Commissariat
à la protection de
la vie privée du Canada

ARGUMENTS EN FAVEUR DE LA RÉFORME DE LA *LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET LES DOCUMENTS ÉLECTRONIQUES*

Mai 2013

TABLE DES MATIÈRES

SOMMAIRE

L'environnement dans lequel les renseignements personnels sont recueillis, utilisés et communiqués a grandement changé depuis l'adoption de la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE) au début du XXI^{e} siècle.

Au cours de cette courte période, les percées dans le domaine de la puissance de traitement et de la capacité de stockage des ordinateurs, ainsi que l'augmentation importante de la quantité de renseignements personnels sur les individus que les organisations peuvent recueillir, emmagasiner, utiliser et communiquer ont conjointement préparé le terrain pour une explosion du rôle que les renseignements personnels jouent dans l'économie numérique. À ces changements se sont joints les risques que les renseignements personnels des individus soient utilisés d'une façon qui peut être intrusive, ou non sciemment prévue ou choisie par les personnes, alors que les organisations s'empressent de créer de nouveaux services et produits. Dans certains cas, les renseignements personnels sont susceptibles d'être volés ou perdus en raison de l'absence de mesures de sécurité appropriées.

Il faut pouvoir compter sur des mesures incitatives pour s'assurer que les organisations intègrent dès le début des mesures de protection de la vie privée à leurs produits et services, par exemple, un régime d'application de la loi plus strict. Parmi d'autres mesures incitatives, mentionnons des mécanismes de reddition de comptes et de vérification de la transparence plus vigoureux, afin de veiller à ce que les renseignements personnels des Canadiennes et des Canadiens soient adéquatement protégés dans un environnement complexe et branché sur le monde.

Ces mesures permettront de relever les défis actuels et futurs en matière de protection de la vie privée, d'accroître la confiance des Canadiennes et des Canadiens dans l'économie numérique, de renforcer l'innovation et la croissance au pays, ainsi que d'assurer que le Canada reste un pays dont le cadre de protection de la vie privée est approprié, à jour et équilibré.

Le présent document recommande les changements suivants à la LPRPDE afin d'établir de telles mesures incitatives :

- Réformer la LPRPDE afin de pouvoir compter sur de plus grands pouvoirs en matière d'application de la loi. Cela pourrait comprendre des dommages-intérêts légaux (administrés par les tribunaux fédéraux), ou le fait d'accorder à la commissaire le pouvoir d'émettre des ordonnances ou d'imposer des sanctions administratives pécuniaires, ou une combinaison de ces options;
- Obliger les organisations à signaler les atteintes à la protection des renseignements personnels à la commissaire et à aviser les personnes concernées, s'il y a lieu, afin que les mesures d'atténuation appropriées puissent être prises en temps opportun;
- Exiger des organisations qu'elles rendent public le nombre de communications effectuées à des autorités chargées de l'application de la loi en vertu de l'alinéa 7(3)*c.1*), à l'insu de l'intéressé et sans son consentement, et sans mandat, afin de faire la lumière sur la fréquence à laquelle cette exception extraordinaire est invoquée et sur l'utilisation qui en est faite.
- Modifier le principe de responsabilité énoncé à l'annexe 1 pour indiquer que les organisations ont l'obligation de démontrer, sur demande, qu'elles prennent leurs responsabilités, pour inclure le concept d'« ententes exécutoires », et pour assujettir à l'examen de la Cour fédérale certaines dispositions relatives à la responsabilité.

La LPRPDE est neutre sur le plan technologique et est fondée sur des principes — deux qualités qui doivent être conservées, car elles constituent des forces de la loi. Grâce aux changements recommandés, la LPRPDE pourra devenir une loi sur la protection des renseignements personnels plus moderne qui reflète les forces des autres lois sur la protection des données au Canada et à l'échelle internationale et les améliorations qui y ont été apportées, assurant ainsi la protection des renseignements personnels des Canadiennes et des Canadiens dans l'économie numérique.

INTRODUCTION

La *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE) a reçu la sanction royale le 13 avril 2000 et est entrée en vigueur par étapes à compter du 1er janvier 2001. Elle est entrée pleinement en vigueur le 1er janvier 2004.

La LPRPDE a été « adoptée pour atténuer les inquiétudes des consommateurs concernant le respect de la vie privée et pour permettre au milieu des affaires canadien de soutenir la concurrence dans l'économique numérique mondiale[1] ». La *Loi* avait pour objectif stratégique de renforcer la confiance à l'égard du commerce électronique[2].

La loi s'applique aux organisations qui recueillent, utilisent ou communiquent des renseignements personnels dans le cadre de leurs activités commerciales. Elle s'applique également à la collecte, à l'utilisation et à la communication des renseignements personnels des employés des entreprises fédérales — banques, transporteurs aériens, entreprises de télécommunication et de radiodiffusion, et autres industries sous réglementation fédérale[3].

La LPRPDE renferme une disposition énonçant qu'un examen de la loi est prévu aux cinq ans pour s'assurer que la loi produit les effets attendus et qu'elle permet d'obtenir les résultats souhaités. Le premier examen a commencé en 2006 et a donné lieu à des recommandations du Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique (ETHI) à l'intention du gouvernement. Le gouvernement a répondu au Comité en présentant un projet de loi en 2010, qui est mort au Feuilleton près d'un an plus tard lors du déclenchement d'élections. Il a été déposé de nouveau en tant que projet de loi C-12 à l'automne 2011, mais, à la date de la présente publication, il n'avait pas encore franchi l'étape de la deuxième lecture. Le deuxième examen de la LPRPDE accuse aussi du retard.

En 2012, le Comité ETHI s'est penché sur la protection de la vie privée et les médias sociaux. Le 23 avril 2013, le Comité a présenté son rapport, qui comporte sept recommandations et demande au gouvernement de donner une réponse. Annexé au rapport, on trouve le rapport dissident du Nouveau Parti démocratique (NPD), qui comprend neuf recommandations. L'étude a fourni une occasion importante d'examiner un grand nombre des nouveaux enjeux en matière de protection de la vie privée qui sont liés aux nouvelles technologies[4].

Au fil des années, le Commissariat à la protection de la vie privée du Canada (le Commissariat) a mené diverses études et consultations pour mieux comprendre les défis de l'environnement actuel et évaluer l'efficacité de la loi. Nous comptons également plus d'une décennie d'expérience pratique dans la réalisation d'enquêtes sur les plaintes, la conduite de vérifications et la surveillance des atteintes à la protection des renseignements personnels — du moins les quelques incidents qui sont portés à notre attention de façon volontaire ou par le biais des médias.

Le présent exposé de position présente nos observations sur la façon dont l'environnement a changé depuis le début du XXIe siècle, et décrit certains des plus importants points de pression qui font qu'il est ou qu'il sera difficile de faire respecter la LPRPDE et de veiller à ce que les organisations respectent la loi. L'exposé de position présente également notre point de vue sur la façon dont la *Loi* pourrait être améliorée pour favoriser une conformité proactive.

DÉFIS LIÉS À LA PROTECTION DES RENSEIGNEMENTS PERSONNELS DANS L'ÉCONOMIE NUMÉRIQUE

L'environnement dans lequel les renseignements personnels sont recueillis, utilisés et communiqués a grandement changé depuis l'entrée en vigueur de la LPRPDE. En 2001, les sites de réseautage social, les sites de partage de vidéos et le microblogage étaient pratiquement inexistants. Les téléphones cellulaires devenaient de plus en plus répandus, mais leur utilisation n'était pas généralisée, et ils ne servaient pas à naviguer sur le Web, à jouer à des jeux ou à révéler leur emplacement. Au début de la décennie, le Web était en expansion et certaines entreprises commençaient à faire des affaires en ligne, mais pas au niveau actuel. Depuis le dernier examen de la *Loi*, qui a eu lieu en 2006, les percées dans le domaine de la puissance de traitement et de la capacité de stockage des ordinateurs, ainsi que l'augmentation importante de la quantité de renseignements personnels sur les individus que les organisations peuvent recueillir, emmagasiner, utiliser et communiquer ont conjointement préparé le terrain pour une explosion du rôle que les renseignements personnels jouent dans l'économie numérique.

La technologie évolue rapidement et le monde virtuel s'est transformé grâce aux nouvelles façons dont les personnes peuvent communiquer et partager des renseignements personnels. L'adoption et l'utilisation à grande échelle de divers sites de médias sociaux par les organisations et les personnes brouillent toutefois les frontières entre les activités commerciales et non commerciales, de même qu'entre l'univers public et privé. Les conséquences sont d'ailleurs de plus en plus évidentes.

Mégadonnées et géants des données

Un grand nombre de gens passent une bonne partie de leur vie en ligne. Selon certaines estimations, les Canadiennes et les Canadiens sont des chefs de file dans l'utilisation d'Internet, y consacrant une moyenne de 43,5 heures par mois, soit deux fois la moyenne mondiale[5].

Lorsque nous naviguons sur Internet, faisons des recherches, communiquons avec nos amis ou téléchargeons de la musique, nous laissons des traces sous forme de données qui en disent long sur qui nous sommes — nos intérêts, nos habitudes, nos opinions — et, dans bien des cas, même l'endroit où nous nous trouvons.

Nous vivons à l'époque des « mégadonnées ». Selon IBM, nous créons, à l'échelle mondiale, 2,5 quintillions d'octets de données par jour (ce qui équivaut à environ 57,5 milliards d'iPads de 32 Go[6]). Quatre-vingt-dix pour cent des données qui existent dans le monde aujourd'hui ont été créées au cours des deux dernières années[7].

Les renseignements personnels sont au cœur de l'économie numérique mondiale. Certaines organisations qui recueillent de grandes quantités de renseignements personnels des Canadiennes et des Canadiens sont devenues des géants des données, des quasi-monopoles qui permettent de bien connaître les intérêts, les habitudes et les opinions des internautes. Certaines des plus importantes entreprises se réjouissent d'avoir des centaines de millions de consommateurs ou d'utilisateurs. Facebook, par exemple, compte plus d'un milliard d'utilisateurs à l'échelle mondiale, y compris près de 20 millions d'utilisateurs au Canada. Pour sa part, Twitter compte actuellement plus de 500 millions d'utilisateurs. Même les plus petites organisations, en particulier celles qui ont une présence numérique, recueillent de plus en plus d'importantes quantités de renseignements personnels[8].

La majorité des sociétés Internet offrent leurs services sans frais. Elles subissent toutefois de plus en plus de pressions pour trouver des façons de rentabiliser leurs services, une des options les plus évidentes étant de tirer parti de leur richesse inouïe en renseignements personnels. Il s'agit d'un environnement hautement concurrentiel dans lequel apparaissent de nouveaux intervenants presque chaque jour. Les habitudes des personnes et les détails personnels les concernant sont suivis, profilés et ciblés dans l'empressement d'innover, d'améliorer les services et de trouver de nouveaux marchés. De plus en plus d'entreprises souhaitent regrouper les données en ligne et les données hors ligne, ce qui leur permettrait de mieux connaître leurs consommateurs et d'anticiper leurs besoins et désirs — parfois même avant que les personnes concernées en soient elles-mêmes conscientes[9].

Par ailleurs, la confiance des personnes, qui est nécessaire pour que l'économie numérique prospère, a également été menacée. Soizante-dix pour cent des Canadiennes et des Canadiens que nous avons interrogés en 2012 sont d'avis que leurs renseignements personnels sont moins bien protégés qu'il y a dix ans. Cinquante-six pour cent affirment ne pas savoir quelle est l'incidence des nouvelles technologies sur le respect de la vie privée, ce qui représente une augmentation par rapport aux quarante-sept pour cent obtenus en 2000[10]. Comme l'indiquait le Comité ETHI, les médias sociaux forment une industrie en rapide évolution, « un secteur confronté aux limites de la vie privée et se devant de garantir la vie privée pour susciter la confiance des consommateurs[11] ». Selon nous, il en va ainsi pour tous les intervenants de l'économie numérique.

Les risques en matière de protection de la vie privée croissent avec l'évolution de l'environnement. Les organisations utilisent les renseignements personnels de façons antérieurement inimaginables. Même si bon nombre de ces nouvelles utilisations pourraient profiter aux personnes et à la société, le risque que les renseignements personnels puissent être utilisés de façons extrêmement intrusives et qui heurtent notre sentiment de vie privée est réel. Même si les renseignements ne sont pas utilisés à mauvais escient, ils pourraient être perdus, consultés sans autorisation ou volés par des pirates informatiques expérimentés.

Compte tenu du fait que l'objectif de la LPRPDE est de trouver un équilibre entre le droit des personnes à la vie privée et les besoins légitimes des organisations de recueillir, d'utiliser et de communiquer des renseignements personnels à une fin appropriée, il est important de vérifier si cet objectif est atteint dans l'environnement en évolution et de déterminer comment la LPRPDE pourrait être améliorée pour mieux atteindre cet objectif.

POINTS DE PRESSION : LES DÉFIS LIÉS À L'APPLICATION DE LA LPRPDE ET LES RECOMMANDATIONS POUR ASSURER LA CONFORMITÉ

Nous avons dégagé quatre points de pression au cours des douze années où nous avons supervisé la conformité à la LPRPDE et surveillé l'évolution du milieu. Ils portent principalement sur le modèle d'application actuel de la LPRPDE, compte tenu d'un contexte international en évolution et de notre capacité à tenir les organisations responsables et à exiger qu'elles fassent preuve de transparence en ce qui concerne leurs pratiques de traitement des renseignements personnels.

Point de pression 1 : Application

En vertu de la *Loi*, la commissaire à la protection de la vie privée est une « enquêteure administrative[12] » dotée d'un éventail de pouvoirs, dont la capacité d'entreprendre ses propres enquêtes et vérifications (avec des motifs raisonnables) ainsi que le pouvoir d'exiger la production de preuves et d'entrer sur les lieux dans le cadre de la réalisation d'une enquête. La commissaire peut chercher à régler une plainte par le biais de la négociation, de la persuasion et de la médiation. Même si elle peut encourager la conformité en nommant les organisations mises en cause s'il est dans l'intérêt public de le faire, elle n'a aucun pouvoir exécutoire direct. La commissaire peut seulement, dans certaines circonstances, demander à la Cour fédérale d'entendre certains éléments soulevés dans les plaintes présentées au Commissariat, ordonner au mis en cause de prendre des mesures pour corriger ses pratiques ou accorder des dommages-intérêts au plaignant.

La pertinence du modèle actuel d'application de la LPRPDE a fait l'objet de débats avant l'entrée en vigueur de la loi et dans les années suivantes. Même si la question a été soulevée durant le premier examen obligatoire de la loi en 2006, la commissaire à la protection de la vie privée a alors choisi de ne pas proposer de changements à la structure d'application pour plusieurs raisons. Le Commissariat sortait à peine d'une période d'instabilité, de surveillance et de capacité réduite, et on en était encore aux débuts de l'interprétation et de l'application de la LPRPDE. Au lieu de cela, le Commissariat a indiqué qu'il avait l'intention de faire un plus grand usage de ses pouvoirs existants pour mener des vérifications, déposer des plaintes et avoir recours aux tribunaux pour encourager un plus grand respect de la loi. En plus d'enquêter sur des milliers de plaintes présentées par des personnes, la commissaire a, de sa propre initiative, lancé 38 enquêtes relatives à des plaintes et mené trois vérifications d'organisations assujetties à la LPRPDE depuis 2001. Toujours depuis 2001, des entreprises ont été nommées dans l'intérêt public à 32 reprises et 17 poursuites ont été lancées en justice.

L'économie du Canada dépend du commerce et de la circulation de l'information. La LPRPDE pourrait bien s'appliquer à plus d'un million d'entreprises au Canada[13]. La mondialisation créant une économie plus ouverte, le Commissariat ne traite toutefois plus uniquement avec des entreprises canadiennes. Le siège social de bon nombre de ces entreprises est situé dans d'autres pays, qui ont établi ou non leurs propres exigences réglementaires en matière de protection des renseignements personnels. Il est légitime de se demander comment une petite entité disposant de ressources limitées, comme le Commissariat, peut attirer l'attention de ces

entreprises et les encourager activement à se conformer à la LPRPDE, alors qu'en réalité, le fait de contrevenir à la loi canadienne en matière de protection de la vie privée entraîne très peu de conséquences. Comme l'indiquait le Comité ETHI dans son rapport : « il importe que les Canadiens qui utilisent les services [médias sociaux] de ces entreprises soient protégés par leurs propres lois et valeurs[14]. »

Nous avons utilisé les outils offerts par la *Loi*, et, dans certains cas, nous avons réussi à susciter un changement — mais souvent après avoir investi d'importantes ressources et presque toujours après coup. Nous avons vu des organisations ignorer nos recommandations jusqu'à ce que la Cour soit saisie de l'affaire. D'autres, au nom d'une consultation avec le Commissariat, répondent pour la forme à nos préoccupations, pour ensuite ignorer nos conseils. Rien dans la loi n'incite les organisations à investir dans la protection de la vie privée de façon notable, dans la mesure où elles peuvent toujours revenir sur leur entente d'apporter des changements à leurs pratiques et décider de ne pas donner suite aux recommandations de la commissaire après l'enquête ou la vérification.

Les recommandations « douces » assorties de peu de conséquences en cas de manquement à la loi[15] ne sont plus efficaces dans un environnement qui évolue rapidement et où les risques pour la vie privée sont à la hausse. Il est temps de mettre en place des mesures incitatives financières pour veiller à ce que les organisations assument de plus grandes responsabilités en ce qui a trait à l'adoption, dès le départ, de mesures de protection adéquates, et de prévoir des sanctions pour les organisations qui ne le font pas. En l'absence de telles mesures, la commissaire à la protection de la vie privée aura une capacité limitée pour ce qui est de s'assurer que les organisations protègent les renseignements personnels adéquatement à l'ère des mégadonnées.

Le contexte national et international

Plusieurs commissaires provinciaux ont le pouvoir de rendre des ordonnances, en plus des autres fonctions prescrites dans la loi qui régit leurs activités, qui sont semblables à celles du Commissariat. Ces autres fonctions concernent notamment la tenue d'enquêtes, la réalisation de recherches ou la sensibilisation des entreprises ou du public aux questions de protection de la vie privée. Ce pouvoir n'entrave pas la capacité des commissaires à s'acquitter d'une vaste gamme de fonctions. De fait, cette multitude de rôles est courante dans de nombreux organismes administratifs.

Dans d'autres juridictions, on constate une tendance à conférer des pouvoirs d'exécution de la loi plus forts, et à imposer des pénalités et des amendes plus importantes.

La Federal Trade Commission (FTC) des États-Unis a négocié de nombreux règlements financiers médiatisés à la suite d'atteintes à la vie privée[16]. Les autorités de protection des données du Royaume-Uni, de l'Irlande, de la Nouvelle-Zélande et de l'Espagne ont également le pouvoir de rendre des ordonnances[17], le Royaume-Uni et l'Espagne disposant en outre de la capacité d'imposer une amende aux organisations. Au Royaume-Uni, ces pouvoirs d'application de la loi plus grands n'ont pas empêché la mise en place d'une approche de type ombudsman. Des amendes sont en effet imposées seulement lorsqu'une méthode plus douce n'a pas fonctionné.

La *Privacy Act* australienne a récemment été modifiée pour donner au commissaire la capacité d'accepter des engagements exécutoires et de s'adresser à la Cour fédérale en vue d'imposer des amendes de plus de 1 million de dollars (australiens) pour une entreprise.

Le 25 janvier 2012, la Commission européenne a publié sa *Proposition de règlement du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (règlement sur la protection des données)*. À l'heure actuelle, les pouvoirs d'application de la loi varient grandement au sein de l'Union européenne. Pour favoriser une certaine uniformité des pouvoirs sur l'ensemble du continent, un aspect du règlement demande que les autorités de protection des données aient le pouvoir d'émettre des ordonnances pour faire cesser certaines activités, corriger, effacer ou détruire des données, et permettre aux personnes d'avoir accès à leurs données. En plus de rendre obligatoire le signalement des atteintes à la protection des données, le règlement proposé permettrait à chaque autorité de protection des données d'imposer des sanctions administratives, allant du simple avertissement à une amende[18].

L'une des raisons pour lesquelles la LPRPDE a été adoptée était la création d'un mécanisme permettant au Canada d'offrir un niveau de protection des renseignements personnels qui faciliterait l'acheminement de renseignements personnels en provenance d'États membres de l'Union européenne au Canada. La Directive de l'Union européenne sur la protection des données actuelle, qui a été adoptée en 1995 (et qui serait remplacée par le règlement proposé), renferme une disposition exigeant que les États membres permettent les transferts de renseignements personnels à un tiers pays comme le Canada, seulement si le tiers pays peut assurer un niveau adéquat de protection de ces renseignements. Le concept de caractère adéquat est conservé dans le règlement. Il reste à déterminer les répercussions que le règlement proposé, s'il est adopté dans sa forme actuelle, pourrait avoir sur la détermination du caractère adéquat de la capacité du Canada de protéger les renseignements personnels, compte tenu de l'état actuel de la LPRPDE[19].

Le risque de prendre du retard

Dans le contexte de ces changements, le modèle d'application de la loi prévu par la LPRPDE semble de plus en plus désuet. Lors de son entrée en vigueur en 2000, la LPRPDE était considérée comme un chef de file parmi les lois en matière de protection des données parce qu'elle était neutre sur le plan technologique et fondée sur les principes. Nous continuons de croire que cette approche de la LPRPDE constitue sa force. Au cours de la dernière décennie, nous avons toutefois assisté à l'adoption ailleurs dans le monde de nouvelles lois qui accordent aux autorités de protection des données plus de pouvoirs qui sont proportionnels aux risques accrus pour les renseignements personnels. Même si la commissaire a, actuellement, le pouvoir de nommer une entreprise si c'est dans l'intérêt public, ce qui peut inciter certaines entreprises à adopter ses recommandations afin d'éviter la publicité négative associée à des pratiques relatives à la protection des renseignements personnels qui contreviennent aux règles, la dénonciation publique des entreprises délinquantes n'est ultimement qu'un moyen d'encourager la conformité à la loi. Compte tenu de la portée ou de la quantité de renseignements personnels détenus par les organisations (particulièrement celles qui opèrent en ligne), il est difficile pour les personnes de « voter avec leurs pieds et d'aller voir ailleurs » lorsque des quantités croissantes de renseignements personnels sont détenues par un nombre sans cesse plus petit d'organisations.

Pour avoir une incidence significative sur la protection de la vie privée, le Canada doit se doter de pouvoirs comparables à ceux des autres gouvernements qui vont de l'avant et qui confèrent à leurs autorités de protection des données le pouvoir d'accorder des dommages-intérêts, d'administrer des amendes, de rendre des ordonnances et d'exiger que les organisations

signalent les atteintes graves. Cela est particulièrement nécessaire compte tenu du contexte de mondialisation du monde des affaires d'aujourd'hui et du fait que les joueurs les plus puissants de l'économie numérique d'aujourd'hui œuvrent à l'échelle internationale.

Le Canada ne peut se permettre d'accuser du retard et de ne pouvoir imposer que des conséquences minimales aux organisations qui ne respectent pas les lois fédérales sur la protection des renseignements personnels.

Recommandation 1 : Renforcer l'application de la* Loi *et encourager une plus grande conformité à celle-ci

Réformer la LPRPDE afin de pouvoir compter sur des pouvoirs d'application plus solides. Cela pourrait comprendre des dommages-intérêts légaux (administrés par les tribunaux fédéraux), ou accorder à la commissaire le pouvoir d'émettre des ordonnances ou d'imposer des sanctions administratives pécuniaires, ou une combinaison de ces options.

Il existe un certain nombre d'options qui, séparément ou conjointement, pourraient renforcer le modèle d'application actuel et encourager une plus grande conformité à la *Loi,* notamment un régime de dommages-intérêts légaux joint aux dispositions révisables[20] de la *Loi* indiquées à l'article 14 de la LPRPDE, administré par la Cour fédérale. Une autre option serait de conférer à la commissaire le pouvoir d'ordonner aux organisations de poser ou de cesser de poser des gestes afin de se conformer à la LPRPDE. Une dernière option consisterait à conférer à la commissaire le pouvoir d'imposer des sanctions administratives pécuniaires dans les cas où cela serait justifié. Toutes ces options sont examinées ci-dessous.

A. Dommages-intérêts légaux

La LPRPDE pourrait être modifiée pour conférer à un tribunal le pouvoir d'ordonner des dommages-intérêts dans le cas de certaines infractions. Conformément à ce modèle, des dommages-intérêts seraient accordés pour les infractions à certaines dispositions de la LPRPDE, sans l'obligation pour un demandeur de prouver une perte réelle découlant de l'infraction. Une fourchette de dommages-intérêts pourrait être établie, et des montants minimum et maximum pourraient être prévus pour les infractions à des dispositions précises. À l'intérieur de cette fourchette, les tribunaux pourraient évaluer les dommages-intérêts en s'appuyant sur divers facteurs explicites à prendre en considération.

D'un point de vue stratégique, les dommages-intérêts légaux sont appropriés dans les cas où il est difficile ou impossible pour le plaignant de prouver une perte quantifiable en raison de la violation de la loi. En établissant une fourchette ou des montants, les dommages-intérêts légaux facilitent les délibérations des tribunaux sur les montants appropriés, particulièrement dans le cas de pertes non financières, comme l'humiliation découlant d'une atteinte à la vie privée. Une certitude accrue relativement aux dommages-intérêts pouvant être accordés pourrait encourager les plaignants à faire respecter leurs droits devant les tribunaux dans des circonstances appropriées (et décourager les plaignants qui ont des attentes irréalistes d'intenter une poursuite en justice). Une certitude accrue dans les dispositions de la loi profiterait également aux organisations, car elles sauraient ce à quoi elles peuvent s'exposer et seraient mieux à même d'évaluer les risques et de prévoir les résultats.

Les dommages-intérêts légaux pourraient permettre l'atteinte d'objectifs stratégiques semblables à ceux qui sont visés par les régimes de sanctions administratives pécuniaires (SAP), à savoir encourager les organisations, sous forme de mesures incitatives financières, à se conformer à la LPRPDE. Il existe toutefois d'importantes différences entre ces deux types de mesures. Premièrement, des dommages-intérêts légaux pourraient être accordés à des victimes d'actes délictuels, alors que les sanctions administratives pécuniaires sont normalement dues au Trésor. Deuxièmement, en vertu d'un régime de dommages-intérêts légaux, la Cour fédérale continuerait d'être l'arbitre des dommages-intérêts accordés dans les limites prévues dans la loi selon une expérience et des procédures judiciaires bien établies.

Exemples de régimes de dommages-intérêts légaux

La *Loi sur le droit d'auteur* prévoit un régime de dommages-intérêts légaux pour la violation du droit d'auteur. Ce régime a été modifié en 2012, de façon à établir des dommages-intérêts minimum et maximum pour les infractions à des fins commerciales et non commerciales. Pour chaque œuvre pour laquelle l'infraction est à des fins commerciales, les dommages-intérêts vont de 500 $ (minimum) à 20 000 $ (maximum). En revanche, dans le cas des infractions à des fins non commerciales, les dommages-intérêts vont de 100 $ (minimum) à 5 000 $ (maximum) pour toutes les œuvres en cause dans l'instance.

Autre exemple, la *Loi canadienne anti-pourriel* prévoit des dommages-intérêts liés à un nouveau droit privé d'action pour toute violation ou des modifications connexes à la *Loi sur la concurrence* ou la LPRPDE. Les dommages-intérêts vont de 200 $ pour chaque infraction jusqu'à un maximum de 1 million de dollars pour chaque journée durant laquelle il y a eu infraction, selon la disposition en question. Il s'agit d'un point à souligner étant donné que le Parlement a déjà estimé qu'il était approprié de créer un régime de dommages-intérêts légaux applicable à diverses infractions à la LPRPDE.

B. Pouvoir de rendre des ordonnances

Si elle avait le pouvoir de rendre des ordonnances, la commissaire pourrait émettre une ordonnance exécutoire obligeant une organisation à poser ou à cesser de poser des gestes afin de prévenir une infraction ou de corriger les conséquences d'une infraction qui a déjà eu lieu. En d'autres mots, la commissaire serait en mesure d'ordonner ce quelle ne peut actuellement que recommander.

Dans le cadre du modèle envisagé (et comme c'est normalement le cas pour les autres tribunaux administratifs fédéraux qui ont le pouvoir de rendre des ordonnances), dans le cas où une ordonnance ne serait pas respectée, le plaignant ou la commissaire pourrait enregistrer l'ordonnance auprès de la Cour fédérale et veiller à ce qu'elle soit exécutée comme une ordonnance de la Cour, conformément aux pouvoirs liés à la sanction d'un outrage de la Cour. Pour sa part, l'organisation pourrait demander un contrôle judiciaire. La portée des dispositions pour lesquelles la commissaire aurait le pouvoir de rendre des ordonnances serait une question de politique législative.

Exemples de pouvoir de rendre des ordonnances dans les lois provinciales sur la protection des données

L'Alberta, la Colombie-Britannique et le Québec se sont dotés de lois qui régissent les activités du secteur privé et qui sont considérées comme essentiellement similaires à la LPRPDE. En vertu de ces lois, des ordonnances peuvent être imposées à l'endroit d'organisations du secteur privé pour certains gestes posés. Les commissaires de ces provinces ont également d'autres fonctions qui leur permettent de jouer de nombreux rôles : éducateur, arbitre, exécuteur, défenseur, etc.

C. Sanctions administratives pécuniaires (SAP)

Les sanctions administratives pécuniaires (SAP) sont des sanctions civiles ou des amendes qui peuvent être imposées dans les cas de non-conformité à la loi. Une SAP n'est pas de nature punitive. Elle a surtout pour but de favoriser la conformité ou, inversement, de prévenir la non-conformité, grâce à un incitatif monétaire. Plus qu'un simple « prix à payer pour faire des affaires », les SAP représentent un moyen rapide et efficace d'amener les organisations à se conformer à la loi.

Les SAP sont imposées par l'organisme qui applique la loi, plutôt que par les tribunaux. Si elles ne sont pas payées, elles deviennent des créances de la Couronne qui peuvent être recouvrées au moyen d'une poursuite civile. La décision d'imposer une SAP, comme toute autre décision d'un organe administratif, pourrait faire l'objet d'un contrôle judiciaire.

Les SAP peuvent être considérées comme une application distincte du pouvoir de rendre des ordonnances, mais elles se distinguent des autres ordonnances exécutoires par le fait qu'elles obligent l'organisation visée à payer un montant d'argent déterminé. Les régimes législatifs de SAP précisent habituellement que la norme de preuve applicable est celle de la prépondérance des probabilités, et ils fixent les montants maximums et minimums; ils peuvent aussi comprendre une liste de critères à utiliser pour déterminer l'importance de la SAP, ou faire état des motifs qui peuvent ou ne peuvent pas être invoqués comme défenses dans les procédures relatives à la SAP. Les régimes législatifs de SAP se caractérisent aussi parfois par des règles procédurales, des délais, et des mécanismes d'examen ou d'appel particuliers.

Exemples de régimes comportant des sanctions administratives pécuniaires (SAP)

Depuis que la LPRPDE a été adoptée, plusieurs régimes de SAP ont été mis en place au Canada. Le CANAFE, par exemple, a été créé en 2000 pour faciliter la détection, la prévention et la dissuasion du blanchiment d'argent et du financement des activités terroristes. En 2008, il a obtenu le pouvoir d'imposer une SAP aux entités déclarantes qui ne se conforment pas à la *Loi sur le recyclage des produits de la criminalité et le financement des activités terroristes*.

La *Loi canadienne anti-pourriel* contient aussi un régime de SAP. En vertu de cette loi, le Conseil de la radiodiffusion et des télécommunications canadiennes (CRTC) pourra imposer des sanctions administratives pécuniaires en cas d'infraction. Le montant maximal sera de 1 million de dollars par infraction dans le cas d'un particulier, et de 10 millions par infraction dans les autres cas (p. ex. les personnes morales). Les entreprises qui enfreignent les dispositions connexes de la *Loi sur la concurrence* lorsqu'elles envoient des messages électroniques peuvent se voir imposer une pénalité pouvant atteindre 10 millions de dollars pour une première infraction et 15 millions de dollars pour les infractions subséquentes. Contrairement à ses partenaires dans l'application de la *Loi canadienne anti-pourriel*, le Commissariat n'a pas la capacité de solliciter ou d'imposer des sanctions administratives pécuniaires en tant qu'outil d'application de la loi.

Parmi les autres agents du Parlement, la commissaire aux conflits d'intérêts et à l'éthique a le pouvoir d'imposer une SAP aux titulaires de charge publique principaux qui ne respectent pas certaines exigences de la *Loi sur les conflits d'intérêts* liées à la production de rapports. Aux termes de la *Loi*, l'amende maximale est de 500 $ et, jusqu'à maintenant, les amendes imposées allaient de 100 $ à 300 $. La *Loi sur les conflits d'intérêts* fait actuellement l'objet d'un examen, et il appert que la commissaire aux conflits d'intérêts et à l'éthique a demandé que le régime de SAP soit élargi pour inclure les violations des dispositions de fond de la loi et que le montant maximal des amendes soit supérieur à 500 $ pour certaines infractions[21].

Point de pression 2 : Atteintes à la sécurité des données et absence de mécanismes rendant obligatoire le signalement

Le fait que les organisations détiennent de vastes quantités de renseignements personnels peut entraîner des risques graves pour la protection de la vie privée des personnes. Les cas d'utilisation inattendue, indésirable ou intrusive résultant de lacunes au chapitre de la sécurité et de la protection des renseignements personnels dans les pratiques des organisations[22] ont énormément augmenté. Certes, ces atteintes ne sont pas nouvelles. Ce qui a changé, cependant, même depuis le premier examen de la LPRPDE entrepris en 2006, c'est la nature, l'éventail et le volume des renseignements vulnérables[23]. Les atteintes représentent une grave menace pour les renseignements personnels de la population canadienne et pour les organisations. Elles risquent de porter atteinte aux mécanismes de protection de l'identité et aux réputations, et les parties concernées peuvent devoir assumer des coûts élevés pour y remédier.

Au cours des dernières années, il y a eu de nombreuses atteintes à la sécurité des données très médiatisées au Canada et à l'étranger qui ont mis en péril la confidentialité des renseignements personnels des Canadiennes et des Canadiens. Ces atteintes peuvent occasionner de multiples effets dommageables, comme le vol d'identité, des pertes financières, des cotes de crédit négatives et même des préjudices physiques.

Si certaines recherches semblent indiquer que, globalement, on s'attend à ce que les organisations augmentent leurs dépenses en matière de sécurité des TI afin de protéger les données qu'elles détiennent contre le vol et les attaques[24], d'autres donnent à penser que les organisations, particulièrement au Canada, n'affectent pas assez de ressources à ce domaine[25]. Nous pensons qu'il faut accorder plus d'attention à ces questions.

Recommandation 2 : Mettre en lumière les atteintes à la sécurité des données

Obliger les organisations à signaler les atteintes à la sécurité des renseignements personnels à la commissaire et à aviser les personnes concernées, s'il y a lieu, afin que les mesures d'atténuation appropriées puissent être prises en temps opportun.

Au Canada, la loi sur la protection des renseignements personnels qui régit les activités du secteur privé de l'Alberta, la *Personal Information Protection Act*, et certaines lois provinciales sur la protection des renseignements personnels en matière de santé, contiennent des dispositions rendant obligatoires les signalements d'atteinte à la vie privée. Cependant, les organisations assujetties à la LPRPDE ne sont pas tenues de signaler les atteintes à la commissaire fédérale à la protection de la vie privée. Si certaines organisations signalent volontairement les incidents, et informent les personnes concernées de l'atteinte à la sécurité des données (dans les cas appropriés), beaucoup ne le font pas, et les personnes concernées se retrouvent ainsi vulnérables. Tant que le signalement des atteintes ne sera pas obligatoire, ce qui permettrait de connaître le nombre, la nature et l'ampleur des atteintes à la sécurité des données, il sera impossible de se faire une idée précise du portrait d'ensemble.

Ce qui est clair cependant, c'est que la situation actuelle crée des inégalités entre les organisations. Celles qui signalent les incidents risquent de voir leur réputation entachée et d'avoir à assumer les frais connexes, tandis que celles qui se taisent peuvent éventuellement s'en tirer sans préjudice pour leur réputation et leurs bénéfices.

Il convient également de mentionner les attentes de la population canadienne. Selon un sondage effectué en 2012 par le Commissariat, 59 % des répondants pensent qu'il est peu probable qu'une organisation les avise en cas d'atteinte à la sécurité des renseignements personnels. Pourtant, presque toutes les personnes sondées (97 %) disaient vouloir être informées dans un tel cas[26].

Ces dernières années, d'autres instances internationales ont mis au point de nouvelles approches pour faire face aux atteintes graves à la sécurité des renseignements personnels, et elles ont pris des mesures pour consolider leurs cadres de protection de la vie privée. Les États-Unis, par exemple, ont été un chef de file dans l'élaboration de lois rendant obligatoire le signalement des atteintes, et la plupart des États ont adopté de telles lois. Comme nous l'avons mentionné précédemment, le Royaume-Uni a aussi le pouvoir d'imposer des amendes aux organisations dans les cas d'atteinte grave. Au début de 2013, le Commissariat à l'information du Royaume-Uni a infligé une amende de 250 000 £ à Sony à cause d'une atteinte à la sécurité des renseignements personnels de millions d'utilisateurs de la Playstation.

Tous les États membres de l'Union européenne doivent adopter des lois sur le signalement en cas d'atteinte qui s'appliquent aux entreprises de télécommunications et aux autres fournisseurs de services de communications électroniques. Le règlement proposé par l'Union européenne élargirait la portée de ces lois pour qu'elles s'appliquent à d'autres organisations.

L'adoption de dispositions rendant obligatoire le signalement des atteintes[27] mettrait donc la LPRPDE au diapason des lois de nombreuses autres juridictions.

En plus d'obliger les organisations à signaler les atteintes au Commissariat et à informer les personnes concernées conformément aux seuils applicables, le défaut d'aviser devrait faire l'objet d'une disposition révisable — tout comme le défaut d'établir des mesures de sécurité — et sujet à une application plus rigoureuse, tel que décrit à la section 1, ci-dessus.

Point de pression 3 : Communication en vertu d'une « autorité légitime » et manque de transparence

Aux termes de l'alinéa 7(3)*c.1*) de la LPRPDE, une organisation peut communiquer des renseignements personnels à une institution gouvernementale — ou à une subdivision d'une telle institution — à l'insu de l'intéressé et sans son consentement si l'institution a demandé à obtenir le renseignement en mentionnant la source de l'autorité légitime étayant son droit de l'obtenir et le fait, selon le cas :

(i) qu'elle soupçonne que le renseignement est afférent à la sécurité nationale, à la défense du Canada ou à la conduite des affaires internationales;
(ii) que la communication est demandée aux fins du contrôle d'application du droit canadien, provincial ou étranger, de la tenue d'enquêtes liées à ce contrôle d'application ou de la collecte de renseignements en matière de sécurité en vue de ce contrôle d'application;
(iii) qu'elle est demandée pour l'application du droit canadien ou provincial.

Cette disposition a été insérée aux étapes finales de l'examen de la LPRPDE par le Parlement, en 1999, à la demande des autorités policières et gouvernementales, pour faire en sorte que les relations de longue date avec les entreprises puissent être maintenues.

À l'heure actuelle, en vertu de cette disposition, les entreprises peuvent contester ou rejeter de telles demandes présentées en vertu de la LPRPDE; beaucoup l'ont fait lorsqu'elles croyaient que l'autorité compétente devait d'abord obtenir une ordonnance de la cour. Mais d'autres opposent parfois moins de résistance étant donné les termes généraux de l'alinéa 7(3)*c.1*) tel qu'il est libellé actuellement. Plus précisément :

- Le terme « institution gouvernementale » n'est pas défini et pourrait s'appliquer à un grand nombre d'organisations provinciales ou fédérales; le terme « autorité légitime » n'est pas défini non plus;
- Le seuil pour le critère « aux fins du contrôle d'application du droit canadien, provincial ou étranger, de la tenue d'enquêtes liées à ce contrôle d'application ou de la collecte de renseignements en matière de sécurité en vue de ce contrôle d'application » décrit des paramètres généraux pour des demandes éventuelles;
- La formule « application du droit canadien ou provincial » est aussi vague.

Nous n'avons aucun moyen de connaître avec certitude le nombre, l'ampleur, la fréquence ou les raisons justifiant de telles communications, mais nous comprenons qu'ils sont importants. Aucune disposition n'oblige les organisations à rendre compte de ces communications, de sorte que les Canadiennes et les Canadiens qui demandent accès à leurs renseignements personnels ne seraient probablement pas en mesure de savoir si ceux-ci ont été divulgués en vertu de l'alinéa 7(3)*c.1*), étant donné que le paragraphe 9(2) de la LPRPDE ne permet pas de donner suite à leur demande.

Ce régime est inquiétant du point de vue de la protection de la vie privée puisqu'il n'y a pas de transparence ni de règles établies concernant les renseignements personnels qui peuvent ou qui devraient être communiqués aux institutions gouvernementales sans l'obtention d'une ordonnance d'une cour ou d'un mandat. Compte tenu de la quantité de renseignements personnels détenus par les organisations, les risques pour la vie privée découlant des communications sans mandat sont considérables et méritent un nouvel examen.

Recommandation 3 : Lever le voile sur les communications autorisées

Exiger des organisations qu'elles rendent public le nombre de communications aux fins d'application de la loi effectuées en vertu de l'alinéa 7(3)c.1), à l'insu de l'intéressé et sans son consentement, et sans mandat, afin de faire la lumière sur la fréquence à laquelle on invoque cette exception et sur l'utilisation qui en est faite.

Les Canadiennes et les Canadiens ont exprimé des inquiétudes importantes au sujet de l'accès sans mandat aux renseignements personnels par les organismes chargés de l'application de la loi. Il est de plus en plus évident qu'une plus grande transparence est requise en ce qui a trait à cette disposition. Les organisations devraient, à tout le moins, être obligées de tenir un registre des données de base se rapportant à ces communications, et elles devraient être tenues de rendre public le nombre de communications qu'elles effectuent chaque trimestre. Cette information pourrait être affichée sur le site Web des organisations. Pour ce qui est de la transparence, certaines organisations ont déjà commencé à montrer la voie[28].

Point de pression 4 : Faire preuve de responsabilité

La LPRPDE a été l'une des premières lois sur la protection des données à faire explicitement référence au principe de la responsabilité et à fournir des précisions à ce sujet. La LPRPDE a beaucoup été influencée par les *Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel* de l'Organisation de coopération et de développement économiques (OCDE), publiées en 1980, qui parlaient pour la première fois du principe de la responsabilité[29].

Ce principe a été inclus dans le cadre de protection de la vie privée de l'APEC (Coopération économique Asie-Pacifique), et le concept de responsabilité a aussi suscité de l'intérêt en Europe. Le nouveau cadre juridique proposé par l'Union européenne contient une disposition sur la responsabilité, y compris une obligation d'être en mesure de *démontrer* sa responsabilité.

Les intérêts commerciaux des États-Unis ont aussi dirigé le débat sur la responsabilité ces dernières années, dans l'espoir de faciliter les transferts internationaux de renseignements personnels avec l'Europe. Bon nombre des mêmes parties se sont intéressées à l'approche et au modèle canadiens.

Le Commissariat, tout comme ses homologues de l'Alberta et de la Colombie-Britannique, a publié des lignes directrices[30] sur ce que devrait contenir le programme de gestion de la protection de la vie privée d'une organisation responsable.

Conformité proactive

Même si la LPRPDE exige des organisations qu'elles rendent des comptes quant à leurs pratiques et à leurs procédures de protection des renseignements personnels, et qu'elle précise comment le faire, elle contient très peu d'éléments pour favoriser et renforcer la conformité proactive. Nos enquêtes ont trop souvent mis à jour des organisations qui avaient à maintes reprises omis d'adapter leurs processus de gouvernance de la protection des renseignements personnels afin de résoudre certains problèmes et ce, parfois, même après que nous ayons fait une enquête à leur sujet. Certains de ces problèmes auraient sauté aux yeux si le produit ou le service avait été examiné plus attentivement dès le départ.

Par exemple :

- Une première plainte contre une grande entreprise de vente au détail a été déposée en octobre 2004; une autre plainte contre la même entreprise a été déposée par une autre personne en février 2006. Les deux plaintes portaient sur l'insuffisance des mesures prises pour supprimer les renseignements personnels des appareils qui avaient été retournés à l'entreprise puis revendus. Dans les deux cas, la commissaire avait formulé des recommandations que l'entreprise avait accepté de mettre en œuvre. Après des reportages dans les médias, en 2009, au sujet de la même entreprise et du même

problème, le Commissariat a effectué une vérification. Ce n'est qu'au terme de cette vérification, en 2011 — près de sept ans après le dépôt de la première plainte — que l'entreprise s'est réellement occupée du problème.

- Il y a eu plusieurs plaintes concernant des activités inappropriées de la part de certains employés du secteur financier. Ces employés semblent faire fi des procédures de l'entreprise pour protéger les renseignements personnels des clients, en dépit du régime de gestion de la protection de la vie privée de leur employeur. Si on prend chaque cas isolément, il semble s'agir d'une erreur ponctuelle d'un employé mais, si on les prend ensemble, il appert que ce sont des erreurs répétées systématiquement auxquelles il faut remédier plus efficacement en renforçant les structures et les processus de gouvernance.

- Plus d'une fois, certaines organisations ont démontré que, dans leur empressement à offrir des produits et des services, elles n'avaient pas prévu les nombreuses difficultés qui en découleraient sur le plan de la protection de la vie privée et n'avaient pas pris les mesures nécessaires pour y faire face dès l'étape de la conception.

- Dans une étude sur les « fuites sur Internet », le Commissariat a constaté qu'un site testé sur quatre soit communiquait, à son insu, des informations à des tierces parties, soit n'informait pas clairement les Canadiennes et les Canadiens qu'il transférait des renseignements personnels à des fournisseurs de services[31].

Nous pourrions donner d'autres exemples. À notre avis, et compte tenu du fait que l'économie numérique repose en bonne partie sur la confiance et que les renseignements personnels y jouent un rôle essentiel, la protection de la vie privée dans les pratiques commerciales ne reçoit pas l'importance qu'elle mérite.

Vu la complexité du traitement des renseignements personnels, l'énorme quantité de renseignements en cause, et la nécessité pour les organisations d'avoir la flexibilité de mettre en œuvre les principes de protection de la vie privée énoncés dans la *Loi*, les organisations doivent créer de meilleurs programmes de gestion de la protection de la vie privée, et elles doivent les appliquer avec diligence et de manière systématique. Les organisations doivent accorder plus d'attention aux questions liées à la protection de la vie privée, de manière à ce que les renseignements personnels des Canadiennes et des Canadiens soient mieux protégés et que l'on évite la gêne et les dépenses après le fait. Il faut accorder une plus grande place à la protection de la vie privée pour appuyer le travail des professionnels de la protection des renseignements personnels au sein des organisations.

Responsabilité à l'égard de la mise en œuvre des recommandations

Le suivi des organisations qui ont accepté de mettre en œuvre les recommandations découlant d'une enquête peut entraîner des facteurs d'incertitude et des défis administratifs pour le Commissariat.

Veiller à ce que les organisations respectent leurs engagements à l'égard des recommandations est devenu un fardeau de plus en plus lourd pour le Commissariat, et requiert beaucoup de temps et de ressources. Même si, techniquement parlant, nos enquêtes sont terminées au moment où la commissaire publie ses conclusions, les Canadiennes et les Canadiens ont besoin de savoir que les organisations prennent leurs responsabilités au sérieux une fois l'enquête

terminée. Surveiller et analyser les actions d'une entreprise par la suite peut cependant prendre autant de temps que la réalisation d'une enquête.

Par exemple, le suivi concernant Facebook, après la publication des conclusions de notre enquête en 2009, a nécessité des ressources considérables et pris toute une année. Le suivi de Nexopia vaut aussi la peine d'être mentionné. Plus d'un an après la publication des conclusions, nous faisions le suivi de l'engagement qu'avait pris l'entreprise de mettre en œuvre nos 24 recommandations.

Aux termes de la LPRPDE, la commissaire ou le plaignant a 45 jours pour demander à la Cour fédérale de faire appliquer les recommandations de la commissaire. Il arrive souvent que les recommandations complexes ne puissent pas être appliquées dans le délai de 45 jours, particulièrement dans les cas exigeant des solutions technologiques. Bien que les demandes puissent être présentées après le délai de 45 jours, il faut pour cela obtenir la permission de la Cour.

Recommandation 4** : **Joindre le geste à la parole

Modifier le principe de la responsabilité énoncé à l'annexe 1 pour : indiquer que les organisations ont l'obligation de démontrer, sur demande, qu'elles prennent leurs responsabilités; inclure le concept d'« ententes exécutoires »; et assujettir à l'examen de la Cour fédérale certaines dispositions relatives à la responsabilité.

Le principe de la responsabilité, tel qu'il est énoncé dans la LPRPDE, pourrait être renforcé afin d'améliorer la protection des renseignements personnels des Canadiennes et des Canadiens.

Démonstration de la conformité

L'un des fondements de la responsabilité, c'est que les organisations doivent être en mesure de démontrer aux organismes de surveillance, sur demande, qu'elles ont mis en place un programme pour s'assurer que leurs pratiques sont conformes à la loi sur la protection des renseignements personnels. Sous sa forme actuelle, la LPRPDE ne prévoit pas une telle obligation. Nous estimons que la loi devrait être modifiée pour exiger des organisations qu'elles démontrent, à la demande de la commissaire, qu'elles ont mis en place un programme de protection de la vie privée. Ce changement harmoniserait la loi avec l'orientation de l'Union européenne à ce chapitre.

Il est peut-être temps d'examiner comment le concept de la responsabilité pourrait servir de mesure incitative en vue d'une plus grande conformité à la LPRPDE. Une organisation sera davantage portée à prendre ses responsabilités, et par conséquent ses obligations en matière de protection de la vie privée, au sérieux si les conséquences d'un manquement à cet égard se répercutent sur ses bénéfices.

Exiger des organisations qu'elles démontrent qu'elles sont responsables pourrait les inciter à vraiment joindre le geste à la parole. Par exemple, en cas d'enquête ou d'atteinte à la sécurité des renseignements personnels, l'existence d'un programme de gestion de la protection de la vie privée[32] qui fonctionne manifestement et qui est à jour (et qui devrait comprendre des évaluations des facteurs relatifs à la vie privée) pourrait constituer un facteur atténuant au moment de l'évaluation des dommages.

On pourrait aussi étudier la question des marques de fiabilité et des certifications par un tiers. Selon ces formules, une organisation montre qu'elle se conforme à certaines pratiques pour obtenir la certification ou la note voulue. Ces formules ont cependant fait l'objet de critiques en raison de l'absence d'un mécanisme d'application.

Ententes exécutoires

La LPRPDE devrait être modifiée afin d'intégrer explicitement le concept d'« ententes exécutoires », qui ferait en sorte qu'une organisation, au terme d'une enquête, accepterait de se conformer aux recommandations de la commissaire et de démontrer qu'elle s'y est conformée dans un laps de temps déterminé. La *Loi* pourrait aussi être modifiée pour indiquer les recours du Commissariat lorsqu'une organisation ne respecte pas ses engagements. De cette façon, on pourrait améliorer la protection des renseignements personnels et utiliser avec plus d'efficacité et d'efficience les ressources publiques du Commissariat.

Si les organisations avaient clairement l'obligation de démontrer qu'elles mettent en œuvre les recommandations du Commissariat et, lorsqu'elles ne le font pas, s'il y avait des options claires en matière de recours, il y aurait moins d'incertitude et le fardeau du Commissariat en ce qui concerne le suivi s'en trouverait peut-être allégé.

Autres changements possibles

Une autre modification possible à la LPRPDE qui permettrait de renforcer la responsabilité organisationnelle et de lui donner un effet positif consisterait à faire en sorte qu'un plus grand nombre des principes relatifs à la responsabilité énoncés à l'annexe 1 figurent dans la liste des dispositions révisables énumérées à l'article 14, qui peuvent faire l'objet d'un examen par la Cour fédérale. Actuellement, seul le principe 4.1.3 peut faire l'objet d'un examen[33].

CONCLUSION

Le Parlement a adopté la LPRPDE pour permettre à l'économie numérique de prospérer en aidant les Canadiennes et les Canadiens à se sentir en sécurité lorsqu'ils utilisent Internet pour faire des affaires et se renseigner. C'est une loi qui est neutre sur le plan technologique et qui est fondée sur des principes. Ce sont là des caractéristiques qu'il faut conserver alors que nous avançons dans le XXI^{e} siècle.

Toutefois, il est de plus en plus clair à notre avis que l'équilibre visé par la LPRPDE n'existe plus. Trop souvent, le droit à la vie privée des personnes est supplanté par les besoins opérationnels des organisations. À cette étape de l'évolution de la LPRPDE, il faut des incitatifs pour encourager les organisations à se conformer rigoureusement au respect de la vie privée dès les premières étapes de la conception d'un produit ou d'un service, et des sanctions devraient être imposées lorsque les choses tournent mal.

Compte tenu des changements remarquables dans la façon dont les renseignements personnels sont recueillis, utilisés et communiqués par les organisations, ainsi que de la dimension mondiale de l'économie numérique d'aujourd'hui, il faut renforcer la loi fédérale de protection des renseignements personnels dans le secteur privé pour la rendre semblable aux lois sur la protection des renseignements personnels qui ont été adoptées ailleurs au Canada et dans le monde.

Il est dans l'intérêt des consommateurs et des entreprises de soutenir une économie numérique florissante à laquelle les gens peuvent participer activement, en sachant que leurs renseignements personnels seront protégés.

NOTES EN FIN DE TEXTE

[1] Du site Web d'Industrie Canada, Protection des renseignements en affaires, Commerce électronique au Canada.

[2] Tiré des notes pour une allocution de l'honorable John Manley, présentation devant le Comité sénatorial chargé d'étudier le projet de loi C-6, 2 décembre 1999.

[3] La LPRPDE ne s'applique pas aux organisations qui recueillent, utilisent ou communiquent des renseignements personnels uniquement dans les provinces qui ont une loi essentiellement similaire — l'Alberta, la Colombie-Britannique et le Québec (ainsi que l'Ontario, le Nouveau-Brunswick et Terre-Neuve-et-Labrador, à l'égard des renseignements personnels sur la santé recueillis, utilisés et communiqués par les dépositaires de renseignements sur la santé). La LPRPDE s'applique à d'autres activités commerciales dans les trois dernières provinces. Le cas échéant, c'est la loi provinciale essentiellement similaire qui s'appliquera au lieu de la LPRPDE, même si la LPRPDE continue de s'appliquer aux transferts interprovinciaux ou internationaux de renseignements personnels et aux renseignements personnels détenus par les entreprises fédérales.

[4] Protection de la vie privée et médias sociaux à l'ère des mégadonnées.

[5] Canadian's Internet usage nearly double the worldwide average [en anglais seulement].

[6] 2.5 Quintillon Bytes Created Each Day, Calculated ViaWest [en anglais seulement].

[7] Bringing smarter computing to big data [en anglais seulement].

[8] Par exemple, avant son achat en 2012 par Facebook, Instagram, un site d'hébergement de photos, comptait environ 13 employés. En 2011, Instagram avait cinq millions d'utilisateurs.

[9] « How companies learn your secrets », Charles Duhigg, *New York Times*, 16 février 2012 [en anglais seulement].

[10] Voir Sondage auprès des Canadiens sur les enjeux liés à la protection de la vie privée.

[11] Page 7 du Rapport du Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique : Protection de la vie privée et médias sociaux à l'égard des mégadonnées.

[12] *Canada (commissaire à la protection de la vie privée) c. Blood Tribe Department of Health*, [2008] 2 R.C.S. 574, 2008 CSC 44.

[13] Le Registre des entreprises ne comptabilise que les entreprises qui répondent à au moins un des critères suivants : « compter au moins un employé rémunéré (versement de retenues salariales à l'Agence du revenu du Canada – ARC), avoir un chiffre d'affaires annuel d'au moins 30 000 $ ou être constituée en société et avoir produit au moins une déclaration fédérale de revenus des sociétés au cours des trois dernières années. »

Le Canada comptait environ 2 428 270 entreprises — si on retire les entreprises du Québec, de l'Alberta et de la Colombie-Britanique, 1 217 410 entreprises sont assujetties à la LPRPDE.

[14] Page 8 du Rapport du Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique : Protection de la vie privée et médias sociaux à l'égard des mégadonnées.

[15] Même si une personne peut désormais poursuivre une entreprise en justice, les dommages-intérêts accordés en vertu de la LPRPDE à ce jour ont été faibles.

[16] Google a accepté de payer une amende de 22,5 millions de dollars pour régler les accusations déposées par la FTC pour de fausses déclarations auprès des utilisateurs du navigateur Safari d'Apple concernant le placement de fichiers témoins, en violation d'une entente antérieure avec la FTC portant sur les pratiques de confidentialité de Google. [traduction, en anglais seulement].

[17] Cette liste n'est pas exhaustive.

[18] Ces renseignements étaient à jour en date du 8 mai 2013.

[19] Une ébauche de rapport de la Commission des libertés civiles, de la justice et des affaires intérieures du Parlement de l'UE propose des modifications au règlement qui exigeraient que l'organisme de contrôle de l'autre pays dispose de « pouvoirs de sanction suffisants » pour arriver à une constatation du niveau de protection adéquat. La Commission et quatre autres comités font des commentaires sur le règlement. L'examen du règlement se poursuit.

[20] En vertu de l'article 14 de la LPRPDE, un plaignant peut adresser à la Cour fédérale une demande d'audience pour toute question pour laquelle il a porté plainte ou pour toute question traitée dans le rapport de conclusions d'enquête de la commissaire. Une telle demande doit porter sur des articles précis de la LPRPDE ou des principes établis à l'annexe 1, qui sont indiqués à l'article 14. Ils sont décrits comme des dispositions « révisables ».

[21] Voir la page 71 du mémoire de la commissaire présenté au Comité ETHI, où on propose que les pénalités maximales dans certains cas (en l'occurrence les « contraventions aux règles de fond » dans les cas où une étude ne s'impose pas puisqu'il est clair qu'il y a eu contravention) « pourraient être supérieures à la limite actuelle de 500 $ ».

[22] OCDE (2011), *The Evolving Privacy Landscape: 30 Years After the OECD Privacy Guidelines*, OECD Digital Economy Papers, n° 176, Publications de l'OCDE [en anglais seulement].

[23] Dans un cas d'atteinte à la sécurité des données visant Sony, 77 millions de comptes d'utilisateurs contenant des noms, des adresses et peut-être des données relatives aux cartes de crédit ont été volés [en anglais seulement].

[24] Global security spending to hit $86B in 2016 [en anglais seulement].

[25] « Le Canada est en retard sur la plupart des pays en ce qui concerne les innovations dans le domaine de la sécurité. En effet, à peine plus de 5 % des dépenses ont été consacrées aux nouvelles technologies et aux processus de gestion ciblant la sécurité de l'information au cours des 12 derniers mois. » [traduction]

[26] Voir Sondage auprès des Canadiens sur les enjeux liés à la protection de la vie privée.

[27] Le projet de loi C-12 contient des dispositions concernant le signalement obligatoire des atteintes. Au moment où le présent document est rédigé, le projet de loi en est à l'étape de la deuxième lecture.

[28] Voir les sites Google's Transparency Report [en anglais seulement], Microsoft's 2012 Law Enforcement Requests Report [en anglais seulement], et Twitter's Transparency Report [en anglais seulement].

[29] Il semble qu'une réflexion plus poussée sur la responsabilité pourrait faire partie de l'examen de ces lignes directrices, qui est en cours. Voir *Terms of Reference for the Review of the OECD Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data*, 31 octobre 2011 [en anglais seulement].

[30] Voir Un programme de gestion de la protection de la vie privée : la clé de la responsabilité.

[31] Voir Projet de recherche du Commissariat à la protection de la vie privée du Canada concernant les « fuites sur Internet » .

[32] Pour de plus amples renseignements sur ce que le Commissariat considère comme un solide programme de gestion de la protection de la vie privée, voir *Un programme de gestion de la protection de la vie privée : la clé de la responsabilité*, publié par le Commissariat et les commissariats à l'information et à la protection de la vie privée de l'Alberta et de la Colombie-Britannique en avril 2012.

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