboration de principes harmonisateurs : l'initiative espagnole et le Projet Gallway

L'initiative espagnole est le fruit des Conférences internationales des commissaires à la protection des données et de la vie privée. Un des objectifs de ces conférences est que « la reconnaissance de ces droits passe par l'adoption d'un instrument juridique universel contraignant consacrant, recensant et complétant les principes communs de protection des données et de respect de la vie privée énoncés dans différents instruments existants et renforçant la coopération internationale entre autorités de protection des données²⁵⁵ ». Aussi, la Conférence des commissaires estimera son travail achevé lorsqu'une convention internationale protégeant les renseignements personnels aura vu le jour. Dans l'attente de cet événement, les commissaires développent des outils ayant pour but de favoriser le rapprochement entre les lois des pays relatives au flux des données transfrontières et desquels les commissaires de la conférence sont des ressortissants

La dernière conférence, qui s'est tenue en Espagne en 2009, était la trente-et-unième et elle a accouché d'une proposition intitulée *Joint proposal for setting international standards on privacy and personal data protection*²⁵⁶. Cette proposition contient des principes, droits et obligations de base et jugés nécessaires par les commissaires de la conférence pour assurer une protection effective des renseignements personnels. Ceux-ci sont : la légalité, l'équité, la spécification du but, la proportionnalité, la qualité des données, la transparence

255 *Résolution sur l'urgence de protéger la vie privée dans un monde sans frontière et l'élaboration d'une proposition conjointe d'établissement de normes internationales sur la vie privée et la protection des données personnelles*, document adopté à Strasbourg, 17 octobre 2008, voir sur le site : <http://www.edps.europa.eu/EDPSWEB/edps/lang/fr/Home/Cooperation/Intconference> (dernière visite : 20 janvier 2010).

256 Conférences internationales des commissaires à la protection des données et de la vie privée, Madrid, 5 novembre 2009. Voir le site : <http://www.edri.org/edri-gram/number7.2/international-standards-data-protection> (dernière visite : 20 janvier 2010).

et la responsabilité²⁵⁷. Certains de ces principes proviennent des lignes directrices de l'OCDE²⁵⁸, d'autres proviennent de la Directive européenne²⁵⁹.

Le projet Galway focalise ses efforts normatifs sur les façons d'améliorer et de clarifier les lois actuelles affectant les entreprises, et ce, dans le but de faciliter le commerce²⁶⁰. Les participants misent sur les pratiques des entreprises et, pour cette raison, ils misent sur la mise en œuvre du principe de la responsabilité des entreprises. À cet égard, les participants s'appuient sur le principe de la responsabilité énoncé dans les Lignes directrices de l'OCDE, tout en développant de manière à rendre possible l'harmonisation des pratiques avec les normes édictées dans les lois diverses²⁶¹. La différence entre le projet Galway et l'initiative espagnole est que le but des participants du projet Galway n'est pas de rédiger une convention internationale, mais d'harmoniser des lois diverses et d'assurer leur mise à jour constante.

En plus de l'objectif d'harmonisation, les acteurs œuvrant sur la scène supranationale, et en particulier les Commissaires à la vie privée de pays

257 *Id.*, art. 6-12.

258 ORGANISATION DE COOPÉRATION ET DE DÉVELOPPEMENT ÉCONOMIQUES (OCDE), *Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel*, supra, note 71, voir notamment les articles 8, 9, 12, 14.

259 PARLEMENT EUROPÉEN ET CONSEIL DE L'EUROPE, *Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données*, supra, note 67, art. 6.1 et 7. [*Directive*] et le principe de proportionnalité. Voir le rapport sur la directive : Commission européenne, Direction générale du marché intérieur et services, *Preparation of a methodology for evaluating the adequacy of the level of protection of individuals with regard to the processing of personal data: annex to the annual report 1998 (XV D/5047/98) of the working party established by article 29 of directive 95/46/EC*, Luxembourg, Bureau des publications officielles des communautés européennes, 1998.

260 « Global Discussion on the Commonly-accepted Elements of Privacy Accountability », Galway, Irlande, 29 avril 2009. (Résumé de la conférence de Galway.) « Bien que les responsables de l'élaboration des politiques aient donné des directives au marché concernant la structure visant à lier les règles professionnelles et les règles transfrontalières sur la protection de la vie privée, et que les principes de base en vue de répondre aux attentes des consommateurs en matière de protection de la vie privée soient bien établis, il existe peu de directives sur la façon dont les entreprises peuvent démontrer leur utilisation et leur gestion responsables des renseignements personnels. Le règlement international des éléments des questions relatives à la responsabilité en matière de protection de la vie privée est particulièrement important, étant donné que l'évolution des processus commerciaux distribués permet le traitement des données et leur accès partout dans le monde. » [traduction]

261 Le projet Galway identifie cinq éléments de la responsabilité. Ils sont : (1) Organisation commitment to accountability and adoption of internal policies consistent with external criteria; (2) Mechanisms to put privacy policies into effect, including tools, training and education; (3) Systems for internal, ongoing oversight and assurance reviews and external verification; (4) Transparency and mechanisms for individual participation; and (5) Means for remediation and external enforcement.

membres de l'OCDE, ont constaté que la montée en flèche dans la dernière décennie des échanges de données transfrontières rendait plus difficile l'application des législations existantes. Afin de faire face aux nombreux nouveaux défis posés par la multiplication des normes nationales et de leur exécution efficace, les Commissaires à la vie privée de pays membres de l'OCDE se sont réunis à Paris au mois de mars 2010 et ils ont jetés les bases d'un *Global Privacy Enforcement Network* (GPEN)²⁶².

B. L'exécution des normes de protection : le GPEN

Le GPEN consiste en une nouvelle forme de coopération supranationale dans le domaine du contrôle des flux de données transfrontières. Dans cette section, nous résumerons les débats et les documents ayant précédés ce plan, ainsi que les principes qui le sous-tendent. Il sera aussi question de la portée envisagée, et de la nature des mécanismes projetés, du GPEN par ses créateurs. Nous verrons que le GPEN ne vise pas à remettre en question les lignes directrices sur la vie privée de l'OCDE (*OCDE Privacy Guidelines*) ou à favoriser une uniformisation des régimes nationaux, mais bien à mettre en place un organe de coopération entre les différentes autorités, et ce afin de favoriser l'application des législations déjà en place. Enfin, nous traiterons de la première démonstration de l'efficacité de ce mécanisme de coopération puisqu'il a été utilisé dans le cadre de l'affaire Google Buzz.

Le GPEN prend ses racines dans le paragraphe 21 des *Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnelles* de l'OCDE dans lesquelles il y est prévu que « [the] Member countries should establish procedures to facilitate information exchange related to these Guidelines, and mutual assistance in the procedural and investigative matters involved »²⁶³. Contrairement aux autres lignes directrices qui portent plus sur la mise en œuvre de l'objectif d'harmonisation des normes, le paragraphe 21 vise plutôt la coopération entre les différentes autorités dans l'application des lois nationales. Cette distinction est importante puisque l'idée qui sous-tend le plan d'action du GPEN est essentiellement celle d'améliorer l'efficacité des régimes nationaux pour contrôler les problématiques liées aux flux transfrontières des données. Selon les Commissaires membres du GPEN, cet objectif ne sera pas atteint par une réforme des *Lignes directrices de l'OCDE* (datant de 1980), mais par la mise en œuvre d'un mécanisme de coopération permettant une action concertée des différentes autorités. La portée de ce paragraphe est donc déterminante dans la portée de ce nouveau réseau.

En 2007, un pas important est franchi par l'adoption de la *Recommandation de l'OCDE relative à la coopération transfrontière dans l'application des législations*

262 *Un mécanisme de coopération élaboré lors du colloque « 30 Years After : The impact of the OECD Privacy Guidelines »*

263 OCDE, *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, 1980, en ligne : http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html (consulté le 31 mai 2010).

protégeant la vie privée. Cette recommandation, portée par la Commissaire canadienne à la vie privée Jennifer Stoddart, s'appuie sur un consensus quant à « la nécessité de promouvoir une coopération plus étroite entre les autorités chargées de faire appliquer la législation sur la vie privée, afin de les aider à échanger des informations et procéder à des enquêtes avec leurs homologues à l'étranger.»²⁶⁴

Bien qu'émanant des pays membres de l'OCDE, cette recommandation vise la création d'un nouvel instrument ayant une portée mondiale, soit « la mise en place d'un réseau informel des Autorités chargées de protéger la privée et autres parties prenantes intéressées pour débattre des aspects pratiques de la coopération pour l'application des lois protégeant la vie privée, pour échanger des pratiques exemplaires face aux problèmes transfrontières, pour œuvrer à la définition de priorités communes en matière d'application des lois, et pour soutenir des initiatives et campagnes conjointes en matière d'application des lois et de sensibilisation.»²⁶⁵ Cette recommandation prend donc pour point de départ qu'«une coopération efficace pour l'application des lois peut s'instaurer malgré des variations dans les approches nationales»²⁶⁶. Prenant pour modèle la *Recommandation du Conseil concernant des Lignes directrices régissant la protection des consommateurs contre les pratiques commerciales transfrontières frauduleuses et trompeuses* [C(2003)116] et la *Recommandation relative à la coopération transfrontière dans l'application des législations contre le spam* [C(2006)57], le texte de 2007 formule quatre recommandations :

- 1) Améliorer leurs cadres nationaux pour l'application des lois sur la vie privée afin que leurs autorités puissent mieux coopérer avec les autorités étrangères.
- 2) Élaborer des mécanismes internationaux efficaces destinés à faciliter la coopération transfrontière pour l'application des lois sur la vie privée.
- 3) Se prêter mutuellement assistance dans la mise en application des lois protégeant la vie privée, notamment par des actions telles que la notification, la transmission des plaintes, l'entraide pour les enquêtes et l'échange d'information, assorties de garanties appropriées.
- 4) Associer les parties prenantes intéressées aux discussions et activités visant à développer la coopération dans l'application des lois protégeant la vie privée.

Cette recommandation pose les fondements des discussions qui ont eu lieu lors du colloque tenu à Paris (dont nous avons fait mention) plus haut et ces

264 OCDE, *Recommandation de l'OCDE relative à la coopération transfrontière dans l'application des législations protégeant la vie privée*, 2007, en ligne : <http://www.oecd.org/dataoecd/12/48/38876531.pdf> (consulté le 31 mai 2010), p. 4

265 *Id.*, p. 11.

266 *Id.*, p. 5.

quatre principes seront explicitement repris et intégrés dans le Plan d'action du GPEN. Plusieurs intervenants ayant œuvrés ou œuvrant au sein d'organismes publics et privés ont discuté des principes fondateurs des *Lignes directrices sur la vie privée* et de leur efficience eu égard aux défis contemporains. À la suite des différentes interventions, le consensus suivant s'est dégagé²⁶⁷ : malgré l'innovation technologique soutenue des trente dernières années, les lignes directrices adoptées en 1980, par leur souplesse et leurs termes technologiques neutres, ne nécessitent pas une réforme en profondeur. Le défi résiderait plutôt dans l'amélioration de l'application des régimes nationaux découlant de ces lignes directrices. En effet, les flux transfrontières de données ayant augmenté substantiellement dans les dernières années, les autorités doivent maintenant traiter de nombreux cas dont les effets s'étendent à l'extérieur de leurs frontières. Une amélioration de l'application des législations passent donc nécessairement par une coopération plus étroite entre les autorités compétentes.

Cette coopération, selon le plan d'action, consiste à partager les informations relatives aux problèmes surgissant lors de l'application des lois et celles relatives aux solutions qui sont apportées (techniques d'investigation efficaces, législations efficientes, etc.) pour régler ces problèmes. On y prévoit aussi un mécanisme visant à synchroniser le dialogue avec le secteur privé et à faciliter l'application transfrontière des lois par la création d'une liste de contacts des autorités intéressées à coopérer bilatéralement lors d'enquêtes d'envergure internationale²⁶⁸. Plus spécifiquement, le GPEN souhaite établir un Secrétariat chargé de mettre en ligne un site web, de coordonner des campagnes de sensibilisation et de mettre à la disposition des autorités membres des informations pertinentes quant aux différents régimes nationaux. La création de ce Secrétariat constitue une initiative notable, puisque, à l'exception des groupes de travaux des organismes régionaux tel que l'OCDE et des Conférences annuelles rassemblant les autorités compétentes, aucun organe international visant la coopération dans ce domaine n'existe présentement. En outre, les membres du GPEN s'engagent à participer périodiquement à des appels conférences et à certaines rencontres. Ce nouveau réseau entend concentrer ses efforts sur les défis touchant le secteur privé, sans toutefois exclure la

267 Jane HAMILTON, *30th Anniversary of the OECD Privacy Guidelines, Remarks by Jane Hamilton, Industry Canada*, en ligne : http://www.oecd.org/findDocument/0,3354,fr_2649_34255_1_119802_1_1_1,00.html (consulté le 31 mai 2010) ; Peter HUSTINX, *Recent developments in the European Union*, 2010, en ligne : http://www.oecd.org/findDocument/0,3354,fr_2649_34255_1_119802_1_1_1,00.html (consulté le 31 mai 2010) ; Michael KIRBY, *The History, Achievement and Future of the 1980 OECD Guidelines on Privacy*, 2010, en ligne : http://www.oecd.org/findDocument/0,3354,fr_2649_34255_1_119802_1_2_1,00.html (consulté le 31 mai 2010) ; Hugh G. STEVENSON, *30 Years After : The Impact of the OECD Privacy Guidelines, Remarks of Hugh G. Stevenson*, 2010, en ligne : http://www.oecd.org/findDocument/0,3354,fr_2649_34255_1_119802_1_1_1,00.html (consulté le 31 mai 2010).

268 OCDE, *Action Plan for the Global Privacy Enforcement Network (GPEN)*, 2010, p. 1 et 2

coopération concernant les renseignements personnels détenus par le secteur public²⁶⁹.

Le GPEN souhaite s'en tenir aux aspects pratiques de la coopération transfrontière. La prise de position sur des questions de fond concernant les politiques publiques ne fait donc pas parti de son mandat²⁷⁰. De plus, malgré qu'il s'agisse d'une initiative menée par les pays de l'OCDE, le GPEN est ouvert à tous les pays désirant s'y joindre. Plus d'une autorité par pays peuvent même y adhérer. Enfin, soulignons que le plan d'action du GPEN ne crée aucune obligation légale, mais l'action concertée de ses membres a déjà montré son efficacité à l'occasion de l'affaire Google Buzz.

En avril 2010, un premier geste du GPEN, dont l'initiative revient à la Commissaire Stoddart, fut posé. Après la mise en service de Google Buzz, une application portant atteinte à la vie privée des usagers de Gmail, plusieurs autorités protégeant les renseignements personnels, incluant les commissaires du Canada, de l'Allemagne, de la France, du Royaume-Uni et de plusieurs autres nations, ont écrit une lettre publique au président de Google lui rappelant ses obligations légales²⁷¹. Bien que Google ait elle-même retiré ce service rapidement, cette action concertée montre bien que ces autorités peuvent établir un rapport de force et ainsi faire reculer des acteurs économiques d'envergure tels que la compagnie Google. D'ailleurs, il est utile de mentionner que Michael Geist, professeur titulaire de la Chaire de recherche canadienne en droit de l'Internet et du e-commerce à l'Université d'Ottawa, voit dans cette action concertée « a major step forward toward the globalization of privacy enforcement »²⁷².

En somme, les défis de plus en plus importants découlant des flux transfrontières de données ne semblent pas pouvoir être surmontés par la simple application des régimes nationaux déjà en place, ces derniers s'arrêtant à leurs frontières respectives. Cependant, la similitude des normes émanant de plusieurs de ces régimes, et découlant des lignes directrices émises par l'OCDE en 1980, permet d'envisager une coopération plus efficace entre les autorités protégeant les renseignements personnels. Le Global Privacy Enforcement Network vise donc à mettre en place un système permettant une application plus efficiente des différentes législations. Grâce à un organisme permanent coordonnant les efforts et à une coopération accrue entre les autorités membres, une meilleure protection des renseignements personnels transférés au-delà des frontières semble maintenant possible.

269 *Id.*, p.4

270 *Id.*

271 Cette lettre peut être consultée sur le site de la Commissaire à la vie privée du Canada, à l'adresse suivante : http://www.priv.gc.ca/media/nr-c/2010/let_100420_e.cfm (consulté le 31 mai 2010)

272 Michael GEIST, «Privacy Takes Step Towards Global Enforcement», 2010, en ligne :<http://www.michaelgeist.ca/content/view/4994/135/> (consulté le 31 mai 2010)

2.3.2.2 Un réseau de norme de portée particulière : l'Agence mondiale anti-dopage

L'Agence mondiale anti-dopage (AMA) constitue un objet de recherche du droit administratif global riche d'enseignements pour le Commissariat à la protection de la vie privée. D'abord par son design institutionnel, ayant connu des succès probants au cours des dernières années, mais aussi en raison des solutions qui ont été retenues afin de protéger les renseignements personnels des athlètes en particulier.

Dans un premier temps, nous ferons un survol historique et institutionnel de l'AMA afin d'examiner les mécanismes qui ont été créés pour contrôler et surveiller les pratiques de dopage dans le sport et pour explorer l'idée de savoir si ces mécanismes pourraient servir d'exemple pour améliorer l'efficacité de la LPRPDE. En effet, l'AMA et ses fondateurs ont réussi à atteindre des objectifs collectivement rationnels (et inspirés de la théorie des jeux) en intégrant fortement les acteurs privés qu'elle régleme. Cette intégration dans le cadre de la lutte anti-dopage s'organise de manière pyramidale. En effet, les fédérations sportives nationales et internationales sont les intervenantes de première ligne et elles doivent adhérer à un cadre normatif clair et explicite, le Code mondial anti-dopage, de sorte que l'AMA est en mesure d'appliquer un système de sanction axé sur la dissuasion. Ce système semble rapporter des dividendes. Nous verrons en outre que les succès dans la lutte anti-dopage sont aussi attribuables à la mission éducative que s'est donnée l'AMA. Dans un deuxième temps, nous explorerons les solutions proposées par l'AMA pour résoudre le problème de la protection des renseignements personnels des athlètes qui migrent au-delà des frontières d'un État. Les renseignements personnels recueillis pour les tests anti-dopage étant intimement liés aux droits les plus fondamentaux des athlètes, l'AMA s'est dotée de Standards internationaux afin d'éviter les dérapages.

A. Survol historique et institutionnel

L'Agence mondiale anti-dopage a pour mission « de promouvoir, coordonner et superviser la lutte contre le dopage dans le sport sous toutes ses formes »²⁷³. Cet organisme nongouvernemental tire ses racines de l'art. 4 de la Déclaration de Lausanne de 1999²⁷⁴ et constitue une réponse au scandale du Tour de France de 1998. Cette déclaration fut signée par les représentants des gouvernements, les organisations non-gouvernementales, incluant plusieurs fédérations sportives, et les athlètes ayant participé à la conférence. D'abord financée à part entière par le Comité international olympique, l'AMA est, depuis 2002, soutenue à parts égales par les gouvernements et le CIO.

273 AGENCE MONDIALE ANTI-DOPAGE, *À propos de l'AMA*, 2010, en ligne : <http://www.wada-ama.org/fr/Apropos-de-lAMA/> (consulté le 23 juin 2010).

274 Le lecteur peut consulter cette déclaration à l'adresse suivante : http://www.sportunterricht.de/lksport/Declaration_e.html (consulté le 23 juin 2010).

Afin de remplir adéquatement ses objectifs de coordination internationale, l'AMA adopte en 2004 un Code mondial anti-dopage, code révisé en 2009. À l'occasion des Jeux olympiques d'Athènes en 2004, toutes les fédérations sportives participantes adoptent ce code. En 2005, la *Convention internationale contre le dopage dans le sport de l'UNESCO* est adoptée afin de rendre possible l'incorporation du Code mondial dans les législations nationales²⁷⁵. À ce jour, 141 pays ont ratifié ce traité²⁷⁶.

La lutte anti-dopage peut donc se comparer à une pyramide, l'AMA se trouvant au sommet et les organisations sportives nationales se trouvant à la base. Les fédérations internationales se situent quant à elles au milieu de cette pyramide. Toutes sont liées par le Code mondial. L'art. 20.3.2 prévoit que les fédérations nationales doivent adopter le code pour être membre d'une fédération internationale. Autant les organisations sportives nationales qu'internationales sont responsables des tests périodiques et des sanctions en cas de contravention au Code (art. 5 et 10). Les décisions de ces organismes peuvent être portées en appel devant le Tribunal arbitral du sport²⁷⁷. Les organisations sportives sont aussi responsables de la promotion des campagnes éducatives.

Les gouvernements, par leur signature de la Convention de l'UNESCO, s'engagent quant à eux à respecter le cadre réglementaire du Code mondial et à modeler leurs législations sur ses principes²⁷⁸. L'AMA, au sommet de cette pyramide, élabore le cadre réglementaire et coordonne les efforts dans l'application du code (art. 20.7.1 du Code mondial). Ces efforts peuvent se traduire par la création de campagnes éducatives (art. 20.7.6), par l'accréditation de laboratoires nationaux (art. 20.7.4), par la recherche et l'innovation technologique dans les techniques de dépistage (art. 20.7.6), etc. L'Agence peut en outre prendre part aux procédures d'appel des décisions des organisations sportives.

En somme, l'AMA coordonne et fournit des ressources à des partenaires fortement intégrés au système. Leurs actions permettent de mieux rejoindre les athlètes et de leur expliquer les conséquences de leurs actes. De plus, la participation des différents acteurs à l'élaboration des principes généraux à la

275 UNESCO, *Convention internationale contre le dopage dans le sport*, 2005, en ligne : <http://www.unesco.org/new/fr/social-and-human-sciences/themes/sport/anti-doping/international-convention-against-doping-in-sport/> (consulté le 23 juin 2010). certains pays ne pouvant ratifier un document rédigé par une ONG indépendante

276 AGENCE MONDIALE ANTI-DOPAGE, *La Convention de l'UNESCO dépasse la marque des 140 ratifications*, 2010, en ligne : <http://www.wada-ama.org/fr/Centre-media/Nouvelles/La-Convention-de-l-UNESCOdepasse-la-marque-des-140-ratifications/> (consulté le 23 juin 2010).

277 Tribunal arbitral du sport, *Historique du TAS*, 2010, en ligne : <http://www.tas-cas.org/historique> (consulté le 23 juin 2010).

278 Voir, par exemple, la *Politique canadienne contre le dopage dans le sport* à l'adresse suivante : <http://www.pch.gc.ca/pgm/sc/pol/dop/index-fra.cfm> (consulté le 25 juin 2010).

base de la lutte anti-dopage assure leur adhésion et leur participation. Leur engagement prend la forme des obligations prescrites au Code mondial anti-dopage.

- **Le Code mondial anti-dopage**

Le Code mondial anti-dopage se divise en trois parties. La première porte sur le contrôle du dopage (art. 1 à 17). On y définit les pratiques de dopage et les substances interdites. Cette section met ensuite en place les procédures de dépistage et de gestion des résultats. Les sanctions et les procédures administratives (droit d'appel, droit à une audition équitable, etc.) y sont ensuite balisées. Notons que c'est dans cette section, soit à l'art. 14, que les garanties de confidentialité sont explicitées.

La deuxième partie du Code traite de l'éducation et de la recherche (art. 18 et 19). Il est utile de souligner ici que les succès de la lutte anti-dopage s'expliquent en partie par l'efficacité des campagnes éducatives menées par les diverses institutions liées par le code. Cette efficacité s'explique aussi par l'engagement des acteurs privés dans ces campagnes. Par exemple, à l'occasion de la dernière Coupe du Monde, la FIFA s'est jointe à l'AMA et à sa campagne « Dis NON ! au dopage »²⁷⁹. On y reconnaît la forme pyramidale décrite précédemment : une campagne est élaborée et coordonnée par l'AMA et une organisation sportive, dans ce cas-ci la FIFA, en fait la promotion auprès des athlètes. L'art. 19 fixe des objectifs de recherche sur le dopage afin d'assurer la conformité à la réglementation. L'AMA est responsable de la coordination entre les différentes agences et de la transmission des résultats scientifiques (art. 19.3).

La troisième partie prescrit les obligations de tous les acteurs, y compris les acteurs privés (art. 20 à 23). Une section est consacrée à chaque type d'acteurs (CIO, organisations sportives nationales, fédérations internationales, personnel médical, athlètes, gouvernements, etc.). En plus de permettre une meilleure coordination des efforts pour contrer le dopage, ce cadre normatif sert de fondement au système de sanction institué par le code et axé sur la dissuasion.

La problématique du dopage sportif peut être analysée sous l'angle de la théorie des jeux : s'il est individuellement rationnel pour un sportif de se doper, afin d'améliorer ses performances et de se donner un avantage comparatif sur ses compétiteurs, il est collectivement irrationnel de tolérer ces pratiques, dans la mesure où le principe « jouer franc jeu » est une valeur importante. On peut même considérer qu'elle constitue l'essence même du sport²⁸⁰. Cependant, il est

279 AGENCE MONDIALE ANTI-DOPAGE, *La FIFA se joint à la campagne Dis NON! au dopage de l'AMA pendant la Coupe du monde*, 2010, en ligne : <http://www.wada-ama.org/fr/Centre-media/Nouvelles/La-FIFA-se-jointa-la-campagne-Dis-NON-au-dopage-de-lAMA-pendant-la-Coupe-du-monde/> (consulté le 21 juin 2010).

280 Cette opposition est explicitée dans la section *Fondements* du Code mondiale anti-dopage. AGENCE MONDIALE ANTI-DOPAGE, *Code mondial anti-dopage*, 2009, p. 14.

difficile de prouver une faute subjective dans les cas litigieux (le sportif pouvant facilement plaider l'ignorance des traitements reçus). Ainsi, afin de contrer le dopage le plus efficacement possible dans cet univers particulier, les auteurs du Code ont retenu l'idée de créer une norme de responsabilité objective fondée sur la négligence et renversant la charge de la preuve (art. 10.5.1). Il est donc exceptionnel qu'un athlète puisse se dégager de sa responsabilité une fois les éléments matériels prouvés (test de dépistage positif)²⁸¹. Les sportifs sont donc tenus personnellement responsables de tout dopage. Ce sont eux qui doivent « s'assurer que tout traitement médical reçu ne viole en aucune manière les règles antidopage applicables »²⁸². Cette responsabilité objective est acceptée par les acteurs du milieu, ceux-ci considérant qu'un trop haut degré de preuve en matière d'intention coupable rendrait la lutte anti-dopage inefficace.

En plus de la responsabilité objective, le principe de proportionnalité de la sanction, quasi absent, est l'une des caractéristiques marquantes de ce système axé sur la dissuasion. Les périodes de suspension, allant d'une année à la suspension à vie, sont, de manière générale, automatiques. L'art. 10.5 rend très restrictive la prise en compte de circonstances particulières afin d'ajuster une sanction. Ainsi, une violation du Code entraîne des sanctions sévères, dans un but avoué de dissuasion. Le TAS déclare d'ailleurs, dans l'arrêt Hondo, qu'« une interprétation plus souple dudit système qui permettrait par exemple une atténuation de la sanction même en l'absence des circonstances particulières prévues aux articles 264 et 265 RAD [Article 10.5 du Code], pourrait mettre en danger son application uniforme et son efficacité»²⁸³.

L'adhésion libre des fédérations internationales, nationales et des athlètes au Code sert d'appui à ce type de réglementation de nature pénale. Le juge Claude Rouiller rappelle, dans son avis juridique sur la compatibilité entre le Code et le droit suisse et le principe de la proportionnalité, que les athlètes adhérant à une fédération appliquant le Code «acceptent délibérément l'éventualité d'une sanction abrupte»²⁸⁴. Ce cadre réglementaire rappelle donc les principes d'une obligation contractuelle, où le contrat constitue la loi des parties. Il faut donc souligner cette relation, dans le design institutionnel de la lutte anti-dopage, entre un système de sanction sévère d'une part, et une légitimation de ce système d'autre part par l'adhésion volontaire des acteurs privés à un cadre réglementaire clair et explicite. Le juge Rouiller résume bien la situation :

281 Olivier NIGGLI et Julien SIEVEKING, « Éléments choisis de jurisprudence en application du code mondial antidopage », (2006) 20 *Jusletter*, p. 2.

282 *Id.*, p. 4.

283 *Hondo c. UCI, Swiss Olympic and WADA*, TAS, 10 janvier 2006, par. 142, en ligne : http://www.wadaama.org/rtecontent/document/CASELAW_Hondo.pdf (consulté le 22 juin 2010).

284 284 Claude ROUILLER, *Avis de droit sur la compatibilité de l'article 10.2 du Code mondial antidopage avec les principes fondamentaux du droit national suisse*, 2005, en ligne : <http://www.wadaama.org/fr/Programmmondial-antidopage/Juridique-articles-jurisprudence-et-lois-nationales/Avis-consultatif-et-avis-de-droit-sur-le-Code/> (consulté le 22 juin 2010).

« Le but du Code est l'éradication totale du dopage, dont il est dit qu'il pourrait être fatal pour l'avenir des grandes compétitions sportives. Même si la dissuasion ne justifie pas tous les moyens, le régime répressif, qui assume aussi un rôle de prévention générale, doit être à la mesure des enjeux. Si les sportifs eux-mêmes estiment avec raison ce régime adéquat et nécessaire, il n'y a plus guère de place pour sa critique sous l'angle de la proportionnalité proprement dite concrétisée en définitive par l'art. 27 CCS.»²⁸⁵

Le problème du dopage chez les athlètes comporte, dans une certaine mesure, des similitudes avec celui de la protection des renseignements personnels détenus par le secteur privé. En effet, dans une perspective de théorie des jeux, une compagnie privée peut ne pas avoir suffisamment d'incitatifs pour respecter les prescriptions réglementaires, alors que les violations peuvent avoir des conséquences importantes sur le jeu de la concurrence et les droits des consommateurs (l'intérêt général). La réglementation effective du flux des données pourraient donc passer par une concertation entre les différents acteurs, afin de mieux cerner les intérêts rationnels à poursuivre, et la mise en œuvre de systèmes de sanctions plus musclés. Toutefois, quelques nuances doivent être faites concernant le régime pénal applicable par l'AMA et sa transposition dans la cadre de la LPRPDE.

Un système axé sur la dissuasion est plus facilement acceptable pour les acteurs privés lorsque les objectifs collectifs à poursuivre font consensus. En effet, le consensus quant à l'irrationalité de la pratique individuelle est beaucoup plus marqué en matière de lutte antidopage qu'en ce qui concerne les renseignements personnels. Dans les faits, la problématique du dopage sportif s'interprète dans l'esprit de la plupart des acteurs dans des termes très simples de « bien » et de « mal ». Il est donc plus facile d'obtenir l'adhésion des acteurs privés à un système fortement répressif reposant sur le principe de la dissuasion lorsque des principes moraux aussi simples s'affrontent. Il en est tout autrement pour l'objet de la LPRPDE, où plusieurs principes s'opposent (liberté d'entreprise, confiance du consommateur, droit quasi-constitutionnels, etc.).

De plus, les sanctions du Code mondial anti-dopage s'appliquent dans un cadre où les enjeux économiques ne sont pas du même ordre que dans le cas des compagnies assujetties à la LPRPDE. Est-ce qu'un régime de protection des renseignements personnels axé sur la dissuasion, et comportant des sanctions sévères, serait accepté par les acteurs privés réglementés par la LPRPDE? La réponse à cette question repose sans aucun doute sur le degré du consensus atteint sur les objectifs collectifs souhaitables.

En somme, les succès de la lutte anti-dopage sont attribuables à un design institutionnel faisant une place importante aux acteurs privés. La forte

285 *Id.*, p. 36 - 37.

intégration des acteurs privés permet, en plus d'une proximité essentielle à l'éducation des membres et à l'application du cadre normatif, la légitimation d'un système de sanctions sévères, mais efficace, axé sur la dissuasion. Bien que quelques nuances s'imposent dans le cadre d'une comparaison avec la LPRPDE, certaines pratiques de l'AMA et son organisation institutionnelle pourraient y être transposables.

B. Initiatives relatives à la protection des renseignements personnels

Dans cette deuxième section, notre attention se portera sur les pratiques de l'AMA en matière de renseignements personnels. L'AMA et ses partenaires rassemblent une grande quantité de renseignements personnels lorsqu'ils font des tests de dépistage. Puisque ces tests sont souvent réalisés dans le cadre de manifestations internationales, les renseignements recueillis passent d'un territoire à l'autre. La gestion des résultats peut aussi faire l'objet d'un flux transfrontière, par exemple lorsque des résultats sont transmis d'une organisation sportive nationale à l'AMA, située au Canada. La lutte anti-dopage implique donc des transferts de données personnelles transfrontières constants.

Pressée par les gouvernements européens, l'AMA s'est dotée du *Standard international sur la protection des renseignements personnels* afin de «fixe[r] un ensemble minimum commun de règles auxquelles les organisations antidopage doivent se conformer lorsqu'elles recueillent et gèrent des renseignements personnels conformément au Code»²⁸⁶. Ce standard sous-tend le Code mondial anti-dopage et les pratiques de ses signataires. Selon les *Lignes directrices de l'OCDE de 1980*, il a pour principal objectif de «veiller à ce que les organisations antidopage protègent de façon appropriée, suffisante et efficace les renseignements personnels qu'elles traitent dans le cadre des programmes antidopage, en reconnaissance»²⁸⁷. Nous examinerons ci-après les droits et obligations contenues dans ce Standard international afin de mieux comprendre les mécanismes mis en place pour traiter les renseignements personnels des athlètes dans le respect de leur vie privée.

- **Un périmètre de sécurité créé par un ensemble minimum commun de règles**

Le *Standard international* prescrit un minimum de règles afin de garantir la protection des renseignements personnels des athlètes. Malgré les disparités législatives entre les États dans lesquels ces données voyagent, tous les acteurs impliqués dans leur gestion sont liés d'une manière ou d'une autre par les règles énoncées dans le *Standard international*.

286 AGENCE MONDIALE ANTI-DOPAGE, *Standard international sur la protection de la vie privée*, 2009, p. 1, en ligne : <http://www.wada-ama.org/fr/Programme-mondial-antidopage/Sport-et-Organisations-antidopage/Standards-internationaux/> (consulté le 22 juin 2010).

287 *Id.*

Selon son art. 4.1, une organisation anti-dopage agissant dans un État où la législation est plus souple que le Standard se doit d'harmoniser ses pratiques avec ce dernier (dans la mesure toutefois où cette harmonisation n'entraînera pas une violation d'une loi applicable). Une organisation anti-dopage ne respectant pas ces contraintes minimales risque la mise à l'écart puisque les autres organisations ont l'obligation de la dénoncer à l'AMA et de refuser de partager ses renseignements personnels avec elle (art. 8.2). En outre, toujours dans cette optique de délimiter un environnement présentant des garanties harmonisées de protection des renseignements personnels des athlètes, les compagnies sous-traitantes (laboratoires, fournisseurs de services informatiques, etc.) des organisations antidopages doivent, en plus d'être choisies selon les garanties de mesures de sécurités techniques et organisationnelles qu'elles peuvent fournir, être tenues contractuellement de la confidentialité du traitement des données (art. 9.4 et 9.5). Dans tous les cas, l'organisation anti-dopage demeure responsable de la protection des renseignements personnels des participants (ce qui inclut les athlètes et les employés de l'organisation). Le *Standard international* crée donc, en quelque sorte, un périmètre de sécurité autour des athlètes, en liant les acteurs traitant leurs renseignements personnels au-delà de l'organisation sportive.

Afin d'éviter que les renseignements personnels des athlètes sortent de ce périmètre de sécurité, le Standard interdit de communiquer à des tiers les données recueillies, à moins que l'organisation y soit tenue par la loi, qu'elle obtienne le consentement du participant concerné ou que les forces de l'ordre en fasse la demande dans le cadre d'une enquête (art. 8.3). Puisque le *Standard international* constitue un ensemble minimum de règle, il n'entre pas en conflit avec les législations régionales plus strictes. Ainsi, les organisations anti-dopage exerçant leurs activités dans des États possédant des régimes plus exigeants doivent se conformer à ces standards plus élevés (art. 4.2). Il en est ainsi, par exemple, des organisations anti-dopage européennes. En effet, malgré les craintes initiales du Groupe de travail Article 29, il est maintenant reconnu par tous que le Standard n'abaisse pas les exigences législatives de l'Union européenne en matière de protection de renseignements personnels²⁸⁸.

En somme, le Standard international crée une sorte de périmètre de sécurité autour de l'athlète en établissant des normes minimales de protection des renseignements personnels et en limitant le nombre de personnes morales et physiques pouvant y avoir accès. Ainsi, bien que les données personnelles recueillies par les organisations anti-dopage traversent différents territoires étatiques ayant adoptés des régimes de protection différents, et peut-être divergents, elles ne passent finalement qu'entre les mains d'acteurs liés aux exigences du Standard international.

288 AGENCE MONDIALE ANTI-DOPAGE, *Déclaration de l'AMA à propos de l'avis du Groupe de travail européen sur la protection des données*, 2009, p.1, en ligne : http://www.wada-ama.org/Documents/World_Anti-Doping_Program/WADP-IS-PPPI/WADA_Statement_WP29_FR.pdf (consulté le 22 juin 2010).

- **Un contrôle des renseignements centralisé**

L'organisation en pyramide de la lutte anti-dopage se retrouve aussi au niveau de la protection des renseignements personnels. Ainsi, selon l'art. 14.5 du *Code mondial anti-dopage*, les organisations anti-dopage nationales et internationales doivent remettre tous les résultats et données recueillis à l'AMA. En centralisant l'information, cette mesure permet, en plus d'éviter le dédoublement des dépistages et d'accroître l'efficacité, de sécuriser les transferts transfrontières des données sensibles. En effet, l'AMA a mis en place un système informatique sécurisé permettant l'accès à ses données, le *Anti-doping Administration and Management System* (ADAMS). Cette base de données est accessible à tous les acteurs signataire du Code, des fédérations nationales et internationales au CIO, en passant par le sportif lui-même.

Il va sans dire que l'accès aux données est limité en fonction du type d'acteur s'y connectant. Par exemple, un athlète peut avoir accès à son dossier sur ADAMS afin d'y inscrire ses coordonnées de localisation dans le cadre des dépistages surprises. Une organisation nationale anti-dopage a, quant à elle, accès aux données des athlètes habitant sur son territoire. Dans l'éventualité où elle souhaiterait disposer d'informations sur un athlète étranger afin de planifier un dépistage dans le cadre d'une manifestation sportive sur son territoire, elle devra obtenir l'autorisation de la fédération nationale sportive du participant en question. Ce dernier sera alors informé que ses renseignements personnels sont disponibles - temporairement - pour cette organisation anti-dopage²⁸⁹.

L'AMA s'engage, toujours selon l'art. 14.5 du Code, à produire annuellement des rapports sur la gestion de ses données et à se rendre disponible «pour des discussions avec les autorités nationales et régionales compétentes en matière de protection des renseignements personnels». Enfin, notons que l'AMA, ainsi que son système ADAMS, sont soumis à l'autorité de la Commissaire à la protection de la vie privée puisque son siège social est situé à Montréal. Cette réglementation s'ajoute donc au *Standard international* de l'AMA.

- **Autres obligations des organisations anti-dopage**

Certaines autres obligations sont imposées aux organisations anti-dopage afin d'assurer une protection égale aux données traversant les frontières.

D'abord, les organisations anti-dopage sont tenues de ne traiter que les renseignements pertinents aux tests de dépistage et dans le seul but de la réalisation de ces tests (art. 5.2 et 5.3 du *Standard international*). Les opérations des organisations anti-dopage étant limitées, il est ainsi plus facile de gérer les accès à la base de données ADAMS, en plus de garantir un minimum d'intrusion dans la vie privée des participants. De plus, à moins de pouvoir invoquer un motif juridique valide tel que l'exécution d'un contrat ou la

289 AGENCE MONDIAL ANTI-DOPAGE, *Q - R : ADAMS*, en ligne : <http://www.wada-ama.org/fr/ADAMS/Q-R--ADAMS/> (consulté le 30 juin 2010).

protection d'un intérêt essentiel d'un participant, ce dernier doit donner son consentement avant que des renseignements personnels le concernant soient traités (art. 6.1).

Afin de donner un consentement éclairé, le participant doit recevoir certaines informations de la part des organisations anti-dopage, informations énumérées à l'art. 7.1. Par exemple, l'organisation doit divulguer «les autres destinataires potentiels des renseignements personnels, y compris les organisations antidopage situées dans d'autres pays où le participant pourrait participer à des compétitions, s'entraîner ou voyager » ainsi que « les fins auxquelles les renseignements personnels peuvent être utilisés et la durée de leur conservation ». Le participant garde ainsi un certain contrôle sur ses renseignements personnels. Bien entendu, le refus d'un participant de participer au processus anti-dopage peut entraîner certaines sanctions (art. 6.3).

Enfin, notons que les organisations anti-dopage doivent mettre en place certains mécanismes afin d'assurer la sécurité des renseignements personnels. Ces mécanismes peuvent être des mesures « physiques, organisationnelles, techniques, environnementales et autres » afin de prévenir la divulgation des données personnelles (art. 9.2). Les renseignements dits «sensibles» (informations génétiques, médicales, judiciaires) doivent faire l'objet de mesures plus strictes (art. 9.3).

De plus, les organisations anti-dopage doivent désigner une « personne responsable de la conformité [de l'organisation] à ce *Standard international* et à toutes les lois localement applicables sur la protection des renseignements personnels (art. 9.1). Cette personne doit être accessible aux participants. Enfin, les organisations anti-dopage ont l'obligation de détruire les renseignements personnels après leur vie utile (art. 10).

En somme, le *Standard international sur la protection des renseignements personnels* assure une protection équivalente aux données personnelles des athlètes passant d'une frontière à l'autre.

2.3.3.3 L'APEC Privacy Framework

La Coopération économique pour l'Asie-Pacifique (APEC) est un forum regroupant 21 économies recouvrant la région de l'Asie-Pacifique. Fonctionnant par consensus, ce regroupement d'États vise à développer le commerce transfrontière en adoptant des résolutions non-contraignantes juridiquement. Devant l'importance stratégique des renseignements personnels et la disparité des législations des économies membres, l'APEC a souhaité, depuis 2003, fournir des guides et des outils afin d'assurer la sécurité de ces données et, par le fait même, intensifier les échanges commerciaux.

C'est en 2005 que l'APEC adopte son *Privacy Framework*. Fondé sur les principes de l'OCDE de 1980, ce cadre réglementaire constitue un plancher en matière de protection des renseignements dans la région. Tout comme pour l'Initiative espagnole, ce projet est aussi le fruit d'une conférence qui a été organisée par le Center for Information Policy leadership et l'Office of the

Data Protection Commissionner et les participants à cette conférence sont des titulaires de charge publique responsables de la protection des renseignements personnels dans leurs États respectifs, ainsi que des personnes provenant du milieu des affaires.

Très critiqué, plusieurs commentateurs y ont vu une simple version diluée des principes de l'OCDE²⁹⁰. Toutefois, il faut souligner que, tout comme l'Initiative espagnole, le cadre législatif de l'APEC est une entente qui rassemble un bon nombre de pays. Ce cadre se présente moins comme un effort législatif relatif à la protection des renseignements personnels, mais plus comme un effort d'harmonisation et développement des lois facilitant les échanges et le commerce des entreprises²⁹¹. Il ne s'agit pas d'un document voulant établir des normes, mais des principes²⁹². Les liens entre les principes de l'APEC et ceux énoncés dans les Lignes directrices de l'OCDE sont explicitement tissés dans le cadre de l'APEC²⁹³. De plus, bien que les économies membres ayant légiféré en la matière l'ont fait avec plus de vigueur, les effets pratiques de ce cadre dans les autres économies sont limités par sa nature non-contraignante.

En 2007, le *Data Privacy Subgroup* propose les projets *Pathfinders* afin de contrôler la sécurité des données traversant les frontières. Ces projets, reposant sur les principes de l'*APEC Privacy Framework*, s'inspirent de l'approche américaine en matière de protection de données, le *US Safe Harbour*. En effet, les projets *Pathfinders* mettent en place des mécanismes d'accréditation à la disposition des entreprises. Ces « trustmark », comme les nomme le projet, assureraient aux consommateurs la sécurité de leurs données personnelles entre les mains des entreprises accréditées.

Cette approche fondée sur l'accréditation s'appuie sur les consensus et les acteurs privés. Elle se distingue donc de l'approche européenne, mettant de l'avant des législations nationales harmonisées par des standards internationaux ainsi que le concept de « législation adéquate ». Nous étudierons donc dans un premier temps le fonctionnement du système « Cross-Border Privacy Rules » de l'APEC et de ses *Pathfinders*. Dans un deuxième temps, nous nous pencherons sur les nombreuses critiques qui ont été faites à l'endroit de ce projet de l'APEC.

A. Les projets *Pathfinders* et le *Cross-Border Privacy Rules System*

Les projets *Pathfinders* découlent d'une mise en application du neuvième principe à la base de l'*APEC Privacy Framework* relatif à la reddition de compte.

290 Voir par exemple à ce sujet la première partie de Graham GREENLEAF, « Five years of the APEC Privacy Framework : Failure or promise ? » (2009) 25 *Computer Law & Security Rev.* 28.

291 COOPÉRATION ÉCONOMIQUE ASIE-PACIFIQUE, *APEC Privacy Framework*, 2005, APEC#205-SO-01.2, art. 3.

292 *Id.*, art. 14-26.

293 *Id.*, art. 5.

Dès 2006, les représentants des économiques membres ont planché sur ces neuf projets visant, notamment, la mise en place de critères d'accréditation pour les entreprises et pour les agents accréditeurs eux-mêmes.

Le *Cross-Border Privacy Rules System* (CBPRS) est fondé, comme le modèle *Safe Harbour*, sur la mise en place volontaire par une entreprise d'un système de protection des données. À la suite d'une auto-évaluation de son régime corporatif en cette matière, une entreprise pourra recevoir une accréditation d'un agent privé ou d'une autorité gouvernementale²⁹⁴.

L'APEC identifie donc quatre piliers soutenant son CBPRS²⁹⁵. Premièrement, l'autoévaluation : les organisations développent des règles et des procédures afin de protéger les renseignements personnels. Deuxièmement, l'examen de conformité : un agent d'accréditation s'assure que les règles élaborées sont conformes à l'*APEC Privacy Framework* et les autres documents nationaux ou internationaux contraignant dans une certaine juridiction. Certains auteurs expriment certaines réserves quant à la nécessité de la conformité avec d'autres documents que le cadre de l'APEC (ou seulement une portion de celui-ci). Nous reviendrons sur la portée de l'accréditation dans la deuxième section. Troisièmement, l'accréditation : l'APEC met en place un système d'accréditation, un « trustmark ». Quatrièmement, l'application et l'arbitrage de conflit : les organisations mettent en place des procédures afin de répondre aux plaintes des consommateurs.

Par la mise en place de ces piliers, l'APEC souhaite produire des modèles de mécanismes de révision, de résolution de plaintes, d'auto-évaluation organisationnelle, etc. Ces modèles pourront ensuite être utilisés par les entreprises soucieuses d'améliorer leur efficacité en cette matière. Le CBPRS se rapproche donc de l'approche américaine, ce système se penchant cependant plus précisément sur les problématiques de transferts internationaux de données.

Les neuf projets *Pathfinders*²⁹⁶ visent à tester ce système par l'élaboration de critères clairs et d'expériences pratiques. Ils constituent en fait l'expression pratique des piliers décrits précédemment.

Projet 1 : Principes pour les auto-évaluations corporatives

294 HUNTON & WILLIAMS LAW FIRM, *Background paper on APEC Privacy Framework Pathfinder Projects*, 2008, p. 3, en ligne : http://www.hunton.com/files/tbl_s47Details/FileUpload265/2302/Bruening_APEC_Privacy_Framework.pdf (consulté le 5 juillet 2010)

295 *Id.*

296 ASIA-PACIFIC ECONOMIC COOPERATION, *APEC Data Privacy Pathfinder Projects Implementation Work Plan -Revised*, Doc. off. 2009/SOM1/ECSCG/SEM/027 (23 février 2009), en ligne : aimp.apec.org/Documents/2009/.../09_ecsg_sem1_027.doc (consulté 2 juillet 2010)

Ce projet vise à développer un formulaire standard d'auto-évaluation pour les organisations participant au processus d'accréditation. Ce document permettra à celle-ci d'évaluer leurs pratiques internes en matière de protection des renseignements personnels.

*Projet 2 : Principes pour les agents d'accréditation
(« Trustmark » guidelines)*

Ce projet vise à développer les critères à remplir pour un agent d'accréditation issue du secteur public ou privé. Pour pouvoir dispenser la marque d'accréditation APEC, l'agent devra répondre à certains critères d'indépendance, d'impartialité dans la résolution de plaintes et de mécanismes d'évaluation de la conformité des organisations avant et après leur accréditation.

Projet 3 : Évaluation de la conformité des règles corporatives de protection transfrontières des données

Ce projet développe des principes à utiliser par les agents d'accréditation lors de leurs évaluations de la conformité du régime des organisations avec l'*APEC Privacy Framework*. Ce projet vise donc la mise en place d'un processus standard de révision des auto-évaluations corporatives.

Projet 4 : Répertoire des organisations accréditées

L'APEC mettra éventuellement en place un répertoire des entreprises accréditées.

Les projets 5, 6 et 7 visent une plus grande coopération entre les autorités de protection de la vie privée. Ces projets s'inspirent des avancées de l'OCDE en matière de coopération.

Projet 5 : Répertoire des autorités en matière de protection des renseignements personnels

L'APEC mettra en place un répertoire des autorités pertinentes de ses économies membres.

Projet 6 : Coopération des autorités de l'APEC dans l'application des règles de protection transfrontières

Ce projet vise à développer un système de coopération entre les autorités pertinentes. Sur une base volontaire, les autorités pourront se transmettre de l'information afin de faciliter les enquêtes et l'application des règles de protection. Il semble que ce projet de coopération incluse autant les

agences gouvernementales des économies membres que les agents d'accréditation du secteur privé.

Projet 7 : Formulaire standardisé de demande d'assistance

Ce projet vise à développer un formulaire standardisé de demande d'assistance entre les différentes autorités. Les problématiques seront de cette manière mieux cernées et pourront être référées à l'acteur compétent (système interne de gestion de plainte d'une organisation, agent d'accréditation du secteur privé, agence de protection gouvernementale, etc.).

Projet 8 : Principes directeurs et procédures pour les procédures d'application au sein du CBPRS

Ce projet se rattache au précédent, en ce qu'il vise à développer des critères et des procédures afin de référer les plaintes aux acteurs compétents. Le CBPRS sera organisé en pyramide, différents régulateurs étant affectés à différents types de plaintes.

Projet 9 : Programme pilote pour tester et analyser les résultats des projets précédents afin d'en arriver à l'établissement du système complet

Certaines économies se porteront volontaires, ainsi que des entreprises issues de ces économies, pour tester le CBPRS. Conformément au projet 1, ils soumettront une autoévaluation de leur régime de protection de données personnelles. Cette auto-évaluation sera analysée par les agents d'accréditation suivant les modalités du projet 3. Les mécanismes de règlements des projets 6 et 7 seront ensuite testés afin d'évaluer leur efficacité.

Les économies membres sont libres de participer à tous les projets, à quelque uns d'entre eux ou de ne participer à aucun de ceux-ci. Le *International Chamber of Commerce*, les États-Unis, l'Australie et le Canada sont les participants les plus enthousiastes. Plusieurs économies participent à certains projets seulement alors que d'autre se contentent du rôle d'observateur.

B. Une approche qui soulève plusieurs critiques

Aux yeux de certains auteurs²⁹⁷, l'approche traditionnelle de l'APEC, fonctionnant par consensus et plaçant les entreprises au centre de l'élaboration réglementaire, n'est pas compatible avec un système d'accréditation. En effet, leurs principales critiques s'articulent autour de l'idée que des critères trop permissifs ou différents d'un territoire à l'autre créeront un système d'accréditation trompeur pour les consommateurs soucieux de faire affaire avec des entreprises protégeant adéquatement leurs données.

- **Les standards applicables aux entreprises**

Ces auteurs prennent donc pour cible les projets 1 à 3, concernant les critères d'accréditation des compagnies et des agents eux-mêmes et leur relation avec l'*APEC Privacy Framework*. Ils estiment, par exemple, que les standards auxquels les entreprises doivent se conformer dans leur auto-évaluation (projet 1) et dans l'évaluation des agents d'accréditation (projet 3) sont encore indéterminés. Lorsque les économies n'auront pas légiféré à l'égard de ces projets, ils craignent que les entreprises auront pour seule obligation de se conformer au neuvième principe du cadre de l'APEC portant sur la reddition de compte et que le plancher réglementaire de référence sera, en conséquence, celui de l'*APEC Privacy Framework*. Ce neuvième principe, trop flou à leurs yeux, se rapporte précisément aux mouvements transfrontières de données. Il prévoit que l'entreprise doit soit obtenir le consentement du consommateur à l'égard de ce transfert ou qu'elle doit «vérifier de manière diligente et raisonnable que les informations reçues par une organisation ou une personne seront traitées par cette dernière en conformité avec les principes de l'APEC»²⁹⁸.

À la lumière de la documentation officielle et rendue publique, les craintes de consommateurs vont dans le même sens. Ils se demandent si l'accréditation se limitera aux principes de l'APEC relatifs aux mouvements transfrontières. Ainsi, certains principes, tel que les limitations dans la collecte de données et le choix du consommateur dans l'utilisation de ses données, pourraient, selon les documents de travail des projets 1 et 3, ne pas être inclus dans l'accréditation APEC. Si ce scénario venait à se concrétiser, certains commentateurs ont émis l'opinion que les entreprises pourraient être inscrites au *Répertoire des organisations accréditées* de l'APEC (projet 4) sans s'être conformées à tous les

297 Graham GREENLEAF, « Five years of the APEC Privacy Framework : Failure or promise ? » (2009) 25 *Computer Law & Security Review* 28. ; N. WATERS, « The APEC Asia-Pacific Privacy Initiative - a new route to effective data protection or a trojan horse for self-regulation ? » (2008) *U. New South Wales Faculty of Law Research Series 2008, Working Paper 59*.

298 *Id.*, Greenleaf critique la formulation de ce principe, laissé sans définitions plus précises de pratiques raisonnables, y voyant une occasion pour la première organisation de se délier de ses obligations envers le consommateur. Il en irait de même pour la deuxième organisation, même si une clause lierait les deux compagnies pour un traitement de données adéquat, du moins dans les juridictions où les stipulations pour autrui ne sont pas reconnues.

principes de l'APEC. De plus, en ce qui concerne les données ne traversant pas les frontières, ces entreprises ne seront tenues à aucun principe de l'APEC. L'accréditation de l'APEC pourrait alors devenir source de confusion dans l'esprit des consommateurs et des autres entreprises partenaires d'affaires²⁹⁹.

- **Les standards applicables aux agents d'accréditation**

Comme pour le projet 1 et 3, le projet 2 reste flou quant aux standards auxquels doivent se conformer les agents pour être accrédités. Un premier problème mis au jour est le suivant : à quel degré d'impartialité peut-on s'attendre d'une compagnie qui 'vend' son accréditation à d'autres compagnies privées, et ce plus particulièrement lorsque viendra le temps d'arbitrer un conflit entre un consommateur et une entreprise, cliente de l'agent? Les critiques concernant le modèle d'accréditation par des agents privées remontent au début des années 2000³⁰⁰. Howes y a vu à l'époque un système trop mou ne favorisant que les entreprises. Les consommateurs y seraient les grands laissés pour compte, les compagnies d'accréditation n'ayant de sympathies et d'intérêts qu'en commun avec les compagnies qu'elles doivent réglementer.

Dans une étude de 2008, Connolly trace quant à lui un bilan sombre du modèle d'accréditation par des agents privés. Les standards de ces agences seraient plus bas que n'importe quelle législation nationale ou internationale et l'application des règles aux entreprises délinquantes serait inefficace³⁰¹. Ici aussi, l'auteur se montre sceptique face aux garanties d'indépendance d'une agence privée et ne voit dans ce modèle qu'une opération marketing potentiellement trompeuse pour les consommateurs.

En revanche, le projet 2 ne réfère cependant pas uniquement aux agents d'accréditation du secteur privé. En effet, il n'est pas exclu que certaines autorités gouvernementales se voient attribuer le statut d'agent d'accréditation. Dans une telle éventualité, les législations nationales de plusieurs pays, incluant le Canada, pourraient être modifiées afin de conférer de nouveaux pouvoirs à une autorité publique, telle le Commissariat à la protection de la vie privée. Cette avenue apparaîtrait, du moins à première vue, plus prometteuse lorsqu'elle est examinée sous l'angle d'assurer à une autorité publique une plus grande

299 Notons cependant que la littérature scientifique soulève ces questions à la lumière des documents officiels publiés jusqu'en 2009. Puisqu'il ne s'agit que de documents de travail, ces problématiques seront peut-être réglées avant le lancement du programme d'accréditation.

300 R. GELLMAN, « TRUSTe fails to justify its role as privacy arbitrator » (2000) 25 *Privacy Law & Policy Reporter* (2000), en ligne : <http://www.austlii.edu.au/au/journals/PLPR/2000/53.html> (consulté le 2 juillet 2010) ; E. HOWES, *No guarantee of privacy*, 2002, en ligne : <http://spywarewarrior.com/uiuc/privpol.htm#no-guarantee> (consulté le 2 juillet 2010)

301 C. CONNOLLY, *Trustmark schemes struggle to protect privacy*, 2008, en ligne : http://www.galexia.com/public/research/assets/trustmarks_struggle_20080926/trustmarks_struggle_public.pdf (consulté le 2 juillet 2010)

impartialité lors de la prise de décision relative à l'octroi ou au rejet d'une demande d'accréditation.

Le deuxième problème est celui de l'harmonisation. En effet, puisque l'APEC fonctionne par consensus et que les économies membres semblent vouloir éviter la voie de l'harmonisation des législations, les commentateurs se demandent si chaque économie ne développera pas son propre système d'accréditation des agents du secteur privé, rendant les fondations du système inégales. Ici, la question qui est posée est de savoir s'il est possible d'éviter l'harmonisation des législations nationales.

Malgré l'approche d'accréditation de l'APEC, tentant de contourner l'approche européenne de législation 'adéquate' (et d'harmonisation des législations qui en découle) par une approche calquée sur le modèle *Safe Harbour, Waters* (2008) et l'assistant Commissaire de la Nouvelle-Zélande Stewart (2003) croient que ce concept de législation adéquate ne peut pas être totalement évacué³⁰². En effet, selon eux, aucun État ne pourra éviter d'évaluer la valeur de l'accréditation d'une autre État; il en viendra forcément juger de la conformité des critères d'accréditation des entreprises et des agents d'une autre économie avec ses propres règles nationales.

Au-delà de ces critiques, Waters soulève quelques points positifs découlant des auto-évaluations corporatives³⁰³. En effet, il estime que ces auto-évaluations iraient plus loin que celles prévues par les lois nationales puisque celles-ci sont instiguées à la suite d'une plainte et qu'elles postulent la conformité de l'entreprise avec la législation nationale. L'auto-évaluation découlant du projet 1 irait au contraire beaucoup plus en profondeur et serait plus systématique. De plus, l'information fournie par les entreprises aux agents d'accréditation serait beaucoup plus volumineuse et précise que celle qui serait fournie sous n'importe quel autre modèle dans ce domaine, incluant les législations européennes. Cependant, les documents officiels ne nous renseignent pas à savoir si ces informations ou une portion d'entre elles seraient rendues publiques. La publication de ces auto-évaluations, permettant à la société civile de mener ses propres analyses, pourrait être une solution envisageable pour contrer les problèmes d'impartialité auparavant soulevés.

Enfin, comme le notent même les commentateurs les plus sceptiques, les critiques soulevées précédemment peuvent encore être réglées d'ici la mise en place définitive de l'accréditation APEC. L'avenir nous dira donc si cette accréditation ne constituera qu'une manière bon marché pour les entreprises

302 WATERS, *supra* note 297; B. STEWART, A suggested scheme to certify substantial observance of APEC Guidelines on data privacy, APEC E-commerce Steering Group Meeting, 2003, en ligne : http://www.apec.org/apec/documents_reports/electronic_commerce_steering_group/2003.MedialibDownload.v1.html?url=/etc/medialib/apec_media_library/downloads/taskforce/ecsg/mtg/2003/pdf.Par.0009.File.v1.1 (consulté le 5 juillet 2010)

303 WATERS, *supra* note 297.

de rassurer les consommateurs sans leur offrir la protection dont ils croient bénéficier ou si elle sera, au contraire, une manière originale de rendre les entreprises plus responsables. L'avènement du premier scénario pourrait porter un dur coup à la globalisation du modèle *Safe Harbour*. Un tel système, ne profitant finalement qu'à quelques entreprises, ne réglerait pas la problématique des transferts de données personnelles et les différents pays participants, déçus par cette approche non concluante, considéreraient peut-être alors de se tourner vers une approche de type 'législation adéquate' et fondée sur l'adoption de standards internationaux.

* *
*

Pour résumer cette section sur la construction du droit administratif global relatif à la protection des renseignements personnels, un premier constat s'impose. Ces nouveaux réseaux de normes supranationales sont déjà bien implantés et donnent des résultats notables sur le plan de la conformité des acteurs visés par celles-ci. En effet, bien que notre brève description des initiatives supranationales visant la création de mécanismes d'harmonisation et d'exécution ne rende pas compte de toutes les initiatives relatives à la protection des renseignements personnels³⁰⁴, elle avait pour objectif de montrer qu'il y a une véritable construction supranationale d'un système d'intégrité relatif à la protection des renseignements personnels dont les faisceaux de normes et de mécanismes qui ont des portées générales et particulières. Ce système comprend des mécanismes d'élaboration des normes, par lesquels l'adoption de principes harmonisateurs est visée, ainsi que des mécanismes de coopération, dont l'objectif est une exécution plus efficace des normes de protection. À ce système d'intégrité se greffe tant les initiatives fédérales, notamment avec la LPRPDE, que provinciales et territoriales mais également celles des entreprises qui mettent aussi sur pied des mécanismes pour traiter les plaintes des consommateurs. Ce qui est intéressant de toutes ces initiatives c'est qu'elles mettent en relief l'émergence d'un principe d'une responsabilité horizontale interpellant tous les acteurs impliqués dans l'échange et le commerce des renseignements personnels³⁰⁵. Ainsi, certaines institutions en surveillent d'autres qui en surveillent également d'autres, etc. Il s'agit d'un vaste réseau reliant les institutions publiques et privées et mettant en œuvre un système fondé sur la surveillance mutuelle.

C'est en raison de ce complexe de normes inter-relies que la métaphore du nid d'oiseau a été proposée par des chercheurs australiens pour décrire ce

304 Pour un portrait plus complet du réseau de normes, on peut lire, entre autres, le discours de la commissaire adjointe de la commissaire à la protection de la vie privée, Elizabeth Denham, pour le *2009 Privacy Invitational Forum*, Cambridge (Ontario), 19 novembre 2009.

305 KEY CENTRE FOR ETHICS, LAW, JUSTICE AND GOVERNANCE, Université Griffith et Transparency International Australia, *supra*, note 211 (Nisa Report), p. 14-18.

phénomène³⁰⁶. Ils expliquent le choix de cette métaphore en faisant valoir que le nid d'oiseau est un élément de la nature qui occupe une fonction vitale et qui protège quelque chose de fragile. Ils ajoutent que si quelques brindilles qui composent le nid se rompent, le nid est construit de manière à ce que les œufs demeurent tout de même en sécurité. Les brindilles ne forment un nid solide que si elles sont assemblées. Ils terminent en insistant sur le fait que les brindilles ne sont pas les institutions elles-mêmes mais les liens entre elles.

En guise de remarque finale, soulignons également que les auteurs identifient trois différents types de relations que peuvent entretenir les institutions faisant partie du système entre elles : celles qui se passent à un niveau « politique (dans le sens du développement de “*policies*”) », « opérationnel » et « constitutionnel ». Il serait utile de faire des recherches additionnelles pour mieux comprendre ces rapports de relevance juridique entre les institutions chargées de la protection des renseignements personnels. En effet, elles pourraient permettre de mieux comprendre dans quelle mesure ces relations entre l'énoncé des politiques et leur mise en œuvre engendrent une normativité de type constitutionnelle ou quasiconstitutionnelle³⁰⁷. Cette recherche pourrait également avoir pour objectif de mieux comprendre les forces et les faiblesses des systèmes qui sont mis en réseau, notamment le système canadien.

Conclusion de la partie I

Dix ans après l'adoption de la LPRPDE, quels sont les points de convergence et de divergence entre le contexte économique, juridique et politique du début des années 2000 et les nouvelles réalités contemporaines qui ont émergé dans les dix dernières années qui se sont écoulées depuis son adoption?

D'abord, le discours économique favorise toujours l'imposition d'un minimum de contraintes aux entreprises dans le but de garantir l'accès aux marchés nationaux et internationaux. Cependant, la réflexion sur le rôle de la réglementation sociale (catégorie à laquelle fait partie la LPRPDE) a progressé vers une plus grande sensibilité vers une plus grande protection des consommateurs. En effet, que l'État ait pour objectif de protéger ses citoyens (consommateurs) contre les abus de pouvoir des entreprises est conçu comme étant un rôle tout à fait légitime.

De plus, cette protection doit être pensée au niveau intranational, mais aussi au niveau extranational puisque les États doivent, dans la mesure du possible, harmoniser leurs réglementations sociales de manière à garantir une protection efficace contre les échanges d'information entre les États. Ce dernier objectif est d'autant plus important que les développements technologiques du Web 2.0

306 *Id.*

307 Sur cette question, on peut lire l'excellent ouvrage de David SCHNEIDERMAN, *Constitutionalizing Economic Globalization, Investment Rules and Democracy's Promise*, Cambridge, Cambridge University Press, 2008

laissent présager la nécessité d'une telle harmonisation pour être effective. Lorsqu'on tient compte de ces nouveaux développements technologiques, en particulier, l'idée de consolider le système d'intégrité sur les plans national et international prend tout son sens.

À cet égard, des recherches additionnelles et ciblées sur les répercussions de ces changements technologiques sur la capacité des organismes publics à mettre en œuvre leur mission de protection des renseignements personnels seraient essentielles à la réflexion sur l'effectivité de la LPRPDE. Cette réflexion doit être menée non seulement dans une perspective économique. Il s'agit d'ici de faire un examen approfondi des multiples et nouvelles applications rendant possibles les abus à l'égard de la protection des renseignements personnels par les entreprises à l'égard des consommateurs. Elle doit aussi être menée dans une perspective publique. Il s'agit ici de faire un examen des abus possibles des gouvernements canadiens et des États étrangers à l'égard de la protection des renseignements personnels des citoyens canadiens. Enfin, elle doit aussi être menée dans une perspective où il y a un amalgame de relations entre les secteurs privé et public et nuisant à l'établissement de rapports éthiques équilibrés (tel que noté par Gunasekara en faisant état des problèmes liés à l'interaction entre les deux secteurs vue sous l'angle de la lutte anti-terroriste et l'accumulation de renseignements personnels par le secteur privée).

Ces problèmes soulèvent des questions à plusieurs niveaux et ayant des répercussions politiques et juridiques importantes. En effet, il faut d'abord souligner les difficultés sur le plan de l'organisation institutionnelles. Dans le but de penser à des solutions qui puissent régir l'ensemble des problèmes liés à l'utilisation des données par les entreprises du secteur privé, par les gouvernements canadiens et étrangers, et par les interactions entre les secteurs privé et public, il serait utile de s'interroger sur le maintien de deux lois fédérales distinctes : la Loi sur la protection des renseignements personnels et la LPRPDE. Par ailleurs, il faut aussi une réflexion sur le type d'organisme administratif qui pourrait être créé pour faire face à ces nouveaux défis, de façon à le doter des fonds et du personnel adéquat, mais aussi des fonctions et pouvoirs adaptés aux nouvelles réalités contemporaines.

À cet égard, bien que le discours politico-administratif sur l'organisation et les pouvoirs des organismes publics chargés de mettre en œuvre les lois n'ait pas changé de façon radicale, le dogmatisme des idées qui prévalaient durant les années 1980 et qui militaient contre la mise sur pied de nouveaux organismes publics semble s'être estompé. Ceci est particulièrement vrai lorsqu'on recense le nombre d'organismes créés aux fins de consolider notre Système national d'intégrité. En effet, on peut noter un réel engouement des politiciens pour les organismes parlementaires de surveillance des activités gouvernementales depuis les quatre dernières années. Il serait utile de mieux comprendre les fondements et les limites aux compétences qui peuvent être attribuées à ce type d'organisme, surtout lorsqu'ils sont appelés à agir dans le secteur privé. Cette réflexion et vérification seront particulièrement pertinentes dans le contexte où le législateur envisagerait d'ajouter des pouvoirs (tels des pouvoirs de nature réglementaire et pénale) au Commissariat, pouvoirs qui ne sont pas normalement associés à ceux d'un ombudsman ou d'un ombudsman de

type parlementaire. Une question qui se pose à leur égard est de savoir si les compétences attribuées à ces organismes peuvent être étendues au secteur privé sans indûment sacrifier la cohérence institutionnelle étatique au nom de ce qui semble être des solutions plus pragmatiques.

Sur ce point, il apparaît que le remplacement du Commissariat par un organisme faisant partie de la catégorie des organismes décentralisés et, plus précisément, par un organisme de régulation sociale (« sociale » et non « économique » puisque la LPRPDE est une réglementation sociale et non économique) et doté de pouvoirs de nature administrative (par exemple le pouvoir d'enquête), décisionnelle (par exemple le pouvoir d'émettre des ordonnances et d'infliger des peines) et réglementaire est une option qui mériterait d'être étudiée.

Enfin, au moins trois observations peuvent être faites à l'égard du contexte juridique et allant du niveau macro-juridique au niveau micro-juridique.

Premièrement, il faut noter la construction du droit administratif global relatif à la protection des renseignements personnels qui se poursuit et se complexifie. Des recherches additionnelles seraient nécessaires afin de mieux comprendre quelles sont les forces et les faiblesses de notre système canadien de protection des renseignements au regard de ce réseau de normes. Il pourrait aussi être utile d'envisager l'attribution de pouvoirs au Commissariat afin qu'il puisse clairement participer aux débats à l'échelle supranationale. Il pourrait être ainsi envisagé de constituer un comité de coopération (composé du commissaire fédéral et des commissaires provinciaux, de fonctionnaires fédéraux et provinciaux, de représentants d'industries (petites, moyennes et grandes), de groupes d'intérêts (notamment de protection des consommateurs) et de citoyens. Il s'agirait en quelque sorte de créer une délégation canadienne (sous forme d'un conseil consultatif) ayant suffisamment d'autorité pour discuter des questions relatives à la protection des renseignements personnels et intervenir sur la création des normes et mécanismes du droit administratif global dans ce domaine.

Deuxièmement, il faut souligner que les problèmes constitutionnels soulevés par l'adoption de la LPRPDE en 2000 ne sont toujours pas résolus. Il faudra exercer une vigile juridique sur les débats des cours de justice sur la validité des processus d'harmonisation notamment. S'il était envisagé d'attribuer des pouvoirs d'ordonnance au Commissariat et que ceux-ci pouvaient être appliqués à toutes les entreprises canadiennes, cela susciterait des débats fédéraux-provinciaux houleux. Ce type de question devrait être d'abord discuté entre les entités de la fédération pour voir dans quelle mesure une entente fédérale-provinciale pourrait être envisageable. Dans cette optique, le dossier relatif à la création d'un organisme de réglementation fédérale relatif aux valeurs mobilières (proposition actuelle du gouvernement Harper) est à suivre puisqu'il met aussi en jeu des questions d'interprétation des articles 91.2 et 92.13 de la *Loi constitutionnelle de 1867*, tout comme la LPRPDE. Les arguments qui seront présentés par les gouvernements fédéral et provinciaux seront déterminants pour fixer des balises à l'interprétation de ces articles puisque de ceux-ci découleront les motifs de la Cour. Bien qu'au moment de la rédaction

de ce rapport les mémoires des gouvernements n'étaient pas disponibles, il est raisonnable de penser que certains arguments du gouvernement fédéral seront de nature fonctionnelle. Il serait donc possible que la Cour suprême les déclare valide, ce qui pourrait donner le signal de départ avalisant la mise en œuvre d'une interprétation plus fonctionnelle de notre constitution et créant ainsi des ouvertures vers la mise en œuvre d'une forme de fédéralisme en réseau. Quoi qu'il advienne à cet égard, il demeure que si une approche plus fonctionnelle était envisagée pour régler certains problèmes d'application de la LPRPDE, les paramètres d'action du Commissariat devront faire l'objet de recherches et d'analyses plus poussées. À tout le moins, la possibilité de créer un secrétariat coordonnant la réflexion et la recherche à tous les niveaux de gouvernements (incluant les gouvernements municipaux) pourraient être un point de départ fructueux dans la recherche des meilleures solutions et pratiques administratives.

Troisièmement, et s'agissant de l'attribution d'éventuels pouvoirs de nature pénale, il faut souligner que, pour l'heure, et au sein du gouvernement fédéral, il semble bien que seul le CRTC (un organisme de régulation économique) en soit pourvu. Au Québec, le Tribunal des droits de la personne peut octroyer des dommages-intérêts punitifs aux personnes physiques et morales violant sciemment la *Charte des droits et libertés de la personne*. Il est intéressant de noter à cet égard que le Tribunal des droits de la personne se penche sur la violation de droits de nature quasi-constitutionnelle. Puisque la protection des renseignements personnels a vraisemblablement acquis ce statut juridique, des analogies pourraient être faites pour justifier l'attribution de tels pouvoirs au Commissariat.

Enfin, bien qu'il y ait un fort mouvement allant dans le sens d'octroyer de plus grandes protections aux citoyens et consommateurs eu égard à la circulation de leurs données personnelles, il faut aussi mentionner l'importance de tenir compte de leur liberté et de maintenir un juste équilibre entre les droits et les libertés. À cet égard, il serait utile de mieux connaître ce que les citoyens et consommateurs avisés veulent. Veulent-ils plus de protection? Peut-on observer des tendances distinctes selon les générations en cause? Afin de comprendre ces changements de perspectives, le Commissariat pourrait être conçu non seulement comme un lieu où on éduque le public, mais aussi comme un lieu où *on apprend du public*. En conséquence, il pourrait être utile que le Commissariat soit pourvu des pouvoirs et fonds nécessaires pour tenir périodiquement des fora de citoyens afin de prendre connaissance de leurs attentes en plus de celles de l'industrie et des groupes d'intérêts.

Partie II – Démarches et modes d'évaluation de la compétence du Commissariat à la protection de la vie privée du Canada aux termes de la LPRPDE

L'objectif de l'étude consiste à élaborer un cadre conceptuel destiné à évaluer l'efficacité et l'efficacités du Commissariat à la protection de la vie privée du Canada (CPVP) quant à la compétence qu'il exerce aux termes de la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE), et d'appliquer ce cadre en fonction des activités du CPVP. Comme nous avons déjà élaboré un cadre conceptuel dans la partie 1, notre analyse portera désormais sur l'efficacité du CPVP en ce qui concerne l'atteinte des objectifs de

la LPRPDE. Le concept de l'efficacité, dont il a été question dans la partie 1, vise à saisir une variété de rapports relatifs à l'environnement interne et externe du CPVP. La partie 1 examinait en profondeur le macro-environnement dans lequel se déroulent les activités du CPVP touchant la LPRPDE tandis que la partie 2 est axée sur le micro-environnement.

L'évaluation de l'efficacité et de l'efficacit  necessite la r alisation d' valuations empiriques, comparatives et normatives. Les  valuations empiriques portent sur les donn es quantitatives et qualitatives permettant de mesurer le niveau d'activit  du CPVP, la valeur de l'investissement et la perception du rendement. Les  valuations comparatives concernent l' valuation du CPVP du point de vue d'organismes analogues canadiens ou d'administrations homologues. Finalement, les  valuations normatives servent   d terminer si le CPVP atteint les buts vis s, explicitement ou implicitement, par l'adoption de la LPRPDE.

Ceci soul ve la question de savoir quel crit re servira    valuer la mani re dont le CPVP surveille l'application de la LPRPDE. Pour y r pondre, il est n cessaire de comprendre la port e et le but de la comp tence du Commissariat et, plus pr cis ment, le mod le de l'« ombudsman » qu'il a adopt . Autrement dit, dans le cadre de l' valuation du rendement du CPVP, il importe de se pencher d'abord sur son mandat et sa mission, puis sur les lois qu'il interpr te et applique (en l'occurrence, la LPRPDE).

La partie 2 se divise en quatre sections. La premi re section porte sur le mandat et la mission du CPVP dans le contexte de la LPRPDE et de l'adoption du mod le d'ombudsman. Elle passe  galement en revue les pouvoirs et les outils dont dispose le CPVP pour assurer le respect de la LPRPDE. La deuxi me section compare les pouvoirs du CPVP avec ceux d'autres organismes canadiens de protection de la vie priv e et d'organismes de protection des donn es personnelles d'administrations homologues. La troisi me section, qui poursuit l'analyse comparative, est ax e sur les organismes de r glementation de questions analogues au Canada et aux  tats-Unis. Finalement, la quatri me section examine les le ons retenues gr ce   l'analyse du CPVP et   l'analyse comparative sur les approches en mati re d' valuation. Cette section comprend  galement un examen qualitatif de la perception du CPVP.

Section 1. Le mandat et la mission du Commissariat   la protection de la vie priv e du Canada et le mod le d'ombudsman aux termes de la LPRPDE

La port e de la LPRPDE et le mandat du CPVP

En vertu de son mandat, le Commissariat   la protection de la vie priv e du Canada (CPVP) a la responsabilit  de surveiller le respect de la *Loi sur la protection des renseignements personnels*, laquelle porte sur les pratiques de traitement des renseignements personnels utilis es par les minist res et organismes f d raux, et de la LPRPDE. Le CPVP a pour mission de prot ger et de promouvoir le droit des personnes   la vie priv e. Le mandat du CPVP est d'agir   titre d'ombudsman pour le droit   la vie priv e et   la protection des

renseignements personnels des Canadiennes et des Canadiens, ce qui inclut un volet de défense et un volet de protection.

Le commissaire travaille de façon indépendante à l'examen des plaintes provenant de personnes concernant le secteur public fédéral et le secteur privé. En ce qui concerne le secteur public, les personnes peuvent porter plainte auprès du commissaire sur toute question précisée à l'article 29 de la *Loi sur la protection des renseignements personnels* (qui s'applique aux renseignements personnels que détiennent les institutions fédérales).

La LPRPDE s'applique à toute organisation à l'égard des renseignements personnels qu'elle recueille, utilise ou communique dans le cadre d'activités commerciales. Elle s'applique également à toute organisation à l'égard des renseignements personnels qui concernent un de ses employés et qu'elle recueille, utilise ou communique dans le cadre de ses opérations.

Le fédéralisme fait aussi partie des facteurs qui ont une incidence sur l'application de la LPRPDE. Les incidences constitutionnelles de la LPRPDE ont été abordées dans la partie 1; c'est en partie en raison de ces incidences que la LPRPDE a été conçue pour fonctionner de pair avec les lois provinciales. La LPRPDE vise à harmoniser la protection de la vie privée à l'échelle provinciale et fédérale. Pour ce qui est des questions ayant trait aux renseignements personnels dans le secteur privé, le commissaire peut examiner toutes les plaintes déposées en vertu de l'article 11 de la LPRPDE, sauf dans les provinces qui ont adopté des lois essentiellement similaires à la loi fédérale en matière de protection des renseignements personnels, soit le Québec, la Colombie-Britannique et l'Alberta. L'Ontario se classe également dans cette catégorie en ce qui concerne les renseignements personnels sur la santé que détiennent les dépositaires de cette information en vertu de la loi ontarienne sur la protection des renseignements personnels sur la santé. Cependant, même dans les provinces qui ont adopté une loi essentiellement similaire, et partout ailleurs au Canada, la LPRPDE s'applique toujours à tous les renseignements personnels recueillis, utilisés ou communiqués par toutes les entreprises fédérales, y compris les renseignements personnels au sujet des employés de celles-ci. En outre, la LPRPDE s'applique à toutes les données personnelles qui circulent d'une province ou d'un pays à l'autre, dans le cadre d'activités commerciales impliquant des organisations assujetties à cette loi ou à une loi essentiellement similaire.

Les pouvoirs d'exécution du commissaire ont été une considération principale dans l'élaboration de la LPRPDE. Le commissaire tient à régler les plaintes par le biais de la négociation et de discussions persuasives, en utilisant la médiation et la conciliation s'il y a lieu. Cependant, si les parties ne collaborent pas, le commissaire a le pouvoir de convoquer des témoins, de faire prêter serment et d'exiger la production d'éléments de preuves. Dans les cas qui demeurent toujours non résolus, plus particulièrement en vertu de la LPRPDE, le commissaire peut saisir la Cour fédérale de l'affaire et demander à cette dernière d'émettre une ordonnance pour rectifier la situation. En application de la LPRPDE, le CPVP a pour mandat de préparer et de diffuser des documents

d'information publique sur la protection de la vie privée, afin que la prévention soit pour le Commissariat une activité aussi importante que l'exécution de la loi.

En 2008, la Direction des enquêtes et des demandes de renseignements du CPVP a traité 6 344 demandes de renseignements ayant trait à la LPRPDE, elle a reçu 422 nouvelles plaintes en vertu de la LPRPDE et a réglé 412 plaintes³⁰⁸. Ces nombres en soi sont peu révélateurs de l'efficacité du CPVP dans le contexte de la LPRPDE, bien que la commissaire précise que « le nombre imposant d'appels et de lettres que nous recevons démontre à quel point les Canadiennes et Canadiens reconnaissent et ont à cœur leur droit à la vie privée³⁰⁹ ».

L'examen des tendances au fil des ans permet d'obtenir un autre point de vue sur l'efficacité du CPVP. Par exemple, le nombre de plaintes reçues en 2008 et en 2006 est équivalent, tandis qu'il était inférieur en 2007. À l'inverse, le nombre de demandes de renseignements est en baisse, tandis qu'il était en croissance au cours des trois années précédentes. Bien que le nombre de plaintes et de demandes de renseignements reçues constitue une donnée importante, il est impossible de s'en servir pour tirer des conclusions sur le rendement. Par exemple, la diminution du nombre de plaintes reçues en 2008 pourrait être un indicateur de la réussite de l'initiative du CPVP incitant les consommateurs à faire part de leurs préoccupations relatives à la protection de la vie privée directement aux entreprises qui disposent de leurs renseignements personnels, ou encore, elle pourrait révéler l'érosion de la confiance à l'endroit du CPVP ou la méconnaissance de celui-ci. Il faut interpréter ce type de données dans leur contexte, en fonction des facteurs conceptuels traités dans la partie 1 et des facteurs empiriques, comparatifs et normatifs traités dans la présente partie. Dans ce contexte, il faut se pencher sur les plaintes et les demandes de renseignements qui n'ont pas été présentées parce que les activités de prévention, d'éducation et de diffusion, qui assurent le respect de la LPRPDE, sont tout aussi importantes, sinon plus, que les occasions où les gens demandent au CPVP d'intervenir.

L'évaluation des activités du CPVP doit aussi tenir compte des buts de la LPRPDE, soit de régir la façon dont les entreprises du secteur privé effectuent la collecte, l'utilisation et la communication de renseignements personnels d'une manière qui tient compte du droit des personnes à la vie privée à l'égard des renseignements personnels qui les concernent. Plus précisément, la LPRPDE a été rédigée en fonction de la circulation accrue de l'information et des données à l'ère électronique.

308 Rapport annuel au Parlement 2008 : rapport sur la *Loi sur la protection des renseignements personnels et les documents électroniques*, Commissariat à la protection de la vie privée du Canada (août 2009), à l'adresse suivante : http://www.priv.gc.ca/information/ar/200809/2008_pipeda_f.pdf.

309 *Id.*, p. 2.

L'obligation prévue par la LPRPDE se fonde sur le *Code type sur la protection des renseignements personnels* de l'Association canadienne de normalisation, qui prévoit les dix principes fondamentaux suivants :

- 1) Responsabilité;
- 2) Détermination des fins de la collecte des renseignements;
- 3) Consentement;
- 4) Limitation de la collecte;
- 5) Limitation de l'utilisation, de la communication et de la conservation;
- 6) Exactitude;
- 7) Mesures de sécurité;
- 8) Transparence;
- 9) Accès aux renseignements personnels;
- 10) Possibilité de porter plainte à l'égard du non-respect des principes.

La LPRPDE comprend une règle générale (paragraphe 5(3)), qui prévoit que l'organisation ne peut recueillir, utiliser ou communiquer des renseignements personnels qu'à des fins qu'une personne raisonnable estimerait acceptables dans les circonstances. La LPRPDE prévoit un mécanisme permettant aux personnes de présenter au CPVP une plainte écrite contre une organisation qui enfreint des dispositions particulières de la *Loi*. La LPRPDE autorise également le commissaire à prendre l'initiative d'une plainte s'il a des motifs raisonnables de croire qu'une enquête devrait être menée sur une question.

Préoccupations au sujet de la compétence du CPVP aux termes de la LPRPDE

Depuis 2001, les activités menées par le CPVP aux termes de cette loi font l'objet d'un examen minutieux, tant à l'interne qu'à l'externe, du point de vue des milieux universitaire, des affaires, gouvernemental, juridique et parlementaire.

Dans le but d'examiner ses sept premières années d'activité aux termes de la LPRPDE, le CPVP a préparé *Tracer le chemin : Principaux développements au cours des sept premières années d'application de la Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE)*³¹⁰, une étude dans laquelle il passe en revue de grandes conclusions qu'il a tirées, quelques enjeux juridiques importants de la LPRPDE et certains sujets sur lesquels il se penchera ultérieurement, mais il s'abstient d'évaluer de quelque façon que ce soit la LPRPDE ou ses propres activités. Le rapport démontre l'incidence marquée de la LPRPDE et des activités du CPVP relatives au respect de la *Loi*, plus particulièrement en ce qui concerne ses réponses aux plaintes écrites.

Le Parlement a effectué un examen important de la LPRPDE en 2006-2007, conformément au paragraphe 29(1) de la LPRPDE, qui prévoit la réalisation d'un examen tous les cinq ans. Le Comité permanent de l'accès à

310 Accessible en ligne à l'adresse suivante : http://www.priv.gc.ca/information/pub/lbe_080523_f.pdf.

l'information, de la protection des renseignements personnels et de l'éthique de la Chambre des communes a tenu des audiences entre le 20 novembre 2006 et le 22 février 2007, entendu 67 témoins et reçu 34 présentations de particuliers et d'organisations du Canada (dont le CPVP).

L'Examen, prévu par la loi, de la Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE) : quatrième rapport du Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique, qui comprend 25 recommandations, a été présenté à la Chambre des communes le 2 mai 2007. Il convient de souligner la recommandation 18 : « Le Comité recommande qu'aucun pouvoir de rendre des ordonnances ne soit octroyé pour l'instant à la commissaire fédérale à la protection de la vie privée. » Cependant, le Comité a recommandé d'octroyer au CPVP un pouvoir additionnel en ce qui concerne l'obligation de signaler certaines atteintes à la protection des renseignements personnels au Commissariat³¹¹.

La réponse du gouvernement au rapport du Comité révèle que la *Loi* ne nécessite aucune « modification radicale » avant l'obtention de données supplémentaires³¹².

L'examen du Parlement n'a pas eu pour effet d'exiger la révision approfondie du modèle du CPVP se rapportant à la LPRPDE, mais le milieu universitaire et de défense des droits s'est montré plus critique. Dans *Reviewing PIPEDA: Control, Privacy and the Limits of Fair Information Practices*³¹³, Lisa Austin soutient que l'évaluation de l'efficacité du CPVP devrait être associée aux enjeux que sa compétence aux termes de la LPRPDE était destinée à régler. Elle maintient que la LPRPDE a comme principal objectif de veiller à ce que le contrôle des renseignements personnels assure aux personnes la confidentialité de leurs renseignements. Elle ajoute que la protection des renseignements peut viser un large éventail de valeurs, dont la prise de décisions concernant les différentes solutions relatives à la protection de la vie privée. Autrement dit, l'évaluation du modèle d'ombudsman du Commissariat ne peut pas être effectuée indépendamment des normes de la LPRPDE. M^{me} Austin critique particulièrement le fait que le CPVP ne publie que des « résumés » de ses conclusions et qu'il s'abstient d'y révéler l'identité des répondants. Ainsi, le CPVP n'établit aucun précédent faisant autorité et ses conclusions ne peuvent s'inscrire dans la jurisprudence qui pourrait régir les normes relatives à la vie privée en application de la LPRPDE.

De même, la Clinique d'intérêt public et de politique d'Internet du Canada (CIPPIC) conclut que le CPVP manque de « mordant », ce qui confirme à

311 Se reporter aux recommandations 23 et 24.

312 Consulter le site suivant : <http://www2.parl.gc.ca/HousePublications/Publication.aspx?Mode=1&Parl=39&Ses=1&DocId=3077726&File=0&Language=F>.

313 Lisa Austin, « Reviewing PIPEDA: Control, Privacy and the Limits of Fair Information Practices », (2006) 44 *Revue canadienne du droit de commerce* = *Canadian Business Law Journal* 21.

son avis la conclusion d'une de ses études, selon laquelle le non-respect des exigences de la LPRPDE est répandu³¹⁴.

Les personnes à l'origine des critiques se sont non seulement montrées préoccupées par l'efficacité du modèle actuel du CPVP en ce qui concerne le respect de la LPRPDE, mais elles estiment aussi que le choix du modèle d'ombudsman en soi avait pour *objectif* d'être moins efficace. Christopher Berzins, qui critique le choix du modèle d'ombudsman, a relevé sept facteurs qui, à son avis, ont incité le CPVP à choisir ce modèle précis pour appliquer la LPRPDE : 1) le désir de conserver les intérêts commerciaux organisés « en jeu »; 2) l'absence à l'époque d'une mobilisation à l'égard de la protection de la vie privée et d'une capacité à exercer une influence politique; 3) les défenseurs de la protection de la vie privée qui, à l'époque, étaient prêts à compromettre l'application de la loi afin de garantir une loi sur la protection des renseignements personnels s'appliquant au secteur privé; 4) des spécialistes ont mis l'accent sur des stratégies de conformité très larges allant au-delà des mécanismes relatifs aux plaintes et des pouvoirs en matière d'application; 5) le gouvernement fédéral avait l'habitude de faire appel à la surveillance d'un ombudsman dans des contextes semblables, comme le commissaire à la protection de la vie privée en place et le commissaire à l'information; 6) le commissaire à la protection de la vie privée à l'époque, Bruce Phillips, était favorable à l'adoption du modèle d'ombudsman pour la LPRPDE; 7) le gouvernement n'était pas disposé à établir une surveillance plus rigoureuse pour le secteur privé que la norme acceptable dans sa propre sphère d'activité³¹⁵.

1.1. Le modèle d'ombudsman du CPVP

L'aspect le plus important de la compétence du CPVP aux termes de la LPRPDE est le modèle d'ombudsman que le CPVP a choisi pour régir la protection de la vie privée dans le secteur privé. Dans une publication parue en 2005, intitulée *Distinguer le seigle du blé : réorientation de l'actuel débat sur la fonction d'ombudsman telle que définie dans la LPRPDE*³¹⁶, la commissaire Jennifer Stoddart explique les raisons justifiant ce choix et répond à certaines critiques à l'endroit de celui-ci. Voici la définition du modèle d'ombudsman adoptée par M^{me} Stoddart :

314 Clinique d'intérêt public et de politique d'Internet du Canada, « Compliance with Canadian Data Protection Laws: Are Retailers Measuring Up? », Ottawa, 2006, [http://www.cippic.ca/documents/bulletins/compliance_report_06-07-06_\(color\)_\(cover-english\).pdf](http://www.cippic.ca/documents/bulletins/compliance_report_06-07-06_(color)_(cover-english).pdf) [en anglais seulement – pour un résumé en français, voir http://www.cippic.ca/uploads/CIPPIC_PC_ÉxSum_FR.pdf].

315 Christopher Berzins, « Protecting Personal Information in Canada's Private Sector: The Price of Consensus Building », 27 *Queen's Law Journal* 609, 2001. L'avis de Berzins quant au CPVP est traité en détail dans la partie 1.

316 Se reporter à l'adresse suivante : http://www.priv.gc.ca/information/pub/omb_051021_f.cfm.

[...] mécanisme utilisé pour surveiller les activités de l'administration publique afin d'en assurer la légalité et l'équité. Les fonctions d'ombudsman sont généralement exercées par une seule personne, mais, à l'occasion, par un groupe de personnes. L'ombudsman, généralement nommé par le pouvoir législatif d'un gouvernement, est chargé de scruter les activités administratives du pouvoir exécutif³¹⁷.
[traduction]

L'ancien commissaire Bruce Phillips explique qu'il préfère le modèle d'ombudsman comme mécanisme de résolution des problèmes, qui constitue un incitatif au changement progressif :

Le commissaire fédéral à la protection de la vie privée est un ombudsman et n'a pas le pouvoir d'ordonner quoi que ce soit à qui que ce soit. Je suis parfaitement heureux de ne pouvoir donner d'ordres, car j'estime que la principale qualité de ma fonction, c'est que je n'ai pas à jeter le blâme sur qui que ce soit, mais plutôt à trouver des solutions aux problèmes. Entre nous, et même si cela semble peu modeste, j'aime à croire que nous avons connu un succès énorme car depuis que je suis entré en fonction il y a environ huit ans, nous avons été saisis de centaines sinon de milliers d'affaires et nous avons pu, grâce à la négociation, à la discussion et à un examen attentif des problèmes, recenser des domaines de la fonction publique fédérale où notre loi s'applique et où la gestion de l'information s'est améliorée considérablement relativement à la protection des renseignements personnels³¹⁸.

Cependant, le modèle d'ombudsman ne se limite pas à l'absence de coercition. Ses caractéristiques particulières peuvent être résumées ainsi :

- il favorise l'atteinte des objectifs en matière d'impartialité, de transparence, de responsabilité et d'équité;
- il s'engage à résoudre les conflits par entente mutuelle ou par consensus;
- la flexibilité;

317 Cette définition est tirée du document de Linda C. Reif, « Building Democratic Institutions: The Role of National Human Rights Institutions in Good Governance and Human Rights Protection », 13 *Harvard Human Rights Journal*, 2000, 1 à 8.

318 Présentation au Comité permanent de l'industrie de la Chambre des communes, 2 décembre 1998, accessible en ligne à l'adresse <http://www2.parl.gc.ca/HousePublications/Publication.aspx?DocId=1039144&Language=F#T1532>, début à 1625. Pour consulter d'autres discussions sur le modèle d'ombudsman dans les débats et travaux des comités parlementaires, se reporter à Jennifer Barrigar, *Consider Consideration and Order-Making* (document préparé à l'intention du CPVP, septembre 2009).

- la confidentialité;
- l'indépendance du gouvernement;
- le pouvoir de mener des enquêtes;
- le pouvoir de publier des rapports publics;
- l'absence d'ordonnances exécutoires, de sanctions réparatrices ou de pouvoirs disciplinaires.

Comme le prouvent ces caractéristiques, l'ombudsman joue un rôle institutionnel unique puisqu'il assure la reddition de comptes entre la personne et l'État administratif.

La Cour suprême du Canada a caractérisé le rôle important de l'ombudsman en ce qui concerne sa contribution à la responsabilité sur le plan démocratique; elle a conclu que « les pouvoirs que possède l'ombudsman lui permettent d'aborder les problèmes administratifs que les pouvoirs judiciaire, législatif et exécutif ne peuvent résoudre efficacement³¹⁹ ». Bien que le modèle d'ombudsman ait fait son apparition en Suède au début du 19^e siècle, il n'a été adopté à l'extérieur de la Scandinavie qu'au milieu du 20^e siècle. Le modèle d'ombudsman s'est répandu en raison de la demande croissante de la responsabilité accrue du gouvernement et, selon les estimations, il a été adopté par quelque 90 pays avant la fin des années 1990³²⁰. Ce modèle, dont la popularité était croissante, a été adopté par tous les ordres de gouvernement ainsi que par les industries privées et le monde universitaire.

Le modèle d'ombudsman s'est propagé sous différentes formes, qui peuvent généralement être divisées dans les deux catégories suivantes : l'ombudsman « classique », dont le pouvoir est conféré par la loi, et l'ombudsman « organisationnel » privé, qui travaille au sein d'institutions, comme des universités et des sociétés³²¹.

La fonction de surveillance de la LPRPDE exercée par le Commissariat est un amalgame des deux principaux modèles de l'ombudsman, soit l'ombudsman du secteur public et l'ombudsman du secteur privé. Bien que le Commissariat soit subventionné par l'État et que son mandat soit prévu dans une loi, il régit le secteur privé. Contrairement à l'objectif général du modèle d'ombudsman adopté par les parlements provinciaux au Canada, le Commissariat applique un modèle d'ombudsman doté d'un mandat particulier puisqu'il régit un domaine précis de l'administration.

319 *B.C. Development Corp. c. Friedmann*, 1984, 2 R.C.S. 447, au paragr. 40.

320 Roy Gregory et Philip Giddings, « The Ombudsman Institution: Growth and Development », dans Roy Gregory et Philip Giddings (éditeurs), *Righting Wrongs: The Ombudsman in Six Continents*, Washington, IOS Press, 2000, p. 1, à la page 1.

321 Howard Gadlin, « The Ombudsman: What's in a Name? », 16(1) *Negotiation Journal* 37, 2000, p. 38-39.

Malgré la multitude de formes dans lesquelles le modèle d'ombudsman a été utilisé afin de s'adapter aux besoins locaux au fil des ans, le modèle demeure caractérisé par des éléments communs. Généralement, l'ombudsman dispose du pouvoir nécessaire pour mener des enquêtes relatives aux plaintes déposées par le public et est souvent en mesure de lancer ses propres enquêtes. Dans de nombreuses administrations, l'ombudsman peut également mener des enquêtes sur des questions qui lui ont été présentées par des législateurs ou des ministres. Contrairement au système judiciaire, le modèle d'ombudsman est conçu de sorte à être accessible et peu coûteux pour les plaignants, tout en laissant une grande place à la flexibilité et à la créativité en ce qui concerne ses recommandations.

À la différence de la méthode controversée utilisée par les tribunaux de common law, l'ombudsman mène des enquêtes inquisitoires sur les plaintes. Le rôle de l'ombudsman ne s'exerce pas dans un contexte d'« affrontement ». Il ne s'agit pas non plus d'un modèle de médiation ou de résolution des conflits à proprement parler. L'ombudsman ne tente pas de régler les conflits, mais bien de favoriser l'atteinte de différents buts, dont l'intégrité, la transparence, l'impartialité et l'équité³²².

André Legrand a fait observer que « la principale particularité de l'institution de l'ombudsman réside dans le fait qu'il ne fait pas partie de l'administration, mais qu'il possède tout de même une grande capacité d'accès à l'information³²³ » [traduction]. Par conséquent, les enquêtes de l'ombudsman sont habituellement effectuées de façon rapide, informelle et impartiale. En règle générale, l'ombudsman a le pouvoir de demander aux personnes de produire des renseignements et aux organisations de lui donner accès à leurs dossiers et procédures.

1.2 Pouvoirs et outils dont dispose le CPVP

De façon générale, bien que l'ombudsman ne possède pas le pouvoir de prendre des décisions ou de rendre des ordonnances imposant des obligations au gouvernement, son pouvoir découle de la qualité de son enquête et de la légitimité continue du Commissariat. Par conséquent, l'exactitude, l'impartialité et la crédibilité sont des facteurs essentiels de la réussite des enquêtes de l'ombudsman. Afin de faciliter la réalisation d'enquêtes efficaces, l'ombudsman dispose généralement de pouvoirs étendus et possiblement intrusifs en matière d'enquête.

Autrement dit, les pouvoirs étendus de l'ombudsman en matière d'enquête sont atténués par la nature non coercitive de ses décisions. Après la réalisation

322 Se reporter à la description du rôle de l'ombudsman dans la lettre du commissaire Bruce Phillips destinée à Susan Whelan, députée, présidente du Comité permanent de l'industrie, 8 février 1999, en réponse aux présentations du Comité demandant l'octroi au CPVP du pouvoir de rendre des ordonnances exécutoires (dans le dossier des auteurs).

323 Rhita Boust, « The Ombudsman: Proposal for a Definition », 9 *The International Ombudsman Yearbook* 36, 2005, p. 49.

d'une enquête, l'ombudsman peut faire connaître ses conclusions et émettre des recommandations visant à la fois à améliorer les systèmes et souvent à accorder une réparation aux personnes ayant subi des conséquences négatives en raison de l'activité administrative examinée.

De nombreuses personnes soutiennent que la plus grande force des pouvoirs de l'ombudsman réside dans leur nature non coercitive. Stephen Owen a formulé l'observation suivante :

Bien qu'un processus coercitif puisse entraîner la modification à contrecœur d'une décision ou d'une mesure, par définition, une partie devient nécessairement perdante, et il est peu probable que celle-ci adopte les recommandations ultérieurement. En revanche, lorsque la modification résulte d'un processus de raisonnement, elle change la façon de penser et le résultat demeure à l'avantage des plaignants subséquents³²⁴. [traduction]

Comme les décisions prises par les ombudsmans n'entraînent pas d'obligations juridiques, leur flexibilité est supérieure à celle des tribunaux, qui sont assujettis aux règles de droit procédural. Ainsi, les pouvoirs réparateurs des ombudsmans, en apparence restreints, consolident en fait leurs capacités en matière d'enquête et de persuasion.

Le caractère non obligatoire du rôle de l'ombudsman peut également atténuer l'opposition à l'endroit de ses objectifs. Il semble que cette dynamique ait été prise en compte dans le choix du modèle d'ombudsman pour le CPVP. À titre d'ancien commissaire à la protection de la vie privée, Bruce Phillips a précisé ce qui suit dans sa justification concernant le choix du modèle d'ombudsman pour le CPVP :

La raison pragmatique justifiant mon refus d'accorder le pouvoir de rendre des ordonnances réside dans l'hostilité et l'intransigeance que ce pouvoir entraînera presque certainement dans le milieu des affaires. C'est une chose d'entrer en contact avec une entreprise afin de discuter de pratiques inacceptables en matière de protection de la vie privée et de trouver des moyens d'éviter qu'elles ne se reproduisent; c'en est une autre d'entrer en contact avec la même entreprise lorsque ses gestionnaires savent très bien que vous avez le pouvoir de les forcer à coopérer. Dans ce dernier cas, l'entreprise risque fort de sortir l'artillerie lourde — les conseillers juridiques et les experts-conseils — et d'avoir des doutes importants si elle reçoit une demande

324 Stephen Owen, « The Ombudsman: Essential Elements and Common Challenges », dans Linda C. Reif (éd.), *The International Ombudsman Anthology*, The Hague, Kluwer Law International, 1999, p. 51, à la page 52.

visant la discussion, l'examen ou la modification des pratiques utilisées. Le processus s'enlise dans des formalités juridiques et autres, ce qui retarde la résolution de l'enjeu et augmente grandement la frustration du plaignant déjà mécontent³²⁵. [traduction]

M. Phillips a ajouté qu'à son avis, le modèle d'ombudsman ne manque pas de « mordant » puisqu'il permet au CPVP de publiciser très efficacement les questions relatives au traitement inadéquat des renseignements personnels. Autrement dit, le CPVP dispose d'une « voix » pour influencer sur les pratiques dans l'ensemble de l'industrie.

L'intervention du CPVP concernant les mesures de protection de la vie privée de Facebook constitue un exemple concret de cette fonction. Après avoir reçu une plainte de la part de la Clinique d'intérêt public et de politique d'Internet du Canada (CIPPIC), le CPVP a mené une enquête portant sur les mesures de protection de la vie privée soi-disant inadéquates du site de réseautage social, qui a suscité l'intérêt des médias nationaux et internationaux. Le CPVP a mené une enquête sur 24 allégations distinctes et il a trouvé 8 infractions à la *Loi* dans l'exploitation du site de réseautage social Facebook; 4 d'entre elles ont été corrigées au moment de la publication des conclusions, et Facebook s'est vu accorder un délai de 30 jours pour prouver qu'il a mis en œuvre les recommandations énoncées dans le rapport afin de corriger les 4 autres infractions à la *Loi*³²⁶. La publicité entourant cette enquête et le rapport ont permis au CPVP de profiter d'une occasion sans précédent de faire de la sensibilisation au sujet des questions relatives à la protection de la vie privée dans les réseaux sociaux. Michael Geist, professeur de droit à l'Université d'Ottawa, qualifie cette enquête et son issue de grande réussite³²⁷.

Un mois après la publication du rapport de conclusions, le CPVP a publié un communiqué de presse précisant que « Facebook a[vait] accepté d'ajouter de nouvelles mesures de protection des renseignements personnels significatives et d'apporter d'autres modifications à la suite d'une enquête menée par la commissaire à la protection de la vie privée du Canada concernant les politiques

325 Voir la note 322 ci-dessus.

326 Les différentes allégations et conclusions sont présentées dans le *Rapport de conclusions de l'enquête menée à la suite de la plainte déposée par la Clinique d'intérêt public et de politique d'Internet du Canada (CIPPIC) contre Facebook inc. aux termes de la Loi sur la protection des renseignements personnels et les documents électroniques*, 16 juillet 2009, à l'adresse suivante : http://priv.gc.ca/cf-dc/2009/2009_008_0716_f.pdf.

327 Michael Geist, *Facebook Settles Privacy Commissioner of Canada*, 29 août 2009, accessible en ligne à l'adresse suivante : <http://www.michaelgeist.ca/content/view/4330/196/> [en anglais seulement]. Consulter également Michael Geist, « Standing on Guard for Privacy – Before Facebook », *Toronto Star*, 14 septembre 2009, accessible en ligne à l'adresse suivante : <http://www.thestar.com/business/article/695147> [en anglais seulement].

et pratiques en matière de protection des renseignements personnels du populaire site de réseautage social ».

Bien qu'il reste des problèmes quant au respect des principales recommandations concernant le partage excessif de renseignements personnels avec des tiers développeurs des applications de Facebook, comme les jeux et les questionnaires, la commissaire a déclaré qu'elle « considère que Facebook est en bonne voie de combler les lacunes en matière de protection des renseignements personnels sur son site ».

Comme nous l'avons mentionné à la partie 1, les préoccupations sur le plan de la vie privée sont de plus en plus mondiales, et de plus en plus liées aux percées technologiques visant la collecte, l'analyse et la diffusion de renseignements. La commissaire Stoddart formulait l'observation suivante dans son rapport annuel de 2009 concernant la LPRPDE : « Le nombre d'enquêtes marquées par les nouvelles technologies a connu une croissance exponentielle. Il semble clair que les enjeux technologiques auront une influence dominante sur nos travaux pour les années à venir.³²⁸ » En janvier 2010, le CPVP annonçait qu'il se penchait sur le suivi, le profilage et le ciblage en ligne des consommateurs par l'entremise de Facebook et d'autres sites de réseautage social tels MySpace et LinkedIn³²⁹.

Ce virage amènerait également les autorités de protection des données à travailler de concert afin d'être efficaces. En avril 2010, la commissaire s'est jointe à des autorités de protection des données de l'Allemagne, de l'Espagne, de la France, de l'Irlande, d'Israël, de l'Italie, de la Nouvelle-Zélande, des Pays-Bas et du Royaume-Uni afin d'exprimer des inquiétudes significatives au sujet de l'application Buzz, lancée par Google. Cette application était décrite en ces termes :

Essentiellement, vous avez pris Google Mail (Gmail), un service de courriel Web privé de personne à personne, et en avez fait un service de réseautage social, ce qui a soulevé des inquiétudes parmi les utilisateurs quant à la communication de leurs renseignements personnels. Google a attribué automatiquement aux utilisateurs un réseau d'« amis » constitué des personnes avec lesquelles ils communiquent le plus fréquemment, sans informer d'abord de manière adéquate les utilisateurs quant au fonctionnement de ce nouveau service ni leur fournir assez d'information pour leur permettre de donner un consentement éclairé. Attribuer automatiquement aux utilisateurs un réseau d'« amis » constitué des personnes avec lesquelles ils

328 Commissariat à la protection de la vie privée du Canada, Rapport annuel au Parlement 2009, accessible à l'adresse suivante : http://www.priv.gc.ca/information/ar/200910/2009_pipeda_f.pdf (consulté le 2 août 2010).

329 Voir http://www.priv.gc.ca/media/nr-c/2010/nr-c_100601_f.cfm (consulté le 12 juillet 2010).

communiquent le plus fréquemment va à l'encontre du principe fondamental selon lequel les personnes doivent pouvoir contrôler l'utilisation faite de leurs renseignements personnels.³³⁰

Les signataires de la lettre en ont appelé à Google (et aux autres entreprises de réseautage social) d'intégrer des mesures de protection de la vie privée à même leurs services en ligne, y compris la collecte du moins de renseignements personnels possible, et de faire en sorte que les mesures de protection de la vie privée soient disponibles, évidentes et faciles à régler.

En juin 2010, le Commissariat a lancé une enquête distincte de l'initiative Street View de Google, dans le cadre de laquelle des voitures-caméras saisissaient des images à l'échelle de la rue dans les zones urbaines du Canada. Google a signalé qu'elle avait également recueilli des données portant sur les réseaux Wi-Fi en présence dans les endroits sillonnés par ses voitures-caméras, afin d'améliorer ses services géodépendants. La commissaire Stoddart a déclaré ce qui suit :

Nous avons de sérieuses inquiétudes quant aux conséquences pour la vie privée qui découlent de la confirmation par Google que des données Wi-Fi ont été capturées dans des quartiers canadiens et partout au monde ces dernières années. Nous avons un certain nombre de questions, à savoir comment une telle collecte a-t-elle pu se produire et quel sera l'impact sur la vie privée des personnes. Nous avons déterminé qu'une enquête est le meilleur moyen d'obtenir des réponses.³³¹

Dans ses démarches auprès de multinationales du domaine de la technologie telles que Google ou Facebook, l'attention des médias est tout aussi important pour l'efficacité du CPVP que ne le serait tout pouvoir de réglementation que le Commissariat pourrait tenter d'exercer auprès de ces entreprises.

L'enquête sur Facebook de 2009 a été un moment tournant pour le CPVP, non pas en raison de l'enquête elle-même, mais bien à cause de l'attention médiatique mondiale que cette enquête a suscité et, peut-être encore davantage, en raison de l'appui populaire que cette couverture médiatique est venue refléter et attiser.

330 « Lettre au chef de la direction de Google », accessible à l'adresse suivante : http://www.priv.gc.ca/media/nr-c/2010/let_100420_f.cfm (consulté le 12 juillet 2010).

331 La commissaire à la protection de la vie privée mène une enquête sur la collecte des données Wi-Fi par Google (le 1^{er} juin 2010), accessible à l'adresse suivante : http://www.priv.gc.ca/media/nr-c/2010/nr-c_100601_f.cfm.

Cependant, la capacité à attirer l'attention du public et, par le fait même, à l'exploiter est la seule caractéristique faisant en sorte que le modèle actuel du CPVP a du mordant. Comme le prouvent les exemples de Facebook et de Google, le commissaire dispose d'une gamme d'outils de conformité afin de s'acquitter de son mandat en ce qui a trait à la LPRPDE :

- examiner les plaintes et publier des rapports contenant des recommandations adressées aux institutions fédérales et à des organisations du secteur privé pour remédier à des situations, s'il y a lieu;
- intenter des poursuites devant la Cour fédérale lorsque les questions ne sont toujours pas réglées;
- évaluer le respect des obligations énoncées dans la *Loi sur la protection des renseignements personnels* et la LPRPDE en menant des activités indépendantes de vérification et d'examen, et en publiant les conclusions;
- examiner les évaluations des facteurs relatifs à la vie privée (EFVP) des initiatives gouvernementales nouvelles et existantes et donner des conseils en la matière;
- fournir des analyses juridiques et stratégiques et l'expertise nécessaire pour guider le Parlement dans son examen des lois en constante évolution afin d'assurer le respect du droit des personnes à la protection de la vie privée;
- répondre aux demandes des parlementaires, des Canadiennes et des Canadiens et des organisations qui veulent obtenir des renseignements et des directives et prendre les mesures proactives nécessaires pour les informer des questions émergentes concernant la protection de la vie privée;
- promouvoir la sensibilisation du grand public et le respect des lois, favoriser la compréhension des droits et obligations en matière de protection de la vie privée par l'entremise de la participation proactive des institutions fédérales, des associations industrielles, de la communauté juridique, des universitaires, des associations professionnelles et d'autres intervenants; préparer et publier des documents d'information publique, des positions sur les lois nouvelles, les règlements et les politiques, des documents d'orientation et les conclusions de recherche que pourront utiliser le grand public, les institutions fédérales et les organisations du secteur privé;
- fournir des opinions juridiques et entamer des poursuites pour faire avancer l'interprétation et l'application des lois fédérales sur la protection des renseignements personnels;
- surveiller les tendances relatives aux pratiques en matière de protection de la vie privée, repérer les enjeux systémiques en la matière qui doivent être abordés par les institutions fédérales et les organisations du secteur privé et promouvoir l'intégration des pratiques exemplaires;
- travailler en collaboration avec les intervenants œuvrant dans le domaine de la protection de la vie privée dans les provinces et territoires au Canada ainsi que sur la scène internationale pour aborder les enjeux internationaux relatifs à la protection de la vie privée qui

résultent de la circulation transfrontalière de plus en plus grande des données³³².

De plus, le Commissariat dispose d'une variété d'outils et de pouvoirs en vertu de la LPRPDE, dont des rapports, des recherches, la sensibilisation du public, les enquêtes relatives aux plaintes et les vérifications. La commissaire Stoddart, qui décrivait la façon dont elle utilise le modèle d'ombudsman dans le contexte de la LPRPDE, a tenu les propos suivants :

Plus qu'un moyen de trouver des solutions rémédiatrices, les fonctions de l'ombudsman constituent un moteur de changement et d'amélioration. L'objectif consiste bien sûr à résoudre les plaintes mais aussi à établir, grâce à la volonté et à la participation des parties concernées, une culture durable de conscientisation à la protection de la vie privée. Pour atteindre ce but, il faut donc que le processus soit souple, qu'il favorise la participation et qu'il soit adapté à chacun.

Comment est-il possible d'évaluer l'efficacité du Commissariat en ce qui concerne l'atteinte de ces buts jumelés? Bien qu'il existe toujours un élément subjectif dans le choix des critères d'évaluation, compte tenu du mandat, de la mission, des activités et des pouvoirs du CPVP, ainsi que des buts généraux du modèle d'ombudsman, certains types de mesures objectives semblent convenir davantage à ce contexte, y compris, sans s'y limiter, les suivants :

- 1) le niveau d'activité du Commissariat (p. ex. le nombre d'enquêtes ou de vérifications effectuées au cours d'une année particulière ou le nombre d'actions judiciaires entamées à la Cour fédérale);
- 2) l'incidence des activités du Commissariat sur le comportement des organisations du secteur privé, y compris les changements mesurables dans la culture organisationnelle, la prévention des conflits, etc.;
- 3) le degré de satisfaction des plaignants et la confiance des personnes visées par les plaintes en ce qui concerne l'impartialité du processus du Commissariat;
- 4) la réputation du Commissariat au sein de l'industrie, de la clientèle et des autres groupes touchés;
- 5) la facilité d'accès pour le public (p. ex. coût et commodité) et le degré de visibilité du Commissariat auprès des plaignants possibles;
- 6) la contribution du Commissariat à la sensibilisation du public et aux mesures visant à leur faire comprendre leurs droits aux termes de la LPRPDE (y compris la couverture médiatique des enquêtes et des rapports, les visiteurs du site Web du CPVP, les initiatives de sensibilisation du public financées par le Commissariat, etc.).

332 Ces renseignements proviennent du site Web du Commissariat à la protection de la vie privée du Canada.

Les critères énoncés ci-dessus sont axés sur les mesures empiriques servant à évaluer la mesure dans laquelle le CPVP atteint ses objectifs prévus par la loi et les politiques. Cependant, si la recherche empirique vise à évaluer l'efficacité du modèle d'ombudsman, le rendement du Commissariat devrait également être comparé à celui d'organismes de réglementation de la vie privée homologues. Par exemple, la comparaison de la réputation et de la réussite du CPVP quant à la modification des comportements avec celles d'autres organismes de protection de la vie privée, ou d'organismes de réglementation homologues dans d'autres domaines, qui disposent du pouvoir de rendre des ordonnances et d'imposer des obligations, pourrait constituer le fondement des conclusions concernant la réussite et l'efficacité relatives du modèle d'ombudsman.

Que le CPVP soit comparé à des organismes de réglementation de la protection de la vie privée homologues ou à d'autres types d'organismes de réglementation, il est évident que, pour être jugée sérieuse, l'évaluation du CPVP devra être effectuée d'un point de vue interne et comparatif. Nous nous pencherons désormais sur l'élaboration de ces points de vue.

Section 2. Les pouvoirs du commissaire à la protection de la vie privée du Canada en ce qui a trait à la LPRPDE par opposition à ceux des organismes de réglementation provinciaux et de certains organismes de réglementation internationaux choisis de même qu'aux organismes de surveillance homologues

Au cours des trente dernières années, les lois sur la protection des données se sont propagées à l'échelle mondiale, et on les considère maintenant à titre d'outils essentiels pour la réglementation de l'utilisation des données personnelles de même qu'à titre de fondement pour le travail des organismes de réglementation qu'elles créent. Tout récemment, la modification législative la plus notoire a été effectuée en Europe, alors que les pays en voie de démocratisation rédigent des lois sur la protection de la vie privée et que les pays dotés de lois modifient les régimes de protection des données afin de se conformer à la Directive de l'Union européenne. Au Canada, bien que nous ayons des lois sur la protection des données et des commissaires indépendants à la protection de la vie privée en place depuis longtemps, nous n'avons que tout récemment élargi cette protection au secteur privé de la manière dictée par notre système constitutionnel fédéral.

Dans le cadre de l'accroissement et de la réforme des lois sur la protection de la vie privée d'un pays, l'établissement de solides pouvoirs de surveillance s'est avéré essentiel. Les bonnes lois à elles seules sont peu susceptibles d'être mises en œuvre de façon adéquate et n'arrivent pas à favoriser une culture de la vie privée³³³. Malgré l'importance de solides pouvoirs de réglementation, Colin Bennett et Charles Raab ont fait valoir qu'un pouvoir de réglementation

333 Colin J. Bennett et Charles D. Raad, *supra*, note 74, p. 107.

actif et assertif ne constitue qu'un facteur identifiable servant à mesurer l'efficacité d'un système de protection des données. Bennett et Raab font valoir qu'un bon régime de protection de la vie privée doit également être associé à ce qui suit : 1) une loi solide et claire; 2) des procédures d'exécution efficaces destinées aux responsables de la cueillette des données; 3) des incitatifs au sein du marché afin de favoriser la conformité du secteur privé; 4) une population vigilante et intéressée; 5) une utilisation accrue des technologies visant à améliorer la protection de la vie privée³³⁴.

Bennett et Raab avancent également que, bien qu'un commissaire à la protection de la vie privée et des données puisse agir à titre d'ombudsman, il le fait en association avec ses rôles de vérificateur, de consultation, d'éducateur, de négociateur, de conseiller en politiques et d'exécuteur³³⁵. Une autorité indépendante en matière de protection des données doit donc assurer un équilibre entre un large éventail de rôles, et l'évaluation de son rendement quant à tous ces volets est une entreprise nécessairement complexe. Néanmoins, une telle évaluation est importante à la fois en vue d'une réforme institutionnelle et dans la quête d'un niveau optimal de sécurité des données. Par conséquent, le point de départ d'une évaluation de l'efficacité du régime de protection de la vie privée d'un pays constitue l'analyse intergouvernementale.

2.1. Organismes provinciaux de protection de la vie privée

Les régimes de protection de la vie privée à l'échelle mondiale ont adopté diverses approches de surveillance de l'exécution de leurs lois sur la protection des données ou de la vie privée. Les autorités en matière de protection des données peuvent suivre le modèle d'octroi de licences (p. ex. Suède), le modèle d'enregistrement (p. ex. le R.-U. en vertu des lois de 1984), le modèle du commissaire (p. ex. Allemagne) et le modèle de l'autoprotection (p. ex. É.-U.), bien que la plupart des pays soient dotés d'un système hybride au sein duquel un de ces modèles prédomine³³⁶. Selon les pays, des responsables, un commissaire, un ombudsman ou un greffier auxquels des pouvoirs variés ont été conférés peuvent surveiller la réglementation en matière de vie privée. Le Canada est doté d'un régime de protection de la vie privée particulièrement complexe étant donné que les gouvernements fédéral et provinciaux ont adopté des lois et habilité des organismes de surveillance afin de protéger la vie privée.

Bien que la LPRPDE ait été mise en œuvre par étapes à partir de janvier 2001, les provinces pouvaient choisir de ne pas l'appliquer aux activités commerciales dans les secteurs de réglementation provinciale en adoptant des lois « essentiellement similaires ». Malgré que l'ensemble des provinces et des territoires canadiens soient dotés de lois sur la protection des données du secteur public et de lois sur la protection de la vie privée propres à certains

334 *Id.*, p. 207.

335 *Id.*, p. 109.

336 *Id.*, p. 107.

secteurs (p. ex. lois régissant les soins de santé), il n'en est pas de même pour les lois sur la protection de la vie privée réglementant le secteur privé. Au moment de la mise en œuvre de la LPRPDE, le Québec était la seule province dotée de lois sur la protection de la vie privée essentiellement similaires; toutefois, l'Alberta et la Colombie-Britannique ont toutes deux mis en œuvre les leurs avec succès.

En janvier 2004, la Colombie-Britannique et l'Alberta ont toutes deux adopté une loi, la *Personal Information Protection Act* (PIPA); les deux versions de la loi sont très similaires étant donné qu'elles ont été élaborées en vertu d'un processus commun³³⁷. Bien que de telles lois infranationales créent un régime de protection de la vie privée beaucoup plus complexe, le Canada n'est pas le seul pays à adopter des règlements sur la protection de la vie privée qui se chevauchent. Divers États des États-Unis et de l'Australie de même que des Länder de l'Allemagne ont adopté des régimes de protection de la vie privée nationaux et infranationaux similaires. Dans le cadre de l'évaluation des différences entre les ombudsmans provinciaux chargés des questions relatives à la protection de la vie privée et le commissaire fédéral à la protection de la vie privée, il apparaît évident que, bien que les commissariats provinciaux soient grandement similaires à celui du commissariat fédéral, les ombudsmans provinciaux ont de plus grands pouvoirs d'exécution. De plus, la tendance générale au sein des ombudsmans canadiens en matière de protection de la vie privée et du commissaire à l'information du Royaume-Uni (qui vient de subir d'importantes réformes structurelles fondamentales) consiste à étendre les pouvoirs de surveillance en matière de vie privée au secteur privé, ce qui donnerait aux ombudsmans des outils afin de traiter de questions de plus en plus complexes et envahissantes touchant la protection de la vie privée.

2.2. La Commission d'accès à l'information du Québec

À une époque où les questions relatives à la protection des renseignements personnels dans le secteur privé du Canada étaient régies par un système d'autoréglementation, le Québec avait adopté les règles les plus strictes de l'Amérique du Nord en matière de protection de la vie privée³³⁸. Dans la *Loi sur la protection des renseignements personnels dans le secteur privé* (la loi régissant le secteur privé au Québec), en vigueur depuis 1994, quatre principes clés sont énoncés en vue d'orienter la réglementation des renseignements personnels :

1. Une personne ou une société doit avoir une raison sérieuse et légitime de créer un dossier sur une personne;

337 Colin J. Bennett et Robin M. Bayley, « Video Surveillance and Privacy Protection Law in Canada », dans Sjaak Nouwt, Berend R. de Vries et Corien Prins (éd.), *La Haye, Asser Press*, 2005, p. 65.

338 Vagelis Papakonstantinou, « Self-Regulation and the Protection of Privacy », Baden-Baden, *Nomos Verlagsgesellschaft*, 2001, p. 127.

2. Tous ont le droit d'accéder à leur dossier, à moins que les droits des tiers doivent être protégés ou qu'il y ait un motif sérieux de refuser l'accès;
3. Tous ont le droit de rectifier un dossier incorrect, incomplet ou désuet;
4. Toute personne ou société qui ouvre un dossier sur une personne est tenue à la confidentialité.

Au Québec, la Commission d'accès à l'information (CAI) supervise l'application de la loi du secteur privé et celle du secteur public, la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* de 1982. En décembre 2003, au moment où le Canada se préparait à mettre en œuvre la LPRPDE au sein du secteur privé, la loi du Québec en matière de protection de la vie privée avait été jugée essentiellement similaire à la loi fédérale à venir.

La CAI a trois principales fonctions. En premier lieu, elle joue un rôle juridique étant donné qu'elle examine la décision des autorités publiques de refuser l'accès de particuliers à des documents administratifs ou à leur dossier personnel. La loi québécoise régissant le secteur privé autorise de plus la CAI à régler les mécontentes relatives à la protection des renseignements personnels dans le secteur privé. La CAI tient des audiences uniquement lorsque la médiation n'a pas suffi et émet des conclusions de fait obligatoires; les questions de droit ou de compétence peuvent être portées en appel devant la Cour du Québec. En deuxième lieu, la CAI joue un rôle de supervision et surveille le respect des règlements sur la sécurité des données dans les secteurs public et privé. En troisième lieu, la CAI joue un rôle de conseiller afin de veiller au respect de l'esprit et de la formulation des lois du Québec en matière de protection de la vie privée.

Le 14 juin 2006, l'Assemblée nationale du Québec a adopté le projet de loi 86 (*Loi modifiant la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels et d'autres dispositions législatives*³³⁹), qui a modifié la structure de la CAI en la scindant en deux unités : la section de surveillance et la section juridictionnelle. Les modifications ont été apportées à la suite du 4^e examen quinquennal de la CAI³⁴⁰. Cette réforme a été entreprise en réponse aux critiques voulant que la CAI avait mis son indépendance et son impartialité en jeu en permettant au même groupe de membres de la CAI de

339 Assemblée nationale du Québec, « *Loi modifiant la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels et d'autres dispositions législatives* », 14 juin 2006, <http://www2.publicationsduquebec.gouv.qc.ca/dynamicSearch/telecharge.php?type=5&file=2006C22F.PDF>.

340 Les changements constituaient également une réponse à l'interprétation de la Cour suprême à l'égard de la protection de l'indépendance et de l'impartialité pour les arbitres contenue dans la *Charte des droits et libertés de la personne* du Québec — voir *2747-3174 Québec Inc. c. Québec (Régie des permis d'alcool)*, [1996] 3 R.C.S. 919 (1996).

statuer et d'exécuter ses pouvoirs de surveillance. Par conséquent, la section de surveillance supervise dorénavant le respect de la loi québécoise visant le secteur privé et la section juridictionnelle règle les mécontentements relatives à l'accès ou aux modifications des renseignements personnels d'une personne.

La CAI s'est montrée critique à l'égard de ces changements structurels et a fait valoir qu'en interdisant tout chevauchement de personnel entre la section de surveillance et la section juridictionnelle, la Commission de la culture de l'Assemblée nationale privait la CAI de sa polyvalence et de sa capacité à atteindre ses objectifs³⁴¹. Le projet de loi 86 comprenait des changements supplémentaires à la loi québécoise régissant le secteur privé qui resserraient le contrôle de la circulation transfrontalière des données, mais ceux-ci ont peu d'incidence sur la structure administrative de la CAI. Les réformes du projet de loi 86 sont entrées en vigueur de façon graduelle entre le 14 juin 2006 et le 14 septembre 2007.

Dans le cadre d'une étude commandée par le CPVP, « Leçons tirées de dix ans d'expérience : la *Loi sur la protection des renseignements personnels dans le secteur privé du Québec* », M^e Karl Delwaide et M^e Antoine Aylwin traitent des caractéristiques distinctives de la loi québécoise régissant le secteur privé. Ils soulignent le fait que l'harmonisation de la protection des données ne signifie pas que toutes les administrations doivent être similaires.

L'expérience du Québec démontre que l'indépendance et l'impartialité, à titre de normes administratives essentielles, offrent les fondements sur lesquels se fondent la conception institutionnelle et la recherche du modèle optimal.

2.3 Le Commissariat à l'information et à la protection de la vie privée de l'Alberta

En mai 2003, l'Alberta a adopté des lois en matière de protection de la vie privée essentiellement similaires à la LPRPDE par l'entremise du projet de loi 44, la *Personal Information Protection Act* (PIPA). Depuis janvier 2004, le commissaire à l'information et à la protection de la vie privée de l'Alberta est responsable de superviser la PIPA. Le Commissariat a été mis sur pied en 1995 étant donné que le commissaire a également compétence sur la *Freedom of Information and Protection of Privacy Act* (FOIP Act) et la *Health Information Act* (HIA). Le commissaire est responsable de ce qui suit :

- Renseigner les Albertains au sujet des lois actuelles et proposées en matière de protection de la vie privée;

341 Commission d'accès à l'information, « La Commission d'accès à l'information se réjouit des mesures de divulgation automatique de l'information annoncées dans le Projet de loi 86 mais s'inquiète de l'affaiblissement des règles de protection des renseignements personnels [...] », 13 septembre 2005, accessible en ligne à l'adresse suivante : http://www.cai.gouv.qc.ca/05_communiques_et_discours/commun_13_09_05.html.

- Émettre des commentaires quant aux conséquences des lois et programmes proposés sur la protection de la vie privée et les renseignements personnels;
- Examiner les décisions relatives à l'accès à l'information prises par les organismes publics, gardiens, organisations et agences régis par la FOIP *Act*, la HIA ou la PIPA;
- Examiner la façon dont les renseignements personnels sont recueillis, utilisés et communiqués afin de veiller au respect de la FOIP *Act*, de la HIA ou de la PIPA;
- Recevoir les commentaires du public au sujet de l'administration de chacune des lois;
- Tenter de trouver tout facteur qui pourrait avoir une incidence sur l'atteinte des objectifs de la FOIP *Act*, de la HIA ou de la PIPA;
- Émettre conseils et recommandations au sujet des lois aux responsables des organismes publics, gardiens et organisations.

Le Commissariat collabore avec les intervenants afin d'éduquer le public, les organisations et les agences assujettis aux lois en matière de protection de la vie privée par l'entremise de la participation dans la communauté, notamment des présentations, la production de documents de sensibilisation dont des guides écrits, des dépliants et des messages d'intérêt communautaire, le parrainage de programmes d'éducation offerts par les établissements d'éducation provinciaux comme l'Université de l'Alberta ou encore le parrainage de conférences de l'industrie³⁴².

L'Alberta a récemment révisé la PIPA. Le 26 mai 2006, l'assemblée législative de l'Alberta a créé un comité spécial composé de toutes les parties, comme l'exige l'article 63 de la PIPA. La révision législative de l'Alberta a été effectuée au moment où la Colombie-Britannique procédait à l'examen de sa propre loi régissant le secteur privé (abordée ci-dessous). Le comité d'examen de la PIPA de l'Alberta a reçu 65 mémoires et entendu 10 présentations orales des Albertains et de diverses organisations, dont le Commissariat à l'information et à la protection de la vie privée, Service Alberta et le comité consultatif sur la PIPA.

Le rapport final du comité a été présenté à l'assemblée législative de l'Alberta le 14 novembre 2007 et comprend 39 recommandations³⁴³. Les principales recommandations sont les suivantes :

342 Commissariat à l'information et à la protection de la vie privée de l'Alberta, <http://www.oipc.ab.ca/pages/About/Commissioner.aspx> [en anglais seulement].

343 Comité spécial d'examen de la *Personal Information Protection Act*, « Review of the *Personal Information Protection Act* », Edmonton, assemblée législative de l'Alberta, 2007, accessible en ligne à l'adresse suivante : www.assembly.ab.ca/committees/reports/PIPA/finalpipawReport111407.pdf [en anglais seulement].

- Exiger des organisations qu'elles informent les personnes au sujet de la circulation transfrontalière de leurs renseignements personnels;
- Créer une nouvelle obligation de déclaration des atteintes à la protection des renseignements personnels;
- Inclure toutes les organisations sans but lucratif dans la portée de la loi;
- Offrir une protection pour les renseignements personnels relatifs à la santé en vertu de la HIA plutôt que de la PIPA;
- Clarifier les règles régissant les renseignements personnels des employés;
- Réviser les dispositions relatives au consentement afin de mieux traiter des pratiques commerciales de longue date;
- Établir des délais pour la conservation des renseignements personnels;
- Élaborer de nouvelles dispositions relatives aux infractions;
- Établir des normes plus appropriées en vue d'intenter des poursuites;
- Rationaliser les processus relatifs au commissaire et clarifier les pouvoirs.

En ce qui a trait à la dernière recommandation demandant un changement institutionnel au sein du Commissariat à la protection de la vie privée, le comité a recommandé trois modifications principales à la PIPA. Premièrement, le comité a recommandé de modifier la PIPA afin de conférer au commissaire le pouvoir explicite de mettre un terme à une enquête ou à un examen lorsqu'il est d'avis que la plainte ou la demande d'examen n'est pas justifiée ou qu'il n'y a pas suffisamment de preuves pour procéder. Deuxièmement, le comité a recommandé de modifier la PIPA de sorte que le commissaire puisse demander à obtenir des renseignements protégés par le secret professionnel sans affecter celui-ci. Troisièmement, le comité a recommandé d'ajouter une disposition à la PIPA afin de permettre au commissaire de communiquer des renseignements relatifs à une infraction, du moment que ceux-ci ne sont pas visés par le secret professionnel.

Ainsi, le comité a recommandé que les pouvoirs et la discrétion du commissaire soient élargis. Toutefois, aucune recommandation voulant que le rôle d'ombudsman du commissaire soit modifié de façon fondamentale n'a été émise. L'exemple de l'Alberta démontre donc qu'un modèle d'ombudsman peut coexister avec un éventail de mesures d'exécution et de conformité et les compléter.

2.4 Le Commissariat à l'information et à la protection de la vie privée de la Colombie-Britannique

En mars 2003, la Colombie-Britannique a adopté des lois sur la protection de la vie privée essentiellement similaires à la LPRPDE par l'entremise du projet de loi 38, la *Personal Information Protection Act* (PIPA). Le Commissariat à l'information et à la protection de la vie privée supervise et exécute les lois sur la protection de la vie privée de la Colombie-Britannique régissant le secteur public, la *Freedom of Information and Protection of Privacy Act* (FIPPA) et la PIPA. Les pouvoirs et responsabilités du Commissariat sont les suivants :

- Enquêter et régler les plaintes alléguant que des renseignements personnels ont été recueillis, utilisés ou communiqués par une organisation en violation de la PIPA;

- Entamer les enquêtes et les vérifications afin de veiller au respect de la PIPA, s'il est d'avis qu'il y a des motifs raisonnables de croire qu'une organisation ne respecte pas la loi, ce qui comprend le fait de prononcer des ordonnances exécutoires;
- Informer le public au sujet de la PIPA;
- Réaliser ou commander les recherches relatives à tout ce qui nuit à l'atteinte des objectifs de la PIPA;
- Émettre des commentaires sur les répercussions des programmes, systèmes automatisés ou du couplage des données proposés par les organisations sur la vie privée;
- Autoriser la collecte de renseignements personnels à partir de sources autres que les personnes visées;
- Enquêter et régler les plaintes selon lesquelles une obligation en vertu de la PIPA n'a pas été respectée, qu'une prolongation d'un délai a été prise de manière inappropriée, que des honoraires sont déraisonnables ou qu'une demande de correction a été refusée sans justification³⁴⁴.

Comme il est mentionné ci-dessus, le Colombie-Britannique a récemment révisé la PIPA. Le comité spécial d'examen de la *Personal Information Protection Act*, présidé par Ron Cantelon, a produit un rapport sur l'examen réglementaire intitulé « Streamlining British Columbia's Private Sector Privacy Law » le 17 avril 2008³⁴⁵. L'article 59 de la PIPA de la Colombie-Britannique exige que la loi soit examinée dans les trois années suivant son entrée en vigueur, puis tous les six ans par la suite. Le comité a reçu 31 mémoires écrits, principalement de l'industrie et d'associations professionnelles de même que de particuliers. Le Commissariat a entendu 12 autres présentations orales d'organisations et de particuliers dans le cadre d'audiences publiques tenues à Victoria et à Vancouver.

Lorsque le rapport a été publié, un porte-parole de McCarthy Tétrault a saisi l'incidence sur le secteur privé en concluant qu'il y avait eu un « léger ajustement par rapport aux lois actuelles », ce qui reflétait « la perception selon laquelle la loi est efficace tant à l'égard des individus qu'à l'égard des organismes³⁴⁶ ». Néanmoins, le comité s'est montré critique à l'égard du manque

344 « OIPC's Role and Mandate », www.oipc.bc.ca/pdfs/public/OIPC-Role-and-Mandate.pdf [en anglais seulement].

345 Comité spécial d'examen de la *Personal Information Protection Act*, « Streamlining British Columbia's Private Sector Privacy Law », Victoria, Assemblée législative de la Colombie-Britannique, 2008, <http://www.leg.bc.ca/cmt/38thparl/session-4/pipa/> [en anglais seulement].

346 Cappone D'Angelo, « Un comité recommande des modifications à la loi de la Colombie-Britannique sur la protection de la vie privée dans le secteur privé », McCarthy Tétrault, 8 août 2008, http://www.mccarthy.ca/fr/article_detail.aspx?id=4101.

de sensibilisation du public quant à l'objet, aux règles et à la portée de la loi³⁴⁷. Le comité a émis 31 recommandations au total dans le but d'harmoniser les pratiques à celles des organismes de réglementation fédéraux et provinciaux et de veiller à l'efficacité continue de la PIPA. Parmi les recommandations clés se trouvent les suivantes :

- Rendre les organisations du secteur privé responsables des renseignements personnels qu'elles transfèrent en vue d'un traitement à l'extérieur du Canada;
- Exiger des organisations qu'elles avisent les personnes visées lorsqu'il y a atteinte à la protection des renseignements personnels dans certaines circonstances;
- Interdire l'utilisation des formulaires de consentement général par les institutions financières sous réglementation provinciale;
- Réviser les exceptions relatives au consentement afin de mieux traiter des pratiques commerciales de l'industrie de l'assurance;
- Permettre la communication des coordonnées personnelles à des fins de recherche en santé;
- Exiger les frais minimaux pour l'accès aux renseignements personnels;
- Rationnaliser le processus de plaintes dans les lois provinciales en matière de protection de la vie privée;
- Renforcer les pouvoirs de surveillance du commissaire à l'information et à la protection de la vie privée.

En ce qui a trait à la recommandation finale voulant que des changements institutionnels soient apportés au Commissariat à la protection de la vie privée, le comité a recommandé deux principales modifications à la PIPA (recommandations 27 et 29). En premier lieu, le comité a recommandé de modifier la PIPA afin de conférer au commissaire le pouvoir explicite de mettre fin à une enquête ou à un examen lorsqu'il est d'avis que la plainte ou la demande d'examen est sans fondement ou lorsqu'il n'y a pas suffisamment de preuves pour procéder. En deuxième lieu, le comité a recommandé de modifier la PIPA de manière à clarifier le fait qu'il est à la discrétion du commissaire de ne pas répondre à une demande de renseignements dans certaines circonstances, et qu'il a le pouvoir de déterminer, de façon raisonnable, son propre processus de sorte qu'il puisse contrôler les délais associés à ses demandes. Ainsi, le processus d'examen de la Colombie-Britannique a donné lieu à des recommandations très similaires à celles du comité d'examen de l'Alberta.

Comme pour l'Alberta, le comité de la Colombie-Britannique a recommandé que les pouvoirs et la discrétion du commissaire soient élargis, bien qu'il n'ait pas suggéré que le rôle d'ombudsman du commissaire soit modifié de façon substantielle.

347 Assemblée législative de la Colombie-Britannique, « Special Committee recommends changes to streamline B.C.'s private-sector privacy law », 17 avril 2008, accessible en ligne à l'adresse suivante : <http://www.leg.bc.ca/> [en anglais seulement].

Le fait que le modèle d'ombudsman en ce qui a trait à la compétence du Commissariat relativement au secteur privé ait été bien reçu par les administrations provinciales ne signifie pas qu'il est des plus efficaces, mais fait état de son attrait général et de la perception globale positive à son égard.

2.5 Comparaison des règlements provinciaux et fédéraux en matière de protection de la vie privée

La LPRPDE et les lois du Québec, de la Colombie-Britannique et de l'Alberta en matière de protection de la vie privée diffèrent dans certains domaines clés³⁴⁸. Tandis que les règles de la LPRPDE sont généralement fondées sur le consentement, les lois provinciales définissent les obligations en la matière selon certains domaines précis comme les renseignements sur les employés et les transactions commerciales. De plus, les lois de la Colombie-Britannique et de l'Alberta contiennent une disposition d'antériorité qui exclut les renseignements recueillis par le secteur privé avant que la loi ne soit entrée en vigueur des exigences relatives au consentement. En outre, ces lois n'exigent pas d'obtenir le consentement pour la collecte, l'utilisation et la communication des renseignements personnels d'un employé, du moment qu'elle est faite à des fins « raisonnables », tandis que la LPRPDE ne fait pas de distinction entre les renseignements personnels recueillis à des fins d'emploi ou de commerce.

En ce qui a trait aux pouvoirs institutionnels, les commissaires à la protection de la vie privée du Québec, de l'Ontario, de la Colombie-Britannique, l'Alberta et du gouvernement fédéral sont dotés des mêmes pouvoirs d'enquête et de médiation, et ont la capacité partagée de déposer des plaintes et de mener des vérifications. La principale différence entre les pouvoirs de ces commissaires provinciaux et ceux du commissaire fédéral à la protection de la vie privée est que les premiers ont le pouvoir ajouté de prendre des décisions finales afin de résoudre les différends relatifs aux plaintes, sous réserve d'un contrôle judiciaire³⁴⁹.

Ces commissaires provinciaux ont plus de pouvoirs exécutoires, ce qui leur permet de mener des enquêtes et d'ordonner aux organisations de prendre les mesures nécessaires afin de se conformer aux lois provinciales en matière de protection de la vie privée. Ce que certains pourraient appeler le modèle de l'« ombudsman avec un bâton » semble être le plus efficace lorsqu'il sert de moyen de dissuasion plutôt que de moyen d'obliger le respect des lois sur la

348 Le Commissariat à l'information et à la protection de la vie privée de l'Alberta a créé un tableau utile comparant les divers volets de la LPRPDE à ceux de la PIPA de l'Alberta et de la Colombie-Britannique : Access and Privacy Service Alberta, « PIPA Compared », 2008, accessible en ligne à l'adresse suivante : <http://pipa.alberta.ca/legislation/pdf/PIPAcompared.pdf> [en anglais seulement].

349 Gérard V. La Forest, « Les commissariats à l'information et à la protection de la vie privée : fusion et questions connexes », Ottawa, ministère de la Justice Canada, 2005, paragr. III, accessible en ligne à l'adresse suivante : <http://www.justice.gc.ca/fra/ip/index.html>.

protection de la vie privée, étant donné que les commissaires ont tendance à préférer régler les plaintes par l'entremise de la conciliation, de la médiation et des mesures informelles³⁵⁰. Il sera important de valider cette allégation.

En Colombie-Britannique par exemple, le Commissariat à l'information et à la protection de la vie privée reçoit environ 200 plaintes chaque année, mais a dû prononcer des ordonnances uniquement dans quelques cas au cours des cinq premières années (2004-2009) (entre 15 et 20 affaires se sont traduites par des demandes officielles). Bien que ce nombre soit important, il est sujet à l'interprétation. Est-ce que le manque de recours à des ordonnances prouve leur nécessité, afin d'encourager le règlement et d'empêcher la non-conformité aux obligations réglementaires, ou est-ce que la même statistique prouve qu'elles ne sont pas nécessaires, étant donné le rare nombre de fois où elles sont invoquées?

À tout le moins, l'expérience des administrations provinciales canadiennes au sein desquelles les obligations similaires et conformes à la LPRPDE sont associées à des responsables de la réglementation qui ont un pouvoir de rendre des ordonnances est instructive. L'expérience de ces provinces démontre par exemple que les entreprises peuvent s'adapter à un environnement réglementaire qui comprend des ordonnances sans problèmes importants. L'expérience du Québec, de l'Alberta et de la Colombie-Britannique est instructive à un autre égard également : toutes ces provinces ont eu la chance d'observer le modèle d'ombudsman du CPVP et, dans le cadre d'examen réglementaires récents, aucune d'entre elles n'a suggéré d'adopter le modèle fédéral. Dans chacun des cas, les examens considéraient les pouvoirs supplémentaires à titre de partie intégrante d'une loi de « deuxième génération » en matière de protection de la vie privée.

2.6 Commissariat à l'information du Royaume-Uni

Le Commissariat à l'information du Royaume-Uni est un organisme officiel indépendant nommé par la Reine qui exécute et met à jour le registre de la *Data Protection Act* (DPA) de 1998 et de la *Freedom of Information Act* (FIA) de 2000. Contrairement au Canada où le Commissariat à la protection de la vie privée et le Commissariat à l'information sont distincts, le commissaire à l'information du Royaume-Uni est un seul et même ombudsman. Le commissaire à l'information tend à promouvoir l'accès du public à l'information officielle et à protéger les renseignements personnels, et est supervisé par les tribunaux et l'Information Tribunal dans la réalisation de sa mission.

La DPA régit l'utilisation des renseignements personnels, qu'ils soient traités par les autorités publiques ou par des organisations privées. Ainsi, le commissaire à l'information a établi des normes de traitement des données de même qu'un système de notification associé à des sanctions pénales lorsque

350 Voir Groupe d'étude de l'accès à l'information, *Accès à l'information : comment mieux servir les Canadiens*, Ottawa, Travaux publics et Services gouvernementaux, 2002.

les organisations qui traitent des renseignements personnels ne répondent pas aux normes. Cette information est publiée dans un registre de contrôleurs des données à des fins d'examen public. Les personnes qui croient que leurs droits ont été violés en vertu de la DPA peuvent déposer une plainte devant le commissaire à l'information qui peut effectuer ce qui suit :

- Entreprendre des évaluations afin de vérifier si les organisations respectent la loi;
- Émettre des avis d'information exigeant des organisations qu'elles transmettent au Commissariat les renseignements visés dans un certain délai;
- Émettre des avis d'exécution et des ordonnances de « cesser immédiatement » lorsqu'il y a eu infraction à la loi en vue d'exiger des organisations qu'elles prennent (ou s'abstiennent de prendre) les mesures précisées afin de respecter la loi;
- Poursuivre les personnes qui commettent un crime aux termes de la loi;
- Procéder à des vérifications afin de déterminer si le traitement des données personnelles effectué par les organisations respecte les bonnes pratiques;
- Rendre compte au Parlement des questions préoccupantes en matière de protection des données³⁵¹.

La DPA a été critiquée depuis son entrée en vigueur et a été décrite par les tribunaux à titre de loi encombrante et peu élégante³⁵². Au cours des dernières années, il y a eu de plus en plus de demandes à l'effet que le Commissariat devrait avoir plus de pouvoirs d'enquête et d'exécution en raison d'une série de fuites et de pertes de renseignements gênantes dont le point culminant a été la perte de 25 dossiers de demandeurs de prestations pour enfants par l'administration fiscale britannique (Her Majesty's Revenue and Customs) en novembre 2007.

Le Commissariat a vu un nombre croissant d'atteintes à la protection des données rapportées. Il a ainsi fait valoir que, d'octobre 2008 à janvier 2009, le nombre d'atteintes rapportées était passé de 277 à 376. Le Commissariat presse le secteur privé de faire de la protection des données une partie intégrante de la gouvernance d'entreprise étant donné que 112 des 376 atteintes à la protection des renseignements personnels émanaient du secteur privé³⁵³. La réaction du

351 *Data Protection Act 1998*, chap. 29 (R.-U.), partie V, accessible en ligne à l'adresse suivante : <http://www.statutelaw.gov.uk/legResults.aspx?LegType=All+Legislation&searchEnacted=0&extentMatchOnly=0&confersPower=0&blanketAmendment=0&sortAlpha=0&PageNumber=0&NavFrom=0&activeTextDocId=3190610> [en anglais seulement].

352 *Campbell c. MGN Ltd*, Cour d'appel (Chambre civile), 2002, EWCA Civ 1373, 2003, QB 633 (R.-U.) (opinion de Lord Phillips).

353 Commissariat à l'information, « Data breaches reported to the ICO », 9 février 2009, accessible en ligne à l'adresse suivante : www.ico.gov.uk/upload/documents/pressreleases/2009/data_breaches_ico_statement20090209.pdf [en anglais seulement].

commissaire Richard Thomas³⁵⁴ à cette augmentation du nombre d'atteintes à la sécurité des données en trois mois a été de demander un accroissement des pouvoirs du Commissariat :

« Pendant plus de 20 ans, le Commissariat n'a pas eu le pouvoir de procéder à une inspection sans obtenir le consentement de l'organisation visée. Au cours des six années et demie de mon mandat à titre de commissaire, j'ai constamment fait valoir que cette situation était inacceptable. On ne demanderait pas à un inspecteur des aliments qu'il obtienne le consentement d'un restaurant avant de procéder à une inspection³⁵⁵. » [traduction]

Le 7 juillet 2008, M. Thomas s'est montré une fois de plus critique à l'égard des pouvoirs du commissaire à l'information dans l'examen du partage des données qu'il a effectué en collaboration avec Mark Walport, directeur de Wellcome Trust³⁵⁶. Dans cet examen, Thomas et Walport ont évalué le cadre relatif à la façon dont les renseignements personnels sont utilisés dans les secteurs public et privé. L'examen demande des changements au sein des organisations du secteur privé, tant en ce qui concerne leur façon de former leurs employés quant au traitement des données personnelles que la culture relative à la façon dont les renseignements personnels sont perçus et traités.

Thomas et Walport demandent de plus grands pouvoirs de réglementation afin de faciliter ces améliorations. L'examen suggère également d'établir de plus grands pouvoirs d'inspection et de vérification, de mettre en œuvre les pouvoirs d'imposer des pénalités promis ainsi que de remplacer le poste unique de commissaire à l'information par une équipe exécutive. L'examen du partage des données a inspiré une série de réformes législatives en vue d'accroître les pouvoirs d'enquête et d'exécution du commissaire³⁵⁷.

Les demandes d'accroissement des pouvoirs du Commissariat de M. Thomas ont obtenu des réponses dans la *Criminal Justice and Immigration Act* qui a

354 En février 2009, le comité de la Chambre des communes a accepté que Christopher Graham devienne le nouveau commissaire à l'information à partir de juin 2009. Au moment de la rédaction, M. Thomas était toujours nommé à titre de commissaire sur le site Web du Commissariat.

355 Alexi Mostrous, « UK citizens' private information being lost at record rate », *London Times*, 9 février 2009, <http://www.timesonline.co.uk/tol/news/politics/article5688347.ece> [en anglais seulement].

356 Richard Thomas et Mark Walport, « Data Sharing Review », ministère de la Justice, juillet 2008, <http://www.justice.gov.uk/reviews/datasharing-intro.htm> [en anglais seulement].

357 Le gouvernement a répondu à l'examen Thomas-Walport : ministère de la Justice, « Response to the Data Sharing Review Report », 24 novembre 2008, <http://www.justice.gov.uk/publications/response-data-sharing-review.htm> [en anglais seulement].

reçu la sanction royale le 8 mai 2008³⁵⁸. L'article 144 de la *Loi* confère au Commissariat le pouvoir d'imposer des amendes aux secteurs public et privé lorsqu'une infraction à l'article 55 de la DPA est commise. Le fait d'obtenir ou de communiquer des données personnelles, en connaissance de cause ou de façon téméraire, sans le consentement de la personne, constitue un acte criminel en vertu de l'article 55. Les pénalités peuvent faire l'objet d'un appel devant l'Information Tribunal; toutefois le nouveau pouvoir du commissaire n'est pas encore en vigueur et le secrétaire d'État n'a toujours pas déterminé la pénalité maximale. Ce pouvoir accru d'imposer des amendes élève les pouvoirs d'exécution du Commissariat au niveau de ceux des autres organismes de réglementation du Royaume-Uni comme la Financial Services Authority qui s'est vue octroyer le pouvoir d'imposer des amendes aux institutions financières pour les atteintes à la sécurité des données en 2001. Bien que le commissaire à l'information ait également demandé le pouvoir d'imposer des peines d'emprisonnement pour l'achat ou la vente de renseignements de manière illégale³⁵⁹, ces pouvoirs n'ont pas encore été octroyés au Commissariat³⁶⁰.

Les activités du commissaire relatives à la liberté d'information sont financées au moyen d'une subvention annuelle du ministère des Affaires constitutionnelles; celles portant sur la protection des données le sont par l'entremise des droits de notification annuels recueillis auprès des contrôleurs des données. En réponse à la demande de M. Thomas en vue d'obtenir un financement accru pour les activités de réglementation du secteur privé du Commissariat, celui-ci prévoit introduire des droits de notification différentiels³⁶¹, ce qui permettrait d'imposer des frais plus élevés aux plus importants contrôleurs des données qui paient actuellement 35 livres par année, ce qui constitue la norme.

La Chambre des lords a entrepris une enquête relative à la protection de la vie privée afin de déterminer l'incidence qu'ont la surveillance et la collecte de données du gouvernement sur la vie privée des citoyens et leur relation avec l'État, de même que de déterminer si les protections nécessaires sont en place.

358 Commissariat à l'information du secteur public, *Criminal Justice and Immigration Act 2008*, http://www.opsi.gov.uk/acts/acts2008/ukpga_20080004_en_1 [en anglais seulement].

359 Commissariat à l'information, « Information Commissioner calls for prison sentences for illegal buying and selling of personal information », 12 mai 2006, accessible en ligne à l'adresse suivante : <http://www.ico.gov.uk/global/search.aspx?collection=ico&keywords=prison> [en anglais seulement].

360 Ministère des Affaires constitutionnelles « Increasing penalties for deliberate and willful misuse of personal data », 30 octobre 2006, accessible en ligne à l'adresse suivante : www.dca.gov.uk/consult/misuse_data/cp0906.htm [en anglais seulement] [*il s'agit d'une étude sur la faisabilité d'établir les peines d'emprisonnement à titre de pénalités*].

361 Commissariat à l'information, « Minutes – Management board », 26 janvier 2009, accessible en ligne à l'adresse suivante : www.ico.gov.uk/upload/documents/library/corporate/notices/minutes_3_march_2008v1.8.pdf [en anglais seulement].

Le rapport a été publié le 21 janvier 2009 et s'intitule « *The Impact of Surveillance and Data Collection upon the Privacy of Citizens and their Relationship with the State*³⁶² ». Le 13 janvier 2009, M. Thomas a exprimé son opinion concernant l'évolution du rôle du commissaire pendant son mandat à la Chambre des lords³⁶³. M. Thomas a souligné le succès du Commissariat dans la sensibilisation accrue du public quant à la protection des données depuis 2004, de même que le fait que l'examen sur le partage des données ait entraîné des résultats législatifs constructifs. L'évaluation positive de M. Thomas quant aux récentes réformes législatives conférant de plus grands pouvoirs et un financement accru s'est grandement reflétée dans l'évaluation du rôle du commissaire à l'information faite par la Chambre des lords. Celle-ci a exprimé sa satisfaction par rapport à l'engagement du gouvernement à établir des obligations de protection des données à plusieurs niveaux en réponse aux recommandations de l'examen de Thomas-Walport. Néanmoins, la Chambre des lords a appuyé la demande du Commissariat visant à élargir au secteur privé le nouveau pouvoir d'inspection publique du commissaire à l'information, énoncé dans le projet de loi des coroners et des juges.

Section 3. Organismes de surveillance homologues

En plus de s'intéresser à différents organismes de réglementation de l'information et de la protection de la vie privée, il pourrait être utile de se pencher sur les modèles choisis par des organismes de réglementation régissant les activités du secteur privé dans l'intérêt public, tant au Canada que dans des pays homologues. Comme dans le cadre de l'analyse des organismes de protection de la vie privée homologues, l'accent sera porté sur les critères ayant servi à évaluer ces organismes.

3.1 Conseil de la radiodiffusion et des télécommunications canadiennes

Créé en 1968, le CRTC est un organisme public indépendant qui réglemente la radiodiffusion et les télécommunications au Canada. Le CRTC est surveillé par un conseil nommé par le gouvernement et il rend des comptes au Parlement par l'entremise du ministre du Patrimoine canadien, qui est responsable de la politique sur la radiodiffusion. Même si, à l'origine, le CRTC ne réglementait que les entreprises de télécommunications privées (p. ex. BC Tel, Bell Canada), des décisions judiciaires rendues dans les années 1990 ont eu pour effet d'étendre la compétence du CRTC dans le secteur privé, notamment sur une cinquantaine de petites entreprises de télécommunications indépendantes.

362 Chambre des lords, « *Surveillance: Citizens and the State* », 6 février 2009, accessible en ligne à l'adresse suivante : <http://www.parliament.uk/hlconstitution> [en anglais seulement].

363 Richard Thomas, « *Evidence to the Justice Select Committee* », janvier 2009, Commissariat à l'information du Royaume-Uni, accessible en ligne à l'adresse suivante : http://www.ico.gov.uk/about_us/news_and_views/current_topics/ic_evidence_to_js_committee.aspx [en anglais seulement].

Le mandat du CRTC est énoncé dans la *Loi sur la radiodiffusion* (1991), dans la *Loi sur les télécommunications* (1993) et dans la *Loi sur le CRTC* (1976).

En matière de radiodiffusion, le CRTC a pour objectif de réglementer et de superviser la variété et la qualité de la programmation canadienne en plus de veiller à ce que les Canadiens aient accès à des emplois dans l'industrie de la radiodiffusion. En matière de télécommunications, le CRTC supervise et réglemente la qualité et le coût des services de téléphonie et de télécommunications pour les Canadiens. Plus précisément, dans le cadre de la réglementation des radiodiffuseurs et des entreprises de télécommunications, le CRTC participe aux activités suivantes :

- l'attribution, le renouvellement et la modification de licences de radiodiffusion;
- la prise de décision sur les fusions, les acquisitions et les changements de propriétés en radiodiffusion;
- l'approbation de tarifs et de certaines ententes de l'industrie des télécommunications;
- l'attribution de licences pour les services de télécommunication internationaux dont les réseaux permettent aux usagers du téléphone d'effectuer et de recevoir des appels à l'extérieur des frontières canadiennes;
- l'encouragement de la concurrence dans les marchés de télécommunications;
- la réponse aux demandes de renseignements et aux préoccupations concernant des questions de radiodiffusion et de télécommunications³⁶⁴.

En plus des activités en matière de réglementation, le CRTC mène des consultations auprès du public et d'organismes de réglementation étrangers. De plus, le CRTC a le pouvoir d'exclure des entreprises de télécommunications publiques de la portée de la *Loi sur les télécommunications*, il peut décider de ne pas réglementer un service suffisamment compétitif, il peut approuver les tarifs de services déjà offerts par les entreprises de télécommunications publiques, et il peut approuver des ententes et régler des différends entre les diverses entreprises de télécommunications. Le CRTC dispose d'un pouvoir d'enquête étendu, et ses décisions peuvent faire l'objet d'un appel devant le CRTC, la Cour d'appel fédérale ou le Cabinet, mais cette dernière solution est peu fréquente. Contrairement aux tribunaux, le CRTC ne peut pas imposer d'amendes de son propre chef³⁶⁵.

En mars 2006, le Groupe d'étude sur le cadre réglementaire des télécommunications a remis son rapport au gouvernement fédéral, dans lequel il recommande en grande partie la déréglementation du marché des

364 Il est possible de consulter la liste des activités dans le site Web du CRTC, à l'adresse suivante : <http://www.crtc.gc.ca/fra/backgrnd/brochures/b29903.htm>.

365 Organisation de coopération et de développement économiques (OCDE), « Canada : rester à la pointe du progrès grâce à l'innovation », Éditions OCDE, 2002, pages 125 et 126.

télécommunications³⁶⁶. Bien que le Groupe d'étude ait conclu que le cadre de politique et de réglementation dans le secteur des télécommunications du Canada a été utile pour les Canadiens, celui-ci doit être mis à jour en fonction des nouvelles technologies et de l'évolution du marché. Le Groupe d'étude a reçu près de 200 mémoires en réponse au document de consultation publié en 2005. Le Groupe d'étude a également bénéficié de deux autres forums en matière de politiques tenus à Whitehorse et à Gatineau, et de vastes consultations menées auprès d'intervenants et de spécialistes de l'industrie des télécommunications.

Le Groupe d'étude recommande de clarifier les passages incohérents de *Loi sur les télécommunications* et de mettre à jour la *Loi* afin de favoriser l'atteinte des objectifs visant à promouvoir l'accès aux services de télécommunications de pointe, à améliorer l'efficacité des marchés de télécommunications et à laisser aux forces du marché la possibilité de favoriser l'atteinte des objectifs de la politique de télécommunication du Canada dans la mesure du possible. En conséquence, le rapport recommande de réduire les activités de réglementation économique du CRTC.

Après avoir comparé le cadre de réglementation canadien à celui utilisé dans d'autres pays de l'OCDE, le Groupe d'étude a recommandé la création d'un tribunal de la concurrence en télécommunications, qui faciliterait l'application d'une politique canadienne sur la concurrence régissant les marchés de services de télécommunications. Ce tribunal temporaire examinerait les allégations d'agissement anticoncurrentiel et il traiterait les questions relatives à la déréglementation. Le Groupe d'étude a recommandé de préciser les pouvoirs du CRTC en matière de résolution des différends (p. ex. en ce qui concerne les tarifs, les modalités d'accès, le partage des pylônes radio). Le rapport recommande également au Conseil de créer un bureau d'ombudsman qui protégerait les intérêts des consommateurs dans le cadre du mandat du CRTC visant à atteindre les objectifs de politique sociale associés à la politique de télécommunication (p. ex. promouvoir un accès accru).

Le Groupe d'étude a recommandé des réformes institutionnelles afin d'accroître la capacité professionnelle du CRTC, notamment par la diminution du nombre de conseillers, ce qui permettrait au CRTC de retenir des experts-conseils, par le transfert au CRTC des responsabilités réglementaires en matière d'octroi de licences actuellement assumées par Industrie Canada, par l'utilisation accrue des consultations publiques et par la rationalisation des exigences en matière d'octroi de licences et des droits de réglementation.

Comme le CPVP, le CRTC a dû s'adapter à l'évolution rapide de l'environnement externe faisant en sorte que les mécanismes de réglementation établis risquaient de tomber en désuétude en raison de l'apparition de nouvelles

366 Groupe d'étude sur le cadre réglementaire des télécommunications, Rapport final 2006, Ottawa, Travaux publics et Services gouvernementaux Canada, <http://www.telecomreview.ca/eic/site/tprp-gecrt.nsf/fra/rx00101.html>.

formes de médias et de nouveaux types de contenu. Par exemple, le rapport énonce ce qui suit :

Selon le Groupe d'étude, le moment est venu de procéder à une réforme du cadre de politique et de réglementation des télécommunications du Canada. Malgré que le Canada dispose de l'un des marchés de télécommunications les plus concurrentiels au monde, il affiche encore l'un des cadres de réglementation les plus détaillés, prescriptifs et coûteux. Ce cadre représente un fardeau particulièrement lourd pour les grands fournisseurs de services de télécommunications du Canada, qui font désormais face à une concurrence plus féroce dans un certain nombre de segments du marché de la part de rivaux bien établis dotés d'installations, ainsi que de la part de nouveaux venus. Le Groupe d'étude est d'avis que l'industrie canadienne des télécommunications a évolué pour atteindre un stade où l'on peut compter largement sur le libre jeu du marché afin de réaliser des avantages économiques et sociaux pour les Canadiens et où, dans bien des domaines, une réglementation détaillée et prescriptive n'est plus de mise³⁶⁷.

L'évaluation de la politique de télécommunication du Canada menée en 2006, notamment sur le rôle du CRTC, semble se fonder davantage sur la perception que sur des données probantes. Le rapport ne cite aucune étude portant sur l'efficacité antérieure des forces du marché ou sur le coût de la réglementation dans ce secteur. Ceci étant dit, les propositions relatives à la politique de communication peuvent refléter une tendance se manifestant dans le secteur de l'information (par opposition par exemple au secteur bancaire) favorisant la diminution de la réglementation par l'État et la mise en œuvre d'une réforme axée davantage sur le marché.

3.2 Bureau de la concurrence du Canada

Le Bureau de la concurrence du Canada est un organisme indépendant responsable de l'application et de l'exécution de la *Loi sur la concurrence*, de la *Loi sur l'emballage et l'étiquetage des produits de consommation*, de la *Loi sur l'étiquetage des textiles* et de la *Loi sur le poinçonnage des métaux précieux*. Le Bureau de la concurrence fait partie d'Industrie Canada, un lien qui a souvent été à l'origine de soupçons quant à l'indépendance du Bureau. Le Bureau est dirigé par le commissaire de la concurrence, qui a le pouvoir d'ouvrir des enquêtes, de contester des questions relatives au droit civil et à des fusionnements devant le Tribunal de la concurrence, de formuler des recommandations relatives à des questions d'ordre criminel au procureur général du Canada et d'agir à titre de promoteur de la concurrence devant des organismes fédéraux et provinciaux.

367 *Id.*, p. 1-25.

Le Bureau répond aux plaintes des consommateurs concernant des questions relatives à la concurrence et il mène des enquêtes sur des pratiques anticoncurrentielles, comme la fixation des prix, le truquage d'offres, les indications fausses ou trompeuses, la documentation trompeuse concernant le gain d'un prix, l'abus de position dominante, l'exclusivité, les ventes liées et la limitation du marché, la fusion, la commercialisation à paliers multiples et les ventes pyramidales, le télémarketing trompeur et les pratiques commerciales déloyales. La *Loi sur la concurrence* fait la distinction entre les actes criminels, qui sont assujettis à des amendes ou à des peines d'emprisonnement, et les pratiques pouvant faire l'objet d'un recours civil, qui sont uniquement assujetties à des ordonnances correctives. Tandis que les infractions criminelles sont traitées par les tribunaux, les pratiques pouvant faire l'objet d'un recours sont traitées par le Tribunal de la concurrence (le « Tribunal »), qui est composé de juges de la Cour fédérale et de non-spécialistes.

Lorsque le Bureau de la concurrence estime qu'il est nécessaire de mener une enquête approfondie, il soumet la question au Tribunal de la concurrence, qui a le pouvoir d'imposer des amendes et d'émettre des ordonnances. Le Canada a un double système d'application des lois relatives à la concurrence; le Bureau mène des enquêtes tandis que le commissaire recommande des mesures et que le Tribunal de la concurrence prend les décisions. L'évolution de ce double système fait l'objet d'un débat puisque le commissaire remplit de plus en plus le rôle principal dans ce système fonctionnel autonome³⁶⁸.

Depuis l'adoption de la *Loi sur la concurrence* en 1986, le Canada a apporté régulièrement des modifications à cette loi. Entre 2002 et 2004, Industrie Canada a mené un processus approfondi d'examen et de consultation publique sur la *Loi sur la concurrence*, qui a mené à l'adoption du projet de loi C-19, mais celui-ci est sombré dans l'oubli avec la chute du gouvernement libéral. Ce projet de loi aurait imposé des sanctions importantes (1 million de dollars pour une première infraction et 15 millions de dollars pour une deuxième) dans les cas d'abus de position dominante, l'augmentation des sanctions relatives aux pratiques commerciales trompeuses, l'augmentation des sanctions relatives aux ententes anticoncurrentielles passées entre des entreprises concurrentes et le renforcement des pouvoirs d'enquête visant les entreprises soupçonnées d'adopter des pratiques anticoncurrentielles³⁶⁹.

Récemment, soit en juin 2008, la *Loi sur la concurrence* a fait l'objet d'un examen important après la publication du rapport du Groupe d'étude sur les politiques en matière de concurrence, intitulé *Foncer pour gagner*, qui porte sur

368 Organisation de coopération et de développement économiques (OCDE), « Canada — Le rôle de la politique de la concurrence dans la réforme de la réglementation », 2002, <http://www.oecd.org/dataoecd/47/49/1960530.pdf>, pages 21 et 22.

369 Ministère de l'Industrie, *Projet de loi C-19*, 2 novembre 2004, <http://www2.parl.gc.ca/HousePublications/Publication.aspx?pub=bill&doc=C-19&parl=38&ses=1&Language=F>.

l'évaluation des politiques et des lois canadiennes en matière de concurrence et d'investissement étranger³⁷⁰. Le Groupe d'étude sur les politiques en matière de concurrence décrit le rapport de la façon que voici : « une série de recommandations stratégiques visant à faire du Canada une destination plus attrayante pour le talent, l'investissement et l'innovation, ainsi qu'un grand programme national de renforcement de la compétitivité se fondant sur la proposition selon laquelle le niveau de vie et la performance économique du Canada seront rehaussés par une concurrence accrue au Canada et de la part de l'étranger³⁷¹ ». Plus précisément, le Groupe d'étude recommande au gouvernement fédéral de prendre des mesures visant à accroître à la fois la transparence et la prévisibilité de l'application des lois sur la concurrence, ainsi que les sanctions que peut imposer le Bureau dans les cas de violation de la *Loi*³⁷². Bien que les réformes de la *Loi sur la concurrence* aient renforcé les pouvoirs du Bureau de la concurrence en matière d'application de la loi, elles ont très peu modifié la structure institutionnelle du Bureau. Les critères orientant la réforme de la politique du Canada en matière de concurrence sont les mêmes que ceux de la réforme proposée du CRTC, c'est-à-dire l'efficacité, l'efficacité et la modernisation.

3.3 Commission fédérale des communications des États-Unis

Comme au Canada, le mot d'ordre en ce qui concerne la façon de composer avec les moyens d'information dans les contextes réglementaires aux États-Unis a fait l'objet de modifications et de réformes.

La Commission fédérale des communications (FCC) des États-Unis a été créée par la *Communications Act* en 1934. Il s'agit d'un organisme indépendant de réglementation du gouvernement des États-Unis dont le mandat consiste à réglementer les communications entre les États ainsi que celles avec les pays étrangers, lorsque ces communications sont effectuées par radio, par télévision, par fil, par satellite ou par câble. La FCC fait partie des différents organismes de réglementation indépendants créés dans les années 1930, à la lumière de la conviction propre à la Nouvelle Donne (New Deal), selon laquelle un groupe bipartite à composition multiple regroupant des commissaires spécialisés pourrait réglementer leur indépendance³⁷³. Ainsi, la FCC est composée de

370 Groupe d'étude sur les politiques en matière de concurrence, « Foncer pour gagner : rapport final juin 2008 », accessible en ligne à l'adresse suivante : http://www.ic.gc.ca/eic/site/cprp-gepmc.nsf/fra/h_00040.html.

371 Groupe d'étude sur les politiques en matière de concurrence, *Le Groupe d'étude sur les politiques en matière de concurrence publie le rapport*, 26 juin 2008, se reporter à : <http://www.ic.gc.ca/eic/site/cprp-gepmc.nsf/fra/accueil>.

372 Bureau de la concurrence, *Foire aux questions — Modifications à la Loi sur la concurrence*, se reporter à : <http://competitionbureau.gc.ca/eic/site/cb-bc.nsf/fra/03046.html>.

373 Randolph J. May, « The FCC's Tumultuous Year 2003: An Essay on an Opportunity for Institutional Agency Reform », 2004, 56 *Administrative Law Review* 1307, pages 1310 et 1311.

cinq commissaires nommés par le président et approuvés par le Sénat pour une période de cinq ans, qui prend fin de façon graduelle. Les seuls motifs de congédiement des commissaires sont la corruption et l'inconduite grave. La FCC se divise en sept services de travail et en dix bureaux qui effectuent l'élaboration et la mise en œuvre des programmes de réglementation, le traitement des demandes de licences et autres, l'analyse des plaintes, les enquêtes et qui participent aux audiences de la Commission.

Bien que la loi de 1934 à l'origine de la FCC demeure le fondement de la réglementation fédérale en matière de communications, la *Cable Act* de 1984 et de 1992 ainsi que la *Telecommunications Act* de 1996 ont grandement modifié les pouvoirs de la FCC³⁷⁴. La *Telecommunications Act* établit que la FCC est responsable de promouvoir la concurrence et de diminuer la réglementation afin d'entraîner la baisse des prix et l'augmentation de la qualité des services offerts aux consommateurs. Pour ce faire, la FCC formule des règles, elle informe le public de la règle qu'elle propose et lui donne l'occasion de faire part de son avis. Ces pouvoirs décisionnels s'ajoutent aux pouvoirs d'octroi de licences de radiodiffusion, que doivent obtenir tous les principaux utilisateurs du spectre électromagnétique.

Le Congrès exerce une influence sur la FCC puisque le Sénat approuve les nominations des commissaires par le président, le Congrès contrôle le budget des organismes fédéraux, la FCC est surveillée par le comité sur l'énergie et le commerce et par le comité du Sénat sur le commerce, la science et le transport, et le Congrès peut orienter les activités de la FCC en adoptant des lois à cette fin. L'industrie réglementée exerce une influence de la même importance sur la FCC par les pressions politiques directes et son influence sur le Congrès³⁷⁵. Par conséquent, malgré le fait que la FCC était destinée à être un organisme de réglementation indépendant, plusieurs pressions partisans ont une incidence sur ses décisions.

L'évolution de la technologie a lancé le débat sur la structure de la FCC, dont on réclame la réforme, dans un contexte où l'industrie des communications est aux prises avec des exigences réglementaires dépassées, les décisions et la réglementation de l'organisme manquent de clarté, en plus du fait que la prise de décisions et la publication des nouvelles règles accusent un retard embarrassant³⁷⁶. La FCC a fait l'objet de nombreuses critiques lui reprochant de prendre des décisions politisées fondées sur des renseignements inadéquats et de compter trop souvent sur les parties qu'elle réglemente pour lui communiquer

374 Michael J. Zarkin, « The Federal Communications Commission », Santa Barbara, Greenwood Publishing Group, 1998, p. xv.

375 *Id.*, p. 49 à 54.

376 R.J. May, *supra*, note 369, p. 1309.

les enjeux et les renseignements sur lesquels elle fonde ses enquêtes³⁷⁷. La Commission a examiné plusieurs centaines de milliers de documents, elle a réalisé 73 entrevues auprès d'employés travaillant pour le compte de la FCC ou ayant travaillé pour celle-ci, ainsi qu'auprès de personnes associées à l'industrie des télécommunications, elle a reçu des courriels des employés de la FCC et d'entrepreneurs après leur avoir transmis des demandes en ce sens et elle a examiné des dizaines d'allégations.

Le 5 janvier 2009, les organisations d'intérêt public Public Knowledge et Silicon Flatirons ont parrainé une conférence et un projet continu intitulé « Reforming the FCC³⁷⁸ ». Dans le cadre de la conférence « Reforming the FCC », le conférencier principal, Philip J. Weiser, a fait l'observation suivante : « Comme l'organisation manque d'imagination, qu'elle n'utilise presque aucune planification ou pensée stratégique et qu'elle ne dispose d'aucune source de donnée bien établie lui permettant d'orienter ses décisions, elle rate souvent l'occasion d'organiser des plans d'action indépendants³⁷⁹. » [traduction] Weiser estime que la FCC doit réformer ses processus institutionnels et qu'elle doit adopter une nouvelle culture. Il ajoute que la FCC manque de transparence et que les intervenants ont généralement tendance à préférer les séances ex parte à huis clos, ce qui limite l'information du public quant à leur position. Weiser juge que les décisions de la FCC sont arbitraires puisque la Commission ne dispose pas d'une vision stratégique générale bien établie ni d'un leadership suffisamment indépendant.

Aux États-Unis, l'abandon de la réglementation spéciale et politisée au profit d'une réglementation stratégique fondée sur des données probantes constitue un exemple significatif.

377 Le 9 décembre 2008, le sous-comité chargé de la surveillance et des enquêtes du comité de la Chambre chargé de l'énergie et du commerce a publié ses conclusions résultant d'une enquête bipartite sur les pratiques de gestion et les processus réglementaires de la FCC. L'enquête a été lancée le 8 janvier 2009 au moment où le président du comité et du sous-comité a envoyé une lettre à Kevin Martin, alors président de la FCC, pour l'informer de la tenue d'une « enquête officielle sur les pratiques réglementaires de la FCC afin de déterminer si elles sont effectuées de façon juste, ouverte, efficiente et transparente » [traduction]. Se reporter à Committee on Energy and Commerce, « Deception and Distrust: The Federal Communications Commission Under Chairman Kevin J. Martin », décembre 2008, accessible en ligne à l'adresse suivante : http://energycommerce.house.gov/index.php?option=com_content&task=view&id=1455&Itemid=1 [en anglais seulement]

378 Il est possible de consulter une bibliographie complète sur la réforme de la FCC ainsi que des documents de travail à l'adresse suivante : <http://fcc-reform.org/> [en anglais seulement].

379 Philip J. Weiser, « FCC Reform and the Future of Telecommunications Policy », 2009, p. 6, accessible en ligne à l'adresse suivante : <http://fcc-reform.org/paper/fcc-reform-and-future-telecommunications-policy> [en anglais seulement].

3.4 Federal Trade Commission des États-Unis

Aux États-Unis, la Federal Trade Commission (FTC) est l'organisme de réglementation stratégique dont le mandat se rapproche le plus de celui qui est conféré au CPVP aux termes de la LPRPDE.

Le gouvernement fédéral a créé le bureau des corporations en 1903. En 1914, le président Woodrow Wilson a signé la *Federal Trade Commission Act*, en vertu de laquelle le bureau des corporations est devenu la FTC. La compétence de la FTC touche à la fois la protection des consommateurs et la réglementation de la concurrence, ce qui fait en sorte que de grands secteurs économiques sont visés par la portée de la FTC. La FTC est un organisme d'application de la loi, contrairement à un modèle d'ombudsman, qui veille à l'application et à l'exécution d'une variété de lois et de règlements, comme la *Federal Trade Commission Act*, l'*Identity Theft Act*, la *Fair Credit Reporting Act* et la *Clayton Act*. L'administration centrale de la FTC se trouve à Washington D.C., et cette commission dispose de sept bureaux régionaux répartis aux États-Unis. En 2009, la FTC comptait plus de 1 100 équivalents temps plein et son budget annuel se chiffrait à 259 millions de dollars américains.

Le bureau de la protection des consommateurs de la FTC participe à une variété d'activités relatives à l'éducation du public, à l'observation de la loi par l'industrie et à l'application de la loi. Ce bureau mène des enquêtes, poursuit des entreprises et des personnes qui n'ont pas respecté leurs obligations juridiques et il partage des renseignements obtenus dans le cadre de ses enquêtes avec d'autres organismes d'application de la loi à l'échelle nationale et internationale. Le bureau élabore et édicte des règles visant à protéger les consommateurs, et il instruit les consommateurs et les entreprises au sujet de leurs droits et de leurs responsabilités.

L'une des sept divisions du bureau (la plus récente) traite précisément des questions relatives à la protection de l'identité et de la vie privée. Cette division a la responsabilité d'assurer la protection des renseignements financiers des consommateurs et elle consacre des ressources aux enquêtes sur les infractions à la sécurité des données ainsi qu'à la prévention du vol d'identité.

Le pouvoir et le mandat de cette division proviennent de différentes lois, dont l'article 5 de la *Federal Trade Commission Act*, qui interdit les agissements injustes ou trompeurs, y compris des déclarations trompeuses et des pratiques injustes comprenant l'utilisation ou la protection de renseignements personnels des consommateurs; la *Fair Credit Reporting Act*, qui assure l'exactitude et la protection des renseignements personnels dont disposent les agences d'évaluation du crédit et d'autres organismes produisant des rapports sur les consommateurs, et qui confère aux consommateurs le droit de connaître les renseignements que communiquent ces organismes à leur sujet aux créanciers, aux compagnies d'assurance et aux employeurs; la *Gramm-Leach-Bliley Act*, qui exige aux institutions financières d'assurer la protection et la confidentialité des renseignements relatifs aux consommateurs, d'informer les consommateurs de leurs pratiques en matière d'information et d'offrir aux consommateurs la possibilité de refuser que leurs renseignements personnels soient transmis

à certains tiers indépendants. Cette division administre également le centre de données sur le vol d'identité (Identity Theft Data Clearinghouse), qui regroupe le registre centralisé du gouvernement fédéral sur les plaintes des consommateurs relatives au vol d'identité. La division analyse les tendances en matière de vol d'identité, elle fait la promotion de l'élaboration et de l'efficacité de stratégies de prévention des fraudes d'identité dans le domaine des services financiers, et elle désigne des cibles qui seront soumises à l'application du droit criminel. Bien que la FTC ait un mandat plutôt restreint en matière de protection des données, elle dispose d'une variété d'outils pour exécuter ce mandat, dont le pouvoir d'imposer des amendes importantes. En février 2010, la juridiction conjointe de la FTC et du département de la Santé et des Services sociaux relative au signalement des atteintes est entrée en vigueur, et celle-ci exige le signalement des atteintes concernant les dossiers médicaux.

L'approche de la FTC en matière d'évaluation comporte différents volets. Elle comprend des examens annuels du rendement et des plans stratégiques périodiques de cinq ans. Le plan stratégique 2009-2014 est axé sur les trois buts suivants : 1) la protection du consommateur; 2) le maintien de la concurrence; 3) l'amélioration du rendement. Chaque but est composé d'un ensemble d'objectifs, et chaque objectif comprend des mesures du rendement, des stratégies visant à atteindre les buts et des méthodes d'évaluation. Par exemple, dans les moyens d'atteindre le but relatif à la protection des consommateurs, la FTC établit l'objectif suivant : « La fraude d'identité, la tromperie et les pratiques injustes causant le préjudice le plus important aux consommateurs. » [traduction] Les stratégies utilisées pour atteindre cet objectif comprennent un « réseau sentinelle de consommateurs » [traduction] responsable de la réception des plaintes, de la collecte de données sur la fraude et du partage de ces renseignements avec un vaste réseau d'organismes d'application de la loi. Parmi les mesures du rendement se trouvent le nombre de plaintes et de demandes reçues, le pourcentage de mesures de protection du consommateur prises par la FTC visant le motif des plaintes des consommateurs et le taux de satisfaction des consommateurs concernant le centre d'appel de la FTC. L'annexe du plan stratégique comprend des mesures générales du rendement et des données annuelles. Par exemple, en 2009, le pourcentage des plaintes reçues par la FTC qui ont été gagnées au moyen d'un procès, d'un règlement à l'amiable ou de l'émission d'un jugement par défaut se chiffre entre 75 % et 80 %. Bien que cette statistique soit impressionnante, elle n'est pas décomposée de sorte à permettre au lecteur d'évaluer si un procès ayant mené à une décision est plus ou moins efficace qu'un règlement à l'amiable.

Section 4. **Mesure du rendement du Commissariat à la protection de la vie privée : leçons retenues**

Bien qu'il existe une certaine convergence à l'échelle internationale en ce qui concerne les pratiques exemplaires en matière de protection de la vie privée (par exemple, la principale directive européenne 95/46/CE se fonde sur les obligations et les droits énoncés dans la convention n° 107 du Conseil de l'Europe de 1981, qui ressemblent aussi aux lignes directrices de 1980 de l'OCDE et aux lignes directrices de 1990 de l'ONU), aucun consensus n'a été

atteint quant au mode d'évaluation du rendement des organismes de protection de la vie privée.

Ceci étant dit, les observateurs spécialisés s'entendent habituellement quant à l'évaluation des forces relatives de différents régimes de protection de la vie privée. Par exemple, celui des États-Unis est généralement perçu comme un régime fondamentalement plus faible que la majorité des autres régimes, tandis que les régimes européens sont les mieux reconnus. Ce classement non officiel s'explique grandement par le fait que les États-Unis ne comptent pas d'organisme fédéral responsable des données ni de lois complètes régissant la protection des données dans le secteur privé³⁸⁰. Néanmoins, mis à part ces évaluations comparatives hâtives, quelques études universitaires rigoureuses ont analysé les modes d'évaluation des organismes de protection de la vie privée.

L'ancien commissaire à la protection de la vie privée de l'Australie, Malcolm Crompton, a signalé le manque d'importance accordé au fonctionnement des organismes de protection de la vie privée puisque « l'accent est souvent porté sur la nature des structures juridiques et sur les facteurs incitatifs qu'ils engendrent sur le plan économique, et non sur la réussite ou l'échec de l'organisme de réglementation en soi en fonction des limites de la loi et du contexte³⁸¹ » [traduction]. Comme les recherches universitaires portant sur des enjeux relatifs à la protection de la vie privée sont généralement axées sur les enjeux en soi et non sur le discours en matière de théorie et de science politique analytique, il existe peu d'évaluations globales des systèmes de protection de la vie privée³⁸².

380 Lee A. Bygrave, « Privacy Protection in a Global Context — A Comparative Overview », « Privacy Protection in a Global Context — A Comparative Overview », 2004, 47 *Scandinavian Studies in Law* 319, p. 344.

381 Malcolm Crompton, « 'Light Touch' or 'Soft Touch' — Reflections of a Regulator Implementing a New Privacy Regime », Australie, Commissariat à la protection de la vie privée, 2004, accessible en ligne à l'adresse suivante : http://www.privacy.gov.au/news/speeches/sp2_04p.html#link04 [en anglais seulement]. Crompton a prononcé un discours en mars 2004, dans lequel il a proposé un cadre de mesure du rendement des organismes de réglementation. Il estime que ces derniers doivent agir de façon éthique, efficace et efficiente, et il présente un cadre de travail permettant de mettre à l'essai leur rendement relatif à ces mesures. Crompton est d'avis que ce rendement doit être établi dans le cadre d'une analyse de ses conséquences économiques, des résultats sociaux, de la responsabilité publique des ressources, de l'indépendance, de la justice, de la transparence et de la responsabilisation des décisions, de l'engagement actif dans l'élaboration des politiques ainsi que dans l'efficacité, la responsabilité et la transparence des services offerts. Crompton propose d'évaluer tous ces points de référence en fonction du contexte dans lequel l'organisme de réglementation agit. Il examine différents facteurs ayant une incidence sur la capacité de l'organisme de réglementation à exercer ces pouvoirs, dont les suivants : la loi, les ressources à sa disposition, les attentes du gouvernement, le contexte général, les forces du marché, l'envergure de l'évolution de la technologie.

382 Charles Raab, « Beyond Activism: Research Perspectives on Privacy », *TILT Law & Technology Working Paper Series* (22 février 2008), n° 007/2008.

4.1 Le modèle de l'Union européenne

La Directive de l'Union européenne relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données établit des principes directeurs à l'intention des rédacteurs de lois nationales sur la protection des données. L'article 29 de la Directive prévoit l'institution d'un organisme consultatif (« groupe ») composé d'un représentant de l'autorité de contrôle de chaque État membre, de la Commission européenne et d'autres organismes communautaires. Le groupe évalue la pertinence d'assurer la protection des renseignements personnels de l'État et de tiers puisque l'article 35 interdit aux États membres d'effectuer le transfert de données à caractère personnel à d'autres pays sans bénéficier d'une protection adéquate. Les critères utilisés par le groupe pour évaluer les régimes de protection de la vie privée constituent désormais un point de référence important, comme le soulignent Raab et Bennet, « les dispositions de l'UE quant à la pertinence sont des règles de la route de facto concernant le caractère de plus en plus mondial des activités de traitement des données personnelles, qui ont suscité beaucoup d'attention, de débats et de controverse à l'échelle internationale³⁸³ ». [traduction].

En juillet 1998, le groupe prévu à l'article 29 a élaboré une méthode permettant de déterminer à quel moment un pays atteint un « niveau de protection adéquat » dans le cadre du traitement des données à caractère personnel³⁸⁴. Dans le document de travail intitulé « Transferts de données personnelles vers des pays tiers : Application des articles 25 et 26 de la directive relative à la protection des données³⁸⁵ », le groupe conclut que l'évaluation du caractère adéquat d'un régime de protection des données devrait porter tant sur le contenu des règles de protection des renseignements personnels que sur les systèmes visant à assurer leur efficacité.

En prenant la directive 95/46/CE comme point de départ et en gardant à l'esprit les dispositions d'autres documents internationaux sur la protection des données, il devrait être possible de dégager des principes « fondamentaux » touchant au « contenu » des règles sur la protection des données et aux

383 Charles Raab et Colin Bennett, « The Governance of Global Issues: Protecting Privacy in Personal Information », *European Consortium for Political Research*, 2003, p. 6.

384 Peter J. Hustinx, « Adequate Protection — Opinion 6/99 s Article 29 Working Party revisited », *Ten Years of DP & FOI Commissioner's Office, 2006*, p. 251, se reporter à l'adresse suivante : <http://www.edps.europa.eu/EDPSWEB/edps/site/mySite/pid/231> [en anglais seulement].

385 Groupe de protection des personnes à l'égard du traitement des données à caractère personnel, *Transferts de données personnelles vers des pays tiers : application des articles 25 et 26 de la directive relative à la protection des données*, Commission européenne, Marché intérieur et services financiers, 24 juillet 1998, accessible en ligne à l'adresse suivante : http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/1998/wp12_fr.pdf.

exigences « en matière de procédure/d'application », le respect de ces principes et de ces exigences pouvant être considéré comme une condition minimale pour que l'on puisse parler d'un niveau de protection adéquat³⁸⁶.

Bien que ces exigences soient conçues de sorte à s'adapter au contexte, le groupe a dressé deux listes d'exigences fondamentales permettant de déterminer le caractère adéquat des règles relatives aux données et des mécanismes d'application.

Voici les principes fondamentaux concernant le contenu de la réglementation relative à la protection des renseignements personnels :

1. Limitation des transferts à une finalité spécifique : les données doivent être traitées dans un but spécifique et utilisées ultérieurement à des fins connexes, à quelques exceptions près;
2. Qualité et proportionnalité des données : les données doivent être exactes, mises à jour, adéquates, pertinentes et non excessives au regard des finalités de leur transfert ou de leur traitement ultérieur;
3. Transparence : les personnes physiques doivent recevoir des informations sur les finalités du traitement et sur l'identité du responsable de ce traitement dans le pays tiers, à quelques exceptions près;
4. Sécurité : le responsable du traitement des données doit prendre des mesures de sécurité, sur les plans technique et organisationnel, qui soient appropriées au regard des risques présentés par le traitement;
5. Droits d'accès, de rectification et d'opposition : à quelques exceptions près, toute personne concernée doit avoir le droit d'obtenir une copie de toutes les données la concernant, un droit de rectification lorsqu'elles sont inexactes et le pouvoir de s'opposer à leur traitement;
6. Restrictions aux transferts ultérieurs : les transferts ultérieurs de données à caractère personnel effectués par le destinataire du transfert initial ne doivent être autorisés que lorsque le second destinataire est également soumis à des règles offrant un niveau de protection adéquat, à quelques exceptions près.

Le groupe a élaboré d'autres exigences s'appliquant au traitement de données sensibles, de données servant au marketing direct ou de données servant à des décisions individuelles automatisées.

Le groupe a fixé trois objectifs relatifs aux systèmes de protection des données qui permettent d'évaluer les mécanismes d'application. Voici les trois objectifs choisis, que partagent les systèmes de protection des données :

1. Garantie d'un niveau satisfaisant de respect des règles, où le système se caractérise par la conscience aiguë qu'ont les responsables du

³⁸⁶ *Id.*, p. 5.

traitement de leurs obligations et les personnes concernées de leurs droits et des moyens de les exercer. L'existence de sanctions efficaces et dissuasives est importante pour garantir ce respect des règles, de même que les dispositifs de vérification directe par les autorités, par des commissions de contrôle ou par des responsables indépendants chargés de la protection des données;

2. Soutien et assistance aux personnes concernées afin qu'elles soient en mesure de faire valoir leurs droits rapidement et efficacement, sans subir des coûts prohibitifs. À cet effet, il faut qu'il existe un mécanisme institutionnel permettant l'instruction des plaintes par une instance indépendante.
3. Mise à disposition de voies de recours appropriées à la personne concernée en cas de non-respect des règles, ce qui requiert l'institution d'une instance de jugement ou d'arbitrage indépendante permettant d'obtenir une indemnisation et, au besoin, d'infliger des sanctions.

L'évaluation menée en novembre 2006 par la Commission européenne au sujet de la LPRPDE illustre la façon dont les critères et les principes directeurs devraient être appliqués³⁸⁷. La Commission a conclu que la LPRPDE « continue d'offrir un niveau de protection adéquat des données à caractère personnel au sens de l'article 25 de la Directive³⁸⁸ » [traduction]. La Commission juge que la LPRPDE applique les principes de la Directive puisqu'elle exige que les transferts de données ne soient effectués qu'à des fins particulières (à l'exception des cas où ces transferts sont nécessaires dans une société libre et démocratique) et que les données soient exactes, exhaustives et mises à jour au regard des finalités de leur collecte et de leur traitement. De plus, la LPRPDE exige la transparence, le droit d'accéder aux données et d'y apporter des corrections ainsi que des mesures de sécurité visant à protéger les renseignements, tandis que les transferts subséquents ne sont autorisés qu'à ceux qui sont aussi assujettis aux règles assurant une protection adéquate. La Commission se réjouit du fait que les exigences de la LPRPDE relatives au consentement varient en fonction du degré de sensibilité des renseignements. De plus, les autorités responsables de la protection des données des autres États membres n'ont pas éprouvé de difficulté avec les transferts de données au Canada. Finalement, la Commission salue l'indépendance et les pouvoirs du CPVP puisque les plaignants peuvent se tourner vers la Cour fédérale en cas d'atteinte à la protection de leurs renseignements personnels, ce qui, à son avis, compense le manque de pouvoir d'application de la commissaire.

387 Commission européenne, *The application of Commission Decision 2002/2/EC of 20 December 2001 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documentation Act*, novembre 2006, accessible en ligne à l'adresse suivante : http://ec.europa.eu/justice_home/fsj/privacy/docs/adequacy/canada_st15644_06_en.pdf [en anglais seulement]. Se reporter au site Web du Contrôleur européen de la protection des données : <http://www.edps.europa.eu/EDPSWEB/edps/site/mySite/pid/78>.

388 *Id.*, p. 6.

Il convient de noter les préoccupations de l'Europe quant aux pouvoirs d'application limités d'un organisme de réglementation canadien. Dans une étude portant sur la réglementation de la vie privée en Europe (France, Grande-Bretagne, Allemagne et Italie) publiée récemment, Francesca Bignami établit un lien entre, d'une part, la transformation structurelle massive observée en Europe au cours des vingt-cinq dernières années (une transformation marquée par la privatisation des industries de l'État, la libéralisation des marchés et la montée de l'Union européenne) et, d'autre part, le changement tangible des styles de réglementation en Europe. Généralement, la culture de réglementation européenne donnait l'impression d'être non officielle et flexible comparativement au style réglementaire américain légaliste axé sur les litiges. Bignami soutient que les pays européens se dirigent vers des modèles d'administration fondés sur l'application légaliste de la réglementation qui accordent aux intervenants du marché de nombreuses occasions d'appliquer une autoréglementation, mais qui conservent les styles de réglementation antérieurs. Plus précisément, contrairement aux allégations d'américanisation, les litiges demeurent une composante relativement insignifiante du processus réglementaire. Les motifs expliquant ce nouveau modèle réglementaire — qu'elle appelle « juridisme de coopération » [traduction] — témoignent à la fois de la diffusion de l'autoréglementation des pays septentrionaux aux pays méridionaux de l'UE et de la pression exercée sur les gouvernements nationaux afin qu'ils démontrent leur engagement relatif aux politiques de l'UE par des mesures d'application³⁸⁹.

Le juridisme de coopération tient compte de deux tendances liées, soit le désir d'accroître l'application et la préférence accordée à l'autoréglementation. Bignami explique que cette dynamique jumelée est particulièrement présente dans le contexte de la réglementation de la protection des renseignements personnels :

La sévérité accrue des mesures d'application et l'expansion de l'autoréglementation sont des réalités que doivent confronter les décideurs et les administrateurs qui tentent de composer avec un marché compliqué qui change rapidement. Cette situation s'observe particulièrement dans un secteur de politique comme la protection des données, où les nouvelles technologies de l'information ont eu pour effet d'augmenter de façon spectaculaire le nombre d'entreprises et de citoyens régis par la réglementation, et l'évolution rapide de la technologie fait en sorte qu'il est particulièrement difficile pour les organismes de réglementation d'être au fait des réalités socio-économiques. D'une part, ces derniers, qui sont

389 Francesca Bignami, « Cooperative Legalism », 2009, (inscrite avec les auteurs; veuillez prendre note que nous n'avons pas encore obtenu l'autorisation de la professeure Bignami pour faire circuler son article à l'extérieur de notre équipe, mais nous l'obtiendrons d'ici la préparation de la version définitive du rapport).

beaucoup moins nombreux que les intervenants du marché et qui doivent répondre aux demandes sociales croissantes, ne disposent pas des ressources nécessaires pour appliquer avec souplesse le mandat prévu par les politiques à la situation de chaque entreprise. Ils ne peuvent pas se fier non plus sur des mécanismes non officiels fondés sur la confiance en ce qui concerne les marchés en expansion. Par conséquent, ils doivent établir des règles selon lesquelles les contrevenants ont de fortes probabilités d'être repérés et de subir les conséquences de leurs actes (inspections et sanctions). D'autre part, cette même surcharge sociétale et la complexité du marché poussent les organismes de réglementation à faire participer les intervenants du marché dans la conception des solutions en matière de réglementation et dans l'atteinte des objectifs publics. Les bureaucrates, dont l'expertise et les ressources sont limitées, demandent aux intervenants du marché de s'autoréglementer³⁹⁰. [traduction]

Le juridisme de coopération représente un cadre de travail utile pour comprendre le soutien manifesté au Canada envers l'accroissement du rôle de l'État et de celui du marché. L'évaluation du CPVP à l'avenir pourrait bien se fonder sur son efficacité à démontrer ses progrès et ses réalisations dans les deux contextes.

Les pays européens appliquent également une grande variété de solutions réglementaires. L'un des organismes de réglementation les plus activistes est l'Agence espagnole de protection des données (AEPD). En Espagne, la protection des données est établie par l'article 18.4 de la Constitution, qui prévoit que « la loi limitera l'usage de l'informatique afin de préserver l'honneur, l'intimité personnelle et familiale des citoyens, et le plein exercice de leurs droits » [traduction].

Cette disposition a été élaborée par la loi organique n° 15/1992 sur la réglementation du traitement automatique des données à caractère personnel³⁹¹. L'AEPD a été créée officiellement par le décret royal 428/1993 du 26 mars.

L'AEPD dispose d'une gamme d'outils réglementaires³⁹², dont l'imposition d'amendes et un registre général de protection des données (en 2007, plus d'un million de systèmes d'enregistrement étaient inscrits; l'augmentation la

390 *Id.*, p. 11.

391 La loi 5/1992 a été modifiée ultérieurement par la loi organique n° 15/1999 sur la protection des données à caractère personnel. La loi organique n° 15/1999 a transposé la Directive 95/46/CE dans le droit espagnol.

392 À des fins de discussion, le dépliant d'information sur l'AEPD est accessible à l'adresse suivante : https://www.agpd.es/portalweb/canaldocumentacion/publicaciones/common/pdfs/AEPD_en.pdf [en anglais seulement].

plus marquée a été relevée dans les systèmes d'enregistrement appartenant à des entreprises privées, plus particulièrement à des petites et à des moyennes entreprises ainsi qu'à des professionnels indépendants). L'AEPD participe également à une multitude d'activités d'application de la loi, ce qui est essentiel pour améliorer l'image des droits des citoyens, et ceci augmente à son tour le nombre d'atteintes déclarées à l'organisme de réglementation. En 2007, le nombre de plaintes a connu une hausse de 7 % (il s'est chiffré à 1 263 pour l'année), et celles-ci étaient principalement axées sur les institutions financières et les télécommunications. Le nombre de plaintes relatives à la vidéosurveillance a augmenté de façon exponentielle, soit de 400 %, par rapport à l'année précédente, à la suite d'une campagne de sensibilisation et d'éducation du public. L'AEPD a réglé 399 affaires comprenant des sanctions, une augmentation de 32,5 %, qui représentent des amendes s'élevant à plus de 19,5 millions d'euros. Bien que le nombre d'enquêtes et de règlements soit en hausse, le nombre de règlements accompagnés d'amendes est à la baisse, ce qui, selon l'AEPD, prouve qu'elle arrive à assurer le respect de la loi par la crainte associée aux amendes et aux ordonnances, sans nécessairement recourir à ces mesures fréquemment. Dans un certain sens, le système espagnol peut constituer un exemple concret du juridisme de coopération.

4.2 Vers un cadre d'évaluation

Tandis que certains spécialistes, comme Bignami, ont tenté d'examiner les tendances concernant la réglementation de la protection des renseignements personnels, Charles Raab et Colin Bennett ont travaillé à l'élaboration d'un cadre d'évaluation destiné aux organismes de réglementation de la protection des renseignements personnels³⁹³. Dans leur article de 1996 intitulé « Taking the measure of privacy: can data protection be evaluated? », Raab et Bennett se sont penchés sur les dangers associés à l'évaluation de la protection des données, et ils ont abordé cette question sous un autre angle dans leur livre publié en 2003, intitulé *The Governance of Privacy*, dans lequel ils évaluent la possibilité de « mesurer » l'efficacité des systèmes de protection des données en examinant « la mesure dans laquelle certaines normes en matière de protection des données peuvent être choisies de façon objective puis intégrées à un instrument fiable de mesure du rendement de ces systèmes, tant au fil du temps que de façon comparative³⁹⁴ » [traduction].

Raab et Bennett ont fixé deux buts principaux qui servent de points de référence pour évaluer la protection des données : 1. la protection de la vie privée; 2. la promotion des bonnes pratiques informatiques. Ils soutiennent que les régimes de protection des données tentent généralement d'équilibrer ces deux buts; ils visent à assurer la protection des renseignements personnels sans nuire aux

393 Raab et Bennett ont préparé une série de rapports au fil des ans, qui a mené à la publication de *The Governance of Privacy* en 2003, où ils consacrent un chapitre à la mesure des régimes de protection des renseignements personnels.

394 C. Raab et C. Bennett, *supra*, note 74, p. 187.

activités du gouvernement ou des entreprises³⁹⁵. Dans ce contexte, Raab et Bennett proposent quatre mesures de la qualité des régimes de protection des données, soit les suivantes :

- **l'économie** : le coût des ressources d'intrant, c.-à-d. l'argent et le personnel utilisés par l'organisme de protection des données et par les contrôleurs des données;
- **l'efficience** : le lien entre les intrants et les extrants, ces derniers étant beaucoup plus difficiles à évaluer. Les extrants d'un organisme de réglementation peuvent comprendre des directives et des conseils destinés au public et aux décideurs, la négociation de codes de pratique, du matériel publicitaire, des décisions concernant l'application de la loi, et le maintien d'un registre des contrôleurs de données;
- **l'efficacité** : le lien entre les extrants et les objectifs finaux, qui peut être difficile à évaluer lorsque les buts sont multiples ou vagues et lorsque que l'association entre un but particulier et un résultat précis n'est pas évidente. Comme les résultats ne sont pas nécessairement établis par consensus, il est possible que les intrants et les extrants servent d'indicateurs des résultats. Une vision plus complexe de l'efficacité et des facteurs qui la différencient de l'efficience, est présentée dans la partie 1;
- **l'équité** : bien que ce critère de répartition ne fasse pas partie des analyses classiques de la protection de la vie privée, il permet d'évaluer qui bénéficie de la protection des données et de savoir qui bénéficie de la protection des données la plus étendue.

Raab et Bennett soutiennent que les évaluateurs des régimes de protection des données peuvent prendre en compte au moins cinq sujets d'évaluation, soit les suivants :

- **la loi** : sa portée (c.-à-d. si elle régit à la fois le secteur privé et le secteur public), sa clarté, la cohérence (c.-à-d. si ses définitions laissent place à l'interprétation et la façon dont les responsabilités et les droits sont répartis), la portée des exceptions, les recours et les sanctions possibles, les mécanismes d'application de la loi, la mesure dans laquelle la loi est associée aux technologies;
- **les mécanismes d'application** : prise en compte des évaluations officielles effectuées par des organismes indépendants, des mesures internes et des rapports sur les activités qui donnent une idée de la productivité au moyen de statistiques sur le nombre de demandes traitées, de brochures d'information distribuées, d'ordonnances ou de jugements rendus, etc.;
- **le rendement des utilisateurs de données** : la mesure dans laquelle les utilisateurs des données respectent la loi et les principes équitables de traitement de l'information, ce qui peut être évalué en examinant les « vérifications de la protection de la vie privée » effectuées directement par

395 *Id.*, p. 193.

les utilisateurs de données, qui sont parfois exigées par les organismes de réglementation de la protection des renseignements personnels;

- **le rendement des personnes concernées** : la mesure dans laquelle le grand public connaît les dangers associés à la protection des renseignements personnels et les façons de les enrayer, ce qui peut être évalué par l'examen du comportement du public en matière de protection, p. ex. le nombre de plaintes ainsi que des enquêtes sur l'attitude du public à l'égard de la protection des renseignements personnels;
- **le système de protection des données dans son ensemble** : mesures visant à déterminer si le système présente les caractéristiques suivantes : 1. une loi rigide et sans équivoque; 2. une autorité réglementaire active et assertive; 3. un engagement marqué des utilisateurs; 4. une population vigilante, intéressée et activiste. Des évaluations si globales peuvent permettre de cerner les relations entre les différentes parties du régime de protection des renseignements personnels, mais elles ne sont pas aussi efficaces pour trouver des moyens d'améliorer le rendement.

Raab et Bennett font remarquer que l'évaluation du rendement des autorités réglementaires peut être simplifiée à l'aide des dossiers internes généralement conservés par les autorités à des fins de production de rapports annuels et de réalisation d'examen internes semblables. Néanmoins, ils insistent sur le fait que ces mesures quantitatives peuvent induire en erreur puisqu'il est difficile de traduire les statistiques sur les intrants et les extrants en indicateurs du rendement. De plus, les extrants ne doivent pas nécessairement être associés à l'atteinte des buts (p. ex. l'augmentation du nombre de plaintes peut révéler une sensibilisation accrue du public à l'égard de l'organisme de réglementation, et non une insatisfaction accrue). Ainsi, Raab et Bennett laissent entendre que l'utilisation d'indicateurs plutôt qualitatifs peut donner un aperçu moins contradictoire dans le cadre de l'évaluation de la façon dont un organisme de réglementation influence les politiques gouvernementales ou commerciales. Leur conclusion est énoncée ci-dessous.

L'utilisation d'indicateurs quantitatifs révèle généralement que l'évaluation a été effectuée de façon « descendante » : une définition sans équivoque des buts et une mesure des buts atteints au fil du temps, au sein des organisations, des secteurs, de la technologie et finalement, des systèmes. En revanche, l'utilisation d'indicateurs qualitatifs témoigne généralement d'une méthode « ascendante » qui aborde l'évaluation d'une façon qui se rapproche du diagnostic. Bien que la mesure du rendement et l'utilisation des indicateurs appartiennent davantage à une méthode « descendante », le réalisme de la méthode « ascendante » peut être beaucoup plus révélateur puisqu'il permet d'analyser les situations où la formulation et la mise en œuvre des politiques vont de pair³⁹⁶ [traduction].

396 Charles Raab et Colin Bennett, « Évaluation du droit à la vie privée : la protection des données peut-elle être évaluée? », 1996, 62 *Revue internationale des sciences administratives*, 1996, 641, à 659-60.

Nous estimons que la solution optimale consiste à évaluer le CPVP de façon équilibrée. Dans le contexte du CPVP, il semble possible d'effectuer des analyses qualitatives et quantitatives si l'on se fie à l'examen quinquennal de la LPRPDE effectué en juillet 2007, au nombre important et croissant de recherches universitaires analysant la LPRPDE, aux données abondantes sur les activités du CPVP et sur les renseignements contenus dans ses rapports annuels. Nous sommes également d'avis qu'il est nécessaire d'étayer cette analyse avec des entrevues menées auprès d'intervenants importants et de spécialistes, des comptes rendus journalistiques et d'autres ressources détaillées.

4.3 Processus d'examen des organismes de réglementation provinciaux en matière de protection de la vie privée

La dichotomie de Raab et Bennett relative aux approches d'évaluation qualitative et quantitative correspond aux deux principaux types d'examen habituellement entrepris par les organismes de réglementation : examens périodiques et rapports annuels.

L'Alberta, la Colombie-Britannique et le Québec sont dotés de leurs propres lois en matière de protection de la vie privée dans le secteur privé qui vise les mêmes domaines que la LPRPDE dans les autres provinces. Les trois provinces ont entrepris assez récemment un vaste examen de leur régime de protection de la vie privée applicable au secteur privé.

En Alberta, le processus d'examen a abouti en novembre 2007 à un rapport intitulé *Review of the Personal Information Protection Act*³⁹⁷. La Colombie-Britannique a entrepris un processus d'examen similaire qui a entraîné la publication d'un rapport en 2008 intitulé *Streamlining British Columbia's Private Sector Privacy Law*³⁹⁸. De façon similaire, le Québec a réalisé l'examen quinquennal de son régime provincial en matière de protection de la vie privée qui a débuté par un examen interne de la Commission d'accès à l'information, qui a donné lieu à un rapport intitulé *Une réforme de l'accès à l'information : le choix de la transparence*³⁹⁹. Aux termes de l'examen quinquennal, ce rapport interne a entraîné la publication d'un rapport de la Commission de la culture en mai 2004, lequel misait sur le processus d'examen public⁴⁰⁰,

397 Comité spécial d'examen de la *Personal Information Protection Act*, « Streamlining British Columbia's Private Sector Privacy Law » Victoria, Assemblée législative de la Colombie-Britannique, 2008, <http://www.leg.bc.ca/cmt/38thparl/session-4/pipa/> [en anglais seulement].

398 Comité spécial d'examen de la *Personal Information Protection Act*, *supra*, note 331.

399 Commission d'accès à l'information du Québec, *Une réforme de l'accès à l'information : le choix de la transparence*, novembre 2002, voir : <http://www.cai.gouv.qc.ca/>.

400 Assemblée nationale, Commission de la culture, « Observations, conclusions et recommandations à la suite de la consultation générale et des auditions publiques à l'égard du document intitulé : *Une réforme de l'accès à l'information : le choix de la transparence* », mai 2004, voir : <http://www.cai.gouv.qc.ca/>.

de façon similaire aux examens des régimes de protection de la vie privée applicable au secteur privé entrepris par les gouvernements de l'Alberta et de la Colombie-Britannique. Le rapport émanant de l'étude de la Commission de la culture sera évalué ci-dessous, en plus des rapports de l'Alberta et de la Colombie-Britannique. L'examen quinquennal du Québec visait l'ensemble du régime de protection de la vie privée de la province, toutefois seules les sections visant la réglementation du secteur privé en matière de protection de la vie privée sont évaluées ci-dessous.

| Administration | Organe d'examen | Méthode |
|-----------------------|---|---|
| Alberta | Comité spécial d'examen de la Personal Information Protection Act | La consultation a été lancée en juillet 2006 lorsque le comité a distribué un guide de discussion à plus de 362 organisations. Le comité a reçu 65 soumissions à titre de réponse, dont 24 provenaient de l'industrie et d'associations commerciales ou professionnelles, 18 d'organisations individuelles, 13 d'organismes de réglementation professionnels et 7 de particuliers. Le comité a également entendu 10 présentations orales de la part de diverses personnes et organisations. |
| Colombie-Britannique | Comité spécial d'examen de la Personal Information Protection Act | Le comité a publié deux invitations à soumissionner dans les quotidiens de la province et a transmis des invitations électroniques à plus de 130 organisations afin qu'elles participent au processus d'examen législatif. Au total, 31 personnes et organisations ont présenté des soumissions écrites, et le comité a tenu 11 audiences publiques à Victoria et à Vancouver, au cours desquelles il a entendu 12 présentations de personnes et organisations. |
| Québec | Commission de la culture | Au total, 45 personnes et organisations ont présenté des soumissions écrites et 37 d'entre elles ont également fait des présentations dans le cadre des audiences publiques (septembre à octobre 2003). |

| Critères | Autorités de réglementation |
|---|------------------------------------|
| Conformité de la loi provinciale en matière de protection de la vie privée à la LPRPDE | Alberta |
| Caractère adéquat de la protection des renseignements transférés en dehors de la province | Alberta, C.-B., Québec |
| Est-ce qu'il devrait y avoir une exigence de notification obligatoire pour les atteintes à la protection des renseignements personnels? | Alberta, C.-B. |
| La loi provinciale en matière de protection de la vie privée devrait-elle s'appliquer aux organisations sans but lucratif? De quelle façon devrait-elle être appliquée? | Alberta |
| La loi provinciale en matière de protection de la vie privée devrait-elle s'appliquer à l'information en matière de santé? De quelle façon devrait-elle être appliquée? | Alberta |
| Caractère approprié des exigences en matière de consentement | Alberta, C.-B. |
| Caractère adéquat de la protection des renseignements personnels des employés | Alberta |
| Caractère adéquat de la réglementation de l'accès d'une personne concernée à ses renseignements personnels | Alberta, C.-B. |
| Caractère adéquat de la réglementation des frais d'accès et de correction des dossiers personnels | Alberta |
| Caractère adéquat de la réglementation des organismes de réglementation professionnels (p. ex. pour les médecins et les avocats) | Alberta, Québec |
| Caractère adéquat de la réglementation contrôlant la façon dont les dossiers sont gérés au sein d'une organisation | Alberta |
| Pouvoirs d'enquête et d'exécution du commissaire (rejet précoce des plaintes, secret professionnel, pouvoirs d'exécution, délais associés aux demandes, pouvoirs de vérification, pouvoirs d'enquête, etc.) | Alberta, C.-B., Québec |
| Fréquence à laquelle la loi en matière de protection de la vie privée doit être examinée | Alberta |
| Est-ce que les organisations devraient être tenues de publiciser leurs politiques sur la protection de la vie privée? | C.-B. |
| Est-ce que des procédures institutionnelles devraient être entreprises afin de diminuer le nombre de retards? | Québec |
| Accessibilité des mesures de protection de la vie privée pour les personnes handicapées? | Québec |

Rapports annuels

En plus des examens périodiques du rendement, les provinces dotées de leurs règlements en matière de protection de la vie privée applicables au secteur privé publient des états financiers et des rapports sur le rendement annuels⁴⁰¹. Ces rapports sur le rendement offrent des extraits de suivi sur les données quantitatives au fil de leur évolution. Les données quantitatives qui doivent être mesurées et rapportées chaque année font l'objet d'un vaste consensus. Les tendances de production de rapports en la matière sont indiquées ci-dessous :

| Critères | Autorités de réglementation |
|--|-----------------------------|
| Nombre de dossiers ouverts | Alberta, C.-B., QC |
| Responsable des dossiers (c.-à-d. commissaire, public ou organisme public) | Alberta, C.-B. |
| Types de dossiers ouverts (p. ex. demande d'information, demande d'examen, plaintes, etc.) | Alberta, C.-B. |
| Temps requis pour fermer les dossiers | C.-B., QC |
| Nombre de dossiers fermés | Alberta, C.-B., QC |
| Types de dossiers fermés | Alberta, C.-B. |
| Méthode de règlement (p. ex. par ordonnance ou par l'entremise de la médiation/d'une enquête) | Alberta, C.-B., QC |
| Résumés des dossiers médiatisés choisis | C.-B., QC |
| Nombre de rapports d'enquête publiés et détails connexes | Alberta |
| Nombre de résumés de dossiers publiés et détails connexes | Alberta |
| Nombre de ressources sur la conformité publiées en collaboration avec d'autres organismes de réglementation du secteur privé | Alberta, C.-B. |
| Conférences et examens législatifs/institutionnels. | Alberta, C.-B., QC |
| Résumés des décisions rendues | Alberta, C.-B. |
| Résumés des décisions des tribunaux et des contrôles judiciaires | Alberta, C.-B. |

Ainsi, bien qu'il n'y ait pas d'étude généralement reconnue sur la façon d'évaluer les organismes de réglementation en matière de protection de la vie privée, un consensus approximatif peut être tiré des tendances dans la façon dont

⁴⁰¹ Pour l'Alberta, voir : <http://www.oipc.ab.ca/pages/About/AnnualReports.aspx> [en anglais seulement]; pour la C.-B., voir : http://www.oipc.bc.ca/ann_report.htm [en anglais seulement]; pour le Québec, voir : <http://www.cai.gouv.qc.ca/index.html>.

les organismes de réglementation provinciaux s'évaluent eux-mêmes ou sont évalués par le gouvernement/Parlement. Les critères qu'ils utilisent présentent une importante convergence.

4.4 Examen des approches d'évaluation existantes

Notre analyse a pour but de miser sur les connaissances actuelles à propos de l'efficacité de l'application de la compétence relative à la LPRPDE par le CPVP, et de les accroître. De quelle façon le rendement du Commissariat à la protection de la vie privée est-il mesuré actuellement?

Comme il a été mentionné précédemment, en 2006-2007 le Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique de la Chambre des communes a lancé le premier examen quinquennal de la LPRPDE. Le Comité a reçu 42 soumissions de la part des organisations, 16 de la part de particuliers et 5 de la part de défenseurs de la protection de la vie privée et des consommateurs et de commentateurs en matière de protection de la vie privée. Le document de consultation a cerné 12 questions clés à examiner qui allaient des pouvoirs du commissaire aux normes et procédures relatives à la LPRPDE. Le Comité a remarqué que les répondants n'étaient souvent pas du même avis, ce qui n'est pas surprenant étant donné le caractère très large des questions du document de consultation. Le CPVP examine également ses propres activités dans le rapport annuel au Parlement et dans des études périodiques comme *Tracer le chemin : Principaux développements au cours des sept premières années d'application de la LPRPDE*.

Bien que ces rapports annuels et autres rapports comprennent de vastes examens des principales questions et enquêtes, ils se centrent principalement sur les mesures du rendement des extrants⁴⁰². Par l'entremise de ces rapports annuels, le commissaire à la protection de la vie privée consigne des mesures comme le nombre de demandes relatives à la LPRPDE, le nombre d'enquêtes, le temps requis pour clore les enquêtes, etc. Le CPVP produit également des vérifications annuelles du Bureau du vérificateur général du Canada et de la Commission de la fonction publique qui donnent une idée du rendement du CPVP en ce qui a trait aux mesures du rendement des intrants⁴⁰³. Le rapport annuel du CPVP et les rapports ministériels sur le rendement offrent une évaluation quantitative plus empirique du rendement du commissaire, par opposition à l'examen quinquennal plus impressionniste. L'association de ces efforts d'évaluation offre un point de départ constructif pour la présente analyse.

402 Rapports concernant la *Loi sur la protection des renseignements personnels et les documents électroniques*, voir : http://www.priv.gc.ca/information/02_05_b_f.cfm#contenttop.

403 Vérifications du CPVP menées par le Bureau du vérificateur général et la Commission de la fonction publique, voir : http://www.priv.gc.ca/information/an-av_f.cfm#contenttop.

Nous croyons que l'évaluation actuelle de la LPRPDE et du CPVP peut être améliorée par l'intégration des leçons susceptibles d'être tirées d'autres administrations canadiennes (notamment le Québec, l'Alberta et la C.-B.) de même que des É.-U. et du R.-U. Nous croyons également que les données qualitatives sur les évaluations des intervenants et universitaires quant au CPVP peuvent enrichir l'analyse comparative présentée ci-dessus.

4.5 Étude des perceptions à l'égard du CPVP

Aux termes de notre analyse, nous avons réalisé une série d'entrevues afin de mieux comprendre la façon dont le modèle actuel des activités du CPVP en vertu de sa compétence relative à la LPRPDE est perçu. Nous traitons des questions posées dans le cadre des entrevues et des réponses fournies ci-dessous.

1) Est-ce que le Commissariat à la protection de la vie privée du Canada (CPVP) respecte son programme législatif en vertu de la LPRPDE?

Les répondants ont fait valoir que le CPVP était généralement bien perçu et qu'il avait réussi à encourager la conformité volontaire aux obligations de la LPRPDE, particulièrement en ce qui a trait aux grandes industries établies. Dans une certaine mesure, l'efficacité du CPVP va de pair avec l'efficacité de la LPRPDE elle-même. Les résultats du sondage laissent entendre que la LPRPDE a eu un effet positif dans le traitement des renseignements personnels des clients par les grandes entreprises (100 employés et plus), les moyennes (de 21 à 100 employés) et les petites (de 1 à 20 employés).

Un sondage EKOS mené en mars 2010 démontre l'impact de la LPRPDE⁴⁰⁴. On a posé aux répondants de ce sondage des questions au sujet de l'incidence de la LPRPDE sur leur entreprise. Plus des deux tiers des répondants ont signalé qu'ils se préoccupaient davantage de protéger les renseignements personnels de leurs clients en raison de la LPRPDE et environ le même nombre ont répondu que la LPRPDE les avait rendus plus conscients de leurs obligations en matière de protection de la vie privée. Plus de la moitié des répondants considéraient que les mesures de sécurité entourant les renseignements personnels s'étaient améliorées en raison de la LPRPDE et le tiers croyaient que la LPRPDE a eu comme résultat de réduire le nombre d'atteintes à la sécurité des renseignements personnels de leurs clients.

Bien que le sondage n'ait pas abordé directement les activités du CPVP, les personnes avec qui nous avons communiqué perçoivent le Commissariat comme étant innovateur concernant le rayonnement, son soutien à la recherche et les initiatives locales.

404 Voir EKOS, Les entreprises canadiennes et la protection des renseignements personnels (mars 2010), http://www.priv.gc.ca/information/survey/2010/ekos_2010_01_f.pdf (consulté le 15 juillet 2010), p. 21

L'enquête relative à la protection de la vie privée dans Facebook en 2009 a été citée par de nombreux répondants à titre de point tournant en vue d'accroître la crédibilité du CPVP et de le faire mieux connaître, particulièrement chez les jeunes Canadiennes et Canadiens.

Bien que le règlement relatif à Facebook montre le côté positif des activités de conformité fondées sur les plaintes, certains répondants ont également souligné que le CPVP était restreint par son manque de ressources, particulièrement en ce qui a trait à la prévention et au rehaussement de sa crédibilité.

Même si les répondants ont une opinion positive quant à l'évolution du CPVP, tous s'entendent pour dire qu'il a moins bien réussi à respecter son programme par rapport au secteur des moyennes entreprises, et particulièrement des petites entreprises. Environ 85 % de l'ensemble des entreprises canadiennes sont de petites entreprises. Les petites entreprises tendent à percevoir les questions de protection de la vie privée comme des coûts supplémentaires apportant peu de valeur ajoutée, et c'est dans ce contexte que les répondants soulignent les lacunes du modèle du CPVP et son manque de pouvoirs d'exécution en particulier. Dans ce secteur, le CPVP n'a pas su établir des mesures incitatives importantes en vue de la conformité.

Le sondage EKOS abordé ci-dessus rapporte que les petites entreprises sont moins susceptibles d'être au courant des lois sur la protection des renseignements personnels, moins susceptibles d'avoir en place des politiques sur la protection de la vie privée, moins susceptibles d'avoir mis en œuvre les politiques dont elles disposeraient, et moins susceptibles d'avoir en place des mesures de protection des renseignements personnels⁴⁰⁵.

Les arriérés constituent un domaine où le progrès est reconnu, mais où il y a place à l'amélioration.

D'autres répondants ont souligné le défaut du CPVP à « nommer des noms » relativement aux entreprises visées par des plaintes, ce qui limite son levier publicitaire.

Les répondants étaient d'avis que la qualité des motifs et des conclusions s'améliorait au fil du temps, bien que, selon certains, un des défauts du modèle d'ombudsman était le caractère limité des détails à l'appui des décisions.

Tandis que la sophistication de l'administration de la LPRPDE par le CPVP s'accroît, certains répondants estimaient qu'une approche plus consultative relativement aux directives, et l'établissement d'un régime de règlements rapides accroîtraient l'efficacité du CPVP.

405 *Id.*, p. 7, 9-10 et 15.

Enfin, même si les objectifs de la LPRPDE en matière de protection des renseignements personnels puissent sembler évidents, plusieurs répondants ont souligné le fait que le CPVP n'avait pas accordé suffisamment d'attention à l'établissement d'objectifs de rendement et de points de référence en ce qui a trait à la LPRPDE.

2) Nous sommes particulièrement intéressés de connaître votre opinion quant à la possibilité que le CPVP ait de plus grands pouvoirs d'ordonnances ou d'exécution. Appuyez-vous cette idée? Pouvez-vous exprimer vos pensées à cet égard?

Les répondants des groupes de l'industrie tendent à appuyer les pouvoirs actuels du CPVP de même qu'à relever l'efficacité de la Cour fédérale en tant que « dernier recours », mais la plupart des autres répondants sont en faveur de plus grands pouvoirs d'ordonnance, particulièrement à titre de moyen de favoriser et d'assurer la conformité dans les secteurs des petites et moyennes entreprises. Bien que la plupart des répondants aient été en faveur de conférer des pouvoirs d'ordonnance au CPVP, ils étaient également d'avis que ces pouvoirs devaient être utilisés avec modération. Ils estimaient que la menace crédible et efficace du pouvoir de rendre des ordonnances accroîtrait l'efficacité des autres activités proactives et éducatives du CPVP.

Certains répondants ont adopté une approche visant à recourir au pouvoir de rendre des ordonnances si nécessaire seulement. Ils ont souligné les façons dont les pouvoirs existants pourraient être utilisés de façon plus créative afin d'atteindre les mêmes résultats. Ils ont fait valoir que la prudence des premières années de surveillance de la LPRPDE devait faire place à des initiatives plus audacieuses. Par exemple, l'établissement d'un régime d'accréditation pour les entreprises pourrait être beaucoup plus efficace dans le secteur des petites et moyennes entreprises que la menace de sanctions.

D'autres pouvoirs, comme la vérification, pourraient être enrichis de ressources supplémentaires. La déclaration obligatoire des atteintes à la protection des renseignements personnels entraîne d'autres possibilités d'outils de conformité améliorés autres que les pouvoirs de rendre des ordonnances.

Bien que le pouvoir de rendre des ordonnances ne règle pas tous les problèmes qu'a eus le CPVP en vue d'assurer le respect de la LPRPDE, la plupart des répondants ont reconnu que, logiquement, celui-ci améliorerait sa conformité. L'expérience des commissaires à la protection de la vie privée provinciaux veut que la conformité soit améliorée même lorsque les pouvoirs de rendre des ordonnances sont utilisés avec modération. Le BSIF constitue un autre exemple du recours à ce modèle.

Au-delà de l'amélioration de la conformité, les répondants ont souligné d'autres avantages associés aux régimes d'ordonnances, notamment une plus grande rigueur et des détails plus précis dans les conclusions émises par les organismes de réglementation. La crédibilité et l'importance des agents de conformité de l'industrie seraient également améliorées si ces personnes étaient responsables

d'éviter les sanctions, ce qui serait susceptible d'entraîner l'affectation de meilleures ressources au respect de la LPRPDE par le secteur privé.

3) Comment croyez-vous que le secteur privé réagirait si le CPVP avait de plus grands pouvoirs de rendre des ordonnances ou d'exécuter la loi?

Les répondants étaient d'avis que, peu importe si les pouvoirs de rendre des ordonnances nuisaient ou non à l'industrie, celle-ci risquait de s'y opposer par principe, ou parce qu'elle l'avait fait dans le passé et n'avait aucune raison de changer son point de vue. Certains répondants ont fait valoir que l'établissement du modèle d'ombudsman avait été perçu comme une « victoire » pour l'industrie au moment de sa mise en œuvre. D'autres ont mentionné que l'industrie était d'abord sceptique quant aux pouvoirs de rendre des ordonnances et qu'elle était d'avis qu'on n'avait pas établi la preuve de leur nécessité.

De plus, certains répondants ont souligné le fait que le secteur privé s'était bien ajusté à une compétence similaire dans le contexte des commissaires provinciaux à la protection de la vie privée. D'autres ont fait valoir que la relation de confiance entre les industries établies et le CPVP fait en sorte que l'idée d'établir des pouvoirs de rendre des ordonnances est moins inquiétante qu'elle ne l'aurait été il y a dix ans.

4) Quels critères devraient selon vous servir à évaluer les activités du CPVP en vertu de la LPRPDE?

Les répondants ont soulevé un vaste éventail de critères et mesures possibles afin d'évaluer l'efficacité des activités du CPVP relatives à la LPRPDE. Parmi ceux-ci se trouvent les suivants :

- Réaliser des sondages auprès des entreprises de divers secteurs (entreprises, consommateurs, etc.) afin de déterminer la façon dont le CPVP et la LPRPDE sont perçus;
- Mener des enquêtes relatives à la « crédibilité » du CPVP et de la LPRPDE dans les médias;
- Élaborer un plan stratégique associé à des points de référence et objectifs de rendement transparents en ce qui a trait au respect de la LPRPDE et au processus du CPVP (p. ex. réduction de l'arriéré, des retards, etc.);
- Se centrer sur des activités plus stratégiques dans le contexte des domaines à risque élevé;
- Établir des mesures de la conformité afin de permettre une analyse longitudinale et latitudinale;
- Déterminer si le processus de consultation est perçu comme étant utile (de même que son incidence sur les résultats). Obtenir le point de vue des participants à des exercices de consultation multiples quant à la position du CPVP par rapport à ses homologues du domaine de la réglementation comme l'ACFC ou le BSIF.

5) Quels sont les futurs défis qui risquent selon vous d'affecter les activités du CPVP en vertu de la LPRPDE?

Cette question ouverte a généré un vaste éventail de réponses, notamment les suivantes :

- Convergence technologique et nouvelles utilisations (et abus) des renseignements personnels;
- Nouvelle génération de jeunes personnes qui perçoivent la protection de la vie privée d'une manière complètement différente — forgée par l'entremise du réseautage social;
- Une perte importante en matière de litige pourrait miner la crédibilité du CPVP;
- Le besoin croissant de protection de la vie privée au-delà des frontières, et l'attente de leadership de la part du Canada (p. ex. Facebook);
- Besoin accru d'une meilleure coordination avec d'autres organismes de réglementation (p. ex. collaboration avec le CRTC afin d'accroître l'efficacité de la Liste nationale de numéros de télécommunication exclus ou des mesures anti-pourriel).

CONCLUSIONS DE LA PARTIE II

Dans cette partie, nous avons exploré en détail le milieu opérationnel du CPVP relatif à la LPRPDE. En vue de souligner les critères d'évaluation appropriés, nous avons exploré les perspectives empiriques, comparatives et normatives du modèle d'ombudsman du CPVP.

D'un point de vue empirique, nous avons discuté des raisons pour lesquelles un examen des extraits du CPVP fondé sur les dates uniquement n'est pas satisfaisant. Le fait que le nombre de demandes ou de plaintes ait augmenté ou diminué ne révèle pas si le modèle du CPVP visant à assurer la conformité à la LPRPDE fonctionne bien. Les données à elles seules peuvent appuyer les arguments relatifs à l'efficacité ou à l'inefficacité du CPVP. Nous croyons également que les données qualitatives sur les évaluations des intervenants et universitaires quant au CPVP peuvent enrichir les données quantitatives. La perception commune voulant que le modèle du CPVP est beaucoup plus efficace au sein des industries établies comme celle des banques ou de l'assurance qu'au sein des petites entreprises, où les renseignements personnels risquent d'être vulnérables, est particulièrement frappante.

D'un point de vue comparatif, nous croyons que l'évaluation actuelle de la LPRPDE et du CPVP peut être améliorée par l'intégration des leçons susceptibles d'être tirées d'autres administrations canadiennes (notamment le Québec, l'Alberta et la C.-B.) de même que des É.-U. et du R.-U.

Au sein des autres administrations canadiennes, par exemple, nous avons remarqué que l'expérience du Québec démontrait que l'indépendance et l'impartialité, à titre de normes du droit administratif de base, offraient les fondements sur lesquels reposent la conception institutionnelle et la recherche d'un modèle optimal. Les exemples de l'Alberta et de la C.-B. montrent que

le modèle d'ombudsman peut coexister avec d'autres mesures d'exécution et de conformité et les compléter, y compris les pouvoirs de rendre des ordonnances.

Les exemples des É.-U. comme la FCC et la FTC sont le reflet du passage de règlements spéciaux politisés à des règlements stratégiques fondés sur des données probantes. Cette approche envers la réglementation met l'accent sur la planification, l'établissement de points de référence et l'évaluation du rendement. En Europe, nous avons observé que le juridisme de coopération représentait un cadre pratique afin de comprendre la façon dont un plus grand rôle pour l'État et un plus grand rôle pour le marché pouvaient constituer des objectifs complémentaires pour un organisme de réglementation. L'exemple européen, comme celui d'autres organismes canadiens de réglementation en matière de protection de la vie privée, suggère un mélange complexe et complémentaire des modèles d'ombudsman et du pouvoir de rendre des ordonnances.

D'un point de vue normatif, nous avons analysé la façon dont le choix des critères d'évaluation était une expression de certaines valeurs particulières. Par exemple, le fait que Bennett et Raab donnent priorité à l'économie, à l'efficacité, à l'efficacite et à la justice, qui sont liées à la sphère de la protection de la vie privée, donne à penser que la mesure de la justice distributive dans la réglementation en matière de protection de la vie privée (qui offre la meilleure protection des données?) est tout aussi importante que le fait de veiller à ce que l'industrie respecte la loi.

Qu'il soit analysé du point de vue empirique, comparatif ou normatif, nous sommes d'avis qu'il y a des éléments qui confirment que le modèle d'ombudsman du CPVP est un succès, ce qui a eu une incidence concrète et importante sur les objectifs énoncés dans la LPRPDE, et d'autres qui donnent à penser que le CPVP est restreint dans la réalisation de son mandat en vertu de la LPRPDE. Nombreux sont ceux qui appuient l'argument selon lequel une transition vers une LPRPDE orientée vers la protection des consommateurs ou un effort afin de veiller au respect de la LPRPDE par les petites entreprises nécessitent l'obtention de plus grands pouvoirs de rendre des ordonnances afin de compléter les responsabilités d'ombudsman actuelles.

Dans la troisième et dernière section, nous déterminerons la façon dont une utilisation créative des pouvoirs existants et de nouveaux pouvoirs de rendre des ordonnances pourrait donner lieu à des activités plus efficaces et efficientes en vue d'accroître le respect de la LPRPDE.

CONCLUSIONS GÉNÉRALES ET RECOMMANDATIONS

Les conclusions et recommandations qui suivent sont fondées sur notre analyse et informées par notre analyse documentaire, notamment d'études primaires et secondaires, de rapports et d'articles, et de nos discussions avec un grand nombre de personnes possédant des connaissances approfondies sur le modèle d'ombudsman du CPVP, y compris le personnel du CPVP, des universitaires spécialisés en lois et politiques sur la protection de la vie privée, des avocats qui donnent des conseils à leurs clients au sujet de la LPRPDE et des représentants de groupes industriels. Nos discussions n'ont pas été exhaustives; elles ont fourni plutôt une perspective qualitative valable sur les questions que nous voulions aborder dans la présente étude.

Nos conclusions et recommandations comportent également une part de subjectivité. Elles représentent notre plus juste appréciation de l'efficacité du modèle d'ombudsman du CPVP à la lumière des critères que nous avons établis dans les parties 1 et 2 de la présente étude, et des mécanismes qui, à notre avis, pourraient améliorer davantage l'efficacité du CPVP.

Le modèle d'ombudsman et les activités de conformité en place ont permis au CPVP d'atteindre d'importants objectifs, notamment les suivants :

- Élever les niveaux de conformité à la LPRPDE par l'entremise de la collaboration avec certaines industries (p. ex. banques, transporteurs aériens, assurances, etc.) et par le traitement de certains sujets (p. ex. réseautage social, etc.);
- Bâtir une relation de confiance avec le secteur des affaires, collaborer avec les entreprises, les défenseurs de la protection de la vie privée et les ONG, et établir des relations avec les responsables de la protection de la vie privée et de la conformité et les groupes de l'industrie;
- Offrir des directives quant à l'interprétation des normes de la LPRPDE;

- Répondre aux plaintes, aux demandes de renseignements et aux préoccupations;
- Améliorer la crédibilité des questions relatives à la protection de la vie privée de façon générale et à la LPRPDE en particulier.

La couverture médiatique positive des derniers temps quant à la réponse du CPVP aux préoccupations relatives à Facebook et à Google soulignent le succès et le potentiel du modèle d'ombudsman et son rayonnement croissant dans les nouveaux domaines de la protection des consommateurs (c.-à-d. les jeunes qui prennent part à des activités en ligne qui mettent en cause leurs renseignements personnels). Toutefois, à la lumière de ces réalisations, devrions-nous en accomplir davantage et, dans l'affirmative, comment devons-nous procéder?

Comme nous l'avons expliqué dans la première partie, les idées économiques, politiques et juridiques dominantes qui ont circulé dans les années 1990 ont forgé le modèle d'ombudsman du CPVP. Par exemple, au moment de son entrée en vigueur, il constituait le résultat d'un compromis politique dont la forme finale était en partie une réponse à certaines préoccupations du secteur privé quant à une réglementation envahissante et coûteuse, de même qu'à des préoccupations politiques croissantes touchant la vulnérabilité des renseignements personnels dans le secteur privé. Le fait de comprendre l'évolution et le transfert de ces idées est essentiel non seulement pour expliquer l'évolution de l'application de la LPRPDE par le CPVP, mais également pour appuyer son orientation future.

À cet égard, il ne fait aucun doute que des recherches supplémentaires devront être réalisées afin de mieux comprendre l'environnement actuel et de faire des prévisions quant aux tendances futures. En effet, un examen adéquat de l'efficacité d'un modèle institutionnel nécessite qu'on porte attention à plusieurs macro et micro facteurs de son fonctionnement. Par conséquent, notre rapport devrait être perçu comme une exploration des principaux facteurs liant le contexte de l'émergence de la LPRPDE et le contexte actuel en vue de déterminer les avenues à explorer dans les prochaines recherches. À partir de ce point de vue, nous recommandons en premier lieu de procéder à des recherches approfondies dans les domaines suivants :

- **Recommandation 1 : Nouvelles questions de recherche**

- 1) Quels sont les défis à relever dans le contexte du Web 2.0 et quels sont les nouveaux enjeux soulevés par ce nouvel environnement, notamment quant à l'harmonisation des réglementations et mécanismes relatifs à la protection des renseignements personnels à l'échelle nationale et supranationale?
- 2) Est-ce que le modèle d'ombudsman institué par la LPRPDE peut adéquatement répondre à ces nouveaux défis et enjeux contemporains? Bien que nos travaux aient porté sur le modèle d'ombudsman du CPVP, d'autres modifications plus fondamentales pourraient également être envisagées, notamment la création d'un organisme de réglementation décentralisé plutôt qu'une commission administrative. Quels seraient les avantages et les inconvénients de chacune de ces options sur les plans économique, politique et juridique?

- 3) Dans le contexte constitutionnel actuel, jusqu'où est-il possible d'aller pour assurer la cohérence des réglementations fédérale, provinciales-territoriales et supranationales (directives européennes, par exemple) en tenant compte du partage des compétences législatives, des droits des personnes ainsi que des multiples accords et cadres intergouvernementaux, dont l'Accord sur le commerce intérieur? Est-ce que les pouvoirs du commissaire en vertu de la LPRPDE sont suffisants pour agir efficacement sur ces différents plans? Est-ce que le CPVP ne devrait pas être doté de pouvoirs et ressources additionnels (par la mise sur pied et la direction d'un conseil consultatif, par exemple).

Bien que plusieurs pièces du casse-tête manquent pour donner une meilleure idée de l'environnement actuel dans lequel devra s'appliquer la LPRPDE, notre recherche nous a permis de croire qu'un changement s'effectuait vers l'assurance d'une protection accrue pour les consommateurs, particulièrement en ce qui concerne les nouvelles technologies. Toutefois, si ce point de vue s'avérait juste, il faudrait répondre à un certain nombre de questions, par exemple : Quel serait le niveau adéquat de protection à offrir aux consommateurs? S'il fallait accroître ce dernier de manière importante, quel serait son incidence sur la capacité concurrentielle des industries qui œuvrent aux échelles nationales et transnationales? De quelle façon ce niveau accru de protection devrait-il s'inscrire dans la LPRPDE? Est-ce qu'il faudrait accorder davantage de pouvoirs au CPVP pour qu'il puisse s'acquitter de responsabilités plus importantes en vue de protéger les consommateurs?

Si la dernière question, en particulier, recevait une réponse positive, le CPVP aura besoin de ressources financières et humaines supplémentaires dans le but de pouvoir remplir son mandat évolutif. À cette fin, il conviendra de réaliser une analyse significative des coûts-avantages : les ressources limitées doivent être affectées en vue d'atteindre les résultats les plus importants (par exemple, la collaboration avec les médias permet au CPVP de mieux se faire connaître en ce qui a trait à la LPRPDE sans devoir tenter de communiquer directement avec toutes les personnes touchées par celle-ci). À l'heure actuelle, le CPVP dispose d'un budget approximatif de 22 millions de dollars et d'un effectif d'environ 178 ETP. Par conséquent, avec un nombre si peu élevé d'employés à affecter à un large éventail de vérifications ou d'enquêtes, il paraît évident que la capacité du CPVP à remplir son mandat visant à garantir une protection accrue aux consommateurs devra être étayée par d'importantes ressources consacrées à l'exécution.

Outre la capacité et les ressources, d'autres facteurs doivent être pris en compte en réfléchissant aux changements et à ceux qui ont orienté les activités du CPVP en vertu de la LPRPDE. Par exemple, un bureau d'ombudsman peut trouver difficile d'envisager changer son modèle opérationnel compte tenu que le personnel est formé autour du modèle d'ombudsman, lequel a servi à instaurer la culture du bureau. Pour le CPVP toutefois, qui est doté d'importants pouvoirs de rendre des ordonnances en vue d'exécuter la *Loi sur la protection des renseignements personnels* de sorte que ses employés et sa culture soient déjà engagés dans le sens de ces méthodes élargies, ce changement modifierait non seulement le modèle opérationnel pour en faciliter l'application, mais traiterait

aussi de ce que certains répondants à nos entrevues ont décrit comme un fossé institutionnel entre les activités de conformité liées à la *Loi sur la protection des renseignements personnels* et à la LPRPDE au sein du CPVP.

Ces avertissements mis à part et avec cette vaste perspective en tête, nous recommandons l'examen des enjeux suivants :

- **Recommandation 2 : Étendre les limites du modèle d'ombudsman**

Le modèle d'ombudsman connaît beaucoup de succès dans les grandes industries qui sont plus susceptibles d'employer des professionnels de la protection de la vie privée qualifiés, de collaborer avec des organismes de réglementation et d'être vulnérables à une publicité négative. Le modèle convenait particulièrement bien à la première étape de réglementation de l'industrie, qui suscitait de considérables préoccupations à propos des répercussions de la réglementation sur l'entreprise commerciale. Il a ainsi réussi à instaurer la confiance et la crédibilité, à créer un espace pour des occasions de formation et de sensibilisation et à faire accepter le CPVP ainsi que son mandat en vertu de la LPRPDE. Or, les consultations que nous avons menées démontrent clairement que pour plusieurs, le modèle actuel ne semble pas convenir aussi bien au secteur des petites et moyennes entreprises, où les taux de conformité sont plus faibles et le risque à l'égard des renseignements personnels, plus important⁴⁰⁶.

Le CPVP devrait continuer à user de son influence aux termes du modèle d'ombudsman pour parvenir au respect de la LPRPDE, surtout de la part des grandes entreprises (p. ex. les banques, les compagnies d'assurance, les services publics, la technologie de l'information et les médias) et en particulier de continuer de tirer le meilleur parti de l'attention médiatique et sa visibilité, dans ses démarches visant à instaurer une culture de protection du droit à la vie privée au sein de l'industrie des médias sociaux. Le CPVP devrait continuer de cibler les petites et moyennes entreprises à des fins de sensibilisation, d'éducation et de mesures incitatives liées à la conformité. Il se pourrait également que ces deux sphères d'activités de l'ombudsman se renforcent mutuellement. À mesure que le CPVP atteint davantage de visibilité pour ses efforts visant à protéger la vie privée dans le contexte de multinationales des médias sociaux, il pourrait gagner davantage de crédibilité et de poids dans ses démarches visant la protection des renseignements personnels dans le contexte des petites et moyennes entreprises.

406 Voir les différences entre les petites, moyennes et grandes entreprises dans : Les associés de recherche EKOS, « Les entreprises canadiennes et les enjeux liés au respect de la vie privée » (CPVP 2007), section 2 à l'adresse suivante : http://www.priv.gc.ca/information/survey/2007/ekos_2007_01_f.cfm#section2; ainsi que dans le sondage de suivi au http://www.priv.gc.ca/information/survey/2010/ekos_2010_01_f.pdf.

Dans le même ordre d'idées, il serait opportun de souligner que le CPVP a ouvert un bureau à Toronto au cours de l'été 2010. Ce bureau est dirigé par une ancienne agente de la protection des renseignements personnels d'une grande banque canadienne, dans le cadre d'un programme d'échange des cadres. Le recours à de telles mesures innovatrices pourrait également améliorer la portée du CPVP dans la communauté des petites et moyennes entreprises.

- **Recommandation 3 : Accorder des pouvoirs limités pour ce qui est de rendre des ordonnances**

En définitive, nonobstant les importantes réussites du CPVP, les taux de conformité à la LPRPDE demeurent probablement trop faibles, et le risque encouru par les consommateurs eu égard à leurs renseignements personnels détenus par les petites et moyennes entreprises au Canada, probablement trop élevé. Malgré leur importance, les efforts de sensibilisation et d'éducation de même que les mesures incitatives liés à la conformité destinés aux petites et moyennes entreprises peuvent ne pas suffire à atteindre les buts visés. En se fiant à l'expérience des organismes de réglementation provinciaux du Canada ainsi qu'à l'expérience américaine et européenne, la capacité d'imposer une amende et autres possibilités de rendre des ordonnances peuvent entraîner une conformité supplémentaire et constituer un important élément dissuasif malgré un emploi peu fréquent. Les avantages de cette approche paraissent tangibles et les risques, moins préoccupants qu'ils ne l'étaient par le passé. Le risque, par exemple, a tendance à porter sur la réaction négative attendue de la part des entreprises, des tensions contradictoires accrues, la judiciarisation ainsi qu'à des coûts additionnels et une plus grande complexité tant pour le CPVP que pour les entreprises. L'expérience provinciale avec les organismes de réglementation investis du pouvoir de rendre des ordonnances suggère toutefois une surestimation possible de ces risques. Le traitement accordé aux préoccupations en matière de vie privée dans les médias et surtout dans le contexte des médias sociaux et des nouvelles technologies ont établi un climat moins propice à la réglementation, et qui pourrait également avoir suscité des attentes de la part des consommateurs, à savoir que les entreprises se conformeraient aux réglementations sur la vie privée et que les démarches réglementaires entreprises par le CPVP seraient efficaces.

Bien que nous ne soyons assurément pas les premiers à préconiser de plus grands pouvoirs en matière d'ordonnances⁴⁰⁷, nous ne pensons pas qu'en ce moment, le CPVP a besoin de pouvoirs élargis et envahissants, comme des ordonnances de cessation. À notre avis, le renforcement du pouvoir du CPVP en matière d'ordonnances ne devrait cibler que le genre d'activités d'exécution

407 En particulier, la CIPPIC a, de façon constante, préconisé de plus grands pouvoirs réglementaires pour le CPVP. Voir ses observations devant le Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique de la Chambre des communes à l'adresse suivante : http://www.cippic.ca/en/projects-cases/privacy/submissions/CIPPIC_Submission_Nov06wFNs.pdf.

de la loi appropriées pour les petites et moyennes entreprises (par exemple, les amendes et les sanctions). Ce sont ces secteurs où les taux de conformité semblent les plus faibles et où toutes les données disponibles des organismes provinciaux chargés de surveiller le respect de la loi suggèrent que seule la menace de sanctions qui influent sur la rentabilité peut mener à un changement dans le comportement des entreprises et, en définitive, dans la culture entrepreneuriale. Même si le pouvoir de rendre des ordonnances peut ne pas s'avérer aussi nécessaire dans le secteur des grandes entreprises, où le CPVP a déjà réalisé des progrès en ce qui a trait à l'amélioration de la conformité, il pourrait avoir des effets bénéfiques dans ce contexte également. Le pouvoir de rendre des ordonnances peut renforcer l'importance des politiques en matière de protection de la vie privée par l'entremise de ces secteurs ainsi qu'améliorer l'image des agents de vérification de la conformité. De plus, l'expérience positive issue de la collaboration, de la consultation et de l'engagement de ce secteur avec le CPVP a permis de jeter les importantes bases d'un savoir, d'une confiance et d'une crédibilité institutionnels sur lesquelles miser si le CPVP recevait d'autres outils de réglementation.

Nous concluons également que le renforcement de la capacité du CPVP à rendre des ordonnances en vertu de la LPRPDE ne minerait sans doute pas l'efficacité de son modèle d'ombudsman. Le relatif succès des organismes de réglementation hybrides en matière de protection de la vie privée de la Colombie-Britannique, de l'Alberta et d'ailleurs, qui s'ajoute à l'approche de « juridisme de coopération » de plusieurs administrations européennes, suggère qu'un modèle d'ombudsman amélioré avec un pouvoir limité en matière d'ordonnances permet la mise en œuvre de stratégies de conformité efficaces et polyvalentes. En fait, il se pourrait fort bien que le pouvoir le plus efficace de rendre des ordonnances dans le contexte de réglementation de la protection de la vie privée en soit un auquel il est rarement fait recours.

Les pouvoirs supplémentaires décrits feront probablement en sorte que le CPVP devienne un organisme de réglementation plus efficient et efficace en vertu de la portée de la LPRPDE. Le fait d'énoncer à nouveau les quatre critères établis par Bennett et Raab et dont il a été question à la partie 2 permet de constater les améliorations éventuelles suivantes.

- 1) **Économie** (p. ex. le coût correspondant à l'instauration d'un régime réglementaire). Le passage à un modèle hybride peut réduire le besoin de la séparation existante des activités du CPVP en deux sphères distinctes, l'une se rapportant à la LPRPDE et l'autre à la *Loi sur la protection des renseignements personnels*. Des dépenses supplémentaires associées au modèle hybride pourraient s'ajouter, mais en tant qu'approche générale, rien ne justifie un changement important dans le budget ou la dotation du CPVP advenant l'adoption d'un modèle hybride.
- 2) **Efficience** (p. ex. le coût du régime mesuré par rapport à ses résultats). Le passage à un modèle hybride mènerait sans doute à une efficience accrue, surtout dans les secteurs des petites et moyennes entreprises. Une plus vaste incursion dans ces secteurs, typiquement plus sensibles au risque et aux sanctions d'ordre financier, associée à l'effet dissuasif de l'évitement d'une intervention réglementaire a bien des chances d'entraîner

des résultats plus importants pour un investissement égal sur le plan des efforts et des ressources. En outre, ce modèle réglerait la situation actuelle où le fait d'entamer des poursuites à la Cour fédérale constitue le seul, et malheureusement inefficace, moyen par lequel le CPVP peut voir une de ses ordonnances exécutée.

- 3) **Efficacité** (p. ex. la mesure dans laquelle les résultats pratiques du régime lui permettent d'atteindre ses objectifs ultimes). Les études du CPVP et de la CIPPIC abordées dans la partie 2 montrent que le taux de non-conformité demeure élevé. Le passage à un modèle hybride est susceptible de l'accroître, particulièrement dans les secteurs des petites et moyennes entreprises (il est impossible de mesurer l'efficacité sans repères et objectifs précis).
- 4) **Équité** (p. ex. la mesure dans laquelle le régime étend la protection de manière équitable dans l'ensemble des groupes sociaux). Bien que les consommateurs semblent apprécier une protection accrue découlant des activités du CPVP s'il s'agit de clients de banques ou de compagnies d'assurance, de médias sociaux ou grand public, ceux des petites et moyennes entreprises bénéficient d'une protection bien moindre. L'adoption d'un modèle hybride améliorerait l'équité et assurerait que la protection des consommateurs ne dépende pas autant de la taille et de la complexité de l'entreprise comme c'est le cas maintenant.

Pour les raisons énoncées plus haut, et à la lumière de notre analyse des parties 1 et 2, nous sommes d'avis qu'il serait justifié de renforcer de façon restreinte les pouvoirs réglementaires du CPVP, au moins afin de comprendre ceux d'imposer des amendes pour non-conformité.

- **Recommandation 4 : Accorder un pouvoir explicite d'émettre des directives**

Bien que les risques qu'entraîneraient les plus grands pouvoirs et le modèle hybride suggéré ci-dessus ne pourraient pas être exclus, ceux-ci peuvent être atténués de façon significative, par exemple en communiquant clairement la justification des pouvoirs supplémentaires, en publiant des directives afin de rehausser la cohérence et la prévisibilité dans l'exercice de ces nouveaux pouvoirs à la suite d'un processus de consultation et, enfin, en misant sur les liens de confiance déjà tissés par l'entremise du modèle d'ombudsman. L'utilisation de la « réglementation non impérative » par le CPVP a permis de faire le pont entre les pouvoirs législatifs et les pratiques administratives.

Des directives claires quant à l'utilisation de ce pouvoir de rendre des ordonnances, et des mesures de protection afin de garantir l'équité aux personnes qui en font l'objet, représenteront des outils essentiels de responsabilisation et, selon nous, elles devraient accompagner le pouvoir de réglementation supplémentaire. L'élaboration de directives fournit aussi l'occasion de consulter les intervenants, d'analyser les pratiques exemplaires d'organismes de réglementation pairs en plus de constituer un contexte au sein duquel les valeurs du CPVP peuvent être clairement communiquées aux personnes assujetties à la portée de la LPRPDE pour le CPVP.

- **Recommandation 5 : Envisager d'autres pouvoirs réglementaires créatifs**

Notre analyse montre également que le modèle d'ombudsman pourrait étendre sa portée à d'autres secteurs. Comme l'a observé la commissaire Stoddart, « De plus en plus, les responsables de la protection des renseignements personnels au sein des organisations doivent sortir des sentiers battus⁴⁰⁸. »

La portée de cette analyse ne permet pas de prononcer à savoir s'il existerait dans le contexte actuel de la LPRPDE des pouvoirs réglementaires dont le CPVP ne se serait pas prévalu. Toutefois, nos consultations nous amènent à croire qu'il y aurait place à des initiatives réglementaires supplémentaires. Par exemple, un des répondants interviewés a suggéré que le CPVP offre un programme d'accréditation à la suite duquel les entreprises adoptant les « pratiques exemplaires » pourraient recevoir son imprimatur, un peu comme la certification LEED que peuvent obtenir les immeubles appliquant les meilleures pratiques environnementales. De tels systèmes d'accréditation — ou de notation — pourraient alors servir aux gouvernements municipaux et provinciaux à d'autres fins réglementaires ou aux entreprises à des fins commerciales (p. ex. dans le cadre d'une stratégie publicitaire). La LPRPDE n'empêche pas le CPVP d'élaborer des normes d'accréditation, d'ailleurs, d'importants avantages pourraient en découler.

Certaines initiatives privées ont tenté de créer des « sceaux » de garantie, comme TRUSTe⁴⁰⁹. Elles facturent habituellement les entreprises pour le sceau ou pour le processus visant son obtention. Pour cette raison, il y a un conflit possible entre les intérêts commerciaux du fournisseur de l'accréditation et l'intérêt public envers une conformité accrue aux normes en matière de protection de la vie privée. Ce conflit ne survient pas avec un organisme de réglementation public qui entame un processus d'accréditation.

Des initiatives d'accréditation ou d'établissement de normes sont rarement fructueuses en soi. Leur succès dépend plutôt d'autres organismes de réglementation et industries qui devraient trouver des mesures incitatives à l'endroit des entreprises afin qu'elles consentent plus d'argent à la conformité. Par exemple, le fait qu'un gouvernement, un organisme ou une grande société accepte de limiter son appel d'offres aux entreprises ayant obtenu une note particulière relativement à la protection de la vie privée, ou qu'un permis ou une subvention donnés d'un gouvernement étaient liés à une note particulière relativement à la protection de la vie privée, pourrait constituer des mesures incitatives efficaces.

Nous ne suggérons pas que le CPVP accrédite, inspecte ou impose des étiquettes sur l'ensemble du secteur privé; toutefois, une initiative pilote au sein

408 Commentaires émis lors du 10^e anniversaire de l'International Association of Privacy Professionals (IAPP) (16 mars 2010) à l'adresse suivante : http://www.priv.gc.ca/media/nr-c/2010/nr-c_100316_f.cfm.

409 Voir <http://www.truste.com/index.html> [en anglais seulement].

d'une industrie précise affichant un faible taux de conformité ou lorsque des membres vulnérables du public sont particulièrement à risque (p. ex. les jeunes qui partagent leurs renseignements personnels en ligne) pourrait fort bien prouver si cette stratégie réglementaire est efficiente et efficace.

Si le modèle d'ombudsman demeure un élément gagnant de la stratégie réglementaire du CPVP relative à la LPRPDE, il devra évoluer, s'adapter et réagir de manière créative aux défis posés par la rareté des ressources et les besoins des entreprises et du public.

- **Recommandation 6 : Améliorer les mécanismes de reddition de comptes afin d'assurer une planification stratégique à long terme et des repères significatifs**

Peu importe le modèle adopté pour le CPVP (ombudsman, pouvoir de rendre des ordonnances, hybride), la reddition de comptes demeurera un élément clé. La LPRPDE en soi prévoit des examens de la loi et des activités du CPVP, et la documentation découlant de l'examen parlementaire de 2006 a éclairé cette étude. Le CPVP a commandé des examens, et des groupes de défense des droits, comme la CIPPIC, ont également publié des examens de la loi et des stratégies de conformité du CPVP. Ce dernier fournit des rapports annuels détaillés au Parlement concernant ses activités liées à la LPRPDE.

Le rapport annuel contient des statistiques sur les demandes de renseignements, les enquêtes, le règlement des différends, etc., et traite aussi des initiatives et principaux thèmes de l'année précédente (par exemple, le rapport annuel de 2008 avait pour principal thème la « vie privée des jeunes »). En outre, le CPVP publie chaque année un rapport sur les plans et les priorités, lequel établit les orientations et priorités stratégiques en plus de présenter les résultats attendus et les prévisions en matière de dépenses du CPVP pour le prochain exercice. Le Rapport se divise en quatre secteurs d'activités de programmes : 1) activités relatives à la conformité; 2) recherche et élaboration de politiques; 3) sensibilisation du grand public; 4) services internes.

Cette approche envers les priorités, les résultats stratégiques et les objectifs s'avère utile, mais trop générale et de « haut niveau » pour permettre une évaluation significative du rendement. Par exemple, voici les cinq priorités organisationnelles pour 2009-2010 :

- Continuer d'améliorer la prestation des services grâce à la convergence des efforts et à l'innovation;
- Exercer un leadership pour promouvoir quatre domaines prioritaires en matière de protection de la vie privée (technologies de l'information, sécurité nationale, intégrité et protection de l'identité, et renseignements génétiques);
- Promouvoir stratégiquement la protection de la vie privée à l'échelle mondiale pour les Canadiennes et les Canadiens;
- Aider les Canadiennes et les Canadiens, les organisations et les institutions à prendre des décisions plus éclairées;
- Améliorer et soutenir la capacité organisationnelle.

Le CPVP publie également des rapports ministériels sur le rendement, lesquels fournissent une évaluation des activités de l'année précédente. Les objectifs ou cibles sont fixés, les activités, résumées, et une conclusion est formulée pour faire savoir dans quelle mesure ces objectifs ou cibles ont été atteints (« Satisfait à toutes les attentes », « Satisfait à la plupart des attentes », « Satisfait en partie aux attentes » et « Ne satisfait pas aux attentes »). Par exemple, pour 2009, en ce qui a trait aux objectifs de conformité, le CPVP a souligné que les recommandations découlant des enquêtes de la commissaire ont été acceptées dans 13 des 17 enquêtes liées à la LPRPDE (76 %) qui ont donné lieu à des recommandations particulières. Deux des quatre dossiers restants ont abouti à un règlement entre les parties avant d'en arriver à une audience devant la Cour fédérale, un dossier a fait l'objet d'un litige, tandis que le CPVP a décidé, dans le dernier dossier, de ne pas tenter de poursuites. Par conséquent, le CPVP a conclu que ses objectifs avaient « satisfait en partie aux attentes ». Ces instruments de rapport sont complétés par des déclarations et des discours prononcés par le commissaire, lesquels ajoutent texture et contexte à l'obligation de rendre compte du CPVP. Par exemple, les déclarations du commissaire relatives à la portée de la LPRPDE pour le CPVP illustrent une évolution depuis la création du CPVP.

Une fois de plus, malgré l'utilité de telles évaluations du rendement, celles-ci n'ont qu'une incidence limitée. Il manque à l'actuelle structure de reddition de comptes un sens de la planification stratégique à long terme et de repères significatifs. Bien que le CPVP ne soit pas sous-examiné, il s'avère souvent difficile de relever les critères utilisés par les divers examens en vue de son évaluation. Fait encore plus troublant, les normes par rapport auxquelles le CPVP évalue son propre rendement ne sont pas clairement connues. Même s'il recueille des données et note les tendances dans ses activités, ou le degré de plaintes ou de règlements, le CPVP n'a désigné aucun repère ou cible pouvant servir à évaluer ses activités. La FTC fournit un modèle utile à cet égard. Comme il en a été question dans la partie 2, la FTC publie un plan stratégique quinquennal qui met en lumière un nombre de buts généraux (p. ex. protéger les consommateurs) qui comprennent individuellement un ensemble d'objectifs liés aux mesures de rendement, aux stratégies en vue d'atteindre le but en question ainsi qu'à la méthode d'évaluation.

Enfin, nous recommandons que le CPVP adopte une approche de planification stratégique plus claire en ce qui concerne ses activités en vertu de la LPRPDE, y compris ce qui suit :

- L'établissement de points de référence à des fins de conformité à la LPRPDE;
- La surveillance et le suivi de la conformité sur une base continue, au moins dans les secteurs cibles ou prioritaires comme les petites et moyennes entreprises;
- Des mesures d'évaluation du rendement pour les activités du CPVP à cet égard;
- Une planification stratégique à court, moyen et long terme avec des objectifs établis associés à des échéances précises.

TABLES BIBLIOGRAPHIQUES

Textes législatifs

Charte canadienne des droits et libertés, partie I de la *Loi constitutionnelle de 1982*, [annexe B de la *Loi de 1982 sur le Canada* (R.-U.), 1982, chap. 11

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

Code canadien du travail, L.R.C. 1985, chap. L-2

Code civil du Québec, L.Q. 1991, c. 64

Criminal Justice and Immigration Act 2008, chap. 4 (R.-U.), http://www.opsi.gov.uk/acts/acts2008/ukpga_20080004_en_1

Data Protection Act 1998, chap. 29 (R.-U.), <http://www.statutelaw.gov.uk/legResults.aspx?LegType=All+Legislation&searchEnacted=0&extentMatchOnly=0&confersPower=0&blanketAmendment=0&sortAlpha=0&PageNumber=0&NavFrom=0&activeTextDocId=3190610>

Loi canadienne sur les droits de la personne, S.C. 1976-1977, chap. 33

Loi canadienne sur les droits de la personne, L.R.C. 1985, chap. H-6

Loi constitutionnelle de 1867, 30 & 31 Vict., chap. 3 (R.-U.)

Loi électorale du Canada, L.C. 2000, chap. 9

Loi fédérale sur la responsabilité, L.C. 2006, chap. 9

Loi modifiant la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels et d'autres dispositions législatives, L.Q. 2006, chap. 22

- Loi sur l'accès à l'information*, L.R.C. 1985, chap. A-1
- Loi sur l'emploi dans la fonction publique*, L.C. 2003, chap. 22
- Loi sur l'équité en matière d'emploi*, L.C. 1995, chap. 44
- Loi sur l'Office national de l'énergie*, L.R.C. 1985, chap. N-7
- Loi sur la protection des renseignements personnels dans le secteur privé*, L.R.Q., chap. P-39.1
- Loi sur la protection des renseignements personnels et les documents électroniques*, L.C. 2000, chap. 5
- Loi sur la protection des renseignements personnels*, L.R.C. 1985, chap. P-21
- Loi sur le conseil de la radiodiffusion et des télécommunications canadiennes*, L.R.C. 1985, chap. C-22.
- Loi sur le lobbying*, L.R.C. 1985, chap. 44 (4^e suppl.)
- Loi sur le Parlement du Canada*, L.R.C. 1985, chap. P-1
- Loi sur le vérificateur général*, L.R.C. 1985, chap. A-17
- Loi sur les grains du Canada*, L.R.C. 1985, chap. G-10
- Loi sur les langues officielles*, L.R.C. 1985, chap. 31 (4^e suppl.)
- Loi sur les traitements*, L.R.C. 1985, chap. S-3
- Loi concernant la procréation assistée et la recherche connexe*, L.C. 2004, chap. 2
- Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001*, Pub. L. No. 107-56, 272, Stat. 218, en ligne : <http://www.govtrack.us/congress/billtext.xpd?bill=h107-3162&version=enr>

Jurisprudence

- Aubry c. Éditions Vice-Versa inc.*, [1998] 1 R.C.S. 591
- B.C. Development Corp. c. Friedmann*, [1985] 2 R.C.S. 447
- BC Govt Serv. Empl. Union v. British Columbia (Minister of Health Services)*, (2005) BCSC 446, en ligne : <http://www.canlii.org/en/bc/bcsc/doc/2005/2005bcsc446/2005bcsc446.html>
- Bande Kitkatla c. Colombie-Britannique (Ministre des Petites et moyennes entreprises, du Tourisme et de la Culture)*, 2002, 2 R.C.S. 146

- Bombardier c. Bouchard*, 1996 CanLII 6356 (QC C.A.)
- Campbell c. MGN Ltd*, Cour d'appel (Chambre civile), 2002, EWCA Civ 1373, 2003, QB 633 (R.-U.)
- Canada (Commissaire à la protection de la vie privée) c. Canada (Conseil des relations du travail)*, 1996, 3 C.F. 609
- Canada (Procureur général) c. Viola*, 1991, 1 C.F. 373
- Canadian Indemnity Co. et al. c. Procureur général de la Colombie-Britannique*, 1977, 2 R.C.S. 504, 512 et 519
- Charkaoui c. Canada (Citoyenneté et Immigration)*, [2007] 1 R.C.S. 350
- Cheskes c. Ontario*, 2007 CanLII 38387 (ON S.C.)
- Citizens' Insurance Company of Canada c. Parsons*, 1881, 7 App. Cas. 96
- Dagg c. Canada (Ministre des Finances)*, 1997, 2 R.C.S. 403
- Eastmond c. Canadien Pacifique Ltée et Commissaire à la protection de la vie privée du Canada*, 2004, C.F. 852
- General Motors of Canada Ltd. c. City National Leasing*, 1989, 1 R.C.S. 641
- Hunter c. Southam*, 1984, 2 R.C.S. 145
- Kirkbi AG c. Gestions Ritvik Inc.*, 2005, 3 R.C.S. 302
- Lavigne c. Canada (Commissariat aux langues officielles)*, 2002, 2 R.C.S. 773
- Netbored c. Avery Holdings Inc.*, 2005, CF 1405 (CanLII)
- Procureur général (Québec) c. Kellogg's Co. of Canada et al.*, 1978, 2 R.C.S. 211
- R. c. Dymment*, 1988, 2 R.C.S. 417
- R. c. Nova Scotia Pharmaceutical Society*, 1992, 2 R.C.S. 606
- R. c. O'Connor*, 1995, 4 R.C.S. 411
- R. c. Turpin*, 1989, 1 R.C.S. 1296
- Renvoi relatif à la validité de l'alinéa 5a) de la *Loi de l'industrie laitière*, 1949, R.C.S. 1
- Renvoi fait par le gouvernement du Québec en vertu de la Loi sur les renvois à la Cour d'appel, L.R.Q., chap. R-23, relativement à la constitutionnalité des articles 8*

à 19, 40 à 53, 60, 61 et 68 de la *Loi sur la procréation assistée*, L.C. 2004, chap. 2 (Dans l'affaire du), 2008 QCCA 1167

Renvoi relatif à la *Loi sur l'assurance-emploi* (Can.), art. 22 et 23, 2005, 2 R.C.S. 669

Renvoi relatif à la *Loi sur les armes à feu* (Can.), 2000, 1 R.C.S. 783

Renvoi relatif à la sécession du Québec, 1998, 2 R.C.S. 217

Renvoi relatif au mariage entre personnes du même sexe, 2004, 3 R.C.S. 698

Rogers c. Canada (Service correctionnel), 2001, 2 C.F. 586

Hondo c. UCI, Swiss Olympic and WADA, TAS, 10 janvier 2006, en ligne : http://www.wadaama.org/rtecontent/document/CASELAW_Hondo.pdf

Monographies et ouvrages collectifs

BARRIGAR, J. *Consider Consideration and Order-Making*, 2009 (document préparé pour le Commissariat à la protection de la vie privée du Canada).

BENNETT, C. et C. RAAB. *The Governance of Privacy: Policy Instruments in Global Perspective*, Aldershot, Ashgate, 2003.

BENNETT, C. *Regulating Privacy in Canada: An Analysis of Oversight and Enforcement in the Private Sector*, Ottawa, Industrie Canada, 1996.

BLACK, H., *11th Annual Meeting on Regulatory Compliance for Financial Institutions*. 2005, en ligne : http://www.priv.gc.ca/speech/2005/sp-d_051118_hb_e.cfm

BUCHANAN, J. M. et G. TULLOCK. *The Calculus of Consent*, Ann Arbor, University of Michigan Press, 1962.

ELIADIS, P. F., M. M. HILL et M. P. HOWLETT. *Designing Government: from Instruments to Governance*, Montréal, McGill-Queen's University Press, 2005.

GAUTRAIS, V. et P. TRUDEL. *Circulation des renseignements personnels et le Web 2.0*, Montréal, Les Éditions Thémis, 2010, 231 p.

GUERRIEN, B. *L'Économie néo-classique*, Paris, La Découverte, 1989.

HAMILTON, J., *30th Anniversary of the OECD Privacy Guidelines, Remarks by Jane Hamilton*, Industrie Canada, en ligne : http://www.oecd.org/findDocument/0,3354,fr_2649_34255_1_119802_1_1_1,00.html

HAYEK, F. A. von. *La route de la servitude*, (trad. de G. Blumberg de *The Road to Serfdom*), 2^e éd., Paris, PUF, 1985.

HUSTINX, P., *Recent developments in the European Union*, 2010, en ligne : http://www.oecd.org/findDocument/0,3354,fr_2649_34255_1_119802_1_1_1,00.html

JESSUA, C., C. LABROUSSE et D. VITRY (dir.). *Dictionnaire des sciences économiques*, Paris, PUF, 2001, p. 345.

KEY CENTRE FOR ETHICS, LAW, JUSTICE AND GOVERNANCE, GRIFFITH UNIVERSITY et TRANSPARENCY INTERNATIONAL AUSTRALIA, *Chaos or Coherence? Strengths, Opportunities and Challenges for Australia's Integrity Systems: National Integrity Systems Assessment (NISA) Final Report*, Australia, Key Centre for Ethics, Law, Justice and Governance and Transparency International Australia, 2005, <http://www.griffith.edu.au/arts-languages-criminology/key-centre-ethics-law-justice-governance/research/integrity-anti-corruption/projects/?a=37155> (consulté le 20 janvier 2010).

KIRBY, M., *The History, Achievement and Future of the 1980 OECD Guidelines on Privacy*, 2010, en ligne : http://www.oecd.org/findDocument/0,3354,fr_2649_34255_1_119802_1_2_1,00.html

KRASNOW, E. G., L. D. LONGLEY, et H. A. TERRY. *The Politics of Broadcast Regulation*, 3^e éd., New York, Palgrave, 1982.

LAWSON, I. *Protection de la vie privée et l'autoroute de l'information : les options du Canada en matière de réglementation*, Ottawa, Industrie Canada, 1996.

MACKAAY, E. et S. ROUSSEAU. *Analyse économique du droit*, 2^e éd., Montréal, Éditions Thémis, 2008.

MADER, L. *L'évaluation législative. Pour une étude empirique des effets de la législation*, Lausanne, Payot, 1985.

McNAIRN, C. et A. SCOTT. *A guide to the Personal Information Protection and Electronic Documents Act*, Markham, LexisNexis Canada Inc., 2007.

MOCKLE, D. *La gouvernance, l'État et le droit*, Bruxelles, Bruylant, 2007.

MORAND, C.-A. *Le droit néo-moderne des politiques publiques*, Paris, L.G.D.J., 1998.

NISKANEN, W. *Bureaucracy and Representative Government*, Chicago, Aldine Atherton, 1971.

PAPAKONSTANTINO, V. *Self-Regulation and the Protection of Privacy*, Baden-Baden, Nomos Verlagsgesellschaft, 2001.

RONFELDT, D. F., *Tribes, Institutions, Markets, Networks : A Framework about Societal Evolution*. 1996, Santa Monica, CA : Rand.

ROSANVALLON, P. *Le libéralisme économique : histoire de l'idée de marché*, Paris, Seuil, 1989.

SALAMON, L. M. (éd.). *The Tools of Government: A Guide to the New Governance*, Oxford, Oxford University Press, 2002.

SCHNEIDERMAN, D. *Constitutionalizing Economic Globalization, Investment Rules and Democracy's Promise*, Cambridge, Cambridge University Press, 2008.

SHIELDS, R. *Les renseignements personnels accessibles au public et la Loi sur la protection des renseignements personnels et les documents électroniques du Canada*, Ottawa, 12 octobre 2000, McCarthy Tétrault, DMS-Ottawa #5574162/v.2.

SMITH, A. *Recherche sur la nature et les causes de la richesse des nations*, (trad. G. Garnier), vol. 2, Paris, Flammarion, 1991.

STEVENSON, H. G., *30 Years After : The Impact of the OECD Privacy Guidelines, Remarks of Hugh G. Stevenson*, 2010, en ligne : http://www.oecd.org/findDocument/0,3354,fr_2649_34255_1_119802_1_1_1,00.html.

ZARKIN, M. J. *The Federal Communications Commission*, Santa Barbara, Greenwood Publishing Group, 1998.

Articles de revue et études d'ouvrages collectifs

ACKERMAN, B. « The New Separation of Powers », 1999-2000, 113 *Harvard Law Review* 633.

AUSTIN L. « Reviewing PIPEDA: Control, Privacy and the Limits of Fair Information Practices », 2006, 44 *Revue canadienne du droit de commerce* 21.

BECKER, R. « Recent Developments: Transborder Data Flows: Personal Data », 1981, 22 *Harv. Int'l. L. J.* 241.

BENNET, C. et R. M. BAYLEY. « Video Surveillance and Privacy Protection Law in Canada » dans Sjaak NOUWT, Berend R. de VRIES et Corien PRINS (éd.), La Haye, Asser Press, 2005, p. 65.

BERZINS, C. « Protecting Personal Information in Canada's Private Sector: The Price of Consensus Building », 2002, 27 *Queen's Law Journal* 609.

BIGNAMI, F. « Cooperative Legalism », 2009 (dans le dossier des auteurs).

BOISVERT, A.-M., H. DUMONT et A. STYLIOS. « En marge de l'affaire Norbourg : les enjeux substantifs et punitifs suscités par le double aspect, réglementaire et criminel, de certains comportements frauduleux dans le domaine des valeurs mobilières », 2009, <http://hdl.handle.net/1866/2913> (pré-publication).

BOUSTA, R. « The Ombudsman: Proposal for a Definition », 2005, 9 *The International Ombudsman Yearbook* 36.

BYGRAVE, L. A. « Privacy Protection in a Global Context – A Comparative Overview », 2004, 47 *Scandinavian Studies in Law* 319.

CONNOLLY, C., *Trustmark schemes struggle to protect privacy*, 2008, en ligne : http://www.galexia.com/public/research/assets/trustmarks_struggle_20080926/trustmarks_struggle_public.pdf

COURCHENE, Thomas J., « Global Future for Canada's Global Cities », dans *Transitions : fiscal and Political Federalism in an Era of Change*, Kingston, McGill-Queen's University Press, 2009.

FEINBERG, J. « Autonomy, Sovereignty, and Privacy: Moral Ideals in the Constitution? », 1982, 58 *Notre Dame L. Rev.* 445.

FULLER, L. L. « Positivism and Fidelity to Law — A Reply to Professor Hart », 1958, 71:4 *Harvard Law Review* 630.

GADLIN, H. « The Ombudsman: What's in a Name? », 2000, 16(1) *Negotiation Journal* 37.

GEIST, M., « Privacy Takes Step Towards Global Enforcement », 2010, en ligne : <http://www.michaelgeist.ca/content/view/4994/135/> (consulté le 31 mai 2010)

GELLMAN, R., « TRUSTe fails to justify its role as privacy arbitrator », 2000, 25, *Privacy Law and Policy Reporter* (2000), en ligne : <http://www.austlii.edu.au/au/journals/PLPR/2000/53.html>

GREENLEAF G., « Five years of the APEC Privacy Framework : Failure or promise ? » (2009) 25 *Computer Law & Security Review* 28.

GREGORY, R. et P. GIDDINGS. « The Ombudsman Institution: Growth and Development » dans Roy GREGORY et Philip GIDDINGS (éd.), *Righting Wrongs: The Ombudsman in Six Continents*, Washington, IOS Press, 2000, p. 1.

GUNASEKARA, G., « The « Final » Privacy Frontier ? Regulating Trans-Border Data Flows » (2007) 17, *International Journal of Law and Information Technology* 147.

HÉNIN, P.-Y. et P. RALLE. « Les nouvelles théories de la croissance. Quelques apports pour la politique économique », *Revue économique – Hors série* 82.

HOWES, E., « No guarantee of privacy », 2002, en ligne : <http://spywarewarrior.com/uiuc/privpol.htm#no-guarantee>

HUNTON & WILLIAMS LAW FIRM, *Background paper on APEC Privacy Framework Pathfinder Projects*, 2008, p. 3, en ligne : http://www.hunton.com/files/tbl_s47Details/FileUpload265/2302/

KERR, I, J. BARRIGAR, J. BURKELL et K. BLACK. « Soft Surveillance, Hard Consent », 2006, 6 *Personally Yours* 1.

KINGSBURY, B., N. KRISCH et R. B. STEWART. « The Emergence of Global Administrative Law », 2005, 68:15 *Law and Contemporary Problems* 15.

KRISCH, N. et B. KINGSBURY. « Introduction: Global Governance and Global Administrative Law in the International Legal Order », 2006, 17:1 *E.J.I.L.* 1.

LASCOUMES, P. et É. SERVERIN. « Théories et pratiques de l'effectivité du droit », 1986, 2 *Droit et Soc.* 101.

MACDONALD, R. A. « La réforme du droit et ses organismes », dans *Actes de la XIV^e conférence des juristes de l'État*, Cowansville, Les Éditions Yvon Blais Inc., 2000, p. 377.

MAY, R. J. « The FCC's Tumultuous Year 2003: An Essay on an Opportunity for Institutional Agency Reform », 2004, 56 *Administrative Law Review* 1307.

McMILLAN, J. « The Ombudsman and the Rule of Law » 2005, 44 *Australian Institute of Administrative Law Forum* 1.

NIGGLI, O. et Julien Sieveking, « Éléments choisis de jurisprudence en application du code mondial antidopage », (2006) 20 *Jusletter* 2.

NISKER, J. « PIPEDA A Constitutional Analysis », 85 R. du B. Can. 317.

OWEN, S. « The Ombudsman: Essential Elements and Common Challenges », dans Linda C. REIF (éd.), *The International Ombudsman Anthology*, La Haye, Kluwer Law International, 1999, p. 51.

RAAB, C. et C. BENNETT. « Évaluation du droit à la vie privée : la protection des données peut-elle être évaluée? », 1996, 62 *Revue internationale des sciences administratives* 535.

RAAB, C. et C. BENNETT. « The Governance of Global Issues: Protecting Privacy in Personal Information », *European Consortium for Political Research*, 2003, p. 6, également dans M. Koenig-Archibugi et M. Zürn (éd.), *New Modes of Governance in the Global System: Exploring Publicness, Delegation and Inclusiveness*, Londres, Palgrave Macmillan, 2006, p. 125.

RAAB, C. « Beyond Activism: Research Perspectives on Privacy », *TILT Law & Technology Working Paper Series* (22 février 2008), n° 007/2008.

REIF, L. C. « Building Democratic Institutions: The Role of National Human Rights Institutions in Good Governance and Human Rights Protection », 2000, 13 *Harvard Human Rights Journal* 1.

ROCHER, G. « L'effectivité du droit », dans Andrée LAJOIE, Roderick A. MACDONALD, Richard JANDA et Guy ROCHER (dir.), *Théories et émergence du droit : pluralisme, surdétermination et effectivité*, Montréal, Éditions Thémis, 1998, p. 133.

ROUILLER, C., *Avis de droit sur la compatibilité de l'article 10.2 du Code mondial antidopage avec les principes fondamentaux du droit national suisse*, 2005, en ligne : <http://www.wadaama.org/fr/Programmemonial-antidopage/Juridique-articles-jurisprudence-et-lois-nationales/Avis-consultatif-et-avis-de-droit-surle-Code>

SCHWARTZ, P. M. « Privacy and Preemption », 2009, 118 *Yale L. J.* 902.

SPIGELMAN, J. « The Integrity Branch of Government », *Quadrant*, vol. XLVIII, n° 7, juillet-août 2004, p. 51.

STEIN J. G., « Networked Federalism », dans *Transitions : fiscal and Political Federalism in an Era of Change*, Kingston, McGill-Queen's University Press, 2009, p. 347

STEWART, B., *A suggested scheme to certify substantial observance of APEC Guidelines on data privacy*, APEC E-commerce Steering Group Meeting, 2003, en ligne : http://www.apec.org/apec/documents_reports/electronic_commerce_steering_group/2003.MedialibDownload.v1.html?url=/etc/medialib/apec_media_library/downloads/taskforce/ecsg/mtg/2003/pdf.Par.0009.File.v1.1

STUMCKE, A. et A. TRAN. « The Commonwealth Ombudsman: an Integrity Branch of Government? », 2007, 32 :4 *Alternative Law Journal* 233.

TOPPERWIEN, B. « Separation of Powers and the Status of Administrative Review », 1999, 20 *Australian Institute of Administrative Law Forum* 32.

URIO, P. « La gestion publique au service du marché », dans Marc HUFTY (dir.), *La pensée comptable : État, néolibéralisme, nouvelle gestion publique*, Paris et Genève, PUF et Les nouveaux Cahiers de l'IUED, 1998, p. 91.

WATERS, N., « The APEC Asia-Pacific Privacy Initiative - a new route to effective data protection or a trojan horse for self-regulation ? », 2008, *University of New South Wales Faculty of Law Research Series 2008 Working Paper 59*.

WEISER, P. J. « FCC Reform and the Future of Telecommunications Policy », 2009, <http://fcc-reform.org/paper/fcc-reform-and-future-telecommunications-policy>.

Traités, conventions, déclarations

Accord de libre-échange entre le Canada et la République du Pérou, 29 mai 2008, entré en vigueur le 1^{er} août 2009, <http://www.international.gc.ca/trade-agreements-accords-commerciaux/agr-acc/peru-perou/peru-toc-perou-tdm.aspx?lang=fra>.

Accord de libre-échange entre le Canada et le Royaume hachémite de Jordanie, 28 juin 2009, <http://www.international.gc.ca/trade-agreements-accords-commerciaux/agr-acc/jordan-jordanie/agreement-toc-tdm-accord.aspx?lang=fra>.

Accord entre le gouvernement du Canada et la Communauté européenne sur le traitement des données relatives aux informations préalables sur les voyageurs et aux dossiers passagers, 3 octobre 2005, *Journal officiel de l'Union européenne* L 82/15 21.3.2006, entré en vigueur le 22 mars 2006, http://www.canadainternational.gc.ca/eu-ue/assets/pdfs/031005PNR_fra.pdf.

Accord de libre-échange nord-américain entre le gouvernement du Canada, le gouvernement des États-Unis mexicains et le gouvernement des États-Unis d'Amérique, 17 décembre 1992, 1994, R.T. Can. n° 2, entré en vigueur le 1^{er} janvier 1994, http://www.international.gc.ca/trade-agreements-accords-commerciaux/agr-acc/nafta-alena/texte/index.aspx?lang=fra&menu_id=50&menu=r.

Déclaration de Lausanne de 1999, http://www.sportunterricht.de/lksport/Declaration_e.html

UNESCO, *Convention internationale contre le dopage dans le sport*, 2005, en ligne : <http://www.unesco.org/new/fr/social-and-human-sciences/themes/sport/anti-doping/international-conventionagainst-doping-in-sport/>

Documents et rapports d'organismes publics

Canada

ALBERTA, ACCÈS ET PROTECTION DE LA VIE PRIVÉE, *PIPA Compared*, Edmonton, Accès et protection de la vie privée, Service Alberta, 2008, <http://pipa.alberta.ca/legislation/pdf/PIPAcompared.pdf>.

ALBERTA, COMITÉ D'EXAMEN SPÉCIAL DE L'ALBERTA SUR LA *PERSONAL INFORMATION PROTECTION ACT*, *Review of the Personal Information Protection Act*, Edmonton, Assemblée législative de l'Alberta, 2007, www.assembly.ab.ca/committees/reports/PIPA/finalpipawReport111407.pdf.

ASSOCIATION CANADIENNE DE NORMALISATION (CSA), *Code type sur la protection des renseignements personnels*, CAN/CSA-Q830-96, Rexdale, CSA, 1996.

CANADA, *Politique canadienne contre le dopage dans le sport* à l'adresse suivante : <http://www.pch.gc.ca/pgm/sc/pol/dop/index-fra.cfm>

CANADA, BUREAU DE LA CONCURRENCE, *Foire aux questions — Modifications à la Loi sur la concurrence*, <http://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/fra/03046.html>.

CANADA, COMITÉ PERMANENT DE L'ACCÈS À L'INFORMATION, DE LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET DE L'ÉTHIQUE, *Examen, prévu par la Loi, de la Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE), Quatrième Rapport du Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique*, 2007.

CANADA, COMITÉ PERMANENT DE L'INDUSTRIE, *Mémoire au Comité permanent de l'industrie de la Chambre des communes*, 2 décembre 1998, <http://www2.parl.gc.ca/HousePublications/Publication.aspx?DocId=1039144&Language=F#T1532>.

CANADA, COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Distinguer le seigle du blé : réorientation de l'actuel débat sur la fonction d'ombudsman telle que définie dans la LPRPDE*, Toronto, Commissariat à la protection de la vie privée du Canada, 2005, http://www.priv.gc.ca/information/pub/omb_051021_f.cfm.

CANADA, COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *La vie privée sur les sites de réseau social : Analyse comparative de six sites*, Ottawa, Commissariat à la protection de la vie privée du Canada, 2009.

CANADA, COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA. *Rapport annuel au Parlement 2003 2004*, 2004, en ligne : http://www.priv.gc.ca/information/ar/200304/200304_f.pdf.

CANADA, COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Rapport annuel au Parlement 2008 : Rapport sur la Loi sur la protection des renseignements personnels et les documents électroniques*, 2009, http://www.priv.gc.ca/information/ar/200809/2008_pipeda_f.pdf.

CANADA, COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Rapport au Parlement relativement aux lois provinciales essentiellement similaires*, Ottawa, ministère des Travaux publics et Services gouvernementaux, 2002, publication disponible sur le site web du Commissariat : www.priv.gc.ca (consulté le 24 juillet 2009).

CANADA, COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Surveillance, Search or Seizure Powers Extended by Recent Legislation in Canada, Britain, France and the United States*, 2009, en ligne : http://www.priv.gc.ca/parl/2009/parl_bg_090507_e.pdf

CANADA, COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Tracer le chemin : Principaux développements au cours*

des sept premières années d'application de la LPRPDE, http://www.priv.gc.ca/information/pub/lbe_080523_f.pdf.

CANADA, GOUVERNEMENT DU CANADA, *Directive du Cabinet sur la rationalisation de la réglementation*, Ottawa, Sa Majesté la Reine du chef du Canada, 2007, <http://www.tbs-sct.gc.ca/ri-qr/directive/directive00-fra.asp> (consulté le 23 août 2008).

CANADA, GOUVERNEMENT DU CANADA, *Réponse du gouvernement au quatrième rapport du Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique* <http://www2.parl.gc.ca/HousePublications/Publication.aspx?Mode=1&Parl=39&Ses=1&DocId=3077726&File=0&Language=F>.

CANADA, GROUPE D'ÉTUDE DE L'ACCÈS À L'INFORMATION, *Accès à l'information : comment mieux servir les Canadiens*, Ottawa, Travaux publics et Services gouvernementaux Canada, 2002.

CANADA, GROUPE D'ÉTUDE SUR LE CADRE RÉGLEMENTAIRE DES TÉLÉCOMMUNICATIONS, *Rapport final 2006*, Ottawa, Travaux publics et Services gouvernementaux Canada, <http://www.telecomreview.ca/eic/site/tprp-gecrt.nsf/fra/rx00101.html>.

CANADA, GROUPE D'ÉTUDE SUR LES POLITIQUES EN MATIÈRE DE CONCURRENCE, *Foncer pour gagner : rapport final juin 2008*, http://www.ic.gc.ca/eic/site/cprp-gepmc.nsf/fra/h_00040.html.

CANADA, GROUPE D'ÉTUDE SUR LES POLITIQUES EN MATIÈRE DE CONCURRENCE, *Le Groupe d'étude sur les politiques en matière de concurrence publie le rapport*, 26 juin 2008.

CANADA, MINISTÈRES DE L'INDUSTRIE ET DE LA JUSTICE, GROUPE DE TRAVAIL SUR LE COMMERCE ÉLECTRONIQUE, *La protection des renseignements personnels. Pour une économie et une société de l'information au Canada*, Ottawa, Services de distribution, Direction générale des communications, 1998.

CANADA, MINISTÈRES DE L'INDUSTRIE ET DE LA JUSTICE, *La protection des renseignements personnels : Pour une économie et une société de l'information au Canada* — Avis n° IPPB-002-98 — Publication d'un document de discussion sur la protection des renseignements personnels sur le marché, 24 janvier 1998, *Gazette du Canada*, partie I, vol. 132, n° 4.

CANADA, MINISTRE DE L'INDUSTRIE, « Notes pour une allocution : L'honorable John Manley, ministre de l'Industrie, devant le comité sénatorial chargé d'étudier le projet de loi C-6 », 2 décembre 1999, <http://www.ic.gc.ca/eic/site/ecic-ceac.nsf/fra/gv00217.html> (consulté le 23 juillet 2009).

CANADA, MINISTRE DE L'INDUSTRIE, *Projet de loi C-19*, 2 novembre 2004, <http://www2.parl.gc.ca/HousePublications/Publication.aspx?pub=bill&doc=C-19&parl=38&ses=1&language=F>.

CANADA, PARLEMENT, CHAMBRE DES COMMUNES, COMITÉ PERMANENT DE LA JUSTICE ET DU SOLICITEUR GÉNÉRAL, *Une question à deux volets : comment améliorer le droit d'accès à l'information tout en renforçant les mesures de la protection des renseignements personnels, Accès et renseignements personnels : les prochaines étapes*, Ottawa, Sa Majesté la Reine en chef du Canada, 1987.

CANADA, PARLEMENT, COMITÉ PERMANENT SUR LES DROITS DE LA PERSONNE, *La vie privée : où se situe la frontière*, Ottawa, Services et Approvisionnement Canada, 1997.

CANADA, PARLEMENT, *hauts fonctionnaires et officiels du Parlement*, <http://www2.parl.gc.ca/Parlinfo/compilations/OfficersAndOfficials/OfficersOfParliament.aspx?Language=F>.

CANADA, SECRÉTARIAT DU CONSEIL DU TRÉSOR, *Politique de réglementation*, Ottawa, Conseil du Trésor du Canada, 1992.

CANADA, SERVICE CANADIEN DE RENSEIGNEMENTS CRIMINELS, *Dossier spécial : vol et fraude d'identité au Canada*, 2008, http://www.cisc.gc.ca/annual_reports/annual_report_2008/feature_focus_2008_f.html.

CLINIQUE D'INTÉRÊT PUBLIC ET DE POLITIQUE D'INTERNET DU CANADA, *Le respect des lois de protection des données canadiennes : Les commerçants se conforment-ils?*, 2006, Ottawa, Clinique d'intérêt public et de politique d'Internet du Canada, [http://www.cippic.ca/documents/bulletins/compliance_report_06-07-06_\(color\)_\(cover-english\).pdf](http://www.cippic.ca/documents/bulletins/compliance_report_06-07-06_(color)_(cover-english).pdf) [pour un résumé en français, voir http://www.cippic.ca/uploads/CIPPIC_PC_ExSum_FR.pdf].

COLOMBIE-BRITANNIQUE, COMITÉ SPÉCIAL D'EXAMEN DE LA *PERSONAL INFORMATION PROTECTION ACT*, *Streamlining British Columbia's Private Sector Privacy Law*, Victoria, Assemblée législative de la Colombie-Britannique, 2008, <http://www.leg.bc.ca/cmt/38thparl/session-4/pipa/>.

COLOMBIE-BRITANNIQUE, COMMISSARIAT À L'INFORMATION ET À LA PROTECTION DE LA VIE PRIVÉE DE LA COLOMBIE-BRITANNIQUE, *The OIPC's Role and Mandate*, www.oipc.bc.ca/pdfs/public/OIPC-Role-and-Mandate.pdf.

CONFÉRENCE POUR L'HARMONISATION DES LOIS AU CANADA, 1995, Québec, Qc, Annexe M : *Protection de la vie privée dans le secteur privé*, <http://www.ulcc.ca/fr/poam2/index.cfm?sec=1995&sub=1995ac> (consulté le 13 juillet 2009).

CONFÉRENCE POUR L'HARMONISATION DES LOIS AU CANADA, 1998, Halifax, N.-É., Annexe A : *Loi uniforme sur le commerce électronique*, <http://www.ulcc.ca/fr/poam2/index.cfm?sec=1998&sub=1998ja> (consulté le 13 juillet 2009).

DENHAM, E. commissaire adjointe à la protection de la vie privée du Canada, *Rapport de conclusions de l'enquête menée à la suite de la plainte déposée par la Clinique d'intérêt public et de politique d'internet du Canada (CIPPIC) contre Facebook inc. aux termes de la Loi sur la protection des renseignements personnels et les documents électroniques*, 16 juillet 2009, http://priv.gc.ca/cf-dc/2009/2009_008_0716_f.pdf.

HOLMES, N. *Les lois fédérales du Canada sur la protection de la vie privée*, Ottawa, Bibliothèque du Parlement, Service d'information et de recherche parlementaires, 2008.

LA FOREST, G. V. conseiller spécial auprès du ministre de la Justice, *Les commissariats à l'information et à la protection de la vie privée : Fusion et questions connexes*, Ottawa, ministère de la Justice, 2005, <http://www.justice.gc.ca/fra/ip/index.html>.

PHILLIPS, B. commissaire à la protection de la vie privée du Canada, *Response to the Government of Canada, Discussion Paper: « The Protection of Personal Information : Building Canada's Information Economy Society »*, Ottawa, Commissariat à la protection de la vie privée du Canada, 1998.

QUÉBEC, ASSEMBLÉE NATIONALE, COMMISSION DE LA CULTURE, *Observations, conclusions et recommandations à la suite de la consultation générale et des auditions publiques à l'égard du document intitulé : Une réforme de l'accès à l'information : le choix de la transparence*, 2004.

QUÉBEC, COMMISSION D'ACCÈS À L'INFORMATION DU QUÉBEC, *Une réforme de l'accès à l'information : le choix de la transparence*, 2002.

QUÉBEC, MINISTÈRE DU CONSEIL EXÉCUTIF, *La réglementation par objectifs, propositions du Groupe de travail Justice – Secrétariat à l'allègement réglementaire*, Québec, ministère du Conseil exécutif, 2001, http://www.mce.gouv.qc.ca/allègement/documents/reglementation_objectifs.pdf (consulté le 14 juillet 2009).

Documents et rapports d'organismes publics International

AGENCE MONDIALE ANTI-DOPAGE, *À propos de l'AMA*, 2010, en ligne : <http://www.wada-ama.org/fr/Apropos-de-lAMA>.

AGENCE MONDIALE ANTI-DOPAGE, *Code mondial anti-dopage*, 2009, p. 14.

AGENCE MONDIALE ANTI-DOPAGE, *Déclaration de l'AMA à propos de l'avis du Groupe de travail européen sur la protection des données*, 2009, p.1, en ligne : http://www.wada-ama.org/Documents/World_Anti-Doping_Program/WADP-IS-PPPI/WADA_Statement_WP29_FR.pdf

AGENCE MONDIALE ANTI-DOPAGE, *La Convention de l'UNESCO dépasse la marque des 140 ratifications*, 2010, en ligne : <http://www.wada-ama.org/fr/Centre-media/Nouvelles/La-Convention-de-lUNESCOdepasse-la-marque-des-140-ratifications/>

AGENCE MONDIALE ANTI-DOPAGE, *La FIFA se joint à la campagne Dis NON! au dopage de l'AMA pendant la Coupe du monde*, 2010, en ligne : <http://www.wada-ama.org/fr/Centre-media/Nouvelles/La-FIFA-se-jointa-la-campagne-Dis-NON-au-dopage-de-lAMA-pendant-la-Coupe-du-monde/>

AGENCE MONDIAL ANTI-DOPAGE, Q- R : ADAMS, en ligne : <http://www.wada-ama.org/fr/ADAMS/Q-R--ADAMS>

AGENCE MONDIALE ANTI-DOPAGE, *Standard international sur la protection de la vie privée*, 2009, p. 1, en ligne : <http://www.wada-ama.org/fr/Programme-mondial-antidopage/Sport-et-Organisations-antidopage/Standards-internationaux>

ASIA-PACIFIC ECONOMIC COOPERATION, *APEC Data Privacy Pathfinder Projects Implementation Work Plan -Revised*, Doc. off. 2009/SOM1/ECSG/SEM/027 (23 février 2009), en ligne : aimp.apec.org/Documents/2009/.../09_ecsg_sem1_027.doc

CENTRE FOR INFORMATION POLICY LEADERSHIP et OFFICE OF THE DATA PROTECTION COMMISSIONER, « Global Discussion on the Commonly-accepted Elements of Privacy Accountability », Galway, Irlande, 2009.

COMMISSION EUROPÉENNE, *The application of Commission Decision 2002/2/EC of 20 December 2001 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documentation Act*, novembre 2006.

COMMISSION EUROPÉENNE, DIRECTION GÉNÉRALE DU MARCHÉ INTÉRIEUR ET SERVICES, *Preparation of a methodology for evaluating the adequacy of the level of protection of individuals with regard to the processing of personal data : annex to the annual report 1998 (XV D/5047/98) of the working party established by article 29 of directive 95/46/EC*, Luxembourg, Bureau des publications officielles des communautés européennes, 1998.

COMMISSION EUROPÉENNE, GROUPE DE PROTECTION DES PERSONNES À L'ÉGARD DU TRAITEMENT DES DONNÉES À CARACTÈRE PERSONNEL, *Transferts de données personnelles vers des pays tiers : Application des articles 25 et 26 de la directive relative à la*

protection des données, Commission européenne, Marché intérieur et services financiers, 24 juillet 1998, http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/1998/wp12_fr.pdf.

CONFÉRENCES INTERNATIONALES DES COMMISSAIRES À LA PROTECTION DES DONNÉES ET DE LA VIE PRIVÉE, Madrid, 5 novembre 2009, voir le site <http://www.edri.org/edri-gram/number7.2/international-standards-data-protection> (dernière visite : 20 janvier 2010).

CONFÉRENCE MONDIALE DES COMMISSAIRES À LA PROTECTION DES DONNÉES ET DE LA VIE PRIVÉE, *Résolution sur l'urgence de protéger la vie privée dans un monde sans frontière et l'élaboration d'une proposition conjointe d'établissement de normes internationales sur la vie privée et la protection des données personnelles*, document adopté à Strasbourg, 17 octobre 2008, <http://www.edps.europa.eu/EDPSWEB/edps/lang/fr/Home/Cooperation/Intconference> (consulté le 20 janvier 2010).

COOPÉRATION ÉCONOMIQUE ASIE-PACIFIQUE, *Cadre de protection de la vie privée de l'APEC*, (2005) APEC#205-SO-01.2.

CROMPTON, M. « *Light Touch* » or « *Soft Touch* » — *Reflections of a Regulator Implementing a New Privacy Regime* », Australie, Commissariat à la protection de la vie privée, 2004, http://www.privacy.gov.au/news/speeches/sp2_04p.html#link04.

ESPAGNE, AGENCE ESPAGNOLE DE PROTECTION DES DONNÉES (AEPD), dépliant d'information, https://www.agpd.es/portalweb/canaldocumentacion/publicaciones/common/pdfs/AEPD_en.pdf.

ÉTATS-UNIS D'AMÉRIQUE, COMITÉ DE L'ÉNERGIE ET DU COMMERCE, *Deception and Distrust: The Federal Communications Commission Under Chariman Kevin J. Martin*, 2009, http://energycommerce.house.gov/index.php?option=com_content&task=view&id=1455&Itemid=1.

FRANCE, SÉNAT, *Proposition de loi visant à mieux garantir le droit à la vie privée à l'heure du numérique*, 2009, <http://www.senat.fr/leg/pp109-093.html>.

HUSTINX, P. J. « Adequate Protection — Opinion 6/99 of the Article 29 Working Party revisited », dans *Ten Years of DP & FOI Commissioner's Office*, 2006, p. 251, <http://www.edps.europa.eu/EDPSWEB/edps/site/mySite/pid/231>.

ORGANISATION DE COOPÉRATION ET DE DÉVELOPPEMENT ÉCONOMIQUES (OCDE), *Action Plan for the Global Privacy Enforcement Network (GPEN)*, 2010.

ORGANISATION DE COOPÉRATION ET DE DÉVELOPPEMENT ÉCONOMIQUES (OCDE), *Canada — Le rôle de la politique de la concurrence dans la réforme de la réglementation*, 2002, <http://www.oecd.org/dataoecd/47/49/1960530.pdf>.

ORGANISATION DE COOPÉRATION ET DE DÉVELOPPEMENT ÉCONOMIQUES (OCDE), *Declaration on the Protection of Privacy on Global Networks*, 19 octobre 1998, <http://www.oecd.org/dataoecd/39/13/1840065.pdf> (consulté le 23 juillet 2009).

ORGANISATION DE COOPÉRATION ET DE DÉVELOPPEMENT ÉCONOMIQUES (OCDE), *Déclaration sur les flux transfrontières de données*, 11 avril 1985, http://www.oecd.org/document/32/0,3343,fr_2649_34255_1888160_1_1_1_1,00.html (consulté le 23 juillet 2009).

ORGANISATION DE COOPÉRATION ET DE DÉVELOPPEMENT ÉCONOMIQUES (OCDE), *La réforme de la réglementation au Canada : rester à la pointe du progrès grâce à l'innovation*, Publication de l'OCDE, 2002.

ORGANISATION DE COOPÉRATION ET DE DÉVELOPPEMENT ÉCONOMIQUES (OCDE), *Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel*, 23 septembre 1980, http://www.oecd.org/document/57/0,3343,fr_2649_34255_1815225_1_1_1_1,00.html (consulté le 22 juillet 2009).

PARLEMENT EUROPÉEN ET CONSEIL DE L'EUROPE, *Directive 95/46/CE du Parlement européen et du Conseil, 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données*, J.O. L 281, 23 novembre 1995, p. 31, http://eur-lex.europa.eu/smartapi/cgi/sga_doc?smartapi!celexplus!prod!DocNumber&lg=fr&type_doc=Directive&an_doc=1995&nu_doc=46 (consulté le 22 juillet 2009).

ROYAUME-UNI, CHAMBRE DES LORDS, *Surveillance: Citizens and the State*, 6 février 2009, <http://www.parliament.uk/hlconstitution/>.

ROYAUME-UNI, COMMISSARIAT À L'INFORMATION, *Coroners and Justice Bill, Part 8 — Data Protection*, commentaires du Commissariat à l'information, 2009, www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/cj_bill_lords_2nd_reading_v2%200.pdf.

ROYAUME-UNI, COMMISSARIAT À L'INFORMATION, *Data breaches reported to the ICO*, 9 février 2009, www.ico.gov.uk/upload/documents/pressreleases/2009/data_breaches_ico_statement20090209.pdf.

ROYAUME-UNI, COMMISSARIAT À L'INFORMATION, « Information Commissioner calls for prison sentences for illegal buying and selling of personal information », 12 mai 2006, <http://www.ico.gov.uk/global/search.aspx?collection=ico&keywords=prison>.

ROYAUME-UNI, COMMISSARIAT À L'INFORMATION, *Minutes – Management board*, 26 janvier 2009, www.ico.gov.uk/upload/documents/library/corporate/notices/minutes_3_march_2008v1.8.pdf.

ROYAUME-UNI, MINISTÈRE DES AFFAIRES CONSTITUTIONNELLES, *Increasing penalties for deliberate and wilful misuse of personal data*, 2006, www.dca.gov.uk/consult/misuse_data/cp0906.htm.

ROYAUME-UNI, MINISTÈRE DE LA JUSTICE, *Response to the Data Sharing Review Report*, Royaume-Uni, ministère de la Justice, 2008, <http://www.justice.gov.uk/publications/response-data-sharing-review.htm>.

ROYAUME-UNI, PARLEMENT, *Coroners and Justice Bill 2008-09*, Parlement du Royaume-Uni, <http://services.parliament.uk/bills/2008-09/coronersandjustice.html>.

THOMAS, R. et M. WALPORT. *Data Sharing Review*, ministère de la Justice, rapport présenté au premier ministre et au secrétaire d'État à la Justice du Royaume-Uni, 2008, <http://www.justice.gov.uk/reviews/datasharing-intro.htm>.

THOMAS, R. *Evidence to the Justice Select Committee – January 2009*, Royaume-Uni, Commissariat à l'information, 2009, http://www.ico.gov.uk/about_us/news_and_views/current_topics/ic_evidence_to_js_committee.aspx.

TRIBUNAL ARBITRAL DU SPORT, *Historique du TAS*, 2010, en ligne : <http://www.tas-cas.org/historique>

Divers

COMSCORE, « June 2009 U.S. Search Engine Rankings », 2009, http://www.comscore.com/Press_Events/Press_Releases/2009/7/comScore_Releases_June_2009_U.S._Search_Engine_Rankings.

D'ANGELO, C. « Un comité recommande des modifications à la loi de la Colombie-Britannique sur la protection de la vie privée dans le secteur privé », McCarthy Tétrault, 8 août 2008, http://www.mccarthy.ca/fr/article_detail.aspx?id=4101.

GEIST, M. « Facebook Settles Privacy Commissioner of Canada », 2009, <http://www.michaelgeist.ca/content/view/4330/196/>.

GEIST, M. « Standing on Guard for Privacy — Before Facebook », *Toronto Star*, Toronto, 14 septembre 2009 at <http://www.thestar.com/business/article/695147>.

GOOGLE, « Google does not use the keywords meta tag in web ranking », 2009, <http://googlewebmastercentral.blogspot.com/2009/09/google-does-not-use-keywords-meta-tag.html>.

LE TIGRE, « Marc L*** », 2009, <http://www.le-tigre.net/Marc-L.html>.

MOSTROUS, A. « UK citizens' private information being lost at record rate », *London Times*, 9 février 2009, <http://www.timesonline.co.uk/tol/news/politics/article5688347.ece>.

O'REILLY, T. et J. BATTELLE. « Web Squared: Web 2.0 Five Years On », 2009, <http://www.web2summit.com/web2009/public/schedule/detail/10194>.

O'REILLY, T. « What is Web 2.0: Design Patterns and Business Models for the Next Generation of Software », 2005, <http://oreilly.com/pub/a/web2/archive/what-is-web-20.html?page=1>, 2007, 65 *International Journal of Digital Economics* 17. Une version française intitulée « Qu'est-ce que le web 2.0 : modèles de conception et d'affaires pour la prochaine génération de logiciels », 2006, est disponible à l'adresse : <http://www.eutech-ssii.com/ressources/1>.

SPIGELMAN, J. « Judicial Review and the Integrity Branch of Government » discours présenté lors du *World Jurist Association Congress*, Shanghai, 8 septembre 2005, http://www.lawlink.nsw.gov.au/lawlink/supreme_court/ll_sc.nsf/pages/SCO_spigelman080905 (consulté le 14 décembre 2009).

SPIGELMAN, J. « The Integrity Branch of Government — The First Lecture in the 2004 National Lecture Series », discours présenté dans le cadre du *National Lecture Series of the Australian Institute of Administrative Law*, Sydney, 29 avril 2004, http://www.lawlink.nsw.gov.au/lawlink/supreme_court/ll_sc.nsf/pages/SCO_speech_spigelman_290404 (consulté le 14 décembre 2009).

TURBIDE, Mathieu. « Street View est-il une atteinte à la vie privée? », 2009, <http://www.infinet.net/techno/nouvelles/archives/2009/10/20091008-073509.html>.

WORLD PRIVACY FORUM, *Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing*, 2009, <http://www.worldprivacyforum.org/cloudprivacy.html>.

Sites Internet

Assemblée législative de la Colombie-Britannique, <http://www.leg.bc.ca/>.

Commissariat à l'information et à la protection de la vie privée de l'Alberta, <http://www.oipc.ab.ca/pages/About/Commissioner.aspx>

Commissariat à l'information et à la protection de la vie privée de la Colombie-Britannique, <http://www.oipc.bc.ca/>

Commissariat à la protection de la vie privée du Canada, <http://www.priv.gc.ca/>

Commission d'accès à l'information du Québec, <http://www.cai.gouv.qc.ca/>

Conseil de la radiodiffusion et des télécommunications canadiennes, <http://www.crtc.gc.ca/>

Contrôleur européen de la protection des données, <http://www.edps.europa.eu>

Facebook, <http://www.facebook.com>

Faculté de droit de l'Université de New York, Institut de droit international et de justice, Global Administrative Law Project, http://www.iilj.org/global_adlaw

Flickr, <http://www.flickr.com/>

Google images, <http://images.google.ca/>

Google maps, <http://maps.google.ca/>

Google, <http://www.google.ca> et <http://www.google.fr>

Grand Dictionnaire, www.granddictionnaire.com

Groupe d'étude sur les politiques en matière de concurrence, www.competitionreview.ca

Myspace, www.myspace.com

Reforming the FCC, <http://fcc-reform.org/>

Wikipedia, www.wikipedia.org

Yahoo maps, <http://ca.maps.yahoo.com/>

Youtube, www.youtube.com

ANNEXE A

Loi sur l'équité en matière d'emploi, L.C. 1995, chap. 44, partie III (sanctions pécuniaires), art. 35 et s.

PARTIE III SANCTIONS PÉCUNIAIRES

VIOLATIONS

Violation

35. (1) Commet une violation de la présente loi l'employeur du secteur privé qui :

- a) contrairement à l'article 18, sans excuse légitime, ne dépose pas son rapport sur l'équité en matière d'emploi;
- b) sans excuse légitime, ne porte pas au rapport les renseignements exigés en application de cet article ou des règlements;
- c) y consigne des données qu'il sait fausses ou trompeuses.

Violation continue

(2) Il est compté une violation distincte pour chacun des jours au cours desquels se commet ou se continue la violation.

Exclusion du *Code criminel*

(3) La violation n'est pas une infraction et le *Code criminel* ne s'applique pas.

Avis de sanction

36. (1) Dans les deux ans suivant la date à laquelle une violation est portée à sa connaissance, le ministre peut expédier, par courrier recommandé, un avis de sanction pécuniaire à l'employeur du secteur privé.

Plafond

(2) Le plafond de la sanction est de dix mille dollars, et de cinquante mille dollars en cas de récidive ou de violation continue.

Facteurs

(3) En vue d'établir le montant de la sanction, le ministre tient compte des facteurs suivants :

- a) la nature, les circonstances, la portée et la gravité de la violation;
- b) l'intention de l'employeur, le caractère volontaire de ses actions et ses antécédents en matière de violations.

Contenu de l'avis

37. L'avis comporte les éléments suivants :

- a) la caractérisation de la prétendue violation;
- b) le montant de la sanction pécuniaire;
- c) la mention du lieu où l'employeur peut payer la sanction.

OPTIONS

Options de l'employeur

38. (1) L'employeur dispose de trente jours après réception de l'avis pour soit s'y conformer, soit contester la sanction en demandant au ministre, par écrit, la révision de l'affaire par un tribunal.

Double

(2) Sur réception de la demande de révision, le ministre en expédie un double au président.

Défaut

(3) Si l'employeur n'exerce pas son choix dans le délai fixé, le ministre expédie un double de l'avis au président.

1995, chap. 44, art. 38; 1998, chap. 9, art. 40.

Assignation

39. (1) Sur réception du double de la demande ou de l'avis, le président constitue un tribunal composé d'un seul membre choisi parmi les membres du Tribunal canadien des droits de la personne pour réviser la sanction et :

- a) assigne, par courrier recommandé, l'employeur à comparaître devant le tribunal à la date et au lieu indiqués pour y entendre les faits qui lui sont reprochés;
- b) informe par écrit le ministre de la date et du lieu mentionnés dans l'assignation.

Défaut de comparution

(2) En cas de défaut de comparution, le tribunal examine tous les renseignements qui lui sont fournis par le ministre sur la prétendue violation.

Comparution

(3) Lors de la comparution, le tribunal donne à l'employeur et au ministre toute possibilité de lui présenter leurs éléments de preuve et leurs observations sur la prétendue violation, conformément aux principes de l'équité procédurale et de la justice naturelle.

Décision du tribunal

(4) À l'issue de l'instance, le tribunal :

- a) lorsqu'il conclut à l'absence de violation, en informe immédiatement l'employeur et le ministre, nulle autre poursuite ne pouvant être intentée à cet égard;
- b) dans le cas contraire, expédie immédiatement au ministre un certificat, établi en la forme réglementaire, comportant sa décision et le montant de la sanction — à concurrence du plafond prévu au paragraphe 36(2) — , qu'il fait également parvenir, par courrier recommandé, à l'employeur.

Facteurs

(5) Le tribunal tient compte des facteurs mentionnés au paragraphe 36(3) pour fixer le montant de la sanction.

Charge de la preuve

(6) Lors de l'instance, il incombe au ministre de prouver, selon la prépondérance des probabilités, que l'employeur a commis la violation.

Valeur du certificat

(7) Le certificat censé délivré par le tribunal fait foi de son contenu sans qu'il soit nécessaire de prouver l'authenticité de la signature ou la qualité du signataire.

Effet de décision

(8) Les décisions du tribunal ne sont susceptibles de révision qu'au titre de la *Loi sur les Cours fédérales*.

1995, chap. 44, art. 39; 1998, chap. 9, art. 41; 2002, chap. 8, art. 182.

EXÉCUTION DES SANCTIONS PÉCUNIAIRES

Homologation du certificat

40. (1) Le certificat délivré en vertu de l'alinéa 39(4)*b*) peut être homologué à la Cour fédérale; dès lors, toute procédure d'exécution peut être engagée, le certificat étant assimilé à un jugement de cette juridiction obtenu par Sa Majesté du chef du Canada contre l'employeur en cause pour une dette correspondant au montant de la sanction pécuniaire indiqué.

Recouvrement des frais

(2) Tous les frais entraînés par l'homologation du certificat peuvent être recouvrés comme s'ils faisaient partie du montant indiqué sur le certificat homologué en application du paragraphe (1).

ANNEXE B

Loi sur les télécommunications (1993, chap. 38)

Régime de sanctions administratives

Violation

72.01 Toute contravention ou tout manquement à une mesure prise par le Conseil au titre de l'article 41 constitue une violation exposant son auteur à une pénalité dont le montant peut atteindre :

- a) dans le cas d'une personne physique, 1 500 \$;
- b) dans le cas d'une personne morale, 15 000 \$.

2005, chap. 50, art. 2.

Responsabilité indirecte : employeurs et mandants

72.02 L'employeur ou le mandant est responsable de la violation commise par son employé ou son mandataire dans le cadre de son emploi ou du mandat, selon le cas, que l'auteur de la violation soit ou non connu ou poursuivi au titre de la présente loi.

2005, chap. 50, art. 2.

Violation continue

72.03 Il est compté une violation distincte pour chacun des jours au cours desquels se continue une violation.

Pouvoir du Conseil : procès-verbaux

72.04 (1) Le Conseil peut :

- a) désigner, individuellement ou au titre de leur appartenance à telle catégorie, les agents autorisés à dresser des procès-verbaux pour une violation;
- b) établir pour chaque violation un sommaire la caractérisant dans les procès-verbaux.

Certificat

(2) L'agent verbalisateur reçoit un certificat attestant sa qualité qu'il présente, sur demande, à toute personne apparemment responsable du lieu visité.

Obligation d'information

72.05 S'il croit qu'une personne détient des renseignements qu'il juge nécessaires pour l'application de l'article 41, l'agent verbalisateur peut l'obliger à les lui communiquer dans des rapports périodiques ou selon les modalités de forme ou autres qu'il fixe.

Inspections

72.06 (1) L'agent verbalisateur peut :

- a) procéder, à toute heure convenable, à la visite de tout lieu où se trouvent, à son avis fondé sur des motifs raisonnables, des objets, des documents ou des renseignements concernant l'application de l'article 41, examiner ceux-ci et les emporter pour examen et reproduction;
- b) faire usage, directement ou indirectement, de tout système informatique se trouvant dans le lieu pour vérifier les données qu'il contient ou auxquelles il donne accès;
- c) à partir de ces données, reproduire ou faire reproduire le document sous forme d'imprimé ou toute autre forme intelligible qu'il peut emporter pour examen ou reproduction;
- d) utiliser, dans le cadre de sa visite, le matériel de reproduction et les moyens de communication du lieu.

Local d'habitation

(2) Il ne peut toutefois procéder à la visite d'un local d'habitation sans le consentement de l'occupant que s'il est muni d'un mandat.

Délivrance du mandat

(3) Sur demande *ex parte*, le juge de paix, au sens de l'article 2 du *Code criminel*, peut signer un mandat autorisant, sous réserve des conditions fixées, l'agent verbalisateur qui y est nommé à procéder à la visite d'un local

d'habitation si lui-même est convaincu, sur la foi d'une dénonciation sous serment, que sont réunis les éléments suivants :

- a) les circonstances prévues à l'alinéa (1)a) existent;
- b) la visite est nécessaire à l'application de l'article 41;
- c) soit un refus a été opposé à la visite ou il y a des motifs raisonnables de croire que tel sera le cas, soit il n'est pas possible d'obtenir le consentement de l'occupant.

Usage de la force

(4) L'agent verbalisateur ne peut recourir à la force dans l'exécution du mandat que si celui-ci en autorise expressément l'usage et que s'il est accompagné d'un agent de la paix.

Procès-verbal

72.07 (1) L'agent verbalisateur peut, s'il a des motifs raisonnables de croire qu'une violation a été commise, dresser un procès-verbal qu'il fait signifier à l'auteur présumé.

Contenu du procès-verbal

(2) Le procès-verbal mentionne, outre le nom de l'auteur présumé et les faits reprochés :

- a) la pénalité prévue pour la violation;
- b) la faculté qu'a l'auteur présumé soit de payer la pénalité, soit de présenter au Conseil des observations relativement à la violation, et ce dans les trente jours suivant la signification du procès-verbal — ou dans le délai plus long que peut préciser le Conseil —, ainsi que les modalités d'exercice de cette faculté;
- c) le fait que le non-exercice de cette faculté dans le délai imparti vaut aveu de responsabilité et permet au Conseil d'imposer la pénalité.

Paiement

72.08 (1) Le paiement de la pénalité en conformité avec le procès-verbal vaut aveu de responsabilité à l'égard de la violation et met fin à la procédure.

Présentations d'observations

(2) Si des observations sont présentées dans le délai imparti, le Conseil détermine, selon la prépondérance des probabilités, la responsabilité de l'intéressé. Le cas échéant, il peut imposer la pénalité mentionnée au procès-verbal.

Défaut de payer ou de faire des observations

(3) Le non-exercice de la faculté mentionnée au procès-verbal dans le délai imparti vaut aveu de responsabilité à l'égard de la violation et le Conseil peut imposer la pénalité mentionnée au procès-verbal.

Avis de décision et des droits de l'intéressé

(4) Le Conseil fait signifier à l'intéressé une copie de la décision prise au titre des paragraphes (2) ou (3) et l'avise par la même occasion de son droit de faire une demande de révision en vertu de l'article 62 ou d'interjeter appel en vertu de l'article 64.

Créance de Sa Majesté

72.09 (1) La pénalité constitue une créance de Sa Majesté du chef du Canada, dont le recouvrement peut être poursuivi à ce titre devant la Cour fédérale.

Prescript

(2) Le recouvrement de la créance se prescrit par cinq ans à compter de la date à laquelle elle est devenue exigible.

Receveur général

(3) Toute pénalité perçue au titre d'une violation est versée au receveur général.

Certificat de non-paiement

(4) Le Conseil peut établir un certificat de non-paiement pour la partie impayée de toute créance visée au paragraphe (1).

Enregistrement à la Cour fédérale

(5) L'enregistrement à la Cour fédérale confère au certificat la valeur d'un jugement de cette juridiction pour la somme visée et les frais afférents.

Moyens de défense

72.1 (1) L'auteur de la violation peut invoquer en défense dans le cadre de toute procédure en violation qu'il a pris les précautions voulues.

Principes de la common law

(2) Les règles et principes de la common law qui font d'une circonstance une justification ou une excuse dans le cadre d'une poursuite pour infraction à l'égard d'une contravention ou d'un manquement à une mesure prise par le Conseil au titre de l'article 41 s'appliquent à l'égard de toute violation sauf dans la mesure où ils sont incompatibles avec la présente loi.

Admissibilité en preuve

72.11 Dans toute procédure en violation, le procès-verbal apparemment signifié en vertu du paragraphe 72.07(1) ou la copie de la décision apparemment signifiée en vertu du paragraphe 72.08(4) sont admissibles en preuve sans qu'il soit nécessaire de prouver l'authenticité de la signature qui y est apposée ni la qualité officielle du signataire.

Prescription

72.12 (1) Les procédures en violation se prescrivent par deux ans à compter de la date où le Conseil a eu connaissance des éléments constitutifs de la violation.

Certificat du secrétaire du Conseil

(2) Tout document apparemment délivré par le secrétaire du Conseil et attestant la date où les éléments sont parvenus à sa connaissance fait foi de cette date, en l'absence de preuve contraire, sans qu'il soit nécessaire de prouver l'authenticité de la signature qui y est apposée ni la qualité officielle du signataire.

Publication

72.13 Le Conseil peut procéder à la publication de la nature de la violation, du nom de son auteur et de la pénalité.

Exclusion

72.14 S'agissant d'une contravention ou d'un manquement à une mesure prise par le Conseil au titre de l'article 41 et qualifiable à la fois de violation et d'infraction, la procédure en violation et la procédure pénale s'excluent l'une l'autre.

Non-application de l'article 12

72.15 L'article 12 ne s'applique pas aux décisions du Conseil prises au titre des paragraphes 72.08(2) ou (3).

