CI– 023M
C.P. – PL 64
Protection des renseignements personnels

Me MARK PHILLIPS
avocat – lawyer

4104, rue Saint-Denis
Montréal (Québec)
H2W 2M5

avocat@markphillips.ca
Téléph. : 514-441-5054
Téléc. : 438-801-0347

Le 28 septembre 2020

Louisette Cameron
Secrétaire
Commission des institutions
Édifice Pamphile-Le May
1035, rue des Parlementaires, 3e étage
Québec (Québec) G1A 1A3
ci@assnat.qc.ca

Objet : Commentaire sur le projet de loi n° 64, *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*

Madame Cameron,

Tout en accueillant chaleureusement la modernisation des dispositions visés par le projet de loi n° 64 (« PL64 »), révision qui n'a que trop tardé, je me permets à vous communiquer par le présent mes suggestions pour la Commission des institutions relativement à la révision du PL64.

Je suis avocat pratiquant dans le domaine de la protection des renseignements personnels à Montréal. J'ai une perspective unique dans le domaine, œuvrant surtout à protéger le droit à la vie privée des particuliers, étant ancien programmateur de logiciels et ayant fait une contribution doctrinale au domaine par la publication d'articles dans des revues de droit ainsi que des revues scientifiques.

Éviter le retranchement des droits déjà proposés. Certains interlocuteurs représentant les intérêts des grandes entreprises ont imploré aux membres de la Commission des institutions de retrancher les droits prévus par le PL64 afin d'alléger le fardeau de conformité. J'encourage la Commission à éviter de tels retranchements sauf dans les situations les plus claires, et ce pour deux raisons. D'abord, un tel retranchement risque l'auto-sabotage du domaine commercial québécois en le privant d'accès aux marché européen et international. Si ce nouveau cadre juridique passe en dessous du seuil établi en Europe, les flux de renseignements personnels provenant de l'Europe au Québec demeurera strictement réglementé ou bloqué entièrement. En outre, le Québec risque de vivre l'embarras d'une répétition du rejet public en 2014 de la suffisance de ses protections par les autorités en Europe.[1] Ensuite, et ce qui est encore plus important, le retranchement de ces droits ferait échec à l'objectif déclaré du PL64 : la restitution aux québécois-es du contrôle de leurs renseignements personnels, contrôle qui s'est vu sapé au cours des dernières années par les pratiques au sein du secteur des technologies ainsi que la consolidation de monopoles dans ce secteur.

Dépersonnalisation et anonymisation. La création de nouvelles catégories de renseignements

1 https://www.huntonprivacyblog.com/2014/06/25/article-29-working-partys-opinion-adequacy-quebecs-data-protection-regime/

« dépersonnalisés » et « anonymisés » est contre-productive, mêlant et dangereuse. À travers des juridictions internationales et canadiennes l'on voit rarement l'emploi de tels catégories, et ce avec bonne raison. La *dépersonnalisation* n'offre que très peu de protection puisqu'il permet l'identification indirect d'une personne, ce qui est devenu de plus en plus simple. *L'anonymisation*, tel que défini par le PL64, pour sa part, diminue indûment la protection des renseignements personnels en faisant recours à une notion de « meilleure pratiques » alors que dans le contexte d'ensembles de renseignements de plus en plus riches, aucune méthode d'anonymisation suffisante n'existe dans la grande majorité des cas. En de telles situations, les « meilleure pratiques » du PL64 risquent donc à autoriser la libre diffusion de renseignements se voulant « anonymisés » mais suivant une méthode qu'on l'on connaît déficiente. Il serait plutôt souhaitable de maintenir la seule division du droit antérieur entre les renseignements personnels, qui sont assujettis à la loi, et les autres renseignements, qui ne le sont pas.

Transparence des méthodes d'anonymisation. Les renseignements qui ont cessé d'être des renseignements personnels n'ont plus à être traités en conformité aux protections légales. Par conséquent, les organismes ont tout l'intérêt à se soustraire de leurs obligations en prétendant avoir « anonymisé » les renseignements personnels qu'ils contrôlent pour permettre leur libre diffusion. Ce qui est encore plus inquiétant, les particuliers perdent leur droit d'accès et leurs autres droits relativement à ces documents puisque l'organisme cesse de leur qualifier de « renseignements personnels ». Pour combler cette lacune, je recommande à obliger aux organismes de publier dans leurs politiques de confidentialité les méthodes qu'ils emploient pour anonymiser les renseignements personnels, et élargir le droit d'accès aux renseignements personnels pour que ce droit englobe les renseignements immédiatement après qu'ils ont été anonymisés. Je tiens à noter qu'une telle mesure de transparence ne minerait pas l'efficacité de ces méthodes vu le principe cardinal du domaine de la sécurité des donnés qui veut qu'une méthode de chiffrement ou d'anonymisation dont l'efficacité découle de sa propre confidentialité n'offre pas des garanties de sécurité suffisantes.

Réidentification. Je suis inquiet de la nouvelle infraction proposée pour l'article 91(3) de la *LPRPSP* visant une personne qui « procède ou tente 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 ». J'ai effectivement publié un article qui expose les diverses faiblesses d'une telle approche.[2] D'abord, l'on rend illégal le travail de chercheurs universitaires et autres œuvrant à évaluer les forces et faiblesses des diverses stratégies d'anonymisation. En Royaume-Unis, par exemple, le législateur a au moins tenté de prévoir une exception pour une telle situation, malgré la difficulté à circonscrire une telle disposition de manière qui atteint l'objectif visé. Même s'il était possible de résoudre ce problème, un tel approche est à éviter. En pratique, l'on ne connaît très rarement l'identité de, par exemple, un pirate informatique pour pouvoir lui sanctionner par une telle infraction. L'infraction ne fournit donc qu'une simple apparence de protection trompeuse qui permet ensuite la justification de la diffusion de renseignements inadéquatement protégés, dont les renseignements dépersonnalisés ou anonymisés.

Mesures de sécurité. Malgré que le PL64 vise précisément à éviter et à atténuer les fuites de données tels qu'on a vécu dans le cas de Desjardins, il semble paradoxalement ne pas hausser les mesures de sécurité obligatoires. Dans ce sens, il serait souhaitable que le PL64 s'inspire de l'exemple du Commissariat à la protection de la vie privée du Canada dans son rapport d'enquête concernant

2 https://link.springer.com/content/pdf/10.1007%2Fs11673-017-9806-9.pdf

l'atteinte à la sécurité d'Equifax.[3] Dans le cadre dudit rapport, le Commissariat exige l'implantation d'un programme de sécurité efficace, en précisant qu'il doit comprendre des mécanismes de surveillance adéquats. Dans le contexte de la collecte et transmission d'une quantité importante de renseignements personnels sensibles, sont exigés des évaluations internes, des vérifications externes, et des essais d'intrusion internes et externes (fréquence en fonction du contexte).

Désindexation. L'article 28.1 proposé pour la *Loi sur la protection des renseignements personnels dans le secteur privé* (*LPRPSP*), concernant la désindexation, paraît à la fois trop large et trop étroite. Il est trop large puisque le droit à la réindexation est superflue : si la personne autorise la réindexation il n'y a aucune raison de contraindre l'organisme à en donner suite. Un organisme n'avait aucune obligation initiale à indexer le renseignement et, de plus, aura généralement tout l'intérêt à réindexer volontairement le renseignement en question. Le droit existant à la rectification répond déjà à tout risque de préjudice qui pourrait exister. L'article 28.1 est trop étroite dans le sens que le droit au déréférencement ne devrait pas exclure catégoriquement tout matériel journalistique. L'alinéa 4 du premier article de la *LPRPSP* exclut de son champ d'application tout « matériel journalistique » au lieu de ce qu'on voit plus couramment, les renseignements personnels traités pour des fins journalistiques. Le résultat est que, contrairement à l'Europe et les autres juridictions ayant un tel droit, les québécois n'auront aucun droit à la désindexation du moteur de recherche Google pour des articles de journal. Il serait préférable que le champ d'application de la loi n'exclut que le traitement de renseignements personnels pour des fins journalistiques, à l'instar des lois dans d'autres juridictions ou, dans l'alternative, que l'exclusion soit ainsi limitée pour les fins du nouveau article 28.1.

Profilage et traitement automatisé. Les dispositions concernant le traitement automatisé et le profilage ne semblent très peu ajouter aux droits des particuliers, notamment le droit d'accès qui existe déjà. Je recommande au lieu de suivre l'exemple du *Règlement général sur la protection des donnés* (RGPD) de l'Union européenne, qui octroie un droit de s'opposer à de telles traitements.

Divers droits et consentement. Les québécois devraient bénéficier de l'interdiction prévu au fédéral canadien qu'une organisation ne peut pas, pour le motif qu'elle fournit un bien ou un service, exiger d'une personne qu'elle consente à la collecte, à l'utilisation ou à la communication de renseignements autres que ceux qui sont nécessaires pour réaliser les fins légitimes et explicitement indiquées. Ils devraient également bénéficier du droit à l'opposition au traitement de leurs renseignements personnels, tel que prévue par le RGPD. Ils devraient enfin disposer du droit de s'exclure de la vente ou le partage de leurs renseignements personnels, potentiellement avec l'option de s'inscrire à une liste s'inspirant de la *Liste nationale de numéros de télécommunication exclus du Canada*. La revente de renseignements personnels ne devrait être permis que si la personne concernée est avisé explicitement de l'avis de la tierce partie et qu'elle soit donné l'option de s'exclure.

Personne responsable. Pour assurer que la personne responsable de la protection des renseignements personnels puisse exercer correctement ses fonctions, le PL64 devrait prévoir qu'elle doit être en mesure d'exercer ses fonctions en toute indépendance, à l'instar du RGPD. En outre, le PL64 devrait prévoir des protections contre les représailles, ainsi que prévoir l'obligation de dénoncer à la Commission d'accès à l'information le refus soutenu de l'organisme public ou l'entreprise de se

3 https://www.priv.gc.ca/fr/mesures-et-decisions-prises-par-le-commissariat/enquetes/enquetes-visant-les-entreprises/2019/lprpde-2019-001/

conformer à la loi.

Droit d'accès. Afin de résoudre des stratégies trop couramment utilisés afin de bafouer le droit à l'accès, j'invite la Commission à modifier la loi pour que l'application des restrictions sur l'accès soit fait d'une manière intelligible au demandeur. Trop souvent, les organismes publics et les entreprises caviardent les renseignements retranchés en utilisant la couleur blanche, ce qui évite souvent que le demandeur sache que des renseignements y figuraient. L'application des restrictions au droit d'accès devrait donc se faire d'une manière que le demandeur puisse aisément voir quelles portions de la page ont été omis, le nombre de pages qui ont été omises, les dispositions par lesquelles l'organisme justifie chaque omission. Le PL64 devrait également autoriser la Commission d'accès à l'information à sanctionner d'une manière efficace un manquement à une telle obligation.

Communication à l'extérieur du Québec. Pour assurer l'indépendance des décisions prises de toute apparence de considération politique relativement à la liste d'États prévu à l'article 70.2 proposé de la *LPRPSP*, l'inscription et la radiation de ces États sur la liste devrait relever de la compétence de la Commission d'accès à l'information au lieu du ministre suivant des décisions publiques énonçant les motifs de la décision. L'alinéa 4 du premier paragraphe de l'article 70.1 devrait en outre préciser explicitement que cette évaluation doit tenir compte de l'existence d'une programme de surveillance généralisée dans la juridiction pertinente.

La présente communication est concis de nécessité. J'invite toutefois à la Commission des institutions de ne pas hésiter à me contacter pour toute question ou précision supplémentaire qui serait souhaitée.

Espérant le tout utile aux efforts de révision de la Commission, je vous prie d'agréer, Madame Cameron, l'expression de mes sentiments les meilleurs,



Mark Phillips