CONSULTATIONS PARTICULIÈRES ET AUDITIONS PUBLIQUES AU SUJET DU PROJET DE LOI 64 : LOI MODERNISANT DES DISPOSITIONS LÉGISLATIVES EN MATIÈRE DE PROTECTION DES RENSEIGNEMENTS PERSONNELS

Résumé du mémoire présenté par la

Ligue des
droits et **libertés**

Devant la Commission des institutions

Assemblée nationale du Québec

23 septembre 2020

Introduction

Les lois de protection des renseignements personnels comme la Loi sur l'accès à l'information (LAI) et la Loi sur la protection des renseignements personnels dans le secteur privé (LPRPSP) adoptées dans les années 1980 et 1990 sont inadéquates à l'ère d'Internet et particulièrement dans le contexte du développement effréné de l'intelligence artificielle (IA). Le siphonnage massif de données sur les réseaux sociaux, la reconnaissance faciale, l'Internet des objets, les systèmes de localisation GPS, les drones dopés à l'IA, les capteurs de données des villes intelligentes, les assistants vocaux aux noms rassurants : tout cet attirail d'encerclement se développe sans contrôle ni débat public. Nous sommes donc d'avis qu'une mise à jour législative s'impose.

Le projet de loi 64 (PL64) 64 introduit plusieurs éléments tirés du Règlement Général sur la Protection des Données (RGPD) européen (portabilité, effacement, déréférencement, profilage, traitement automatisé de décision). Il s'agit de concepts encore peu ou pas débattus dans le grand public au Québec alors qu'ils sont l'objet de discussions depuis au moins 2012 en Europe. Qui plus est, le PL 64 modifie tant la LAI que la LPRPSP, en plus de modifier dix-neuf autres lois, notamment la Loi concernant le cadre juridique des technologies de l'information et la Loi électorale. Il nous semble pratiquement impossible, à nous comme aux parlementaires, d'approfondir l'ensemble de ces questions dans le cadre d'un projet de loi de soixante pages et d'une commission parlementaire d'à peine quelques jours. Certes, il est urgent de réformer les lois sur la protection des données, mais encore faut-il le faire correctement, sans précipitation et au terme d'une réflexion impliquant l'ensemble de la société.

La Ligue des droits et libertés entretient une autre réserve à l'endroit du PL64; il conforte un modèle d'affaires fondé sur la surveillance et l'accaparement de données personnelles et néglige les enjeux collectifs du Big data. Il apparait de ce fait défaillant.

Consentement

En ce qui concerne le consentement, la LDL rejette l'idée du consentement implicite et favorise le consentement basé sur le modèle du consentement actif (opt-in). Les lois de protection des données devraient aussi énoncer clairement qu'un renseignement qui n'est pas nécessaire ne peut être recueilli, même avec le consentement de la personne concernée.

Utilisation et communication de renseignements personnels (RP) sans consentement

Par son projet de loi, le gouvernement dit vouloir « *redonner aux citoyens le plein contrôle de leurs renseignements personnels* ». Pourtant, il libéralise l'utilisation et la communication des données personnelles sans le consentement des personnes, ce que nous déplorons.

Ainsi, il permettra l'utilisation de RP sans consentement : à des fins compatibles avec celles pour lesquelles il a été recueilli; lorsque cela est manifestement au bénéfice de la personne concernée; si nécessaire à des fins d'étude, de recherche ou de production de statistiques et qu'il est dépersonnalisé.

La communication de RP sans consentement sera autorisée : lorsque cette communication est effectuée dans le cadre d'une transaction commerciale; en cas d'incident de confidentialité à toute personne ou tout organisme susceptible de diminuer le risque de préjudice; si cette communication est nécessaire à l'exercice d'un mandat ou à l'exécution d'un contrat de service ou d'entreprise; si cette communication est effectuée au bénéfice d'un conjoint ou d'un proche parent d'une personne

décédée. Le projet de loi abolit en outre la nécessité d'une autorisation préalable de la Commission d'accès à l'information (CAI) pour la communication sans consentement de RP à des fins de recherche, d'études ou statistiques. Il permet de nombreux échanges de RP sans consentement entre organismes publics (OP).

Tous ces changements contredisent l'idée même d'un meilleur contrôle du citoyen ou de la citoyenne sur ses RP.

Destruction ou anonymisation

Le consentement à fournir un renseignement personnel est en lien avec une fin précise. Une fois celle-ci réalisée, le renseignement doit être détruit. Le PL64 altère substantiellement ce principe de base en permettant aux OP et entreprises de conserver indéfiniment un RP en l'anonymisant. Nous nous opposons à un tel changement, menant en pratique à une expropriation. À quelles nouvelles fins seraient utilisées ces données? Seront-elles vendues? Utilisées par leurs dépositaires ou par des tiers pour des recherches de toutes sortes, plus ou moins nobles? Cela parait d'autant plus inadmissible que l'anonymisation est un procédé faillible. L'utilisation d'autres identifiants ou le recoupement entre banques de données peut permettre la réidentification de renseignements censés sécurisés. Selon une étude de 2019 de l'Université catholique de Louvain en mathématiques appliquées « l'entièreté des techniques [d'anonymisation] qui sont utilisées jusqu'ici ne sont pas assez robustes ».

Profilage

Le projet de loi introduit quelques éléments de transparence dans l'utilisation de technologies permettant d'identifier, de localiser ou de profiler les individus. La personne doit être informée du recours à une telle technologie. Il faut aller plus loin selon nous et s'assurer que ces systèmes seront désactivés par défaut et ne fonctionneront qu'avec le consentement de la personne.

Le profilage discriminatoire doit être prohibé, de même que les systèmes d'intelligence artificielle biaisés, intentionnellement ou non, qui imposent un traitement préjudiciable. La loi devrait tenir compte des motifs de discrimination prohibés par la Charte des droits et libertés de la personne dans l'encadrement du profilage.

Décision fondée exclusivement sur un traitement automatisé

L'entreprise ou l'organisme public qui utilisera des renseignements personnels afin que soit rendue une décision fondée exclusivement sur un traitement automatisé devra en informer la personne concernée. Mais il est essentiel d'accorder aussi un droit d'opposition à l'utilisation d'un tel procédé. De plus, un individu affecté par le traitement automatisé de ses données doit pouvoir savoir comment une décision le concernant a été prise (droit à l'explication). Tout comme il devrait bénéficier d'un droit de contestation de cette décision.

Études, recherches et statistiques

Actuellement, la communication de RP (sans le consentement de la personne concernée) à des fins d'étude, de recherche ou de statistique est sous contrôle de la CAI, qui peut autoriser la communication si elle est d'avis que l'usage projeté n'est pas frivole et que les fins recherchées ne peuvent être atteintes que si les renseignements sont communiqués sous une forme nominative.

Le PL64 abolit le pouvoir d'autorisation préalable de la CAI. Désormais, toute entreprise ou OP pourra communiquer des RP sans consentement à des fins d'étude, de recherche ou de statistiques après avoir effectué une évaluation des facteurs relatifs à la vie privée. Une entente devra être conclue, qui comprend diverses dispositions visant à garantir un accès limité, un risque réduit de réidentification et des mesures de sécurité appropriée. L'entente est transmise à la CAI et entre en vigueur trente jours après réception par celle-ci.

On passe donc d'un régime d'autorisation à un régime d'autorégulation. Le tout pour la communication sans consentement de renseignements nominatifs possiblement très sensibles (santé, éducation, etc.).

La LDL s'oppose à ces amendements. Le contrôle qu'assure la CAI actuellement est un contrôle sérieux. Plusieurs voix s'élèvent contre la lourdeur du processus et les longs délais avant autorisation. Ces critiques sont fondées, mais la solution ne passe pas par l'autorégulation. Le gouvernement devrait maintenir le pouvoir de surveillance de la CAI en l'améliorant : la CAI devrait constituer le guichet unique des demandes; une simplification du processus pourrait être entreprise; l'ajout de ressources humaines et financières permettrait de réduire le délai de traitement des requêtes. L'autorisation devrait aussi être conditionnelle au fait que la divulgation ne soit pas préjudiciable aux personnes concernées et que « les bénéfices attendus de la recherche sont clairement d'intérêt public », comme le recommande la CAI dans son Rapport quinquennal 2016.

Droit au déférencement ou à l'oubli

Le droit à l'effacement est une question délicate, encore peu débattue au Québec. Plusieurs voient dans ce droit une menace à la liberté de presse et à la liberté d'expression. Un écueil important résulte du fait qu'on demande à des intérêts privés, notamment Google ou Facebook, d'agir en censeurs de l'information sur le net. On peut aussi craindre que les entreprises privées acceptent le retrait de renseignements sans trop se poser de questions, afin d'éviter les contestations.

Il convient de bien évaluer les tenants et aboutissants de cette question avant, éventuellement, d'importer pleinement ce droit au Québec. Le format de la présente commission ne permet pas d'approfondir la réflexion à ce sujet ni d'entendre tous les points de vue. Aussi, la Ligue des droits et libertés réserve-t-elle son jugement sur cette question. En revanche, nous convenons qu'une forme de droit à l'oubli devrait s'appliquer pour les enfants.

Communication de renseignements personnels à l'extérieur du Québec

La décision récente du gouvernement du Québec de faire appel au secteur privé pour le stockage des renseignements personnels détenus par les OP et ministères est particulièrement inquiétante. Cette privatisation des données présente bien des dangers : risques accrus de fuites; perte de contrôle sur les données et les coûts d'hébergement; perte d'expertise et dépendance de l'État envers le privé.

Le risque existe aussi que des entreprises étrangères comme Amazon ou IBM obtiennent le contrat, Le cas échéant, les données des Québécois-e-s seraient à la merci de la législation américaine, notamment le *CLOUD ACT* et le *Foreign Intelligence Surveillance Act*.

Le 16 juillet 2020, la Cour de justice de l'Union européenne (la CJUE) a d'ailleurs invalidé l'entente sur le bouclier de protection des données Union européenne–États-Unis. La Cour conclut que le droit américain permet l'ingérence dans la vie privée des personnes et n'assure pas une protection équivalente à celle du RGPD eu égard aux données des citoyens européens.

Ce développement important confirme nos pires appréhensions concernant la communication de RP hors Québec, tant par le gouvernement du Québec que par les entreprises privées. Il devrait à tout le moins convaincre le gouvernement de faire marche arrière et d'affirmer sa souveraineté numérique en développant ses propres infrastructures d'entreposage des données sur ses citoyen-ne-s.

Reconnaissance faciale

La technologie de reconnaissance faciale bat en brèche le droit à la vie privée et à l'anonymat, tout en rendant possible le profilage discriminatoire. Elle semble pourtant se développer sans contrôle, malgré l'existence au Québec de certaines balises légales qui sont, de toute évidence, inefficaces ou non respectées. Le Commissariat à la Protection de la Vie Privée au Canada et les commissaires de quelques provinces viennent de lancer une enquête pancanadienne soulignant leurs « préoccupations croissantes quant à l'utilisation de la reconnaissance faciale ».

Ce dossier met en lumière l'urgence de revoir l'encadrement légal sur cette question. Pourtant le PL64 effleure à peine le sujet. À l'instar d'autres groupes, la LDL demande un moratoire sur l'utilisation de cette technologie et la tenue d'un débat public large pour établir qui peut recourir à cette technologie et prescrire des conditions strictes d'utilisation.

Notification obligatoire d'incident de confidentialité des données

Nous saluons l'ajout de cette obligation, applicable aux secteurs public et privé, et qui aurait dû être inscrite depuis longtemps aux lois de protection des RP. Cela étant dit, le projet de loi comporte une réserve importante: une personne concernée par l'incident n'a pas à être avisée tant que cela serait susceptible d'entraver une enquête en vue de détecter ou réprimer le crime ou les infractions aux lois. Cette exception est préoccupante. L'enquête sur une fuite ou un vol de renseignements peut s'avérer longue; priver les personnes intéressées du droit d'être informées est difficilement justifiable.

Depuis des années, les fuites de RP se multiplient au Québec et au Canada. La série noire met à jour la fragilité étonnante des systèmes de sécurité de grandes institutions ou organismes gouvernementaux; de même qu'une nonchalance inexcusable au plan de la prévention.

Le projet de loi répond à ce fléau par une hausse substantielle des sanctions pénales, l'attribution à la CAI d'un pouvoir d'ordonnance provisoire, d'un droit de poursuite en matière pénale et du pouvoir d'infliger des sanctions administratives sévères en cas d'infraction à la loi. Il s'agit d'avancées appréciables.

Malgré tout, on demeure loin du compte. Ces sanctions apportent peu de réconfort aux personnes faisant les frais d'un vol d'identité et autres fraudes. Les sommes récoltées au plan pénal ou administratif n'iront pas aux victimes. Le législateur devrait songer à établir un mécanisme d'indemnisation des victimes, notamment à même les sommes résultant des sanctions.

Conclusion : Limites de l'approche individuelle : les enjeux collectifs du *Big data*

L'approche individuelle est insuffisante, dans un monde où l'utilisation des données engendre des conséquences importantes au plan collectif. Les enjeux collectifs entourant le traitement de données massives commandent l'édiction d'obligations légales de transparence et d'explication des modes de fonctionnement des systèmes d'intelligence artificielle (SIA). L'utilisation de SIA à des fins décisionnelles soulève aussi des enjeux collectifs.

Par ailleurs, les données que détiennent les organismes publics et les ministères constituent un bien collectif, particulièrement en santé. En octobre dernier, le Rapporteur spécial sur le droit à la vie privée de l'ONU alertait les États membres sur le fait « que la nature très sensible des données sur la santé ainsi que leur énorme valeur commerciale rendent extrêmement préoccupante l'industrie « largement cachée » de collecte, d'utilisation, de vente et de sécurisation de ces données, notamment au vu de son impact sur la vie privée ».

La déclaration récente du ministre de l'Économie et de l'Innovation, M. Fitzgibbon, disant vouloir « attirer quelques pharmas pour venir jouer dans nos platebandes » a suscité de vives réactions et mis à jour la nécessité et l'urgence d'un large débat de société sur le partage des données et la recherche au service du bien commun.

Le PL64 laisse dans l'ombre des enjeux névralgiques, notamment l'illégitimité d'une industrie fondée sur la surveillance et l'appropriation des données personnelles. La longue inaction des gouvernements, tant ici qu'ailleurs dans le monde, a malheureusement permis le déploiement de modèles d'affaires liberticides, une « nouvelle forme de commerce dépendant de la surveillance en ligne à grande échelle.

Une industrie fondée sur l'espionnage de la population et l'appropriation des données résultant de ses activités, de ses pensées, de ses questionnements et de ses interactions est-elle légitime? Est-ce compatible avec le maintien d'une société libre et démocratique ? Nous ne le croyons pas.

Un chantier de réflexion s'impose sur cette nouvelle économie des données. De même que sur l'approche consistant à définir les données collectives comme une « propriété commune devant être juridiquement et économiquement socialisée ».

Un encadrement s'impose aussi dans l'utilisation de l'intelligence artificielle. Le fonctionnement des algorithmes utilisés par l'État et l'entreprise privée doit être divulgué publiquement en vue d'en contrôler l'utilisation et les biais. Des garanties de loyauté, de transparence et de reddition de comptes doivent s'appliquer à l'exploitation de tels systèmes d'intelligence artificielle.