C-27 : Renforcer la protection de la vie privée tout en favorisant l'innovation et en soutenant l'économie numérique du Canada[1]

Par Eloïse Gratton, Andy Nagy et Simon Du Perron[2]

Dans le contexte de la réforme de la législation fédérale sur la protection de la vie privée, nous nous trouvons à un moment critique où nous avons une occasion unique de trouver un équilibre assurant la protection de notre vie privée tout en favorisant un environnement propice à l'innovation. Dans une ère numérique qui évolue rapidement et où l'information circule plus vite que jamais, notre vie privée est de plus en plus menacée. Il est donc impératif de réformer nos lois sur la protection des renseignements personnels pour qu'elles reflètent les réalités d'aujourd'hui. Toutefois, les lois sur la protection des renseignements personnels ne doivent pas entraver l'esprit d'innovation qui nous a propulsé dans le XXIe siècle. L'innovation stimule la croissance économique, crée des emplois et améliore notre qualité de vie. C'est le moteur du progrès. Trouver le juste équilibre entre la protection de la vie privée et l'innovation est une tâche complexe, mais non impossible.

Le projet de loi C-27 prévoit l'adoption de deux lois apportant d'importantes modifications à la législation fédérale actuelle en matière de protection des données, la *Loi sur la protection des renseignements personnels et les documents électroniques* (**LPRPDE**). Premièrement, *la Loi sur la protection de la vie privée des consommateurs* (**LPVPC**) viendrait remplacer la partie 1 de la LPRPDE, qui porte sur la protection des renseignements personnels. Deuxièmement, la *Loi sur le Tribunal de la protection des renseignements personnels et des données* viendrait créer un nouveau Tribunal de protection des données. Le projet de loi C-27 prévoit également l'adoption de la *Loi sur l'intelligence artificielle et les données*, qui créerait un cadre juridique général pour l'intelligence artificielle (**IA**).

D'autres juridictions, comme l'Europe et le Québec, ont déjà mis à jour leurs lois sur la protection des renseignements personnels. Le *Règlement général sur la protection des données* (**RGPD**) de l'Union européenne est entré en vigueur en 2018 et le régime de protection des renseignements personnels du secteur privé du Québec, la *Loi sur la protection des renseignements personnels dans le secteur privé du Québec* (**Loi sur le secteur privé du Québec**), a récemment été amendée par le projet de loi 64 (Loi 25), la plupart des nouvelles modifications entrant en vigueur en septembre 2023. Ces lois sont à bien des égards plus onéreuses que la LPRPDE, mais à d'autres égards, elles établissent un meilleur équilibre entre la protection de la vie privée et l'innovation. En ce sens, nous avons certainement des leçons à tirer de ces juridictions.

Ce mémoire identifie quatre aspects où certaines dispositions proposées par la LPVPC pourraient être améliorées afin de soutenir davantage l'innovation, en tenant compte du RGPD et de la Loi sur le secteur privé du Québec récemment amendée:

---

[1] Mémoire présenté le 24 octobre 2023 au Comité permanent de l'industrie, des sciences et de la technologie de la Chambre des communes du Canada en vue de son étude du projet de loi C-27, Loi édictant la Loi sur la protection de la vie privée des consommateurs, la Loi sur le Tribunal de la protection des renseignements personnels et des données et la Loi sur l'intelligence artificielle et les données et apportant des modifications corrélatives et connexes à d'autres lois.

[2] Eloïse Gratton est associée chez Borden Ladner Gervais S.E.N.C.R.L., S.R.L. et Chef National du groupe de pratique Respect de la vie privée et Protection des renseignements personnels et Andy Nagy et Simon Du Perron sont avocats au sein de ce groupe de pratique. Le contenu de ce document ne doit pas être interprété comme un conseil juridique. Les opinions exprimées dans ce document sont uniquement celles des auteurs en leur qualité personnelle et ne représentent en aucun cas les opinions de Borden Ladner Gervais S.E.N.C.R.L., S.R.L. ou de l'un de ses clients.

1. L'exception du consentement fondée sur l'intérêt légitime

La LPRPDE est fondée sur les Principes relatifs à l'équité dans le traitement de l'information (« Fair information practice principles »), qui ont été initialement rédigées au début des années 1970 – et nous devons garder à l'esprit que leur principal objectif était de répondre à des préoccupations spécifiques concernant les bases de données informatisées et le fait que différentes organisations des secteurs public et privé pouvaient échanger plus facilement des renseignements personnels à l'insu ou sans le consentement des individus. À l'époque, la meilleure manière de répondre à ces nouvelles préoccupations était de faire en sorte que les individus exercent un contrôle effectif sur leurs renseignements personnels.

Un demi-siècle plus tard, ce concept reste l'une des théories les plus répandues en matière de protection de la vie privée et constitue le fondement des lois sur la protection des renseignements personnels dans le monde entier, y compris la LPRPDE au Canada. Mais l'approche « notification et choix » n'est plus réaliste : les individus sont surchargés d'informations et ne peuvent raisonnablement pas les traiter ou les comprendre. Les flux d'informations complexes et les nouveaux modèles commerciaux impliquant divers tiers ont également remis en question le modèle de consentement traditionnel.

Dans ce contexte, l'introduction de nouvelles exceptions au consentement est d'autant plus bienvenue. La LPVPC introduit des exceptions au consentement spécifiquement conçues pour faciliter la collecte et l'utilisation de renseignements personnels en vue d'une « activité d'affaires »[3] énoncée au par. 18(2), ou encore d'une « activité dans laquelle [l'organisation] a un intérêt légitime qui l'emporte sur tout effet négatif que la collecte ou l'utilisation peut avoir sur l'individu », suivant le par. 18(3). Bien qu'on retrouve une formulation semblable dans le RGPD, qui soumet le traitement de données personnelles à un régime distinct fondé sur l'intérêt légitime (voir le par. 6(1)f); considérant 47), notons que la LPVPC se distingue de celui-ci sur plusieurs aspects clés.

Premièrement, les exceptions qu'elle prévoit pour les activités d'affaires et l'existence d'un intérêt légitime prévues par la LPVPC ne sont que des exceptions à l'exigence générale d'obtenir un consentement. Elles ne constituent pas un régime distinct de traitement des renseignements personnels sur un pied d'égalité avec le consentement. Cette distinction est importante en ce que les tribunaux tendent à interpréter les exceptions au consentement de façon restrictive, ce qui, vraisemblablement, serait le cas de celles prévues dans la LPVPC.

Deuxièmement, ces exceptions se limitent à la collecte et à l'utilisation de renseignements personnels. Autrement dit, la communication de renseignements personnels à un tiers dans le cadre d'une « activité d'affaires » ou d'une « activité dans laquelle l'organisation a un intérêt légitime » ne serait pas permise, malgré les mesures appropriées pouvant être prises pour atténuer le risque de préjudice qu'elle suppose. Par exemple, une organisation pourrait devoir communiquer des renseignements personnels à certains tiers pour « la fourniture d'un produit » ou « la prestation d'un service » demandée par un individu (par. 18(2)a)); pensons aux entreprises de traitement de paiements, aux livreurs de colis, aux institutions financières et aux autres intermédiaires qui facilitent les transactions commerciales. Si certains de ces tiers peuvent se qualifier de fournisseurs de services (et profitent à ce titre d'une autre exception relative au

[3] Énumérés à l'article 18(2) LPVPC.

consentement), d'autres pourraient se rapprocher davantage de l'organisation responsable du traitement des renseignements personnels (qui nécessite l'obtention d'un consentement).

De même, il se peut que dans certains cas, l'exception visant les activités dans lesquelles une organisation a un intérêt légitime donne lieu à une distinction arbitraire entre, d'une part, la collecte et l'utilisation de renseignements personnels, et d'autre part, leur communication. Prenons l'exemple de l'organisation qui recueille et utilise des renseignements personnels pour mesurer l'utilisation de ses services et améliorer l'expérience de ses clients. Cette situation pourrait bien tomber sous le coup de l'exception relative à l'intérêt légitime, pourvu que l'organisation ait un intérêt clair à améliorer ses services qui l'emporte sur tout effet négatif pour les individus visés et qu'elle prenne des mesures appropriées pour évaluer et limiter ces effets (par. 18(4)). Cependant, si cette même organisation devait communiquer les renseignements personnels pour cette même fin à un tiers qui agit comme partenaire commercial, cette communication ne serait pas être couverte par l'exception.

Troisièmement, l'exception relative à l'intérêt légitime prévue au par. 18(3) est plus restreinte que la base légale de « l'intérêt légitime » prévue par le RGPD. Le par. 18(3) prévoit qu' « une organisation peut recueillir ou utiliser les renseignements personnels d'un individu à son insu ou sans son consentement si la collecte ou l'utilisation est faite en vue d'une activité dans laquelle elle a un intérêt légitime qui l'emporte sur tout effet négatif que la collecte ou l'utilisation peut avoir pour l'individu et si, à la fois une personne raisonnable s'attendrait à la collecte ou à l'utilisation en vue d'une telle activité et les renseignements personnels ne sont pas recueillis ou utilisés en vue d'influencer le comportement ou les décisions de l'individu. »[4] D'autre part, l'article 6(1) f), du RGPD stipule que le traitement des données personnelles est licite s'il est nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, « à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel. »

Le RGPD prévoit un test de mise en balance des avantages du traitement des renseignements pour la société et pour l'organisation avec les libertés et droits fondamentaux des individus. La LPVPC exige plutôt la considération de « tout effet négatif que la collecte ou l'utilisation peut avoir pour l'individu. » ce qui nous semble moins flexible qu'en vertu du RGPD. Cette exception relative à l'intérêt légitime est de plus soumise à l'exigence supplémentaire prévue au par. 18(3) du LPVPC, qui exige qu'une personne raisonnable s'attende à ce que la collecte ou l'utilisation s'effectue en vue d'une telle activité. Conformément à ce « test de raisonnabilité », une organisation ne peut recueillir, utiliser ou communiquer des renseignements personnels que d'une manière et à des fins qu'une personne raisonnable estimerait appropriées dans les circonstances (art. 12(1) du LPVPC remplaçant l'art. 5(3) de la LPRPDE). La définition de ces « attentes raisonnables » dans un contexte donné et la question de savoir si certaines activités sont légitimes du point de vue de la protection de la vie privée dépendent souvent de nombreux facteurs, notamment des normes sociales en vigueur. Un défi supplémentaire pour l'innovation réside dans le fait

[4] Le par. 18(3) prévoit qu' « une organisation peut recueillir ou utiliser les renseignements personnels d'un individu à son insu ou sans son consentement si la collecte ou l'utilisation est faite en vue d'une activité dans laquelle elle a un intérêt légitime qui l'emporte sur tout effet négatif que la collecte ou l'utilisation peut avoir pour l'individu et si, à la fois une personne raisonnable s'attendrait à la collecte ou à l'utilisation en vue d'une telle activité et les renseignements personnels ne sont pas recueillis ou utilisés en vue d'influencer le comportement ou les décisions de l'individu. » Conditions préalables (4) « Avant de se prévaloir du paragraphe (3) pour recueillir ou d'utiliser des renseignements personnels, l'organisation est tenue : a) de déceler tout effet négatif potentiel que la collecte ou l'utilisation est susceptible d'avoir pour l'individu; b) de trouver et de prendre des moyens raisonnables pour réduire la probabilité que ces effets se produisent ou pour les atténuer ou les éliminer; c) de se conformer à toute autre exigence réglementaire. »

que les normes sociales liées à toute nouvelle technologie ou pratique commerciale peuvent ne pas être encore établies au moment où ce nouveau produit ou service technologique est déployé.

Le fait que l'amendement proposé par la LPVPC soit plus étroit que la base juridique de l'intérêt légitime prévue par le RGPD limite considérablement son utilité. Nous devons également garder à l'esprit que les renseignements personnels recueillis à partir de sources accessibles au public sur Internet ne bénéficient pas d'une exemption de consentement simplement parce qu'elles sont accessibles au public.[5] Bien que cela offre une protection contre les utilisations contraires à l'éthique de renseignements personnels accessibles au public, ceci empêche également les organisations qui développent de façon légitime de nouveaux produits et services susceptibles d'être utiles à la société, d'exploiter le grand volume de données disponibles sur le web.

Pour ces raisons, les exceptions au consentement pour les activités d'affaires et l'intérêt légitime devraient être plus étroitement alignées sur la base juridique de l'intérêt légitime du RGPD afin de s'adapter à des types de modèles commerciaux innovants. Ces ajustements pourraient inclure des mécanismes de responsabilité appropriés, tels que des mesures contractuelles limitant l'utilisation des renseignements par le tiers et une évaluation préalable de l'impact sur les droits et libertés fondamentaux des personnes concernées.

En ce qui concerne l'exception relative au consentement fondé sur l'intérêt légitime (article 18, paragraphe 3, de la LPVPC) :

- **Recommandation n° 1.** Envisager élargir cette exception au consentement pour en faire une nouvelle base juridique autonome ou ajuster l'exception pour l'aligner plus étroitement sur le critère de mise en balance formulé par le RGPD, par exemple en remplaçant « qui l'emporte sur tout effet négatif » par « qui ne prévaut pas sur les droits et libertés fondamentales » et en autorisant les organisations à se fonder sur l'intérêt légitime pour communiquer des renseignements personnels.
- **Recommandation n° 2.** Si la recommandation n° 1 est mise en œuvre, envisager d'inclure des mesures de contrôle renforcées et/ou des exigences de sécurité pour contribuer à garantir l'utilisation ou la mise en œuvre responsable de cette nouvelle exception ou base juridique en matière de consentement.

2. Portée limitée de l'exception au consentement fondée sur les « fins socialement bénéfiques »

L'art. 39 de la LPVPC introduit une exception au consentement pour la communication de renseignements personnels dépersonnalisés à des entités publiques déterminées, par exemple une institution gouvernementale, un établissement de soins de santé, un établissement d'enseignement postsecondaire ou une bibliothèque publique située au Canada. Le fait que cette exception ne s'applique qu'aux communications ayant pour destinataire une entité publique en limite grandement l'utilité.

En limitant les types d'entités avec lesquelles les renseignements personnels dépersonnalisés peuvent être communiqué, cette nouvelle exception au consentement crée des possibilités très limitées pour les organisations de s'en prévaloir dans la pratique. Bien que l'objectif prétendu de cette disposition soit de

[5] Voir *A.T. c. Globe24h.com*, 2017 FC 114 (CanLII), [2017] 4 FCR 310.

renforcer les « partenariats »[6] public-privé, nous nous demandons si cette intention peut être pleinement réalisée étant donné l'absence flagrante de réciprocité, de coopération ou d'échange d'informations entre le secteur public et le secteur privé. En privilégiant nettement le secteur public, cette exception au consentement ne reconnaît pas non plus le rôle précieux joué par les organisations du secteur privé dans la poursuite d'activités qui servent des fins socialement bénéfiques. Le secteur privé peut avoir accès à des talents et à des ressources qui pourraient être mis à profit pour poursuivre des fins socialement bénéfiques de manière plus innovante ou plus rapide. Cela ne veut pas dire que le secteur public ne joue pas un rôle important dans ces situations, mais plutôt qu'il n'y a pas de justification claire, fondée sur des principes, pour laquelle le secteur public devrait bénéficier d'une préférence ou d'un privilège indu dans la poursuite de ces objectifs.

À l'ère numérique, de nombreuses organisations du secteur privé accumulent de grandes quantités de renseignements personnels sur leurs clients, leurs employés et d'autres individus, qui pourraient être utilisées à diverses fins socialement bénéfiques, qui ne correspondent pas toutes à la définition étroite fournie par l'exception au consentement susmentionnée. Par ailleurs, nous avons assisté à l'essor d'initiatives qui favorisent l'adoption de données ouvertes qui permettent à un large éventail de tiers, et pas seulement à des entités désignées du secteur public, d'accéder à des renseignements et de les communiqués à des fins légitimes liées à la science, à la technologie et à l'innovation. Il ne semble donc pas nécessaire de limiter l'exception au consentement à des fins socialement bénéfiques de la LPVPC aux partenariats public-privé, d'autant plus que les organisations du secteur privé sont tout aussi capables d'utiliser ces renseignements pour stimuler la recherche et l'innovation dans un certain nombre de domaines et d'assurer leur protection contre les menaces internes et externes.

Une approche davantage fondée sur les principes consisterait à articuler les exceptions au consentement autour d'exigences de contrôle adéquat et de meilleures pratiques en matière de protection des renseignements personnels, plutôt que d'exclusivités ou de monopoles du secteur public, afin de faciliter et d'encourager un partage responsable des renseignements personnels entre un plus large éventail d'acteurs. Cette même approche aurait l'avantage supplémentaire de combler d'autres lacunes dans la rédaction actuelle de l'exception. Plus précisément, alors que d'autres régimes de protection de la vie privée exigent généralement des organisations qu'elles mettent en œuvre des ententes de protection des données avec leurs fournisseurs de services ou d'autres tiers avec lesquels elles peuvent communiquer des renseignements personnels dépersonnalisées, nous constatons que l'article 39 de la LPVPC ne prévoit actuellement aucune obligation similaire. En d'autres termes, les organisations qui communiquent des renseignements personnels dépersonnalisées avec des entités désignées du secteur public ne seront pas tenues d'obtenir des garanties supplémentaires pour s'assurer que ces renseignements seront protégés de manière adéquate. Ces questions sont potentiellement aggravées par le fait que les entités du secteur public sont généralement soumises à un régime distinct de protection des renseignements personnels, et que ce régime est soumis à un certain degré d'incertitude puisqu'il fait actuellement l'objet de consultations au niveau fédéral. C'est pourquoi nous proposons d'élargir le champ d'application de l'exception relative au consentement prévue à l'article 39 afin de tenir compte des initiatives de partage de renseignements personnels entre organisations du secteur privé, tout en exigeant des organisations qu'elles mettent en œuvre des protections contractuelles minimales limitant les finalités pour lesquelles les renseignements peuvent être utilisés et garantissant que les renseignements bénéficient d'un niveau de protection adéquat.

[6] ISDE, "Renforcer la protection de la vie privée dans l'ère numérique", https://ised-isde.canada.ca/site/innover-meilleur-canada/fr/charte-canadienne-numerique/renforcer-protection-vie-privee-dans-lere-numerique

En résumé, il pourrait y avoir lieu de revoir l'art. 39 pour autoriser et faciliter la communication légitime de renseignements entre un plus vaste éventail d'acteurs (notamment des organisations du secteur privé) pouvant avoir à portée de main le talent et les ressources nécessaires à la poursuite de fins socialement bénéfiques. Cette révision devrait comprendre l'introduction d'exigences de contrôle et de pratiques de protection des données supplémentaires, par exemple par l'obligation de prévoir des mesures contractuelles particulières et de mener une évaluation des facteurs relatifs à la vie privée avant d'invoquer cette exception au consentement.

En ce qui concerne l'exception au consentement pour les « fins socialement bénéfiques » (article 39 de la LPVPC):

- **Recommandation n° 3.** Envisager d'étendre cette exception au consentement pour inclure également les communications faites à des organisations du secteur privé.
- **Recommandation n° 4.** Si la recommandation n° 3 est mise en œuvre, envisager d'inclure des mesures de surveillance renforcées et/ou des exigences en matière de sécurité pour contribuer à garantir l'utilisation ou la mise en œuvre responsable de cette exception en matière de consentement.

3. Un critère d'anonymisation irréaliste en pratique

L'utilisation de données anonymisées est un aspect essentiel des activités d'analyse raisonnables et nécessaires qui contribuent à l'avenir du Canada. La LPVPC vient définir les termes « anonymiser » et « dépersonnaliser »[7], et elle donne plus de latitude quant au traitement de ces catégories de renseignements, notamment à des fins de recherche et d'analyse internes. Toutefois, au sens du par. 2(1) de la LPVPC, pour être « anonymisée », une donnée doit être « modifi[ée] définitivement et irréversiblement, conformément aux meilleures pratiques généralement reconnues [...], afin qu'[elle] ne permet[te] pas d'identifier un individu, directement ou indirectement, par quelque moyen que ce soit. »[8] Cette définition - qui ne figurait pas dans la précédente version de la loi C-11 - semble s'inspirer fortement du projet de loi 64 du Québec, qui prévoit qu'un renseignement personnel est anonymisé « lorsqu'il est en tout temps raisonnable de prévoir dans les circonstances qu'il ne permet plus, de façon irréversible, d'identifier directement ou indirectement cette personne. »[9] Cependant, contrairement au projet de loi 64 du Québec, la LPVPC n'introduit pas de formulation similaire à « raisonnable de prévoir dans les circonstances. » Il s'agit, à notre avis, d'une omission importante compte tenu de la pertinence d'un critère de raisonnabilité lorsqu'il s'agit de techniques sophistiquées de gestion des données telles que l'anonymisation.

Il est pertinent de mentionner que cette formulation a été introduite par un amendement adopté lors de l'étude détaillée du projet de loi 64. Comme l'ont démontré les débats des séances de la Commission des institutions, une notion de raisonnabilité a été introduite dans la définition des renseignements

[7] En vertu de la LPVPC, « dépersonnaliser » signifie « modifier des renseignements personnels afin de réduire le risque, sans pour autant l'éliminer, qu'un individu puisse être identifié directement. » (art. 2).

[8] Pour que des données soient anonymes en vertu de l'article 2(1) de la LPVPC, elles doivent être « modifi[ée] définitivement et irréversiblement, conformément aux meilleures pratiques généralement reconnues, des renseignements personnels afin qu'ils ne permettent pas d'identifier un individu, directement ou indirectement, par quelque moyen que ce soit. »

[9] Voir le nouvel article 23 al. 2 de la Loi sur la protection des renseignements personnels dans le secteur privé du Québec, CQLR c. P-39.1.

anonymisés afin d'éviter d'exiger que les organisations se conforment à une norme absolue qui soit impossible à atteindre en pratique. Voici comment le ministre Éric Caire, parrain du projet de loi, a expliqué l'amendement lors de l'étude article par article du projet de loi 64 :

> « En fait, l'idée de départ, c'était que dans cet article-là tel qu'il avait été rédigé en toute bonne foi, c'était la notion d'irréversibilité. Puis, je pense qu'on a discuté de ça avec les collègues abondamment, la loi exigeait quelque chose qui est… bon, qui n'est pas impossible, mais qui est quasi impossible, et c'est la raison pour laquelle je voulais vraiment valider… Et la notion de… quand on dit « lorsqu'il est raisonnable de prévoir dans les circonstances qu'il ne permet plus de façon irréversible », là, il y a la notion de raisonnabilité. Donc, si je prends vraiment tous les moyens pour le rendre irréversible, je serai conforme à la loi. » (Nos soulignements)

À son tour, Jean-Philippe Miville-Deschênes, le juriste du gouvernement, a fait remarquer que « l'aspect irréversible était un peu, selon les experts, utopique », le ministre Caire ajoutant par la suite :

> « …] Mais la notion d'irréversibilité, sans l'amendement, là, la loi nous amène dans un univers qui n'est pas réaliste. Alors, je voulais apporter cette nuance-là sur ce point-là. » (Nos soulignements)

Comme nous pouvons le constater, l'ajout de l'expression « raisonnable de prévoir dans les circonstances » dans la définition des renseignements rendus anonymes en vertu du projet de loi 64 du Québec vise à refléter un consensus croissant dans la littérature académique et technique concernant l'impossibilité d'atteindre un risque zéro de réidentification au sein d'un ensemble de données anonymisées[10]. Pour cette raison, de nombreuses juridictions ont favorisé une approche plus nuancée, basée sur le risque, de l'anonymisation des renseignements personnels. Par exemple, la conception de l'anonymisation dans le cadre du RGPD exige de prendre en considération « l'ensemble des facteurs objectifs, tels que le coût de l'identification et le temps nécessaire à celle-ci, en tenant compte des technologies disponibles au moment du traitement et de l'évolution de celles-ci. »[11] L'autorité britannique de protection des données a adopté le « test de l'intrus motivé » (*motivated intruder test*) pour évaluer le risque de réidentification[12]. Cette approche fondée sur le risque a été implantée avec succès en Ontario dans la *Loi de 2004 sur la protection des renseignements personnels sur la santé* accompagnée des "*De-identification Guidelines for Structured Data*" du Commissaire à l'information et à la protection de la vie privée de l'Ontario[13].

---

[10] Voir notamment Luc Rocher, Julien M. Hendrickx et Yves-Alexandre de Montjoye, "Estimating the success of re-identifications in incomplete datasets using generative models', (2019) 10-1 Nature Communications 3069 ; Martin Scaiano, Grant Middleton, Luk Arbuckle, Varada Kolhatkar, Liam Peyton, Moira Dowling, Debbie S. Gipson et Khaled El Emam, "A unified framework for evaluating the risk of re-identification of text de-identification tools", (2016) 63 Journal of Biomedical Informatics 174 et Khaled El Emam, Guide to the De-Identification of Personal Health Information, New York, Auerbach Publications, 2013.

[11] Considération 26, RGPD.

[12] L'« intrus motivé » est supposé être raisonnablement compétent, avoir accès à des ressources telles que l'internet, les bibliothèques et tous les documents publics, et utiliser des techniques d'enquête telles que les demandes de renseignements auprès de personnes susceptibles d'avoir des connaissances supplémentaires sur l'identité de la personne concernée ou la publicité pour que toute personne disposant d'informations se manifeste. Toutefois, cette personne n'est pas censée avoir des connaissances spécialisées telles que des compétences en matière de piratage informatique, ni avoir accès à des équipements spécialisés, ni recourir à des actes criminels tels que le cambriolage pour accéder à des données conservées en toute sécurité. Ce test devrait être réévalué périodiquement pour tenir compte des nouvelles technologies et de la disponibilité publique des données, car ces facteurs sont susceptibles d'accroître le risque de réidentification. Voir UK Information Commissioner's Office, "Anonymisation : Managing data protection risk code of practice", pages 22-25, <https://ico.org.uk/media/for-organisations/documents/1061/anonymisation-code.pdf>.

[13] Commissaire à l'information et à la protection de la vie privée de l'Ontario, « De-identification Guidelines for Structured Data », juin 2016, <https://www.ipc.on.ca/wp-content/uploads/2016/08/Deidentification-Guidelines-for-Structured-Data.pdf>. La LPRPS définit « anonymiser »

Certains pourraient suggérer qu'un critère semblable est subtilement incorporé dans la définition de renseignement anonymisé de la LPVPC, étant donné que l'anonymisation en vertu de la LPVPC doit être effectuée « conformément aux meilleures pratiques généralement reconnues » (LPVPC, art. 2(1)). Tel qu'expliqué précédemment, les experts ont généralement reconnu que les techniques d'anonymisation ne produisent pas des ensembles de données pour lesquels la probabilité de réidentification est nulle, mais plutôt des ensembles de données pour lesquels la probabilité de réidentification est très faible compte tenu des caractéristiques spécifiques de l'ensemble de données. Toutefois, afin d'éviter des interprétations contradictoires, la définition d'« anonymisation » de la LPVPC devrait expressément inclure un critère de raisonnabilité. L'inclusion d'une telle norme serait également plus réaliste que de tenir les organisations responsables d'une norme absolue qui pourrait être impossible à respecter dans la pratique.

Recommandation n° 5. Envisager d'inclure un critère de raisonnabilité dans la définition du terme « anonymiser » à l'article 2 (1) LPRVPC afin d'éviter d'imposer une norme irréaliste aux organisations[14].

Veuillez noter que le Canadian Anonymization Network a publié une analyse approfondie de ces difficultés dans la publication "*Proposed amendments to the de-identification and Anonymization provisions in the Digital Charger Implementation Act, 2022 (Bill C-27)*", qui devrait être lue en parallèle avec la présente section.

4. Utilisation de renseignements dépersonnalisés à des fins de recherche, d'analyse et de développement interne.

L'art. 21 de la LPVPC introduit une exception permettant l'utilisation de renseignements dépersonnalisés « à des fins de recherche, d'analyse et de développement internes. » Il permettrait ainsi à une organisation qui détient un grand nombre de renseignements personnels sur des clients, des employés ou d'autres individus, d'utiliser ces renseignements, sans consentement, pour toute une gamme de fins innovantes, pourvu qu'elle les dépersonnalise d'abord. L'ajout du terme « analyse » à l'article 21 de la LPVPC, qui ne figurait pas dans la version précédente de la LPVPC en vertu du projet de loi C-11, permet non seulement d'élargir la portée des activités de recherche couvertes par l'exception relative au consentement, mais aussi d'harmoniser la disposition avec son équivalent dans la Loi sur le secteur privé du Québec, récemment modifiée.

Toutefois, en utilisant le terme « interne » pour qualifier la signification de « recherche, analyse et développement », la LPVPC semble imposer une restriction supplémentaire aux types d'activités de

---

des renseignements personnels sur la santé comme le fait de « retirer les renseignements qui permettent de l'identifier ou à l'égard desquels il est raisonnable de prévoir, dans les circonstances, qu'ils pourraient servir, seuls ou avec d'autres renseignements, à l'identifier. Le terme « anonymisation » a un sens correspondant. (« de-identify ») » (art. 2) (nous soulignons). Il convient de noter que la notion de dépersonnalisation en vertu de la LPRPS ne doit pas être confondue avec la dépersonnalisation en vertu de la LPVPC. En effet, la norme formulée par la LPRPS est celle de l'anonymisation, comme l'illustre la version française de la loi qui utilise le terme « anonymiser ». Ainsi, nous constatons que l'Ontario a également inclus une notion de caractère raisonnable dans sa définition des renseignements rendus anonymes. Lorsqu'elles interprètent le caractère raisonnable de leurs techniques d'anonymisation, les organisations assujetties à la LPRPS peuvent s'appuyer sur les « Lignes directrices sur la dépersonnalisation des données structurées » de l'IPC de l'Ontario, qui fournissent un cadre utile fondé sur le risque. En particulier, les lignes directrices exigent que les organisations déterminent un seuil de risque acceptable pour un ensemble de données spécifique et qu'elles appliquent divers contrôles de sécurité et de protection de la vie privée afin de réduire le risque en deçà du seuil.

[14] Par exemple, l'article 2(1) pourrait être lire: ***anonymiser*** « modifier définitivement et irréversiblement, conformément aux meilleures pratiques généralement reconnues, de sorte qu'il soit en tout temps raisonnable de s'attendre dans les circonstances, des renseignements personnels afin qu'ils ne permettent pas d'identifier un individu, directement ou indirectement, par quelque moyen que ce soit. »

« recherche » qui peuvent bénéficier de l'exception, en limitant son champ d'application aux activités qui sont menées exclusivement par et pour l'organisation elle-même. Restreindre l'utilisation de renseignements dépersonnalisées à des usages internes par l'organisation qui a recueilli les renseignements pourrait entraver le développement de partenariats de recherche innovants qui permettraient à diverses parties prenantes de partager des ensembles de données, sous réserve des pratiques exemplaires du secteur en matière de confidentialité, de sécurité des données et sous réserve de restrictions supplémentaires pour protéger adéquatement les individus (pour n'en citer que quelques-unes), afin de créer des substrats de données suffisamment larges pour la production d'informations utiles et exploitables. Plus précisément, dans une variété d'industries, y compris les soins de santé et autres, la capacité de produire des analyses à l'échelle de l'industrie dépend de la capacité de chaque acteur de participer à des modèles de mise en commun des données rendus possibles par des sociétés d'analyse tierces indépendantes qui fournissent des offres de données syndiquées qui ont été convenablement agrégées et rendue confidentielles afin d'écarter les préoccupations concernant le partage de renseignements sensibles entre concurrents. Toutefois, s'il est possible pour ces sociétés de produire des analyses au niveau du marché en exploitant des ensembles de données anonymes dans le cadre d'un modèle de mise en commun des données, le développement d'analyses plus pertinente est limité dans la mesure où ces mêmes modèles de mise en commun des données sont empêchés d'exploiter des renseignements dépersonnalisés.

Outre l'effet dissuasif que l'article 21 aurait sur la recherche et l'innovation en général, il convient également de souligner le risque de développement d'une dynamique de marché anticoncurrentielle. Plus précisément, il est possible que les différences inhérentes entre les grandes organisations, d'une part, et les petites et moyennes entreprises (**PME**), d'autre part, aggravent les inconvénients de l'article 21 de manière à créer des conditions de concurrence très inégales en ce qui concerne l'accès à la recherche et à l'analyse. Plus précisément, du simple fait de leur taille, les PME tendent à ne pas posséder les ressources ni les données brutes nécessaires pour produire des analyses significatives et des informations factuelles exploitables lorsqu'elles agissent seules.

Sans accès aux modèles de mise en commun des données, aux offres de données de tiers et aux partenariats de recherche, elles ne peuvent tout simplement pas espérer rivaliser avec le type de renseignements que les grandes organisations seront en mesure de tirer des tailles d'échantillons beaucoup plus importantes reflétées dans leurs ensembles de données, et elles prendront inévitablement du retard. De même, en limitant la recherche de chaque organisation à l'utilisation interne des ensembles de renseignement dépersonnalisés qu'elle possède déjà, les organisations seront intrinsèquement limitées dans leur capacité à explorer de nouveaux secteurs, ce qui aura pour effet de supprimer l'innovation et la prospection au sein des grandes comme des petites entreprises.

En résumé, le fait de restreindre l'exception au consentement pour l'utilisation des renseignements dépersonnalisés à des usages internes à l'organisation peut limiter la collaboration et la promotion de partenariats de recherche. Ces partenariats sont essentiels, car ils permettent aux parties prenantes de partager des ensembles de données afin de créer des jeux de données suffisamment vastes pour permettre d'en extraire des connaissances utiles et pratiques.

L'article 21 pourrait être révisé afin d'autoriser l'utilisation et la communication entre organisations de renseignements dépersonnalisés suivant les pratiques exemplaires du secteur en matière de confidentialité, de sécurité des données et sous réserve de restrictions supplémentaires pour protéger adéquatement les individus (comme des mesures contractuelles particulières, ou encore l'exigence de mener une évaluation des facteurs relatifs à la vie privée).

En ce qui concerne l'exception de consentement pour la « recherche, l'analyse et le développement internes » (article 21 de la LPVPC):

- **Recommandation n° 6.** Supprimer le qualificatif « interne » à l'article 21, car il pourrait limiter indûment la portée de cette exception au consentement.

***

Le projet de loi C-27 représente une étape importante pour le Canada dans la modernisation de sa loi fédérale sur la protection des renseignements personnels afin qu'elle soit mieux adaptée aux réalités du XXIe siècle. L'innovation et la protection de la vie privée peuvent coexister, et l'utilisation responsable des renseignements personnels peut être la pierre angulaire de l'élaboration de nouvelles technologies, tout en respectant nos droits fondamentaux. Un certain nombre de suggestions ont été formulées dans ce mémoire, en espérant qu'elles seront prises en compte dans la prochaine version du projet de loi C-27 afin de trouver le bon équilibre.

Les questions d'interopérabilité doivent également être prises en compte lors de l'évaluation du projet de loi C-27. Par exemple, le par. 2(1) définit le terme « système décisionnel automatisé » comme signifiant « une technologie utilisant des systèmes [...] afin d'appuyer ou de remplacer le jugement de décideurs humains. » Contrairement à la Loi sur le secteur privé du Québec qui limite la notion de système décisionnel automatisé aux systèmes entièrement automatisés, la LPVPC va très loin en englobant dans sa définition le système qui ne fait qu'appuyer le jugement d'un décideur humain. La définition devrait être revue et harmonisée avec les autres lois sur la protection des renseignements personnels en limitant son champ d'application aux systèmes entièrement automatisés.

Veuillez noter que les membres de l'équipe de BLG chargée de la protection de la vie privée ont publié plus tôt cette année un article intitulé « Loi sur la protection de la vie privée des consommateurs (projet de loi C-27) : Rétroaction des acteurs de l'industrie au Canada » dans lequel une liste plus complète de défis opérationnels et de préoccupations concernant le projet de loi C-27 est détaillée. Cet article est disponible sur le site web de BLG en français et en anglais.

Nous espérons que ces commentaires et suggestions seront utiles à l'étude du projet de loi et attendons avec impatience de lire la prochaine version du projet de loi C-27. Nous restons à votre disposition pour discuter de ces suggestions à votre convenance.

Eloïse Gratton
Associée et chef national, Respect de la vie privée et Protection des renseignements personnels
Borden Ladner Gervais S.E.N.C.R.L., S.R.L.

Andy Nagy
Avocat, Respect de la vie privée et Protection des renseignements personnels
Borden Ladner Gervais S.E.N.C.R.L., S.R.L.

Simon Du Perron
Avocat, Respect de la vie privée et Protection des renseignements personnels
Borden Ladner Gervais S.E.N.C.R.L., S.R.L.