EYB2020REP3183

Repères, Novembre, 2020

Antoine AYLWIN* et Guillaume PELEGRIN*

Commentaire sur le Projet de loi n° 64 et la réforme des lois québécoises sur la protection des renseignements personnels

TABLE DES MATIÈRES

Résumé

Les auteurs effectuent une synthèse des principales modifications proposées par le Projet de loi nº 64 qui modernise en profondeur la Loi sur la protection des renseignements personnels dans le secteur privé *et la* Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels.

INTRODUCTION

Le Projet de loi nº 64[1], présenté le 12 juin 2020, constitue la plus ambitieuse réforme de la *Loi sur la protection des renseignements personnels dans le secteur privé*[2] (*Loi sur le secteur privé*) depuis son adoption en 1993. En plus de l'assujettissement des partis politiques et de l'augmentation des sanctions atteignant jusqu'à 25 000 000 $ (ou plus), l'inventaire des modifications proposées en date du 12 juin 2020 est important, ces modifications s'inspirant en partie des pratiques d'autres juridictions, tout en conservant certaines particularités québécoises qui doivent être bien comprises.

Nous exposerons d'abord un aperçu des réformes majeures proposées. Nous traiterons par la suite plus en profondeur des modifications en les analysant sous l'angle des thèmes suivant : la communication des renseignements, la conservation des renseignements, l'obligation de nommer un responsable de la protection des renseignements et les responsabilités de cette personne, l'exportation des renseignements personnels, les obligations associées aux incidents de sécurité, les impacts sur les recours civils, incluant les actions collectives, le renforcement des sanctions pénales et enfin les modifications visant spécifiquement les organismes publics.

I– LA COMMUNICATION DE RENSEIGNEMENTS PERSONNELS

A. Le régime actuel

Soulignons d'emblée que, dans sa mouture actuelle, la *Loi sur le secteur privé* requiert en principe qu'un consentement manifeste, libre, éclairé et donné à des fins spécifiques soit obtenu de la part des individus concernés afin qu'une entreprise puisse collecter, utiliser ou communiquer à un tiers leurs renseignements personnels[3]. Afin que le consentement soit éclairé, la personne concernée doit être informée (i) de l'objet du dossier ; (ii) de l'utilisation qui sera faite des renseignements ainsi que des catégories de personnes qui y auront accès au sein de l'entreprise et (iii) de l'endroit où sera détenu son dossier ainsi que (iv) des droits d'accès ou de rectification[4].

Ce mécanisme pose toutefois certains problèmes d'application lorsque vient le temps d'envisager ou de conclure une transaction commerciale d'envergure comme la vente d'une grande entreprise. En effet, un acquéreur diligent voudra préalablement vérifier, entre autres, la liste des clients et des comptes clients, la liste des employés, les régimes de retraite et d'intéressement qui leur sont applicables, les contrats et lettres d'emploi, la liste des consultants et des entrepreneurs indépendants faisant affaire avec la société, le détail de tout différend avec des employés ou des administrateurs, ainsi que tous les droits de propriété intellectuelle des employés, actuels ou anciens, sur les inventions ou les technologies utilisées par la société cible. Cela étant, la plupart du temps il est inconcevable d'obtenir le consentement de toutes ces parties. Ainsi, celui qui désire communiquer des renseignements personnels dans le cadre d'une transaction commerciale d'envergure peut facilement se retrouver dans une impasse.

Ce décalage entre loi et réalité n'a pas empêché la CAI d'appliquer la *Loi sur le secteur privé* au pied de la lettre dans ce genre de situation. En effet, dans une décision concernant la fusion de deux cabinets de courtage d'assurances, la CAI a tranché que le courtier du plaignant aurait dû obtenir le consentement de tous ses clients avant de communiquer leurs renseignements personnels à l'autre cabinet[5].

B. Le consentement

Il semble que les conditions pour l'obtention d'un consentement valide changent peu finalement, le Projet de loi[6] prévoyant plus spécifiquement que le consentement doit être demandé en des termes simples et clairs, distinctement de toute autre information communiquée.

Minimalement, les informations suivantes doivent être communiquées :

- les fins auxquelles les renseignements sont recueillis ;
- les moyens par lesquels les renseignements sont recueillis ;
- les droits d'accès et de rectification prévus par la loi ;
- le droit de retirer son consentement à la communication ou à l'utilisation des renseignements recueillis (il est à noter que ce droit qui existait déjà auparavant sera désormais codifié) ;
- le cas échéant, le nom du tiers pour qui la collecte est faite (nouveau) ;
- le cas échéant, la possibilité que les renseignements soient communiqués à l'extérieur du Québec (nouveau).[7]

Par ailleurs, sur « demande de sa part », la personne concernée doit également être informée des éléments suivants :

- les renseignements personnels recueillis auprès d'elle ;
- les catégories de personnes qui ont accès à ces renseignements au sein de l'entreprise ;
- la durée de conservation de ces renseignements ;
- ainsi que les coordonnées du responsable de la protection des renseignements personnels.

Le Projet de loi prévoit également la possibilité d'obtenir un consentement implicite, et ce via une lecture *a contrario* du texte. En effet, l'article 102 du Projet de loi, créant les nouveaux articles 12 à 14, dispose que « [l]e consentement doit être manifesté de façon expresse dès qu'il s'agit d'un renseignement personnel sensible ». Ce faisant, le Projet de loi s'aligne sur la loi fédérale, la *Loi sur la protection des renseignements personnels et les documents électroniques*[8], et ses *Lignes directrices pour l'obtention d'un consentement valable*, qui prévoient expressément la possibilité d'avoir un consentement implicite dans certaines situations[9].

Pour finir, le Projet de loi présente plusieurs nouveaux articles qui traitent spécifiquement de la question des renseignements concernant les mineurs et du consentement de ces derniers. Les principes énoncés dans ces nouveaux articles revêtent un enjeu de taille pour les entreprises du secteur privé et se résument ainsi :

1. les renseignements personnels concernant un mineur de moins de 14 ans ne peuvent être recueillis sans le consentement du titulaire de l'autorité parentale, sauf lorsque cette collecte est manifestement au bénéfice du mineur[10] ;
2. le consentement du mineur de moins de 14 ans est donné par le titulaire de l'autorité parentale[11] ;
3. le consentement du mineur de 14 ans et plus est donné par le mineur ou par le titulaire de l'autorité parentale.

Les points (1) et (2) peuvent nous laisser perplexes puisque la seule différence entre les deux est que le point (1) précise que le consentement de l'autorité parentale peut être écarté lorsque la collecte « est manifestement au bénéfice du mineur de moins de 14 ans ». Aucune indication dans le Projet de loi ne nous permet de concevoir ce qui constituerait une telle collecte.

C. Les nouveaux droits individuels

1. Le droit lié à l'utilisation des technologies

D'une part, le Projet de loi introduit la notion de « recours à une technologie comprenant des fonctions permettant de l'identifier, de la localiser ou d'effectuer un profilage » d'une personne. Le Projet de loi prévoit que la personne concernée, en plus des éléments mentionnés ci-dessus, devra être informée du recours à une telle technologie et, le cas échéant, des moyens offerts pour désactiver les fonctions permettant de l'identifier, la localiser ou d'effectuer le profilage[12]. Or, cela apparaît complexe d'application dans la réalité.

2. Le droit à l'oubli

D'autre part, le Projet de loi prévoit aussi le « droit à l'oubli » (aussi appelé « droit de déréférencement »[13]), soit la prérogative permettant à une personne d'exiger d'une organisation de cesser de publier des informations personnelles ou de désindexer un hyperlien donnant accès à ces informations lorsque leur diffusion porte gravement atteinte à la réputation ou à la vie privée de la personne et lorsque ce préjudice l'emporte clairement sur l'intérêt du public à connaître ces informations. Ce droit à la désindexation n'implique donc pas la suppression du contenu en ligne qui fait l'objet de la recherche, mais seulement la suppression des résultats de la recherche. Mais il va plus loin, car il permet d'obtenir que l'entreprise privée cesse la diffusion de ce renseignement.

Le Projet de loi encadre ce nouveau droit de façon stricte : le préjudice grave que la personne concernée subit doit être « manifestement supérieur à l'intérêt du public de connaître ce renseignement ou à l'intérêt de toute personne de s'exprimer librement ». Pour ce faire, il faut prendre en compte le fait que la personne concernée est une personnalité publique ou mineure, le fait que le renseignement est à jour et exact, la sensibilité du renseignement, le contexte dans lequel s'effectue la diffusion, le délai écoulé entre la diffusion du renseignement et la demande de désindexation, si le renseignement concerne une procédure criminelle ou pénale, une procédure pour l'obtention d'un pardon ou pour l'application d'une restriction à l'accessibilité des registres des tribunaux judiciaires et si la cessation de la diffusion, la réindexation ou la désindexation demandée n'excède pas ce qui est nécessaire pour éviter la perpétuation du préjudice.

En tout état de cause, ce nouveau droit à l'oubli est similaire à celui prévu par l'article 17 du RGPD[14] de l'Union européenne (ci-après « UE »), expliqué par les décisions de la

jurisprudence européenne telles *Google Spain*[15] et *Google* c. *CNIL*[16].

3. Le droit à la « portabilité des données »

Finalement, inspiré par l'article 20 du RGPD ainsi que du *California Consumer Privacy Act*[17], le Projet de loi présente aussi le « droit à la portabilité des données »[18], c'est-à-dire le droit d'un individu d'obtenir une copie des informations personnelles qu'il a fournies à une organisation dans un format technologique structuré et couramment utilisé. À la demande de cette personne, ces informations doivent être transmises à toute autre personne ou organisation.

Le Projet de loi semble viser un double objectif, soit d'augmenter le contrôle du citoyen sur ses renseignements personnels et de stimuler la concurrence en facilitant le transfert des renseignements et donc la possibilité, pour le citoyen, de changer plus aisément de fournisseur.

L'article 112 du Projet de loi introduit le droit à la portabilité en modifiant l'article 27 de la *Loi sur le secteur privé* relatif au droit d'accès. Ce faisant, il en fait une modalité particulière du droit d'accès, à savoir un droit d'accès sous format technologique.

Ce nouveau droit vise tous les renseignements personnels qu'une entreprise détient sur une personne, à l'exception des renseignements créés, dérivés, calculés ou inférés à partir des renseignements fournis par la personne concernée (ex. : profil d'un utilisateur), lesquels peuvent avoir une valeur commerciale pour les entreprises[19]. Il ne concerne donc que les renseignements personnels fournis par la personne concernée à l'entreprise. Précisons, par ailleurs, que les nouveaux systèmes d'information ou de prestation électronique de services devront permettre la portabilité.

Concernant les renseignements personnels informatisés, ils doivent être communiqués sous la forme « d'une transcription écrite et intelligible », dans « un format technologique structuré et couramment utilisé », cette dernière expression faisant écho à celle du RGPD.

Enfin, il convient de relever que les renseignements faisant l'objet de la demande de portabilité peuvent être transmis à « toute personne ou à tout organisme autorisé par la loi à recueillir un tel renseignement ».

Ce droit à la portabilité n'est pas absolu puisque l'entreprise qui détient les renseignements personnels peut, dans certains cas, refuser de les communiquer. En effet, l'article 46 de la *Loi sur le secteur privé* permet de refuser la portabilité si les demandes sont manifestement infondées ou excessives, notamment en raison de leur caractère répétitif. Mais, contrairement au RGPD, l'entreprise qui ne souhaite pas faire droit à la demande doit s'en référer à la CAI.

Aussi, ce droit à la portabilité au Québec s'apparente plus à une modalité particulière du droit d'accès qu'à un réel nouveau droit, tel qu'il est actuellement rédigé, contrairement à son cousin européen.

D. Les exceptions au consentement

Le Projet de loi comporte de nombreuses nouvelles exceptions à l'exigence d'un consentement. C'est ainsi que l'article 102 ajoute la possibilité d'utiliser un renseignement personnel sans le consentement de la personne concernée lorsque son utilisation est compatible avec celles pour lesquelles il a été recueilli, étant précisé que la prospection commerciale ou philanthropique est expressément exclue des fins compatibles. De plus, le consentement n'est pas requis lorsque l'utilisation est manifestement au bénéfice de la personne concernée ou nécessaire à des fins d'étude ou de recherche et que le renseignement est dépersonnalisé.

1. L'exception spécifique aux coordonnées d'affaires

Une proposition générale du Projet de loi permettrait de circonscrire le champ d'application matérielle des principales dispositions de la *Loi sur le secteur privé* en y retranchant les « renseignements personnels qui concernent l'exercice par la personne concernée d'une fonction au sein d'une entreprise, comme son nom, son titre et sa fonction, de même que l'adresse, l'adresse de courrier électronique et le numéro de téléphone de son lieu de travail »[20].

La CAI a déjà estimé par le passé que le nom et la signature du représentant légal ou du mandataire d'une personne morale, telle une société par actions, ne constituaient pas des renseignements personnels puisqu'une société et son représentant doivent être considérés comme formant un tout indivisible[21]. La CAI motivait ce raisonnement en expliquant qu'une société ne peut agir que par l'entremise de ses représentants et qu'en conséquence, le nom et la signature de ces derniers doivent donc être connus et vérifiés, à tout le moins « au nom de la sécurité juridique des contrats et de leur exécution »[22]. Le Projet de loi va toutefois au-delà de ce raisonnement en excluant également les renseignements personnels concernant l'exercice par toute personne « d'une fonction au sein d'une entreprise ».

Or, l'exclusion proposée dans le Projet de loi, qui qualifie les coordonnées d'affaires uniquement en fonction de la nature des renseignements, est plus catégorique que celles prévues dans les autres lois canadiennes, où la finalité des coordonnées d'affaires est également déterminante pour les soustraire à l'application de ces textes.

2. L'exception spécifique à l'exigence du consentement dans le cadre de transactions commerciales

Le Projet de loi propose également d'introduire une exception spécifique au principe du consentement dans un contexte transactionnel. Le nouvel article 18.4 qui serait ajouté à la *Loi sur le secteur privé* permettrait la communication de tout renseignement personnel entre deux parties à une transaction commerciale envisagée, et ce sans avoir à obtenir le consentement des individus concernés, pour autant que[23] :

- la transaction constitue une « transaction commerciale » au sens de cette disposition, c'est-à-dire qu'elle « implique un transfert de propriété de tout ou partie d'une entreprise »[24] ;
- la communication de ces renseignements personnels soit nécessaire aux fins de la conclusion de cette transaction ;
- une entente soit d'abord conclue entre les parties prévoyant que la partie recevant communication des renseignements s'engage à :
    - n'utiliser ces renseignements qu'aux seules fins de la conclusion de la transaction ;
    - ne pas communiquer ces renseignements sans avoir obtenu le consentement des individus concernés ;
    - prendre les « mesures nécessaires pour assurer la protection du caractère confidentiel »[25] de ces renseignements ; et
    - détruire ces renseignements si la transaction n'est pas conclue ou si leur utilisation n'est plus nécessaire aux fins de sa conclusion.

Ce nouvel article précise également que, suite à la clôture de la transaction, la partie ayant reçu communication des renseignements personnels qui désire continuer à les utiliser ou les communiquer demeure assujettie aux dispositions de la *Loi sur le secteur privé* dans le cadre de son utilisation et de la communication ultérieure de ces renseignements personnels, et doit, dans un « délai raisonnable »[26], aviser les individus concernés qu'elle détient maintenant des renseignements personnels les concernant en raison de la transaction.

En pratique, il s'agirait donc de bien vérifier les ententes de confidentialité habituellement signées à l'amorce de telles transactions pour s'assurer que les stipulations requises s'y trouvent et de notifier les individus concernés par écrit en tant qu'étape post-clôture.

Dans les faits, il s'agit d'un rattrapage partiel par rapport aux autres lois canadiennes alors que les lois fédérale[27], britanno-colombienne[28] et albertaine[29] en matière de protection des renseignements personnels prévoient déjà des exceptions similaires.

Une observation s'impose toutefois quant à la définition plus restrictive qui serait donnée à la notion de « transaction commerciale » faisant l'objet de l'exception au consentement[30], c'est-à-dire une transaction « qui implique le transfert de propriété de tout ou partie de l'entreprise ». Cette définition minimaliste risque de diminuer l'efficacité de l'exception proposée considérant que des transactions comme un financement par la dette ne comportent pas à proprement parler de « transfert de propriété de tout ou partie de l'entreprise ». Il serait donc pertinent de se pencher sur les définitions fournies par les autres lois canadiennes[31]. Par exemple, la loi fédérale définit les « transactions commerciales » de façon beaucoup plus détaillée, en y incluant notamment « le fait de consentir un prêt à tout ou partie d'une organisation ou de lui fournir toute autre forme de financement »[32].

3. L'exception spécifique à l'exigence du consentement dans le cadre d'études et de recherches

Dans le domaine de la recherche, un des aspects les plus controversés de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*[33] et de la *Loi sur le secteur privé* porte sur le processus souvent long et incertain pour que les chercheurs obtiennent la permission d'avoir accès aux banques de renseignements personnels détenues par des organismes publics ou des entreprises privées. L'approbation de la CAI est généralement accordée après une attente d'au moins un an alors que les fonds de recherche sont octroyés sur un cycle de trois ans[34].

Alors que d'autres provinces canadiennes ont déjà simplifié les demandes d'accès des chercheurs dans le but de faciliter l'acquisition de connaissances scientifiques, le Projet de loi apporte des modifications majeures pour les milieux de la recherche au Québec.

Le principe central du consentement à l'utilisation d'un renseignement personnel détenu par une entreprise ou un organisme public est mis de côté dans les cas où « ...son utilisation est nécessaire à des fins d'étude, de recherche ou de production de statistiques... »[35]. Or, cette absence de consentement s'accompagne d'une nouvelle série de protections obligatoires de la part des entreprises et des organismes publics qui donnent accès aux renseignements personnels, mais également de la part de la personne (ou de l'organisme) qui souhaite utiliser ces renseignements pour des fins d'étude, recherche, ou production de statistiques.

Le législateur prend par ailleurs une position importante quant à la définition de ce qui est un renseignement personnel en disposant qu'un « renseignement personnel est dépersonnalisé lorsque ce renseignement ne permet plus d'identifier directement la personne concernée. »[36]

a) Les obligations imputables tant aux entreprises du secteur privé qu'aux organismes publics

Les entreprises et organismes publics peuvent communiquer à une autre personne ou à un autre organisme des renseignements personnels pour fins de recherche, études ou production de statistiques si une évaluation des facteurs relatifs à la vie privée (ci-après « ÉFVP ») est concluante quant aux points suivants[37] :

- l'objectif de l'étude, de la recherche ou la production de statistiques ne peut être atteint que si les renseignements personnels communiqués permettent l'identification des personnes ;
- il serait déraisonnable d'obtenir le consentement des personnes ;
- l'objectif de l'étude l'emporte sur l'impact de la communication et de l'utilisation des renseignements personnels sur la vie privée des personnes concernées ;
- les renseignements personnels sont utilisés de manière à en assurer leur confidentialité ;
- seuls les renseignements nécessaires sont communiqués.

b) Les obligations des chercheurs

Les obligations s'appliquant aux personnes ou organismes qui souhaitent faire de la recherche, des études ou produire des statistiques se lisent comme suit :

- faire la demande par écrit ;
- joindre le protocole de recherche ;
- démontrer que les critères de l'évaluation des facteurs relatifs à la vie privée sont remplis ;
- faire une liste complète des personnes et organismes à qui une demande similaire pour les mêmes fins de recherche a été faite ;
- le cas échéant, décrire les différentes technologies utilisées dans le traitement des renseignements ;
- le cas échéant, transmettre la décision documentée d'un comité d'éthique de la recherche relative à cette étude, etc.

c) L'entente écrite

Lorsque ces critères sont remplis, la communication des renseignements par l'entreprise ou l'organisme public doit faire l'objet d'une entente qui stipule notamment les éléments suivants[38] :

- les renseignements personnels sont accessibles uniquement par les personnes pour lesquelles il est nécessaire d'y avoir accès dans le cadre de leurs fonctions. Ces personnes doivent également signer un engagement de confidentialité ;
- ces renseignements sont utilisés seulement pour les fins prévues au protocole de recherche ;
- ces renseignements ne peuvent être appariés avec tout autre fichier non prévu au protocole ;
- ces renseignements ne peuvent être publiés ou diffusés sous une forme permettant d'identifier les individus sur lesquels portent ces renseignements.

En plus, l'entente doit prévoir :

- l'information à donner aux personnes avec qui on communique en vue de leur participation à la recherche ;
- les mesures prises pour assurer la protection des renseignements personnels ;
- le délai de conservation de renseignements ;
- l'obligation d'aviser l'entreprise ou l'organisme public de la destruction des renseignements ;
- l'avis obligatoire et sans délai à donner à l'entreprise ou à l'organisme qui transmet les renseignements et à la CAI advenant qu'un manquement à une condition de l'entente, un manquement aux mesures de protection prévues ou un autre événement qui pourrait porter atteinte à la confidentialité des renseignements.

Cette entente doit être transmise à la CAI et elle doit entrer en vigueur 30 jours après sa réception.

d) Les biobanques

Le Projet de loi semble marquer la volonté de rendre le processus plus efficace que ce qui est actuellement en place. Dans ce contexte, il modifie également la *Loi concernant le cadre juridique des technologies de l'information*[39] en disposant que la divulgation à la CAI de la création d'une banque de caractéristiques ou de mesures biométriques doit se faire au plus tard 60 jours avant sa mise en service[40].

***e) La* Loi concernant le partage de certains renseignements de santé**

Les dispositions concernant le partage des renseignements de santé pour la recherche, sous réserve de l'autorisation de la CAI, n'ont jamais été mises en vigueur depuis leur adoption en 2012[41]. Cela dit, le Projet de loi modifie l'article 106 et abroge l'article 107 de la *Loi concernant le partage de certains renseignements de santé* en adoptant une nouvelle approche visant à écarter l'implication de la CAI. Les renseignements de santé dans les banques de santé des domaines cliniques (sauf les numéros d'identification uniques) peuvent maintenant être communiqués par le ministre à des personnes ou organismes qui les utilisent pour étude, recherche ou production de statistiques dans le domaine de la santé et des services sociaux[42].

II– LA CONSERVATION DES RENSEIGNEMENTS PERSONNELS

A. La durée de conservation

À ce jour, la *Loi sur le secteur privé* dispose que les renseignements personnels ne peuvent être conservés que pendant le temps nécessaire aux fins identifiées[43] ou pour permettre à la personne concernée d'épuiser les recours prévus par la loi[44] étant précisé que « l'utilisation des renseignements contenus dans un dossier n'est permise, une fois l'objet du dossier accompli, qu'avec le consentement de la personne concernée, sous réserve du délai prévu par la loi ou par un calendrier de conservation établi par règlement du gouvernement »[45], calendrier qui n'a jamais été établi concernant la durée de conservation à laquelle se réfère l'article 10 de la *Loi sur le secteur privé*.

Le Projet de loi va plus loin au chapitre de la conservation des renseignements personnels : une fois que la finalité pour laquelle les renseignements personnels aura été accomplie, et sous réserve d'un délai de conservation prévu par la loi (qui reste toujours à prévoir), il faudra soit détruire le renseignement en question, soit l'anonymiser.

B. La distinction entre « dépersonnalisation » et « anonymisation »

Si la notion de destruction ne pose pas de problème en soi, celle d'anonymisation peut être plus difficile à appréhender. C'est pourquoi le nouvel article 23 introduit par Projet de loi en donne des critères. D'abord, le procédé d'anonymisation doit être irréversible. Ensuite, il doit être impossible d'identifier directement ou indirectement l'individu concerné.

Ce faisant, le Projet de loi vient expliquer la distinction entre « anonymisation » et « dépersonnalisation ». Alors que l'anonymisation est un procédé qui ne permet plus d'identifier directement ou indirectement un individu, la dépersonnalisation[46] est un procédé qui ne permet plus d'identifier directement la personne concernée et qui permet, notamment, de conserver des renseignements « 3° lorsque [l']utilisation est nécessaire à des fins d'étude, de recherche ou de production de statistiques »[47]. L'expression « indirectement » est donc au coeur de la distinction entre anonymisation et dépersonnalisation.

1. La dépersonnalisation

Plus spécifiquement, la notion de renseignements dépersonnalisés s'arrime avec les caractéristiques de données « pseudonymisées » au sens du RGPD : la suppression de tous les attributs des renseignements étant des identifiants directs (par exemple l'adresse courriel, le nom, le numéro d'assurance sociale), tout en y conservant les attributs étant des identifiants indirects (sexe, âge, date de naissance).

Aux termes du Projet de loi, la dépersonnalisation des renseignements personnels permettrait aux organismes publics et aux entreprises du secteur privé d'utiliser à des fins d'étude, de recherche ou de production de statistiques des renseignements personnels déjà en leur possession sans devoir obtenir préalablement le consentement des individus concernés à ces fins spécifiques, dans la mesure où cette utilisation est nécessaire aux fins de l'étude, de la recherche ou de la production de statistiques, selon le cas[48].

La dépersonnalisation se veut aussi une mesure de sécurité et permettrait de diminuer de façon proactive certains risques en matière de protection des renseignements personnels. Notamment, l'accès non autorisé à un jeu de données dépersonnalisées pourrait être moins susceptible de « présenter un risque qu'un préjudice sérieux soit causé »[49] et ainsi, de déclencher l'obligation de signaler cet incident à la CAI et aux individus concernés.

Concrètement, la dépersonnalisation réduirait le risque de mise en corrélation d'un ensemble de données avec l'identité originale d'une personne concernée. Parmi les techniques qui pourraient éventuellement constituer certaines des techniques de dépersonnalisation valable au sens des dispositions proposées dans le Projet de loi, on peut penser au système cryptographique à clé secrète, au hachage et à la « tokenisation »[50].

2. L'anonymisation

D'un autre côté, selon le Projet de loi, une solution adéquate d'anonymisation devrait faire en sorte que les renseignements en résultant ne puissent plus, de quelque façon que ce soit, permettre d'identifier un individu[51].

L'anonymisation des renseignements est introduite dans le Projet de loi comme une alternative à leur destruction, et permettrait donc de conserver ces renseignements indéfiniment[52]. Ainsi, selon la définition donnée à la notion de « renseignements personnels » dans les lois québécoises[53], les renseignements valablement anonymisés échapperaient à l'application de celles-ci.

À noter que, bien que la dépersonnalisation et l'anonymisation des renseignements personnels se prêtent bien à certaines activités de traitement de renseignements personnels nécessitant l'analyse de données brutes (par exemple, dans le domaine de la recherche médicale), les renseignements dépersonnalisés ou anonymisés peuvent, selon le contexte, perdre toute leur valeur et leur utilité. Une analyse préliminaire quant à la nécessité d'utiliser des renseignements personnels identificatoires est donc de mise avant de se lancer dans un projet de dépersonnalisation ou d'anonymisation[54].

Les organisations désirant anonymiser les renseignements qu'elles détiennent devraient plutôt adopter une approche basée sur les risques de réidentification. Ce risque de réidentification doit être apprécié à la lumière, notamment, du contexte ou de l'environnement dans lequel les données seront conservées, utilisées ou communiquées après l'anonymisation, du nombre d'identifiants directs se trouvant dans le jeu de données, et du risque de tentative de réidentification ou d'attaque similaire. Le procédé d'anonymisation devrait alors permettre de minimiser ce risque[55].

Notons que les techniques d'anonymisation sont vouées à rapidement évoluer dans le temps et posent un certain défi pour les législateurs qui doivent suivre la parade. Le projet de loi propose ainsi une exigence évolutive imposant aux organisations de réaliser l'anonymisation des données « selon les meilleures pratiques généralement reconnues »[56].

En 2014, le Groupe de travail « Article 29 » sur la protection des données, qui regroupait autrefois les autorités de protection des données européennes, publiait un avis sur les principales techniques d'anonymisation et leur mise en oeuvre[57]. Cet avis indique qu'une solution d'anonymisation doit être construite au cas par cas et adaptée aux usages prévus, et propose trois critères pour évaluer son efficacité : l'individualisation, la corrélation et l'inférence[58]. Ainsi, selon cet avis, un ensemble de données pour lequel il n'est possible ni d'individualiser ni de corréler ni d'inférer serait a priori anonyme, et un ensemble de données pour lequel au moins un des trois critères ci-dessus n'est pas respecté ne pourra être considéré comme anonyme qu'à la suite d'une analyse détaillée des risques de réidentification[59].

En tout état de cause l'anonymisation devra être considérée comme une meilleure pratique et appliquée à large échelle selon le Projet de loi[60].

C. Les sanctions

Les renseignements personnels, même dépersonnalisés ou anonymisés, peuvent être l'objet d'attaques ou de manoeuvres visant à leur redonner pleinement leur nature identificatoire. Tenant compte de cette réalité malheureuse, il est proposé dans le Projet de loi des sanctions de 15 000 $ à 25 000 000, ou 4 % du chiffre d'affaires mondial (si ce dernier montant est plus élevé) pour toute organisation procédant ou tentant de procéder à « l'identification d'une personne physique à partir de renseignements dépersonnalisés sans l'autorisation de la personne les détenant ou à partir de renseignements anonymisés »[61].

Dans le contexte où les entreprises délinquantes au chapitre de la détention ou de l'utilisation de renseignements personnels pourraient se voir imposer des sanctions pécuniaires[62] ou faire face à des accusations de nature pénale[63], il est fortement recommandé aux organisations de se préparer en amont à cet égard, notamment en identifiant les renseignements collectés, leur durée de conservation et, à l'échéance de cette durée, les procédés mis en oeuvre pour les détruire ou les anonymiser.

III– L'OBLIGATION DE NOMMER UN RESPONSABLE DE LA PROTECTION DES RENSEIGNEMENTS PERSONNELS AU SEIN DES ENTREPRISES DU SECTEUR PRIVÉ

Jusqu'à présent, contrairement à ce qui est actuellement en vigueur en Colombie-Britannique[64], en Alberta[65] et en vertu de la loi fédérale LPRPDÉ, la *Loi sur le secteur privé* ne prévoit pas d'obligation de nommer une personne responsable de la protection des renseignements personnels.

Le Projet de loi[66] vient modifier cet écart en prévoyant expressément non seulement que toute personne qui exploite une entreprise est responsable de la protection des

renseignements personnels qu'elle détient, mais va également plus loin en disposant d'office (et ce, à l'instar de ce qui est actuellement en vigueur dans la *Loi sur l'accès*), que la personne ayant la plus haute autorité au sein d'une entreprise du secteur privé devra exercer la fonction de responsable de la protection des renseignements personnels. Cette fonction pourra être déléguée par écrit, en tout ou partie, à un membre du personnel. En outre, le titre et les coordonnées de cette personne responsable devront être rendus publics.

Le responsable de la protection des renseignements personnels devra s'assurer que l'entreprise respecte les principes applicables en matière de protection des renseignements personnels. À titre d'illustration, le responsable devra établir et mettre en oeuvre au sein de l'entreprise des politiques et pratiques encadrant la protection des renseignements personnels, participer à l'évaluation des facteurs relatifs à la vie privée de tout projet de système d'information et être impliqué dans la gestion d'un incident de confidentialité.

IV– L'EXPORTATION DES DONNÉES PERSONNELLES

En matière d'exportation des données personnelles, le Québec a encore une fois choisi de s'inspirer du modèle européen : la règle pertinente sera que les renseignements personnels ne pourront être communiqués que dans les territoires où il existe un degré de protection équivalent à celui du Québec.

Ce principe dit d'adéquation a suscité des débats et des litiges sans fin, car son application à l'échelle d'une province fortement dépendante des exportations vers d'autres territoires nord-américains constituera, pour les entreprises, une nouvelle exigence onéreuse.

Le Projet de loi prévoit que le gouvernement du Québec publiera à la Gazette officielle du Québec une liste d'États pour lesquels le régime juridique encadrant les renseignements personnels fournit une protection équivalente aux principes de protection des renseignements personnels applicables au Québec[67].

Les entités des secteurs public et privé doivent maintenant se fier à l'évaluation du gouvernement du Québec quant aux territoires de destination des données. On peut supposer que les organismes gouvernementaux partageront les évaluations qu'ils effectueront des régimes juridiques étrangers. Dans le cas contraire, les entreprises à but lucratif qui souhaitent exporter leurs produits ou services ou communiquer des renseignements à leurs succursales à l'extérieur du Québec seront obligées de faire leur propre évaluation, ce qui alourdira leur fardeau réglementaire. De nos jours, il y a peu de transactions qui ne comportent pas la transmission d'au moins quelques renseignements personnels.

A. L'exportation des renseignements personnels détenus par le secteur public

Selon le Projet de loi, avant de communiquer à l'extérieur du Québec un renseignement personnel, un organisme public doit procéder à une évaluation des facteurs relatifs à la vie privée[68]. Il doit notamment prendre en compte la sensibilité du renseignement, la finalité de son utilisation, les mesures de protection dont le renseignement bénéficierait et le régime juridique applicable dans l'État où ce renseignement serait communiqué.

Si l'évaluation démontre que le renseignement bénéficierait d'une protection effectivement équivalente, la communication peut être effectuée, à condition qu'elle fasse l'objet d'une entente écrite qui tient compte notamment des résultats de l'évaluation et, le cas échéant, des modalités convenues dans le but d'atténuer les risques identifiés.

Il en va de même lorsque l'organisme public confie à une personne ou à un organisme à l'extérieur du Québec la tâche de recueillir, d'utiliser, de communiquer ou de conserver pour son compte un renseignement personnel.

Exceptionnellement, dans certains cas, un organisme public peut communiquer un renseignement personnel à l'extérieur du Québec sans suivre une telle procédure[69], notamment s'il y a urgence, si le renseignement est communiqué à un organisme public d'un autre gouvernement au bénéfice d'une personne, si la communication est faite dans le cadre d'un engagement international pris par le gouvernement du Québec et visé au chapitre III de la *Loi sur le ministère des Relations internationales*[70] ou si le Directeur de la santé publique procède à une communication prévue à l'article 133 de la *Loi sur la santé publique*[71].

B. L'exportation des renseignements personnels détenus par les entreprises du secteur privé

Pour les personnes morales et physiques qui recueillent des renseignements personnels dans le secteur privé, le Projet de loi prévoit des exigences supplémentaires comme le devoir d'informer la personne concernée de la possibilité que les données soient communiquées à l'extérieur du Québec[72]. Autrement, les étapes que les entités du secteur privé doivent suivre et les responsabilités qu'elles doivent assumer reflètent celles prévues pour le secteur public[73]. D'ailleurs, le Projet de loi mentionne expressément que l'exception prévue au paragraphe 7 de l'article 18 de la *Loi sur le secteur privé* est maintenue et que, lorsqu'il existe une situation d'urgence mettant en danger la vie, la santé ou la sécurité de la personne concernée, la procédure de communication de renseignements à l'extérieur du Québec ne s'applique pas.

V– L'OBLIGATION DE SIGNALER LES INCIDENTS DE CONFIDENTIALITÉ

A. Le régime actuel

Les moutures actuelles de la *Loi sur le secteur privé* et de la *Loi sur l'accès* ne prévoient aucune obligation légale de signalement d'incidents impliquant la fuite de renseignements personnels, cette démarche étant présentement laissée à la discrétion des entreprises privées et des organismes publics, et cela contrairement aux règles s'appliquant aux organisations assujetties à la loi fédérale[74], à la loi albertaine[75] ou au RGPD en Europe.

B. Les mesures proposées

1. La notion d'« incident de confidentialité »

D'abord, le Projet de loi propose d'introduire la notion d'« incident de confidentialité », laquelle y est définie comme étant un accès, une utilisation ou une communication non autorisé par la loi d'un renseignement personnel, ou bien comme étant la perte d'un renseignement personnel ou une autre atteinte à la protection d'un tel renseignement[76].

Un incident de confidentialité peut donc prendre plusieurs formes : intrusion par un tiers dans le système informatique d'une organisation, attaque par rançongiciel, perte de données provoquée par un virus ou par une faille informatique, extraction non autorisée de données par un employé ou par une personne non autorisée, etc.

2. L'obligation de signalement

Le Projet de loi propose l'ajout d'une obligation d'aviser avec diligence la CAI et toute personne dont les renseignements personnels sont concernés par l'incident de confidentialité si celui-ci présente un risque qu'un préjudice sérieux soit causé[77]. De plus, l'organisation qui subit l'incident pourra aviser tout organisme susceptible de diminuer le risque, en ne lui communiquant que les renseignements personnels nécessaires à cette fin sans le consentement de la personne concernée[78]. Le Projet de loi ne prévoit pas de délai fixe pour aviser ces parties, mais prévoit plutôt un devoir de « diligence »[79].

Si une entreprise omet de notifier les personnes dont les renseignements personnels sont concernés par l'incident, la CAI peut lui ordonner de le faire. Toutefois, il faut prendre note qu'une personne dont un renseignement personnel est concerné par l'incident n'a pas à être avisée tant que cela serait susceptible d'entraver une enquête faite par une personne ou par un organisme qui, en vertu de la loi, est chargé de prévenir, détecter ou réprimer le crime ou les infractions aux lois[80].

Le Projet de loi fournit également des balises permettant d'évaluer s'il existe un risque de préjudice sérieux pour une personne dont un renseignement personnel est concerné par un incident de confidentialité. Les éléments à considérer sont notamment la sensibilité du renseignement concerné, les conséquences appréhendées de son utilisation par un tiers et la probabilité qu'il soit utilisé à des fins préjudiciables[81].

3. L'obligation de tenir un registre des atteintes

Le Projet de loi introduit aussi l'obligation pour une entreprise de tenir un registre des incidents de confidentialité qui devra être transmis à la CAI sur demande[82]. Un incident de confidentialité pourra ainsi laisser des taches persistantes sur l'image des organisations, alors que ce registre sera la plupart du temps demandé lors de vérifications diligentes préalables à la conclusion de partenariats ou d'autres transactions de nature commerciale, ou même, dans le cas de litige mettant en cause la sécurité de l'information.

4. Le pouvoir d'ordonnance découlant du non-respect des nouvelles règles

Dans le cas spécifique d'un incident de confidentialité, la CAI peut ordonner à toute personne d'appliquer toute mesure visant à protéger les droits des personnes concernées, pour le temps et les conditions qu'elle détermine [83].

VI– LES RECOURS CIVILS ET LES ACTIONS COLLECTIVES

Le Projet de loi modifie les règles de droit civil en introduisant une nouvelle cause d'action à l'endroit d'une personne qui conserve un renseignement personnel et en prévoyant une nouvelle catégorie de dommages-intérêts punitifs applicable en cas d'atteinte à un droit protégé par la *Loi sur le secteur privé* ou par les articles 35 à 40 du *Code civil du Québec*.

Par l'ajout d'un seul article à la *Loi sur le secteur privé*, soit l'article 93.1, le Projet de loi a potentiellement la capacité de modifier profondément le régime de responsabilité applicable à une contravention à certains droits protégés par la *Loi sur le secteur privé* et le *Code civil du Québec*.

Le premier paragraphe du nouvel article 93.1 établirait une nouvelle cause d'action à responsabilité sans faute à l'endroit d'une personne qui conserve un renseignement personnel en cas de préjudice résultant d'une atteinte illicite à un droit conféré par la loi ou par les articles 35 à 40 C.c.Q.

Le texte de l'article renverse le fardeau de preuve applicable et prévoit une responsabilité automatique à moins qu'une preuve de force majeure ne soit administrée. Rappelons qu'il est nécessaire d'établir qu'un événement et irrésistible et imprévisible afin qu'une défense de force majeure soit retenue, ce qui constitue un critère particulièrement difficile à remplir. Ainsi, en pratique, une personne qui conserve un renseignement personnel ne pourra s'exonérer en établissant simplement l'absence d'une faute de sa part en cas d'atteinte illicite à la confidentialité d'un renseignement dont elle a la garde, même si l'atteinte illicite est le fait d'un tiers.

Le second paragraphe du nouvel article 93.1 prévoit l'octroi, en cas d'atteinte illicite intentionnelle ou résultant d'une faute lourde, de dommages-intérêts punitifs d'au moins 1 000 $.

Le nouvel article 93.1 de la *Loi sur le secteur privé* soulève plusieurs questions importantes. Mais une chose est certaine : avec un seuil déjà bas à l'étape de l'autorisation d'une action collective au Québec, la modification proposée entraînera sans aucun doute une forte augmentation des demandes découlant de fuites de données.

VII– LE RENFORCEMENT DES SANCTIONS PÉNALES

A. Le régime actuel

À l'heure actuelle, les moyens à la disposition de la CAI pour l'application de la *Loi sur le secteur privé* se limitent au pouvoir d'effectuer des inspections et des enquêtes et, en cas d'identification de manquements, d'ordonner l'application de mesures correctrices. Bien que ce processus soit long et parfois intrusif pour les administrés visés, il n'est pas accompagné de pénalités financières.

La *Loi sur le secteur privé* prévoit également la possibilité d'instituer des poursuites pénales en cas de manquements, mais cette possibilité demeure inexploitée. D'ailleurs, aucun précédent en la matière n'a pu être identifié. Une raison qui pourrait expliquer cette absence de précédent est que, selon la *Loi sur le secteur privé* présentement en vigueur, la CAI ne dispose pas de l'habilitation requise pour instituer une poursuite pénale, cette tâche étant dévolue au Directeur des poursuites criminelles et pénales (ci-après « DPCP ») lequel ne dispose pas d'une expertise en matière de protection de renseignements personnels.

B. Les mesures proposées

1. L'octroi d'un rôle de poursuivante à la CAI

La première série de mesures d'exécution et de contrôle proposées par le Projet de loi concerne les dispositions pénales. D'une part, la CAI se voit reconnaître un rôle de poursuivante. En pratique, cela signifie que des procureurs de la CAI pourront instituer devant la Cour du Québec des poursuites pénales en tenant un rôle analogue à celui du DPCP. D'autre part, les montants des amendes seront substantiellement augmentés pour atteindre, dans le cas des infractions les plus graves, le montant le plus élevé entre 25 000 000 $ ou un montant correspondant à 4 % du chiffre d'affaires mondial de l'entreprise visée.

2. L'implantation d'un nouveau régime de sanctions administratives

La seconde série de mesures d'exécution et de contrôle proposées par le Projet de loi est fondée sur l'introduction d'un nouveau système de « sanctions administratives pécuniaires ». Il s'agit d'un système parallèle aux infractions pénales.

Des systèmes similaires ont fait leur apparition au courant des vingt dernières années dans divers régimes réglementaires complexes, tant dans la législation fédérale que provinciale, afin de donner une flexibilité accrue aux régulateurs. Ils ont pour principal attrait de permettre l'imposition d'une « sanction » sans avoir à respecter les droits fondamentaux des personnes accusées prévus à la *Charte canadienne des droits et liberté*, notamment le droit à un procès devant un tribunal judiciaire, le droit au silence (ou à la non-coopération) ou le fardeau de preuve de l'absence de doute raisonnable. La constitutionnalité de ces pénalités administratives parallèles au régime pénal a été validée par la Cour suprême du Canada dans l'arrêt *Guidon* c. *Canada* [84] même lorsque les pénalités potentielles pouvaient s'élever à des sommes très élevées, se chiffrant en millions de dollars, à condition que l'imposition d'une sanction administrative soit dans l'objectif d'assurer l'observation d'un régime administratif et non d'imposer une peine à travers un régime pénal déguisé.

Le fonctionnement proposé par le Projet de loi s'inspire grandement du modèle mis en place depuis 2012 par le législateur québécois dans la *Loi sur la qualité de l'environnement* [85]. Il prévoit que la CAI désignera un fonctionnaire pour la délivrance des sanctions administratives. Cette personne devra déterminer l'opportunité d'imposer une sanction en se basant sur divers critères prévus à la loi, critères qui seront précisés dans un cadre général d'application que la CAI publiera. C'est notamment ce cadre général qui précisera quand un recours pénal sera envisagé plutôt qu'une sanction administrative pécuniaire. Le Projet de loi prévoit que la décision d'imposer une sanction administrative peut être révisée par un membre de la CAI affecté à la section de surveillance et que cette décision peut elle-même être révisée par la Cour du Québec.

Contrairement à d'autres régimes où les sanctions administratives sont minimes, le Projet de loi prévoit que le montant maximal pouvant être imposé pour les manquements les plus graves par voie de sanctions administratives est le montant le plus élevé entre 10 000 000 $ ou un montant correspondant à 2 % du chiffre d'affaires mondial de l'entreprise visée.

VIII– LES MODIFICATIONS PROPRES AUX ORGANISMES PUBLICS

Tout comme pour les entreprises du secteur privé, le Projet de loi propose une modification visant la responsabilité de la personne ayant « la plus haute autorité » [86] au sein de chaque organisme public, celle-ci exerçant par défaut la fonction de responsable de l'accès aux documents et celle de responsable de la protection des renseignements personnels [87]. L'article 8 de la *Loi sur l'accès*, s'il venait à être modifié comme le propose le Projet de loi, disposerait que cette personne, même si elle conserve le pouvoir de déléguer ces responsabilités par écrit à une autre personne, devra dorénavant veiller à « faciliter l'exercice » [88] de ces fonctions, même « lorsqu'elle n'exerce pas elle-même ces fonctions » [89].

Ainsi, les rôles respectifs de la personne responsable de l'accès aux documents et de celle responsable de la protection des renseignements personnels au sein d'un organisme public seraient dotés d'une visibilité accrue si le Projet de loi venait à être adopté. Le Projet de loi prévoit la nécessité d'avertir dès que possible la CAI des coordonnées des personnes responsables et de la date de leur entrée en fonction [90].

De plus, le plus haut dirigeant d'un organisme serait désormais soutenu par un « comité sur l'accès à l'information et la protection des renseignements personnels », qui relèvera directement de lui. Ce comité sera formé du responsable de l'accès aux documents, de celui de la protection des renseignements personnels et de « toute autre personne dont l'expertise est requise » [91]. On mentionne spécifiquement la possibilité d'y adjoindre les personnes responsables de la sécurité de l'information et de la gestion documentaire.

A. Les règles de gouvernance et l'évaluation des facteurs relatifs à la vie privée

Selon le Projet de loi, tous les organismes publics devront établir et publier des règles de gouvernance relatives aux renseignements personnels, pouvant prendre la forme de politiques, de directives ou de guides, ces règles devant être approuvées par son comité sur l'accès à l'information et la protection des renseignements personnels [92]. Tout organisme public « recueillant par un moyen technologique » des renseignements personnels devra également établir, publier et « diffuser par tout moyen propre à atteindre les personnes concernées » une politique de confidentialité « rédigée en termes simples et clairs » [93].

Les organismes publics désirant mettre en oeuvre un « projet de système d'information ou de prestation électronique de services impliquant la collecte, l'utilisation, la communication, la conservation ou la destruction de renseignements personnels » devront d'abord effectuer une évaluation des facteurs relatifs à la vie privée (ci-après « ÉFVP ») de ce projet [94]. À cet égard, la CAI a récemment publié un guide d'accompagnement afin de réaliser une évaluation des facteurs relatifs à la vie privée.

Les comités sur l'accès à l'information et la protection des renseignements personnels au sein des organismes publics auront leur mot à dire dans le cadre de la réalisation de tels projets et les organismes publics devront, aux fins de l'ÉFVP, les consulter dès le début de ces projets. Ces comités pourront, à toute étape d'un tel projet, suggérer des mesures de protection des renseignements personnels applicables à ce projet [95].

À noter que ces ÉFVP devront également être effectuées par les organismes publics préalablement à certaines collectes et communications de renseignements personnels sans le consentement des personnes concernées [96].

B. Les demandes d'accès abusives, nuisibles, frivoles ou faites de mauvaise foi

Dans les dernières années, la jurisprudence s'est étoffée en ce qui a trait aux demandes d'accès qui semblent, du point de vue de l'organisme public, abusives, répétitives, nuisibles ou frivoles [97]. La CAI manquait toutefois d'outils pour traiter de telles demandes. Le Projet de loi propose ainsi quelques nouvelles modalités dans le traitement de ces demandes d'accès. Par exemple, une demande d'autorisation de ne pas tenir compte de demandes manifestement abusives doit être faite dans une période n'excédant pas 10 jours à compter de la réception de la dernière demande d'accès du requérant [98]. De plus, avec le Projet de loi, la CAI pourra refuser ou cesser d'examiner une affaire s'il s'agit d'une demande frivole ou faite de mauvaise foi. Elle aura aussi de nouveaux pouvoirs. En effet, elle pourra interdire à une personne de faire une autre demande sans l'autorisation du président de la CAI, et même alors, selon les conditions imposées par celui-ci. Elle pourra aussi restreindre de la même manière la possibilité pour toute personne de présenter un acte de procédure dans une instance déjà en cours [99].

C. Les changements à la procédure et aux pouvoirs relatifs à la section juridictionnelle de la Commission

La section juridictionnelle de la CAI, qui s'occupe surtout des demandes d'accès à l'information auprès des organismes publics, se verrait imposer de nouvelles règles de procédure et octroyer de nouveaux pouvoirs.

À cet égard, une des propositions les plus importantes du Projet de loi qui apparaît à son article 134.4, soit l'ajout du facteur de la proportionnalité aux actions des parties et de la CAI elle-même, vise également une plus grande efficacité dans l'administration de la *Loi sur l'accès* [100].

D'autres propositions du Projet de loi visent également à faire entrer la nouvelle *Loi sur l'accès* dans l'air du temps, en mettant de l'avant l'exécution des modalités procédurales et le déroulement des instances à l'aide des technologies de l'information. Par exemple, l'obligation d'aviser un tiers qui a fourni un renseignement personnel qui fait l'objet d'une demande d'accès en cours de révision doit se faire maintenant par « la transmission d'un écrit » plutôt que par « courrier » [101].

Est également digne de mention la proposition d'ajouter une plus grande flexibilité quant à l'utilisation des technologies de l'information pour le déroulement des instances :

> 137.4. La Commission peut, à toute étape de l'instance, utiliser un moyen technologique qui est disponible tant pour les parties que pour elle-même. Elle peut ordonner qu'il soit utilisé par les parties, même d'office. Elle peut aussi, si elle le considère nécessaire, exiger, malgré l'accord des parties, qu'une personne se présente physiquement à une audience, à une conférence ou à un interrogatoire [102].

CONCLUSION

Si elles sont adoptées, les modifications proposées auront un impact majeur, tant sur la conduite des entreprises que sur le fonctionnement de la CAI. Même si le processus parlementaire n'est pas terminé, il est à prévoir qu'une vaste majorité des changements proposés seront adoptés. L'adoption de principe du Projet de loi l'a d'ailleurs été à l'unanimité par l'Assemblée nationale du Québec. Ainsi, il serait prudent pour les entreprises de commencer immédiatement à modifier leurs procédures internes afin d'être prêtes dès l'entrée en vigueur des modifications.

---

* M^e^ Antoine Aylwin, CIPP/C, est associé chez Fasken Martineau DuMoulin S.E.N.C.R.L. Il concentre sa pratique en litige successoral, fiduciaire et administratif. M^e^ Guillaume Pelegrin, avocat au sein du même cabinet, concentre sa pratique en litige administratif. Ils tiennent à remercier Mariya Papancheva, étudiante en droit, pour son aide dans la compilation des bulletins publiés sur le Centre des ressources sur le Projet de loi 64 de Fasken Martineau Dumoulin, lequel est accessible à l'adresse suivante : https://www.fasken.com/fr/knowledge/projet-de-loi-64/2020/06/accueil/.

1. Projet de loi nº 64, *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels* (ci-après « Projet de loi »).

2. RLRQ c. P-39.1 (ci-après « *Loi sur le secteur privé* »).

3. *Loi sur le secteur privé,* art. 14.

4. *Ibid.*, art. 8.

5. *Gerald Desjardins* c. *Groupe Lyras & Godard*, PV 99 17 45 (C.A.I.).

6. Projet de loi, art. 102.

7. *Ibid.*, art. 99.

8. *Loi sur la protection des renseignements personnels et les documents électroniques*, L.C. 2000, c. 5. (ci-après « LPRPDÉ »)

9. Voir notamment l'article 4.3.6 de l'annexe 1 LPRPDÉ.

10. Projet de loi, art. 96.

11. *Ibid.*, art. 102.

12. *Loi sur le secteur privé*, art. 8.1, tel que modifié par le Projet de loi. À noter que le profilage est défini à l'article 8.1, al. 2.

13. *Loi sur le secteur privé*, art. 28.1, introduit par l'article 113 du Projet de loi.

14. Règlement Général sur la Protection des Données, 2016/679 (ci-après « RGPD »).

15. CJUE, 13 mai 2014, C-131/12, *Google Spain SL et Google Inc.* c. *Agencia Española de Protección de Datos (AEPD) et Mario Costeja González*.

16. CJUE, 24 septembre 2019, C-507/17, *Google LLC c. Commission nationale de l'informatique et des libertés (CNIL)*.

17. Title 1.81.5 *California Consumer Act* of 2018, [Cal. Civ. Code §§1798.100-1798.199] (ci-après « CCPA »).

18. Projet de loi, art. 112.

19. Gouvernement du Québec*, Analyse d'impact réglementaire*, 30 juillet 2020, p. 4.

20. *Ibid.*, art. 93.

21. Karl DELWAIDE et Antoine AYLWIN, *Leçons tirées de dix ans d'expérience ; la Loi sur la protection des renseignements personnels dans le secteur privé du Québec*, Commissaire à la protection de la vie privée du Canada, 2005.

22. *Lavoie* c. *Pinkerton du Québec ltée* (C.A.I., 1996-02-05), avant-dernier paragraphe ; voir également à ce sujet *Leblond* c. *Assurances générales des Caisses Desjardins,* [2003] CAI 391 (appel accordé sur des questions de secret professionnel J.E. 2004-2148 (C.Q.), REJB 2004-71721).

23. Projet de loi, art. 107.

24. *Ibid.*

25. *Ibid.*

26. *Ibid.*

27. LPRPDÉ, art. 7.2.

28. PIPA BC, art. 20.

29. PIPA A, art. 22.

30. Projet de loi, art. 107.

31. LPRPDÉ, art. 2(1) ; PIPA BC, art. 20(1) ; PIPA A, art. 22(1)(a).

32. LPRPDÉ, art. 2(1).

33. RLRQ, c. A-2.1 (ci-après « *Loi sur l'accès* »).

34. L'accès aux données sur la santé et aux données connexes. Rapport du Conseil des Académies, 2015, Ottawa, p. 47, 51, 82.

35. Projet de loi, art. 19 et 102.

36. *Ibid.*

37. *Id.*, art. 23 et 110.

38. *Ibid.,* art. 23.

39. RLRQ c. C-1.1.

40. *Ibid.,* art. 77.

41. *Ibid.*, *Loi concernant le partage de certains renseignements de santé,* RLRQ c. P-9.00001 (jamais entré en vigueur).

42. *Ibid., art. 67.2.1, tel que modifié par l'article 91 du Projet de loi*.

43. *Loi sur le secteur privé*, art. 10.

44. *Ibid.*, art. 36.

45. *Ibid.*, art. 12.

46. *Ibid.*

47. Projet de loi, art. 19(1^{o}) et 102.

48. *Ibid.*, art. 102.

49. *Ibid.*, art. 95.

50. Groupe de travail « Article 29 » sur la protection des données, Avis 05/2014 sur les Techniques d'anonymisation, 10 avril 2014, p. 22-23.

51. Projet de loi, art. 111.

52. *Ibid.*

53. « Est un renseignement personnel, tout renseignement qui concerne une personne physique et permet de l'identifier », (*Loi sur le secteur privé*, art. 2).

54. Commissaire à l'information et à la protection de la vie privée de l'Ontario, « De-identification Guidelines for Structured Data », juin 2016, p. 1.

55. *Ibid.*

56. Projet de loi, art. 111.

57. Groupe de travail « Article 29 » sur la protection des données, p. 23-24.

58. *Ibid.*

59. *Ibid.*

60. Projet de loi, art. 23, al. 3.

61. *Ibid.*, art. 151.

62. *Ibid.*, art. 90.12.

63. *Ibid.*, art. 91.

64. Voir à cet égard M^{es} Antoine GUILMAIN et Éloïse GRATTON, « La protection des renseignements personnels dans le secteur privé au Québec : rétrospectives et perspectives », dans *Développements récents en droit à la vie privée*, vol. 465, Service de la formation continue du Barreau du Québec, 2019, Montréal, Éditions Yvon Blais,

p. 96, EYB2019DEV2787.

65. *Ibid.*

66. Projet de loi, art. 95.

67. Projet de loi, art. 27 et 103.

68. *Ibid.*, art. 27.

69. *Ibid.*

70. RLRQ, c. M-25.1.1.

71. RLRQ, c. S-2.2.

72. Projet de loi, art. 99.

73. *Ibid.*, art. 103.

74. *Loi sur les renseignements personnels et les documents électroniques*, L.C. 2000, c. 5.

75. PIPA A.

76. Projet de loi, art. 14 et 95.

77. *Ibid.*

78. *Ibid.*

79. *Ibid.*

80. *Ibid.*

81. *Ibid.*

82. *Ibid.*

83. *Ibid.*, art. 44 et 144.

84. 2015 CSC 41, EYB 2015-254987.

85. RLRQ. c. Q-2.

86. *Ibid.*, art. 8.

87. Projet de loi, art. 1.

88. *Ibid.*

89. *Ibid.*

90. *Ibid.*

91. *Ibid.*

92. *Ibid.*, art. 14.

93. *Ibid.*

94. *Ibid.*

95. *Ibid.*

96. Voir notamment : Projet de loi, art. 15, 23, 25 et 27.

97. Voir notamment à ce sujet *Ville de Ste-Adèle* c. *M.L.*, 2017 QCCAI 27, EYB 2017-298049.

98. Projet de loi, art. 52.

99. *Ibid.*, art. 53.

100. *Ibid.*, art. 49.

101. *Ibid.*, art. 51.

102. *Ibid.*, art. 54.

Date de dépôt : 17 novembre 2020