ORDRE DES COMPTABLES PROFESSIONNELS AGRÉÉS DU QUÉBEC

Mémoire présenté à la Commission des institutions sur le projet de loi nº 64, Loi modernisant des dispositions législatives en matière de protection des renseignements personnels

Octobre 2020

Table des matières

Préambule

Mégadonnées, intelligence artificielle, infonuagique, chaînes de blocs : ces technologies sont à l'origine de ce qu'on appelle aujourd'hui la révolution numérique, un phénomène récent qui est caractérisé par la multiplication des données numériques, accessibles partout et en tout temps.

Devant la croissance exponentielle des données, certains verront de nouvelles possibilités, ou des failles à exploiter. D'autres seront réfractaires aux projets innovants, par manque de connaissances ou d'appétit pour le risque. Dans un contexte où la maturité numérique est inégale, un facteur est essentiel pour que le Québec innove et prospère : la confiance.

- La confiance que les données d'une personne sont collectées éthiquement et utilisées adéquatement.
- La confiance qu'un projet novateur d'exploitation des données est basé sur de l'information exacte et vérifiable.
- La confiance que tous les acteurs jouent selon les mêmes règles.

Sans confiance, le Québec ne pourra se hisser au rang des leaders de la nouvelle économie basée sur la donnée.

De récents incidents survenus au Québec ont démontré toute l'importance d'un encadrement adéquat pour protéger les renseignements personnels, en même temps que la fragilité de la confiance du public à cet égard. En effet, aux risques de vol de données s'ajoutent les cyberattaques dont les entreprises canadiennes et québécoises sont de plus en plus la cible, qu'il s'agisse des PME, des OBNL ou des multinationales.

Non seulement est-il essentiel de protéger efficacement les données personnelles des Québécois afin d'éviter une appropriation ou une altération malveillante de celles-ci, mais il faut aussi que les organisations publiques et privées aient confiance en la qualité et l'exactitude des données qu'elles utilisent aux fins de leurs activités et décisions quotidiennes. Cette confiance doit s'étendre aux citoyens qui, dans leurs interactions avec les institutions et les entreprises, doivent bénéficier d'une expérience client transparente.

Les CPA jouent depuis toujours un rôle crucial dans la confiance du public en assurant la crédibilité et la transparence de l'information financière et non financière. Ils veillent à la saine gestion des données, de la saisie initiale jusqu'à l'archivage et à la destruction, en passant par la sécurité, la disponibilité et la validité. En somme, compte tenu de leur vaste expertise en certification, en normalisation et en gestion des données, les CPA sont bien placés pour contribuer à la réflexion, à l'élaboration et à la mise en œuvre d'initiatives de gouvernance des données. D'ailleurs, au terme d'un exercice de réflexion national sur son avenir, la profession

comptable s'est engagée à collaborer activement à la définition d'un modèle de gouvernance des données.[1]

La valeur potentielle d'un processus de certification des données a par ailleurs fait l'objet de discussions dans le cadre des consultations publiques d'Innovation, Sciences et Développement économique Canada sur le numérique et les données.[2] Un tel système permettrait aux citoyens et aux organisations de s'assurer que la personne ou l'organisation certifiée satisfait à une norme précise en matière de gestion des données qui lui sont confiées ou qu'elle produit. Le Québec devrait lui aussi envisager de se doter de normes et d'un processus de certification des données.

Nous l'avons dit plus haut, le monde change, et vite. La nature et le volume des données et des renseignements recueillis, l'utilisation qui en est faite et la convoitise qu'ils suscitent commandent une action résolue et agile afin de rassurer les citoyens sur la gouvernance et la protection des données qui les concernent.

Pour l'heure, l'Ordre des CPA accueille favorablement le dépôt d'un projet de loi en matière de protection des renseignements personnels. En effet, une réforme de l'écosystème de protection de ces renseignements est réclamée et attendue depuis longtemps puisque le cadre législatif initial établi au début des années 80 n'a pas été conçu de manière à s'adapter au rythme de l'évolution technologique du 21e siècle.

Le projet de loi nº 64 est un jalon important de cette réforme. L'établissement des principes de base de la protection des données personnelles est le premier pas d'un changement de culture qui guidera les entreprises qui tardent à tirer profit de l'ère numérique. Le projet de loi nº 53 concernant les agents d'évaluation du crédit, présentement à l'étude, en est un autre. Les projets de loi annoncés visant à créer une identité numérique citoyenne et à réformer les règles d'accès à l'information viendront compléter le tableau.

Sur l'approche qui le sous-tend et les principes qu'il met de l'avant, le projet de loi nº 64 soulève par ailleurs de nombreuses interrogations, notamment sur la cohabitation de la législation québécoise avec celles des autres juridictions, particulièrement au sein de l'espace économique nord-américain, sur les ressources que devront mobiliser les entreprises pour s'y conformer de même que sur le rythme de mise en œuvre de la loi et le régime de sanctions qu'elle prévoit en cas de défaut. Des précisions devront aussi être apportées à certaines définitions contenues dans le projet de loi.

Cela dit, il serait dommage que les propositions à l'étude deviennent rapidement désuètes, faute pour le législateur d'avoir saisi l'occasion de les actualiser davantage et ainsi, de moderniser réellement la protection des renseignements personnels des Québécois.

C'est dans un esprit constructif et animé par la volonté de contribuer au débat en mettant de l'avant son expertise que l'Ordre des CPA soumet dans les pages qui suivent ses commentaires et recommandations.

[1] https://www.cpacanada.ca/fr/voir-demain-initiative/gouvernance-donnees
[2] CPA Canada, Table ronde sur le numérique et les données: Faire du Canada un chef de file dans une économie axée sur le numérique.

Des concepts clairement définis

L'étude détaillée du projet de loi par les parlementaires constitue une excellente occasion de clarifier et d'actualiser véritablement la terminologie utilisée en matière de protection des renseignements personnels. L'Ordre des CPA du Québec ne saurait trop insister sur la nécessité que les dispositions législatives et réglementaires mises de l'avant soient rédigées en termes clairs afin d'assurer le respect des règles, d'en faciliter la compréhension par les consommateurs et les organisations et ainsi, de susciter l'adhésion du plus grand nombre. Le resserrement des sanctions prévues par le projet de loi milite également en faveur de la clarté afin de ne laisser place à aucune interprétation. À l'heure actuelle, nombreux sont les termes et concepts auxquels il est fait référence dans le projet de loi qui semblent être considérés comme des évidences par le législateur et qui mériteraient pourtant une attention particulière.

Le renseignement personnel

Le renseignement personnel, objet même du projet de loi, demeure défini aussi largement et vaguement qu'il l'était à l'origine dans les deux principales lois encadrant sa protection.

> ***Loi sur la protection des renseignements personnels dans le secteur privé***
>
> **2.** *Est un renseignement personnel, tout renseignement qui concerne une personne physique et permet de l'identifier.*
>
> ***Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels***
>
> **54.** *Dans un document, sont personnels les renseignements qui concernent une personne physique et permettent de l'identifier.*

Nous suggérons que la définition de renseignement personnel soit actualisée dans l'une et l'autre loi et qu'elle soit identique dans tout le corpus législatif québécois. On pourrait pour ce faire s'inspirer de la définition européenne :

> «données à caractère personnel», toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée «personne concernée»); est réputée être une «personne physique identifiable» une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, **des données de localisation**, un **identifiant en ligne**, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale;[3]

Cette définition retient notre attention à plusieurs titres. Résolument moderne, elle fait référence à un identifiant, à des données de localisation ainsi qu'à d'autres caractéristiques personnelles. Elle illustre bien la diversité d'éléments qui peuvent constituer un renseignement ou une donnée à caractère personnel. Ainsi, une donnée financière a un caractère tout aussi personnel qu'un

[3] *Règlement général sur la protection des données (RGPD)*, Article 4(1)

élément propre à l'identité d'une personne, tel son orientation sexuelle ou son numéro d'assurance sociale.

La détermination du caractère sensible d'un renseignement

Par ailleurs, le fait de laisser à chaque organisme ou entreprise le soin de déterminer le caractère sensible d'un renseignement comporte des risques importants qui pourraient être évités. Le projet de loi devrait prévoir des critères d'évaluation objectifs. Suivant le libellé actuel des articles 12 et 102 du projet de loi, « *un renseignement est sensible lorsque, de par sa nature ou en raison du contexte de son utilisation ou de sa communication, il suscite un haut degré d'attente raisonnable en matière de vie privée ».* Nous comprenons le souci du législateur de faire en sorte que la définition puisse s'adapter aux circonstances et évoluer dans le temps. Toutefois, nous sommes d'avis qu'une définition aussi générique comporte plus d'inconvénients potentiels que d'avantages.

L'absence de critères objectifs permettant de déterminer ce qui constitue un haut degré d'attente en matière de vie privée risque d'entraîner des décisions contradictoires d'une organisation à l'autre et donc, d'importantes difficultés d'application puisque ce concept est lié à la nécessité d'obtenir un « consentement manifesté de façon expresse » pour toute utilisation secondaire du renseignement, notamment à des fins de prospection commerciale ou philanthropique, ou pour sa transmission à un tiers.

Aussi, compte tenu de l'importance des sanctions susceptibles d'être imposées à des organisations qui interpréteraient erronément les attentes raisonnables en matière de confidentialité, il est important que le concept de « haut degré d'attente raisonnable en matière de vie privée » soit clarifié. De plus, nous sommes d'avis que cette définition ne peut se limiter aux seuls motifs interdits de discrimination. Il pourrait être opportun ici de s'inspirer du *Règlement général sur la protection des données (RGPD)* qui prévoit un encadrement tout particulier et similaire à celui prévu par le projet de loi pour "le traitement des données à caractère personnel qui révèle l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique".

La clarification du consentement requis

Il est par ailleurs difficile de concilier la possibilité que semblent ouvrir les articles 12 et 13 du projet de loi d'obtenir un consentement implicite lorsque l'utilisation ou la communication ne vise pas un renseignement sensible, et la définition de « consentement » de l'article 14, qui réfère **dans tous les cas** à un consentement « manifeste, libre, éclairé et (...) donné à des fins spécifiques » :

> ***14.*** *Un consentement prévu à la présente loi doit être manifeste, libre, éclairé et être donné à des fins spécifiques. Il est demandé à chacune de ces fins, en termes simples et clairs, distinctement de toute autre information communiquée à la personne concernée.*

Si le législateur veut ainsi définir non pas tout consentement, mais le concept de « consentement manifesté de façon expresse » des articles 12 et 13, il serait souhaitable de le préciser, sans quoi toute possibilité de consentement implicite se trouve évacuée.

De plus, la notion de consentement « donné à des fins spécifiques » et « demandé à chacune de ces fins » donne déjà des maux de tête aux responsables de la protection des renseignements personnels dans les organisations. Doit-on revoir les formulaires de consentement afin d'obtenir un consentement distinct pour chaque utilisation projetée, ou un consentement unique sur un formulaire décrivant toutes ces utilisations sera suffisant? Il serait donc hautement souhaitable que des lignes directrices présentant des exemples de « consentement spécifique » adaptés à diverses situations soient mises à la disposition des organisations afin de les aider à circonscrire leurs obligations.

L'harmonisation de la terminologie

Nous n'insisterons jamais assez sur l'importance d'harmoniser et d'actualiser la terminologie du corpus législatif. L'article 14 du projet de loi qui introduit l'article 63.7 à la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* illustre bien la problématique actuelle Suivant le libellé proposé, le responsable de la protection des renseignements personnels qui, dans le cadre d'un incident technologique, communique un renseignement personnel sans avoir obtenu l'autorisation préalable de la personne concernée doit « enregistrer la communication » Or, l'article 18.1 de la *Loi sur la protection des renseignements personnels dans le secteur privé* prévoit que la communication d'un renseignement personnel doit « faire l'objet d'une inscription ». Nous sommes d'avis que le concept d'enregistrement n'est pas clair et fait référence à une approche désuète.

Transferts inter juridictionnels : des obligations impraticables

La libre circulation des données constitue aujourd'hui un enjeu d'une grande importance. À tel point qu'elle est devenue la cinquième liberté du marché unique, consacrée par le droit européen, sous réserve de la protection des renseignements personnels en vertu du *Règlement général sur la protection des données*[4]. La donnée étant devenue une valeur en soi, l'Union européenne a jugé essentiel d'harmoniser les législations nationales afin de permettre sa libre circulation tout en protégeant les données personnelles.

L'article 103 du projet de loi modifiant l'article 17 de la *Loi sur la protection des renseignements personnels dans le secteur privé* prévoit qu'on ne peut communiquer de renseignements personnels à l'extérieur du Québec qu'après avoir conclu, à la suite d'une évaluation des facteurs relatifs à la vie privée, que les renseignements bénéficieront de la même protection, en vertu du régime juridique applicable, que s'ils étaient conservés au Québec.

Il s'agit d'une exigence très contraignante dans un contexte où les activités des entreprises et des professionnels n'ont pas de frontières et qui pourrait constituer un frein aux échanges économiques et placer les entreprises québécoises dans une situation intenable.

Une telle évaluation exige en effet une étude de droit comparé, et donc, l'intervention de juristes qui pourraient devoir y investir un temps considérable. En d'autres termes, une opération coûteuse et complexe, voire impossible à réaliser pour les PME.

Certes, l'article 17.1 prévoit que le ministre publie « une liste d'États dont le régime juridique encadrant les renseignements personnels équivaut aux principes de protection des renseignements personnels applicables au Québec ». On ignore toutefois si cette liste sera publiée simultanément à l'entrée en vigueur de la loi. De plus, on peut penser qu'elle ne résultera pas d'une étude exhaustive par le gouvernement de l'ensemble des régimes juridiques de tous les États.

D'ailleurs, une liste d'États (soit de pays) est insuffisante pour définir les régimes juridiques équivalents hors Québec. On devrait parler ici de « juridictions » et non d'États, compte tenu du fait que la législation est susceptible de varier à l'intérieur d'un État fédéral, comme c'est le cas au Canada et aux États-Unis.

Il est par ailleurs curieux que l'on impose cette obligation dès que des données sont transmises à l'extérieur du Québec, qui n'est pas un État, et que l'on parle d'État lorsqu'on évalue les régimes juridiques hors Québec. Or, le fait de traiter les autres provinces canadiennes comme des juridictions étrangères pose un problème fondamental pour les entreprises québécoises ayant des ramifications ailleurs au Canada. À moins que le ministre ne publie, simultanément à l'entrée en vigueur de la loi, un décret reconnaissant l'ensemble du Canada comme un État ayant un

[4] MOURON, Philippe, « La libre circulation des données est devenue la cinquième liberté consacrée dans le droit de l'Union européenne », La revue européenne des médias et du numérique, no 49 Hiver 2018-2019.

régime juridique équivalent, les entreprises devront procéder à une évaluation du régime juridique de chaque province où les données qu'elles détiennent pourraient se trouver ou être exploitées.

Les cabinets comptables qui font partie d'un réseau canadien et international constituent un exemple de ce type d'entreprise. Cela signifie-t-il qu'ils devront évaluer le régime juridique applicable pour pouvoir conserver leurs services de facturation dans une autre province canadienne? De concert avec les autres provinces et territoires et le gouvernement fédéral, le gouvernement du Québec doit travailler à l'harmonisation des lois applicables à la protection des renseignements personnels.

Sur le plan international, les échanges commerciaux du Québec pourraient aussi être considérablement alourdis, voire freinés en raison de cette exigence. Il nous semble absurde de demander aux entreprises de réaliser, chacune de leur côté, une évaluation du régime juridique d'un même État. Une telle évaluation devrait être réalisée par le gouvernement et effectuée une seule fois avec un résultat uniforme pour l'ensemble des entreprises. Ainsi, pour les États qui ne se trouveront pas sur la liste publiée par décret en vertu du projet d'article 17.1, le gouvernement pourrait offrir un service d'évaluation du régime juridique d'un État sur demande des entreprises. Si des lacunes sont constatées, le rapport d'évaluation devrait déterminer précisément les modalités à inclure dans une entente « dans le but d'atténuer les risques identifiés dans le cadre de cette évaluation ». Une fois de plus, nous sommes d'avis que le projet de loi ajoutera au fardeau réglementaire et administratif des entreprises québécoises, particulièrement celles qui transigent avec les économies émergentes.

La véritable solution à long terme consiste à adopter des standards internationaux en matière de gouvernance des données et des renseignements personnels. Le Conseil canadien des normes a formé un « Collectif de normalisation en matière de gouvernance des données ». Ce collectif a pour objectif de déterminer les besoins et de formuler des suggestions quant à l'adoption de normes encadrant l'évaluation, la collecte, le classement et le partage des données. Pour ce faire, il importe d'examiner ce qui se fait ailleurs dans le monde et d'adopter un cadre harmonisé permettant d'établir des règles minimales devant être respectées par les entreprises pour permettre l'échange et le partage de données dans différentes juridictions. L'Ordre des CPA est disposé à participer à une réflexion en ce sens à l'échelle provinciale et à favoriser le dialogue à l'échelle nationale et internationale.

Régime de sanctions : la nécessité d'une approche modulée

Plusieurs mémoires soumis à la Commission des institutions ont souligné la sévérité des sanctions administratives et pénales prévues par le projet de loi. Bien que nous reconnaissions que la façon la plus efficace de responsabiliser les justiciables soit l'imposition de sanctions dissuasives et qu'un régime de sanctions administratives soit approprié pour assurer l'adhésion et le respect des mesures mises de l'avant, il demeure que plusieurs éléments du régime de sanctions proposé par le projet de loi soulèvent des questions et méritent réflexion.

Tout d'abord, il importe de reconnaître que les organisations qui font appel à un fournisseur de services n'exercent qu'un contrôle restreint sur les données qu'elles collectent, produisent ou utilisent et qu'il est sans commune mesure avec celui des grandes entreprises. Ces dernières peuvent compter sur une équipe de gestion des risques, elles développent leurs propres systèmes informatiques et d'intelligence artificielle et le traitement des données constitue pour elles une opération courante ayant une valeur marchande importante. Ainsi, il nous semblerait logique que les entreprises qui fournissent des services informatiques et de stockage de données soient passibles de sanctions plus sévères que les PME qui recourent à leurs services. Nous proposons donc que les sanctions soient modulées en fonction du degré de sophistication et de l'importance des activités des entreprises en matière de collecte, de production et d'utilisation des données.

Par ailleurs, en calquant les sanctions prévues par le RGPD européen, qui sont fondées sur le chiffre d'affaires mondial des entreprises, le législateur devrait s'interroger sur le risque de décourager certaines entreprises hors Québec, notamment nord-américaines, d'offrir leurs produits et services sur le marché québécois, celui-ci n'étant pas significatif eu égard aux risques de non-conformité et à la sévérité des sanctions. Les Québécois n'en seront pas mieux servis.

Enfin, le champ d'application de la loi devrait être précisé. L'ampleur des sanctions tant pénales qu'administratives calculées sur le chiffre d'affaires mondial d'une entreprise porte à croire qu'on vise à assujettir les entreprises étrangères offrant des services au Québec, même si elles n'y ont pas d'établissement physique. Si telle est l'intention du législateur, il conviendrait de le prévoir par une disposition expresse.

Si, au contraire, la *Loi sur la protection des renseignements personnels dans le secteur privé* ne vise que les entreprises ayant un établissement au Québec, le législateur devrait s'interroger sérieusement sur le préjudice concurrentiel que pourraient subir les entreprises québécoises, notamment celles qui font partie du pôle de l'intelligence artificielle, un secteur de pointe où le Québec fait figure de leader mondial et attire les meilleurs cerveaux du domaine.

Une implantation progressive

Les PME représentent la presque totalité des entreprises québécoises. Selon l'Institut de la statistique du Québec, en 2019, 99,8 % des entreprises étaient des PME, 53 % avaient moins de 5 employés et 32,6 % avaient entre 5 et 19 employés[5]. Il faut rappeler qu'en vertu du droit québécois, un professionnel exerçant seul et offrant des services à des tiers est une entreprise. Ainsi, l'artisan qui utilise les services d'un fournisseur pour héberger son site web afin de vendre ses bijoux est également au sens de la loi une entreprise qui sera assujettie aux modifications apportées par le projet de loi.

Il importe de ne pas perdre de vue cette réalité. Si la modernisation de la législation encadrant les renseignements personnels est essentielle, elle exigera néanmoins des entreprises québécoises une mise à niveau considérable et conséquemment, des investissements importants en termes d'argent, de temps et de mobilisation du personnel.

Ainsi, les entreprises qui font affaire avec des fournisseurs de services pour héberger leurs données ou leur site internet n'ont guère plus de pouvoir de négociation avec ces fournisseurs que le simple consommateur. Elles sont pourtant tenues par le projet de loi aux mêmes obligations d'évaluation des risques relatifs aux données personnelles et elles doivent s'assurer que le contrat qui les lie au fournisseur de services prévoit les mesures que celui-ci devra prendre pour protéger les données personnelles de leurs clients. Or ici, c'est le fournisseur de services qui détient l'expertise en matière de sécurité des données. Les entreprises devront donc évaluer la portée du contrat d'adhésion avec le fournisseur de services et faire appel à un autre fournisseur si le contrat ne respecte pas les exigences de la loi. C'est là un bien lourd fardeau pour une très petite entreprise.

Il est utopique de penser que toutes les entreprises disposent de ressources internes qui ont l'expertise nécessaire pour réaliser une évaluation des facteurs relatifs à la vie privée (EFVP) ou pour élaborer une politique de gouvernance des données. L'immense majorité d'entre elles devront faire appel à des ressources externes pour les accompagner aux divers stades de mise en œuvre du projet de loi. En auront-elles la capacité financière? La simple obligation de publier la politique de gouvernance des données sur le site web de l'entreprise et de la maintenir à jour représentera, pour plusieurs PME, un défi important.

L'Ordre des CPA estime que le délai de mise en œuvre de la loi pourrait facilement dépasser deux ans, et ce, bien qu'il dispose de l'expertise interne en la matière et qu'il soit hautement sensibilisé à l'importance de ses obligations de confidentialité. Ce délai s'explique par la nécessité de réviser les politiques, les processus et l'ensemble des contrats existants à la lumière du texte final, de développer de nouveaux systèmes d'information et de mettre le site web à jour. On peut donc facilement imaginer ce que cela représentera pour des entreprises privées moins aguerries, qui n'ont à leur emploi aucun employé détenant une quelconque expertise en matière de gestion des risques ou de gestion des données ou dont les ressources financières limitées ne leur permettent pas de recourir à l'expertise particulière requise. Il nous apparaît essentiel que la mise en œuvre de la loi et l'atteinte des objectifs louables qui sont visés par le législateur ne soient pas

[5] NIKUZE, Pascasie, Les entreprises québécoises de moins de 5 employés – Portrait et contribution à la dynamique des entreprises et de l'emploi, 13 juillet 2020, Institut de la statistique du Québec.

compromis par un fardeau réglementaire et administratif tel qu'il nuirait à la productivité des organisations et irait à l'encontre des objectifs d'allégement mis de l'avant par le ministère de l'Économie et de l'Innovation.

Le projet de loi devrait donc prévoir des mesures transitoires échelonnant son entrée en vigueur et reportant la mise en œuvre des sanctions administratives et pénales, afin de permettre aux organisations de se conformer aux nouvelles exigences de la loi, de sensibiliser et de former l'ensemble de leurs employés et d'avoir ainsi internalisé leur politique de gestion des données personnelles. Pour être efficaces, les mécanismes de protection des renseignements personnels ne doivent pas être l'affaire de la seule haute direction. Ils relèvent de la responsabilité de l'ensemble des employés.

Ces mesures transitoires pourraient différer selon la taille de l'entreprise et la nature de ses activités, comme c'est le cas dans certains projets de loi qui prévoient des délais d'entrée en vigueur modulés pour les grandes, moyennes et petites entreprises. Cela permettrait de tenir compte de la réalité des entreprises, qui ne disposent pas toutes de la même expertise et des mêmes ressources financières pour se conformer aux nouvelles obligations prescrites par ce projet de loi.

Un accompagnement pour les organisations et le public

La meilleure politique de gestion des données personnelles n'aura d'effet que si elle est comprise et appliquée par l'organisation et par chacun des membres de son personnel. En effet, contrairement à d'autres types de renseignements, les données personnelles sont recueillies et utilisées à tous les niveaux de l'organisation. Il est donc impératif de mettre en place rapidement un accompagnement qui suscitera l'adhésion aux changements proposés par le projet de loi.

C'est pourquoi l'Ordre est d'avis que la mise en œuvre de l'éventuelle loi devrait être précédée d'un programme d'accompagnement et de formation obligatoire, mis en place et géré par la Commission d'accès à l'information (CAI). Des formations devraient ainsi être offertes à toutes les organisations assujetties, de même qu'à leurs employés.

Aussi, des guides explicatifs destinés aux organisations devraient être développés et produits par la CAI afin de les aider à comprendre les différentes notions et obligations introduites par le projet de loi et à illustrer de façon concrète comment elles se traduisent dans leur secteur respectif.

Parallèlement, un programme de littératie numérique devrait être développé pour aider le grand public à s'approprier les notions de protection des données personnelles et à développer de saines pratiques numériques. Les obligations des organisations en matière de consentement éclairé n'atteindront pleinement leur objectif que si le public est sensibilisé aux concepts auxquels font référence les formulaires de consentement et qu'il comprend le vocabulaire utilisé. Il en est de même à l'égard de l'obligation faite aux organisations de publier sur leur site web leur politique de gouvernance des données et leur politique de confidentialité. La profession comptable pourra quant à elle enrichir son programme de littératie financière d'un volet numérique afin de contribuer à l'effort d'éducation citoyenne.

La tenue et la conservation des dossiers des professionnels à l'ère numérique

Le projet de loi nº 64 suscite certaines réflexions quant à l'encadrement législatif des professionnels qui, dans le cadre de leur pratique, détiennent une multitude de renseignements confidentiels, y compris des renseignements personnels et des renseignements concernant des entreprises, qui doivent être protégés en vertu du secret professionnel. Or, la jurisprudence reconnaît que les attentes en matière de protection de la vie privée sont des plus élevées dans le cadre de la relation entre le client et son professionnel.[6]

Les nouvelles technologies font désormais partie intégrante du quotidien des professionnels, notamment des CPA, et elles ont bouleversé leurs pratiques. Que ce soit en termes de téléconsultation, d'outils de travail et de recherche, de communication avec leurs clients et tout particulièrement de protection des renseignements confidentiels, tout a changé rapidement ces dernières années. Les dossiers papiers conservés dans des voutes ont été remplacés par des dossiers virtuels conservés dans le nuage. Il est donc impératif que le système professionnel suive la cadence et fasse preuve de souplesse et d'agilité. Ce n'est malheureusement pas le cas.

Le *Code des professions* habilite les ordres professionnels à déterminer les normes relatives à la tenue, à la détention et au maintien par un professionnel de ses dossiers (art. 91 *Code des professions*). Toutefois, force est de constater à la lecture des règlements adoptés par les différents ordres professionnels que l'encadrement de la tenue des dossiers des professionnels est désuet et qu'il doit être repensé. Dans un souci de cohérence avec les objectifs du projet de loi, il nous semble donc impératif que l'Office des professions élabore des orientations quant à la rédaction des règlements relatifs à la tenue, à la détention et au maintien par les professionnels des renseignements protégés par le secret professionnel.

Ce même code prévoit également que l'Office des professions doit adopter un règlement-cadre sur la détention et la conservation, par les ordres, des documents détenus dans le cadre du contrôle de la profession. Si l'Office souhaite adopter un tel règlement, le moment serait bien choisi de façon à adopter un cadre réglementaire harmonisé aux exigences du projet de loi nº 64.

[6] *(Procureur général)* c. *Chambre des notaires du Québec*, 2016 CSC 20 (CanLII), [2016] 1 RCS 336, para. 35, http://canlii.ca/t/grxb2

Le signalement des incidents de sécurité par les professionnels

L'utilisation de technologies pour la collecte, la conservation et l'utilisation de données comporte des risques. Nul n'est à l'abri de vols ou de cyberattaques. Dans le contexte des récents incidents de sécurité susceptibles d'avoir compromis les renseignements personnels de millions de personnes, l'Ordre salue l'imposition d'une obligation pour les organismes publics et les personnes qui exploitent une entreprise, d'informer toute personne dont un renseignement personnel risque d'avoir été compromis par un incident de sécurité. En ayant un portrait complet des incidents ayant pu affecter la confidentialité de ses renseignements personnels, le citoyen sera en mesure de mieux évaluer ses risques et de prendre les mesures qu'il juge nécessaires pour se protéger, notamment contre le vol d'identité.

Les professionnels régis par le *Code des professions* détiennent plusieurs renseignements confidentiels obtenus dans le cadre d'une relation privilégiée et de confiance. L'obligation explicite d'aviser toute personne dont un renseignement personnel risque d'être compromis par un incident de sécurité s'inscrit parfaitement dans l'esprit des diverses obligations professionnelles existantes, telles que le respect du secret professionnel**,** les devoirs d'objectivité et d'intégrité, ainsi que le devoir de loyauté vis-à-vis de son client.

Toutefois, les renseignements confidentiels détenus par les professionnels ne se limitent pas aux renseignements personnels dont l'accès est encadré par la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* et la *Loi sur la protection des renseignements personnels dans le secteur privé,* qui ne visent par ailleurs que les renseignements personnels d'une personne physique et ne protègent aucunement les renseignements confidentiels d'une entreprise, par exemple. Or, la clientèle de plusieurs professionnels, dont les CPA, comprend autant des entreprises que des particuliers, ces professionnels étant ainsi fiduciaires de renseignements extrêmement sensibles pour les entreprises qu'ils desservent. L'Ordre est d'avis que tous les clients des professionnels devraient profiter des mêmes garanties de signalement et ainsi bénéficier d'une meilleure protection du secret professionnel.

Un incident de sécurité constitue en effet un accroc au secret professionnel, qui comporte deux composantes, soit l'obligation de ne pas divulguer les renseignements confidentiels de son client et l'obligation de les protéger. Rappelons que le droit au respect du secret professionnel est consacré par l'article 9 de la *Charte des droits et libertés de la personne* et l'article 60.4 du *Code des professions*.

Il serait donc opportun d'intégrer au *Code des professions* l'obligation pour tout professionnel d'aviser son client en cas de bris de confidentialité relatif à tout renseignement confidentiel, obligation qui s'ajoutera à celle de divulguer les incidents visant les renseignements personnels.

La levée du secret professionnel

Par ailleurs, si l'incident présente un risque qu'un préjudice sérieux soit causé, les articles 14 et 95 du projet de loi prévoient la possibilité d'aviser toute personne ou tout organisme susceptible de diminuer ce risque, en ne lui communiquant que les renseignements personnels nécessaires à cette fin sans le consentement de la personne concernée.

Suivant le *Code des professions*, le professionnel ne peut être relevé du secret professionnel qu'avec *« l'autorisation de son client ou lorsque la loi l'ordonne ou l'autorise par une disposition expresse ».* Or, le libellé des articles 14 et 95 ne prévoit aucune disposition expresse permettant la levée du secret professionnel, une lacune que le législateur aurait grandement intérêt à corriger.

Conclusion

La réforme que propose le gouvernement avec le projet de loi nº 64 est majeure. Elle nécessitera un changement de culture au sein des organisations, de même que l'allocation de ressources importantes et, pour plusieurs, le développement d'une expertise interne.

Malgré cela, la plupart des organisations n'y arriveront pas seules. Elles devront être guidées, outillées et accompagnées. Cela suppose que la Commission d'accès à l'information joue pleinement son rôle et assume notamment certaines des obligations actuellement dévolues par le projet de loi aux organisations. Elle doit également accompagner le public dans la compréhension de ses nouveaux droits et les organisations, dans l'application de leurs nouvelles obligations.

Pour ce faire, la CAI doit être pourvue des ressources financières, humaines et matérielles lui permettant de concrétiser sur le terrain les ambitions du gouvernement. C'est une condition essentielle au succès de cette réforme.

De plus, il est impératif que les objectifs louables du projet de loi ne soient pas compromis par une lourdeur réglementaire et administrative qui pourrait miner la productivité des organisations et des entreprises. Nous invitons donc les parlementaires à veiller à l'adoption d'un texte clair, faisant appel à une terminologie et à des concepts actualisés, d'un échéancier de mise en œuvre modulé et d'obligations simplifiées.

L'encadrement en place devra enfin rassurer les différents acteurs, dont les citoyens, sur le fait que leurs informations seront recueillies et utilisées selon de saines pratiques de gouvernance. Sans confiance, l'innovation tardera.

Les entreprises qui se démarqueront dans la nouvelle économie seront celles qui tireront profit de toutes les données disponibles. Pour y arriver, dans un monde où les fausses nouvelles sont chose commune et où la confiance envers les institutions traditionnelles s'effrite, l'ensemble de la société a besoin de savoir quelle information ou quelle organisation est fiable, d'autant plus qu'on fait de plus en plus confiance à la technologie plutôt qu'aux personnes[7]. Cela ne s'applique pas qu'aux données personnelles, mais à l'ensemble des informations générées.

Établir des principes de base en protection des données personnelles est un jalon nécessaire pour guider les entreprises qui tardent à tirer profit de l'ère numérique. Toutefois, si l'ambition du Québec est d'être le fer de lance d'une société connectée et innovante, c'est l'ensemble des informations numériques qui devront un jour être encadrées.

[7] CPA Canada, « La voie à suivre », Projet voir demain 2018, p. 18, en ligne : https://www.cpacanada.ca/foresight-report/fr/index.html?sc_camp=2B1B40A7F54A4CCDB896A7AF16B79E21#page=1

Recommandations

En prenant pour assises la protection et l'intérêt du public, l'Ordre des CPA formule les recommandations suivantes :

Recommandation 1

Revoir et actualiser la définition de ce qui constitue un renseignement personnel.

Recommandation 2

Établir des critères objectifs permettant de déterminer ce qui constitue un renseignement sensible comportant un haut degré d'attente raisonnable en matière de vie privée.

Recommandation 3

Modifier l'article 14 de façon à clarifier la distinction entre les notions de « consentement » et de « consentement manifesté de façon expresse » et développer des guides explicatifs et des lignes directrices destinés aux organisations afin de préciser les concepts qui sous-tendent le projet de loi et d'en illustrer l'application par des exemples concrets.

Recommandation 4

Harmoniser la terminologie des différentes lois encadrant l'utilisation et la protection des données et des renseignements personnels.

Recommandation 5

Préciser le champ d'application de la *Loi sur la protection des renseignements personnels dans le secteur privé* à l'égard des entreprises étrangères faisant affaire au Québec.

Recommandation 6

Remplacer le terme « État » par « juridiction » au projet d'article 17.1 de la *Loi sur la protection des renseignements personnels dans le secteur privé.*

Recommandation 7

Reconnaître le caractère équivalent des régimes juridiques ailleurs au Canada tout en travaillant à leur harmonisation.

Recommandation 8

Mettre en place un service d'évaluation des régimes juridiques des États et juridictions hors Canada en ce qui concerne la protection des renseignements personnels.

Recommandation 9

Moduler le régime de sanctions administratives susceptibles d'être imposées par la Commission d'accès à l'information selon la taille et la nature des activités de l'organisation visée.

Recommandation 10

Prévoir des mesures transitoires échelonnant l'entrée en vigueur du projet de loi et reportant la mise en œuvre des sanctions administratives et pénales afin de permettre aux organisations de différentes tailles de se conformer aux nouvelles exigences de la loi.

Recommandation 11

Mettre en place un programme d'accompagnement et de formation, développé et géré par la Commission d'accès à l'information, et destiné aux organisations assujetties.

Recommandation 12

Déployer un programme de littératie numérique, développé et géré par la Commission d'accès à l'information, afin d'aider le public à s'approprier les notions et concepts de protection des renseignements personnels.

Recommandation 13

Que l'Office des professions élabore des orientations quant à la rédaction des règlements relatifs à la tenue, à la détention et au maintien par les professionnels des renseignements protégés par le secret professionnel.

Recommandation 14

Que l'Office des professions adopte rapidement un règlement-cadre sur la détention et la conservation des documents détenus par les ordres professionnels dans le cadre de leur mission de contrôle de la profession.

Recommandation 15

Modifier l'article 60.4 du *Code des professions* afin d'obliger tout professionnel à aviser son client en cas d'incident ayant causé un bris de confidentialité de renseignements confidentiels.

Recommandation 16

Ajouter aux articles 14 et 95 du projet de loi une disposition autorisant expressément la levée du secret professionnel.

Recommandation 17

Fournir à la Commission d'accès à l'information les ressources financières, humaines et matérielles nécessaires afin que celle-ci puisse jouer pleinement son rôle et notamment accompagner le public et les organisations dans la compréhension du nouveau cadre juridique mis en place.

ORDRE DES COMPTABLES PROFESSIONNELS AGRÉÉS DU QUÉBEC

5, Place Ville Marie, bureau 800, Montréal (Québec) H3B 2G2
T. 514 288-3256 1 800 363-4688 Téléc. 514 843-8375
www.cpaquebec.ca