

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

CI- 008M
C.P. – PL 64
Protection des
renseignements
personnels

Mémoire présenté par la



Ligue des
droits et libertés

Devant la Commission des institutions
Assemblée nationale du Québec

23 septembre 2020

Table des matières

| | |
|---|----|
| Présentation de la Ligue des droits et libertés | 3 |
| Introduction | 4 |
| 1. Consentement..... | 5 |
| Navigation sur Internet : Opt-in, Opt-out..... | 5 |
| Libre | 6 |
| Que les renseignements nécessaires..... | 6 |
| Utilisation et communication de renseignements sans consentement..... | 7 |
| Anonymisation ou destruction de RP..... | 8 |
| 2. Droits liés à l'utilisation de certaines technologies : identification, localisation, profilage..... | 9 |
| 3. Décision fondée exclusivement sur un traitement automatisé | 10 |
| 4. Études, recherches et statistiques | 11 |
| Abolition du pouvoir d'autorisation préalable de la CAI | 11 |
| 5. Droit au déferencement ou à l'oubli..... | 13 |
| 6. Communication de renseignements personnels à l'extérieur du Québec | 15 |
| 7. Biométrie | 16 |
| 8. Notification obligatoire d'incident de confidentialité des données | 17 |
| 9. Limites de l'approche individuelle : les enjeux collectifs du <i>Big data</i> | 19 |
| Transparence et reddition de compte | 19 |
| Bien collectif..... | 20 |
| Conclusion..... | 21 |

Présentation de la Ligue des droits et libertés

Fondée en 1963, la Ligue des droits et libertés (LDL) est un organisme à but non lucratif, indépendant et non partisan, qui vise à faire connaître, à défendre et à promouvoir l'universalité, l'indivisibilité et l'interdépendance des droits reconnus dans la Charte internationale des droits de l'Homme. La Ligue des droits et libertés est affiliée à la Fédération internationale des ligues des droits humains (FIDH).

La LDL poursuit, comme elle l'a fait tout au long de son histoire, différentes luttes contre la discrimination et contre toute forme d'abus de pouvoir, pour la défense des droits civils, politiques, économiques, sociaux et culturels. Son action a influencé plusieurs politiques publiques et a contribué à la création d'institutions vouées à la défense et à la promotion des droits humains, notamment l'adoption de la Charte québécoise des droits et libertés de la personne du Québec et la création de la Commission des droits de la personne et des droits de la jeunesse.

Elle interpelle, tant sur la scène nationale qu'internationale, les instances gouvernementales pour qu'elles adoptent des lois, mesures et politiques conformes à leurs engagements à l'égard des instruments internationaux de défense des droits humains et pour dénoncer des situations de violation de droits dont elles sont responsables. Elle mène des activités d'information, de formation, de sensibilisation visant à faire connaître le plus largement possible les enjeux de droits pouvant se rapporter à l'ensemble des aspects de la vie en société. Ces actions visent l'ensemble de la population de même que certains groupes placés, selon différents contextes, en situation de discrimination.

Nous remercions la Commission des institutions de cette invitation à participer à la consultation particulière sur le projet de loi 64.

Introduction

En 2011, le rapport quinquennal de la Commission d'accès à l'information (CAI) signalait l'urgence d'adapter les lois de protection des données personnelles à l'environnement numérique¹. En 2016, la Commission réitérait sa supplique pour une réforme législative: « La Loi sur l'accès et la Loi sur la protection des renseignements personnels dans le secteur privé doivent être actualisées pour apporter des réponses aux questions préoccupantes et urgentes entourant notamment la collecte, le consentement, l'utilisation, la sécurité et l'exportation de ces renseignements² ».

À l'instar de la CAI, nous estimons que les lois de protection des renseignements personnels, la *Loi sur l'accès* (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 ce, particulièrement dans le contexte du développement effréné de l'intelligence artificielle (incluant l'apprentissage machine, l'apprentissage profond et le *Big data*). 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'Intelligence Artificielle (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.**

Ce modèle d'affaires, fondé sur l'espionnage et l'extraction de données, paraît en voie d'anéantir toute possibilité de vie privée. Il affecte aussi d'autres droits humains. La surveillance extrême des individus (tant par des entreprises privées que par l'État) peut altérer le libre arbitre, réduire l'autonomie des personnes et compromettre la liberté d'expression, la liberté d'association et la démocratie³.

Le projet de loi 64 (PL64) reconnaît partiellement ce fait en introduisant diverses mesures comme le droit à l'oubli, l'encadrement du profilage ou du traitement automatisé des décisions. Il poursuit un objectif plus vaste que la seule protection des données : les droits à la réputation, à la dignité, à l'égalité sont concernés. La liberté d'expression et le droit à l'information peuvent aussi être affectés.

C'est dans cette optique que nous faisons nôtre une recommandation de 2015 de la Commission des droits de la personne et des droits de la jeunesse (CDPDJ) à l'effet « qu'il y ait une référence explicite aux droits et libertés protégés par la Charte des droits et libertés de la personne dans les principes et objet de la Loi sur l'accès⁴ ». Cette référence à la Charte devrait aussi se retrouver intégrée à la LPRPSP.

Cela dit, nous émettons deux réserves d'ordre général concernant le PL64.

Premièrement, il ambitionne de mettre à niveau la législation québécoise avec le *Règlement général sur la protection des données* (RGPD) européen⁵. Il introduit nombre de ses concepts (portabilité, effacement, déréférencement, profilage, traitement automatisé de décision) encore peu ou pas débattus au Québec alors

¹ « La constitution de mégabases de données, le vol d'identité, l'utilisation insouciance d'Internet, le profilage des individus, dont les enfants, ne peuvent pas demeurer uniquement les manifestations d'un progrès qui nous dépasse. Il faudra bien un jour ou l'autre s'en préoccuper », Commission d'accès à l'information, Rapport quinquennal 2011 « Technologies et vie privée à l'heure des choix de société », <https://www.cai.gouv.qc.ca/rapport-quinquennal-2011/>

² Commission d'accès à l'information, Rapport quinquennal 2016 « Rétablir l'équilibre », 2016, p. V, <https://www.cai.gouv.qc.ca/le-rapport-quinquennal-2016-de-la-commission-depose-a-lassemblee-nationale/>

³ 1 R. c. Mills, 2019 CSC 22 : « De nombreuses études empiriques ont confirmé l'« effet paralysant » de la surveillance gouvernementale sur les comportements en ligne. Ces études indiquent que la surveillance électronique par l'État incite les gens à exercer l'autocensure sur leur expression en ligne », <https://www.canlii.org/fr/ca/csc/doc/2019/2019csc22/2019csc22.html>

⁴ Commission des droits de la personne et des droits de la jeunesse, MÉMOIRE À LA COMMISSION DES INSTITUTIONS DE L'ASSEMBLÉE NATIONALE SUR LE DOCUMENT D'ORIENTATION INTITULÉ « PLUS DE TRANSPARENCE, POUR UNE MEILLEURE GOUVERNANCE : ORIENTATIONS GOUVERNEMENTALES POUR UN GOUVERNEMENT PLUS TRANSPARENT, DANS LE RESPECT DU DROIT À LA VIE PRIVÉE ET LA PROTECTION DES RENSEIGNEMENTS PERSONNELS », Août 2015, https://www.cdpedj.qc.ca/Publications/memoire_transparence-gouvernance.pdf

⁵ Commission nationale de l'informatique et des libertés (CNIL), « Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016, relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) », entré en vigueur 23 mai 2018, <https://www.cnil.fr/fr/reglement-europeen-protection-donnees>

qu'ils sont l'objet de discussions depuis au moins 2012 en Europe. Qui plus est, il 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*. Ainsi, le recours à la biométrie de même que l'encadrement des partis politiques seront à l'étude. 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.

Deuxièmement, le PL64 conforte un modèle d'affaires fondé sur la surveillance et l'accaparement de données personnelles. Il néglige aussi les enjeux collectifs du *Big data*. Il apparaît de ce fait largement défailant.

1. Consentement

Le modèle législatif basé sur le consentement fait actuellement l'objet de nombreuses récriminations⁶. Il serait inefficace et engendrerait un faux sentiment de sécurité.

Ces critiques sont largement fondées. Le consentement se trouve souvent vicié, notamment par ignorance de l'étendue réelle de la collecte ou de l'utilisation qui seront faites des données. Ce consentement est de plus souvent « extorqué » : nous n'avons pas le choix de consentir si nous voulons profiter du service et n'avons pas le choix d'accepter certaines clauses et d'en refuser d'autres. C'est à prendre ou à laisser. Par ailleurs, les entreprises obtiennent ce consentement sur un simple clic, censé prouver l'acceptation de longues politiques d'utilisation souvent indéchiffrables.

Mais laisser tomber totalement le modèle du consentement signifierait que l'individu n'a plus voix au chapitre sur l'information le concernant. Cela paraît aberrant. **Il faut revoir le modèle, mais non s'en défaire totalement.** Il importe que l'individu puisse invoquer l'absence de consentement. Cependant, le consentement de l'utilisateur ou de l'utilisatrice ne doit pas dégager l'entreprise de toute responsabilité, par exemple, lorsque les données récoltées sont excessives, sans lien avec la finalité ou que la personne n'avait pas le choix de consentir.

Le PL64 énonce les conditions à remplir pour un consentement valable : il doit être **manifeste, libre, éclairé, sollicité à des fins spécifiques et de façon distincte à toute autre information communiquée**. Le PL64 ajoute que **le consentement devra être manifesté de façon expresse, dès qu'il s'agit d'un renseignement personnel sensible**. Dans les autres cas, il apparaît que le consentement pourrait n'être qu'implicite. C'est là selon nous diluer la nécessité d'un consentement clair.

Navigation sur Internet : *Opt-in, Opt-out*

Par ailleurs, la lecture d'interminables politiques de confidentialité ou de mise en garde sur la collecte de données ou l'utilisation de cookies est susceptible de décourager bien des usagers et utilisatrices des plateformes numériques. Comment s'attaquer à ce problème? L'approche que nous privilégions est celle de l'*opt-in* : à savoir qu'aucune donnée ne devrait être récoltée sauf consentement. Comme l'explique Anne-Sophie Letellier :

L'enjeu du consentement éclairé de l'utilisateur est aussi important. Deux grandes approches existent. Le *opt-in*, d'une part, fait référence à l'action que doit accomplir l'utilisateur pour autoriser la collecte de données. Une plateforme utilisant une approche à *opt-in* demandera donc à l'utilisateur d'accepter que ses données soient récoltées.

⁶ Pierre Trudel, « Renseignements personnels : les vraies urgences », *Le Devoir*, 18 février 2020, <https://www.ledevoir.com/opinion/chroniques/573151/renseignements-personnels-les-vraies-urgences>

Le *opt-out*, d'autre part, consiste en une collecte de données par défaut. L'utilisateur peut ensuite s'y soustraire en allant modifier les paramètres de son compte. Les plateformes Facebook et Google, notamment, utilisent cette approche. (...) Cette logique est cohérente avec l'absence – ou le laxisme – de cadres juridiques relatifs à la protection et à la collecte de données des utilisateurs⁷.

À cet égard, le PL 64 introduit le concept de « confidentialité par défaut » en exigeant des entreprises « que les paramètres des produits ou services technologiques qu'elles utilisent pour recueillir des renseignements personnels assurent, par défaut, le plus haut niveau de confidentialité sans aucune intervention de la personne concernée⁸ ». **Le plus haut niveau de confidentialité correspond selon nous à l'*opt-in*.** Le projet de loi devrait se montrer plus clair à ce sujet.

Libre

L'accès aux réseaux sociaux et autres plateformes sur Internet est pratiquement essentiel de nos jours⁹. Aussi les gens se sentent-ils, à tort ou à raison, tenus d'accepter une collecte éhontée d'informations à leur sujet. Comme le rapporte le Commissaire à la protection de la vie privée au Canada (CPVP) :

Les gens nous ont dit, à maintes reprises, qu'ils déploreraient le fait que s'ils souhaitent participer pleinement à la consommation du numérique et accéder à des produits et des services nouveaux ayant remplacé ceux qui n'étaient plus disponibles, le seul choix s'offrant réellement à eux était de « se fermer les yeux », « de se pincer le nez » et de cliquer « J'accepte »¹⁰.

Le consentement libre suppose que le refus de fournir des renseignements personnels non essentiels n'entraînera aucun préjudice¹¹. Le projet de loi n'offre aucune garantie à cet égard. Quant à l'actuel article 9 de la LPRPSP¹², bien qu'il crée une présomption de « non-nécessité » d'un renseignement, en pratique il laisse l'individu sans recours réel : s'il refuse de fournir l'information, il n'aura pas le service, il devra déposer une plainte à la CAI et possiblement attendre plusieurs années avant d'être entendu...

Que les renseignements nécessaires

Contrairement à ce que l'on peut croire, le consentement n'autorise pas la collecte de plus d'informations que nécessaire. Dans son rapport quinquennal de 2016, la CAI rappelle : « Plus de 20 ans après l'adoption de la Loi sur le privé et plus de 30 ans après celle de la Loi sur l'accès, spécifiant que seuls les renseignements personnels reliés et nécessaires aux finalités poursuivies doivent être recueillis, la Commission constate que ce

⁷ Anne-Sophie Letellier, « Données personnelles en ligne : quelque chose à cacher? » L'état du Québec 2020 | Clé 14 <https://inm.qc.ca/edq2020-cle14/>

⁸ Article 9.1. LPRPSP (introduit par l'article 100 du PL 64)

⁹ La Cour suprême notait en 2017 « Comme le souligne l'intervenante Association canadienne des libertés civiles (...) Le choix de « ne pas être en ligne » ne saurait constituer un choix véritable à l'ère d'Internet. » Douez c. Facebook, inc., 2017 CSC 33 <https://www.canlii.org/fr/ca/csc/doc/2017/2017csc33/2017csc33.html?searchUrlHash=AAAAA0A0ZG91ZXogaW50ZXJuZXQAA AAAAQ&resultIndex=1>

¹⁰ Commissariat à la vie privée du Canada, « Les priorités stratégiques liées à la vie privée », 2018-12-14, <https://www.priv.gc.ca/fr/a-propos-du-commissariat/priorites-strategiques-liees-a-la-vie-privee-du-commissariat/les-priorites-strategiques-liees-a-la-vie-privee/>

¹¹ « En général, le consentement ne constitue une base juridique appropriée que si la personne concernée dispose d'un contrôle et d'un choix réel concernant l'acceptation ou le refus des conditions proposées ou de la possibilité de les refuser sans subir de préjudice. Dans le cas contraire, le contrôle de la personne concernée devient illusoire et le consentement ne constituera pas une base valable pour le traitement des données, rendant de ce fait l'activité de traitement illicite », Groupe de travail « Article 29 » sur la protection des données, *Lignes directrices sur le consentement au sens du règlement 2016/679*, https://www.cnil.fr/sites/default/files/atoms/files/Idconsentement_wp259_rev_0.1_fr.pdf

¹² « Nul ne peut refuser d'acquiescer à une demande de bien ou de service ni à une demande relative à un emploi à cause du refus de la personne qui formule la demande de lui fournir un renseignement personnel sauf dans l'une ou l'autre des circonstances suivantes : 1° la collecte est nécessaire à la conclusion ou à l'exécution du contrat; 2° la collecte est autorisée par la loi; 3° il y a des motifs raisonnables de croire qu'une telle demande n'est pas licite. En cas de doute, un renseignement personnel est réputé non nécessaire ».

principe est loin d'être compris par les organismes publics et par les entreprises comme l'illustrent plusieurs de ses décisions¹³ ».

Nous souscrivons donc à la proposition suivante de la CAI : « La Commission recommande donc que les articles 64 de la Loi sur l'accès et 5 de la Loi sur le privé précisent qu'un renseignement qui n'est pas nécessaire ne peut être recueilli, même avec le consentement de la personne concernée¹⁴ ».

Utilisation et communication de renseignements sans consentement

Par son projet de loi, le gouvernement dit vouloir « redonner aux citoyens le plein contrôle de leurs renseignements personnels¹⁵ ». **Pourtant, il libéralise l'utilisation et la communication des données personnelles sans le consentement des personnes.** Ainsi, il sera possible d'utiliser un renseignement personnel (RP) sans le consentement de la personne concernée lorsque son utilisation est :

- à des fins compatibles avec celles pour lesquelles il a été recueilli;
- manifestement au bénéfice de la personne concernée;
- nécessaire à des fins d'étude, de recherche ou de production de statistiques et qu'il est dépersonnalisé¹⁶.

Le PL 64 permet la communication de RP sans consentement :

- lorsque cette communication est effectuée dans le cadre d'une transaction commerciale¹⁷
- en cas d'incident de confidentialité à toute personne ou tout organisme susceptible de diminuer le risque de préjudice¹⁸
- si cette communication est nécessaire à l'exercice d'un mandat ou à l'exécution d'un contrat de service ou d'entreprise¹⁹
- si cette communication est effectuée au bénéfice d'un conjoint ou d'un proche parent d'une personne décédée²⁰.

Le projet de loi abolit en outre la nécessité d'une autorisation préalable de la CAI pour la communication sans consentement de RP à des fins de recherche, d'études ou statistiques²¹. Il permet de nombreux échanges de RP sans consentement entre OP²².

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

¹³ Commission d'accès à l'information, Rapport quinquennal 2016 « Rétablir l'équilibre », 2016, p.92, <https://www.cai.gouv.qc.ca/le-rapport-quinquennal-2016-de-la-commission-depose-a-lassemblee-nationale/>

¹⁴ *Ibid.* Voir aussi Groupe de travail « Article 29 » sur la protection des données, *op.cit.* Ainsi, même si le traitement de données à caractère personnel a reçu le consentement de la personne concernée, cela ne justifie pas la collecte de données excessives au regard d'une finalité spécifique de traitement, ce qui serait foncièrement abusif.

¹⁵ Ministère de la Justice, Communiqué du 12 juin 2020, « Projet de loi 64 - Le gouvernement du Québec redonne aux citoyens le plein contrôle de leurs renseignements personnels », <https://www.quebec.ca/nouvelles/actualites/details/projet-de-loi-64-le-gouvernement-du-quebec-redonne-aux-citoyens-le-plein-controle-de-leurs-renseigne/>

¹⁶ Articles 19 et 102 du PL 64

¹⁷ Article 107 du PL 64

¹⁸ Articles 14 et 95 du PL 64

¹⁹ Article 107 du PL 64

²⁰ Articles 31 et 121 du PL 64

²¹ Articles 23 et 110 du PL 64

²² Articles 21 à 27 du PL 64

Anonymisation ou destruction de RP

Le consentement à fournir un renseignement personnel est en lien avec une fin précise. Une fois celle-ci réalisée, le renseignement doit être détruit²³. **Le PL64 altère substantiellement ce principe de base en permettant aux OP et entreprises de conserver indéfiniment un RP en l'anonymisant²⁴.** Nous nous opposons à un tel changement, menant en pratique à une expropriation : à la fin du cycle de vie utile, le RP appartient à l'OP ou à l'entreprise qui l'a recueilli.

Pourquoi permettre la conservation de RP dont l'objet est accompli? 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? Seront-elles « mises en valeur » sans l'accord de la personne concernée, et sans même qu'elle le sache?

Cela paraît d'autant plus inadmissible que l'anonymisation est un procédé faillible, voire chimérique²⁵. L'utilisation d'autres identifiants ou le recoupement entre banques de données permet souvent la réidentification de renseignements censés sécurisés. Comme le note Sébastien Gambis, professeur au département d'informatique de l'Université du Québec à Montréal (UQAM):

Pris séparément, chacun de ces attributs n'est pas suffisant pour réidentifier quelqu'un, mais dès qu'on commence à combiner des attributs différents, on arrive vite, au bout de trois ou quatre attributs, à une situation unique, c'est-à-dire qu'il n'y a pas d'autres personnes ayant la même combinaison d'attributs²⁶.

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 robustes²⁷ ». De plus, selon Rocher et al., « Using our model, we find that 99.98% of Americans would be correctly re-identified in any dataset using 15 demographic attributes²⁸ ».

La CAI reconnaît les limites importantes du procédé²⁹, rappelant en outre que plus on anonymise des données, plus leur qualité ou l'intérêt de leur réutilisation peuvent en être affectés³⁰. Cette technique exige en outre une mise à jour constante des systèmes³¹ et une expertise peu commune. « Bref, l'anonymisation de données et l'évaluation périodique des risques de réidentification comportent des questions techniques complexes qui devraient continuer d'évoluer au cours des prochaines années. Elles requièrent un niveau d'expertise que peu de gens possèdent au Québec³² ».

²³ C'est ce que prévoit actuellement l'article 73 de la LAI. L'article 12 de la LPRPSP ne mentionne pas la destruction, mais interdit l'utilisation du RP sans consentement une fois la finalité réalisée.

²⁴ « Lorsque les fins auxquelles un renseignement personnel a été recueilli ou utilisé sont accomplies, la personne qui exploite une entreprise doit le détruire ou l'anonymiser, sous réserve d'un délai de conservation prévu par une loi. Pour l'application de la présente loi, un renseignement concernant une personne physique est anonymisé lorsqu'il ne permet plus, de façon irréversible, d'identifier directement ou indirectement cette personne. Les renseignements anonymisés en vertu de la présente loi doivent l'être selon les meilleures pratiques généralement reconnues ». Articles 23 LPRPSP et 73 LAI

²⁵ « La question de l'anonymisation des données devient de plus en plus complexe. En fait, certains affirment même qu'il s'agit d'un mythe dans le contexte actuel », Commission d'accès à l'information, « Rapport quinquennal CAI 2016 », p.157.

²⁶ Pauline Gravel, « Données personnelles: un secret mal gardé », *Le Devoir*, 26 juillet 2019, <https://www.ledevoir.com/societe/science/559444/un-secret-mal-garde>

²⁷ Luc Rocher, « Vos données numériques anonymes sont très faciles à identifier, révèle une étude », *Radio-Canada*, 20 septembre 2019, <https://ici.radio-canada.ca/premiere/emissions/moteur-de-recherche/segments/entrevue/133833/donnees-anonymes-anonymisation-breche-faible-etude-internet-reseaux-sociaux-inquietudes-craintes-luc-rocher>

²⁸ Luc Rocher, Julien M. Hendrickx, Yves-Alexandre de Montjoye, « Estimating the success of re-identifications in incomplete datasets using generative models », *NATURE COMMUNICATIONS* | (2019). <https://www.nature.com/articles/s41467-019-10933-3>

²⁹ « Toutefois, il n'existe pas de recette infaillible applicable dans toutes les situations et à tous les jeux de données, et il est généralement admis qu'aucune ne garantit l'absence de risque de réidentification », Commission d'accès à l'information, « Rapport quinquennal 2016 », p. 160

³⁰ *Ibid* p. 161

³¹ « En effet, d'une part, l'anonymisation et la ré-identification sont des domaines de recherche très actifs où de nouvelles découvertes sont régulièrement publiées et, d'autre part, même des données anonymisées, comme les statistiques, peuvent servir à étoffer des profils existants, créant ainsi de nouveaux problèmes en termes de protection des données », Groupe de travail « Article 29 » sur la protection des données, « Avis 05/2014 sur les techniques d'anonymisation », 10 avril 2014, p. 4.

³² Commission d'accès à l'information, « Rapport quinquennal 2016 », p.162.

L'obligation qu'impose le PL64 d'utiliser « les meilleures pratiques généralement reconnues » en matière d'anonymisation ne nous convainc donc pas.

2. Droits liés à l'utilisation de certaines technologies : identification, localisation, profilage

Le projet de loi introduit quelques éléments de transparence dans l'utilisation de technologies permettant d'identifier, de localiser ou de profiler les personnes³³. Il intègre aussi une notion de profilage similaire à celle du RGPD. Le PL 64 définit le profilage comme : « la collecte et l'utilisation de renseignements personnels afin d'évaluer certaines caractéristiques d'une personne physique, notamment à des fins d'analyse du rendement au travail, de la situation économique, de la santé, des préférences personnelles, des intérêts ou du comportement de cette personne³⁴ ».

Le profilage a généralement un sens péjoratif. On l'associe à des pratiques préjudiciables fondées sur les préjugés. Le profilage est susceptible d'avoir un impact disproportionné sur les groupes racisés, marginalisés ou vulnérables : « The long-established marginalization of these groups is reflected in the data and reproduced in outputs that entrench historic patterns³⁵ ».

Dans le cadre d'une récente consultation sur l'intelligence artificielle, la CAI suggère « d'interdire l'utilisation de certains types de renseignements personnels afin d'effectuer du profilage (ex.: renseignements concernant l'origine raciale ou ethnique, les croyances et les opinions politiques, la santé, l'orientation sexuelle et les renseignements financiers ou biométriques), sauf si certaines conditions prévues dans la loi le permettent³⁶ ». La CDPDJ recommande de son côté de « tenir compte de la totalité des motifs de discrimination prohibés par la Charte dans l'encadrement du « profilage³⁷ ».

La CAI suggère en outre que « Le développement d'un SIA (Système d'Intelligence Artificielle) ou l'utilisation de renseignements personnels à l'aide d'un SIA à des fins illégitimes ou avec des intentions malveillantes comme celles de tromper, de discriminer des personnes ou de leur causer du tort devraient être interdits³⁸ ».

Nous souscrivons à l'ensemble de ces recommandations. Le profilage discriminatoire doit être prohibé de même que les systèmes d'intelligence artificielle biaisés, intentionnellement ou non, qui imposent un traitement préjudiciable en raison d'une différence assignée. « Tout comme dans le cas du profilage racial, l'élément

³³ Article 18 et 99 du PL 64 « En plus des informations devant être fournies suivant l'article 8 (ou 65 si LAI), la personne qui recueille des renseignements personnels auprès de la personne concernée en ayant recours à une technologie comprenant des fonctions permettant de l'identifier, de la localiser ou d'effectuer un profilage de celle-ci doit, au préalable, l'informer: 1° du recours à une telle technologie; 2° des moyens offerts, le cas échéant, pour désactiver les fonctions permettant d'identifier, de localiser ou d'effectuer un profilage. Le profilage s'entend de la collecte et de l'utilisation de renseignements personnels afin d'évaluer certaines caractéristiques d'une personne physique, notamment à des fins d'analyse du rendement au travail, de la situation économique, de la santé, des préférences personnelles, des intérêts ou du comportement de cette personne ».

³⁴ Article 8.1 du PL64.

³⁵ Accesnow, "Human rights in the age of artificial intelligence", Nov. 2018, p. 18,

<https://www.accessnow.org/cms/assets/uploads/2018/11/AI-and-Human-Rights.pdf>

³⁶ Commission d'accès à l'information, « Document de consultation. Intelligence artificielle », février 2020, p. 2,

https://www.cai.gouv.qc.ca/documents/CAI_consultation_IA_02-2020.pdf

³⁷ Commission des droits de la personne et des droits de la jeunesse, « MÉMOIRE À LA COMMISSION D'ACCÈS À L'INFORMATION sur le document de consultation « Intelligence artificielle » », mai 2020, p. 25,

https://www.cdpcj.gc.ca/Publications/memoire_consultation_CAIA.pdf

³⁸ Commission d'accès à l'information, « Document de consultation. Intelligence artificielle », février 2020, p. 3,

https://www.cai.gouv.qc.ca/documents/CAI_consultation_IA_02-2020.pdf

déclencheur des profilages social et politique repose, non pas sur l'appartenance réelle de la victime au groupe « profilé », mais plutôt sur son appartenance présumée à un groupe à risque³⁹ ».

Cette interdiction devrait aussi être intégrée à la Charte des droits et libertés de la personne.

Désactivation de fonctions

Selon le projet de loi, la personne suivie ou profilée devrait être informée des « moyens offerts, le cas échéant, pour désactiver les fonctions permettant d'identifier, de localiser ou d'effectuer un profilage⁴⁰ ».

L'identification, la localisation et le profilage sont des fonctions invasives. Comment expliquer alors que de telles fonctions se trouvent activées par défaut sur la technologie ? Le principe du « plus haut niveau de confidentialité sans aucune intervention de la personne concernée » introduit par l'article 9.1 LPRPSP devrait pourtant faire en sorte que, par défaut, ces fonctions ne soient pas activées. Selon nous, ces technologies ne devraient être utilisées que si la personne y consent, et par un geste actif (*opt-in*).

De plus, pour être valide le consentement doit être libre. Par exemple, selon le projet de loi, le profilage serait possible « notamment à des fins d'analyse du rendement au travail ». Peut-on parler d'un consentement libre pour l'employé-e dans un tel cas de figure? À l'instar du Groupe de travail G29, nous en doutons : « Au vu de la dépendance résultant de la relation employeur/employé, il est peu probable que la personne concernée soit en mesure de refuser de donner son consentement à son employeur concernant le traitement de ses données sans craindre ou encourir des conséquences négatives suite à ce refus⁴¹ ».

Ajoutons que le profilage ne doit pas servir à masquer des pratiques illicites de surveillance des employé-e-s. La personne salariée devrait bénéficier d'une protection contre les mesures de représailles en cas de refus de se soumettre à un profilage⁴².

3. Décision fondée exclusivement sur un traitement automatisé⁴³

L'entreprise ou l'organisme public (OP) qui utilise des renseignements personnels afin que soit rendue une décision fondée exclusivement sur un traitement automatisé doit en informer la personne concernée. Elle doit aussi, sur demande, l'informer : des renseignements personnels utilisés; des raisons et des principaux facteurs et paramètres, ayant mené à la décision; de son droit de faire rectifier les renseignements personnels utilisés pour rendre la décision.

Dans le secteur privé, la personne concernée doit en outre pouvoir présenter ses observations à un membre du personnel de l'entreprise en mesure de réviser la décision.

L'utilisation de l'IA à des fins décisionnelles se généralise à tous les secteurs. Les algorithmes peuvent intervenir dans le recrutement en emploi, l'établissement de cotes de crédit financières, l'accès à des établissements d'enseignement, l'évaluation des demandes d'immigration et de statut de réfugié-e-s, dans le système de justice, la détection de la fraude, le droit à certains services ou prestations, etc. Cette automatisation est susceptible d'affecter de façon disproportionnée les groupes déjà discriminés socialement.

³⁹ Ligue des droits et libertés, « Bulletin automne 2010. Profilage discriminatoire dans l'espace public. Comment cacher ce que l'on ne veut pas voir », automne 2010, p. 8. <https://liguedesdroits.ca/wp-content/fichiers/bulletin-automne2010page-par-page.pdf>

⁴⁰ Article 8.1 du PL64.

⁴¹ Groupe de travail « Article 29 » sur la protection des données, « Lignes directrices sur le consentement au sens du règlement 2016/679 » p. 7.

⁴² Une protection similaire à celle octroyée par l'article 144 du PL64 aux personnes dénonçant une infraction aux dispositions des lois sur la protection des renseignements personnels.

⁴³ Articles 20 et 102 du PL 64.

Le PL 64 n'aménage pas de droit d'opposition au traitement entièrement automatisé d'une décision. Pourtant, en vertu de l'article 22 du RGPD, les individus ont le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé⁴⁴. **Le PL64 devrait prévoir un tel droit d'opposition.** Comme le souligne le CPVP, « Les lois de plusieurs pays prévoient le droit de ne pas être soumis à la prise de décision automatisée, ou un droit analogue de contester le traitement automatisé des données personnelles, ainsi qu'un droit de ne pas être soumis à des décisions fondées uniquement sur l'automatisation⁴⁵ ».

Le RGPD aménage en outre un droit à l'explication et à la contestation supérieur à ce que prévoit le PL 64⁴⁶. **Pour la LDL, il va de soi qu'un individu affecté par le traitement automatisé de ses données doit pouvoir comprendre comment une décision le concernant a été prise. Tout comme il devrait bénéficier d'un droit de contestation de cette décision.**

4. Études, recherches et statistiques⁴⁷

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 CAI⁴⁸, qui peut autoriser la communication si elle est d'avis que:

- 1° 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;
- 2° les renseignements personnels seront utilisés d'une manière qui en assure le caractère confidentiel.

Abolition du 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 si une évaluation des facteurs relatifs à la vie privée (EFVP) démontre que :

- l'objectif de la recherche ne peut être atteint que si les renseignements sont communiqués sous une forme permettant d'identifier les personnes concernées;
- il est déraisonnable d'exiger de la personne ou de l'organisme qu'il obtienne le consentement des personnes concernées;
- l'objectif de la recherche l'emporte sur l'impact de la communication et de l'utilisation des renseignements sur la vie privée des personnes concernées;
- les renseignements personnels sont utilisés de manière à en assurer la confidentialité;
- seuls les renseignements nécessaires sont communiqués.

La personne ou l'organisme qui requiert les RP doit formuler la demande par écrit, joindre le protocole de recherche, exposer les motifs pouvant soutenir que les critères sont remplis, mentionner les autres personnes

⁴⁴ « Certaines exceptions existent cependant : les décisions fondées sur le consentement explicite des personnes concernées, les décisions nécessaires à la conclusion ou à l'exécution d'un contrat et les décisions encadrées par des dispositions légales spécifiques. Dans ces cas, des garanties spécifiques doivent être prévues afin de limiter les risques d'arbitraire soulevés par une telle prise de décision », voir CNIL *op.cit.*

⁴⁵ Commissariat à la protection de la vie privée du Canada, « Consultation sur les propositions du Commissariat visant à assurer une réglementation adéquate de l'intelligence artificielle », mars 2020, https://priv.gc.ca/fr/a-propos-du-commissariat/ce-que-nous-faisons/consultations/consultation-ai/pos_ai_202001/?wbdisable=true

⁴⁶ « Toute personne ayant fait l'objet d'une telle décision peut demander qu'une personne humaine intervienne, notamment afin d'obtenir un réexamen de sa situation, d'exprimer son propre point de vue, d'obtenir une explication sur la décision prise ou de contester la décision », voir CNIL, *op.cit.*

⁴⁷ Articles 23 et 110 du PL 64.

⁴⁸ Article 125 LAI et article 21 LPRPSP.

et organismes à qui des renseignements similaires ont été demandés, décrire les technologies utilisées, et le cas échéant, fournir une copie de la décision documentée d'un comité d'éthique de la recherche. Une entente doit être conclue, qui comprend diverses dispositions visant à garantir un accès limité, un risque réduit de réidentification, des mesures de sécurité appropriées et une conservation minimale. 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.). Il suffit d'exposer des motifs « pouvant soutenir » que les critères sont remplis. La supervision d'un comité d'éthique de la recherche paraît facultative. Nul besoin de démontrer que la recherche vise le bien commun. Il suffit d'établir que l'objectif de la recherche l'emporte sur l'impact de la communication et de l'utilisation des renseignements sur la vie privée des personnes concernées. Et c'est le demandeur qui répondra lui-même à cette question...

Qui plus est, l'article 106 de la *Loi sur le partage des renseignements de santé*⁴⁹ est modifié⁵⁰ en vue d'écarter le contrôle de la CAI sur les données contenues dans les banques de renseignements de santé des domaines cliniques⁵¹. Ces renseignements pourront être communiqués par le ministre de la Santé et des Services sociaux à des fins d'étude, de recherche ou de production de statistiques et conformément à l'article 67.2.1, donc après une Évaluation des Facteurs relatifs à la Vie Privée (ÉEFVP).

La LDL s'oppose à ces amendements. Les demandes d'autorisation pour la recherche sont en hausse à la CAI⁵². Le dispositif de demandes vise tant la recherche universitaire encadrée éthiquement que la recherche à des fins commerciales. Les requêtes peuvent aussi viser des fins d'étude ou de statistiques, sans autres précisions.

Le contrôle mis en place par la CAI est un contrôle sérieux⁵³. 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. La vigilance s'impose, au contraire.**

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

⁴⁹ L.R.Q. chapitre P-9.0001. 106. (Non en vigueur). « Les renseignements de santé contenus dans les banques de renseignements de santé des domaines cliniques, à l'exception des numéros d'identification unique, peuvent être communiqués par le ministre, aux personnes et organismes suivants, pourvu qu'il ne soit pas possible de relier ces renseignements à une personne particulière : 1° à l'Institut de la statistique du Québec; 2° à l'Institut national de santé publique du Québec; 3° à l'Institut national d'excellence en santé et en services sociaux; 4° à une personne autorisée par la Commission d'accès à l'information à utiliser des renseignements à des fins d'étude, de recherche ou de statistique dans le domaine de la santé et des services sociaux, selon les critères établis par l'article 125 de Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (chapitre A-2.1). Les communications prévues au présent article s'effectuent dans le cadre d'une entente écrite.

⁵⁰ Article 91 du PL 64 : L'article 106 de la Loi concernant le partage de certains renseignements de santé (chapitre P-9.0001) est modifié par le remplacement du paragraphe 4° du premier alinéa par le paragraphe suivant : « 4° à une personne ou à un organisme qui peut, conformément à l'article 67.2.1 de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (chapitre A-2.1), utiliser des renseignements à des fins d'étude, de recherche ou de production de statistiques dans le domaine de la santé et des services sociaux ».

⁵¹ À l'exception des numéros d'identification unique.

⁵² Dossiers d'autorisation à recevoir des renseignements personnels à des fins de recherche, d'étude ou de statistique (en hausse de 159%), Commission d'accès à l'information, « Rapport annuel de gestion 2018-2019 », <https://www.cai.gouv.qc.ca/depot-rapport-annuel-2018-2019/>

⁵³ « Quel est le rôle de l'analyste? • L'analyste doit, dans le respect des valeurs de la CAI (respect, impartialité, efficacité et solidarité 1) – Lire tous les documents reçus et rédiger un rapport; – S'assurer de la validité de l'information; – Vérifier auprès des organismes détenteurs la liste des renseignements personnels (disponibilité, exactitude, etc.); – Déposer le rapport auprès de la DS (**Direction de surveillance**) et répondre à toute question de la directrice ou des commissaires; – Soulever toute problématique potentielle quant à la protection des renseignements personnels. (...) Le rapport est transmis à la directrice de la DS puis à un commissaire en surveillance; • Le commissaire peut questionner la directrice ou l'analyste. Il peut exiger une rencontre avec le chercheur; • Le commissaire rend sa décision, laquelle comprend des conditions d'autorisation et une période de conservation des renseignements personnels; • Ultimement, les organismes détenteurs sont responsables d'accepter ou de refuser une demande », Commission d'accès à l'information, Louise Ringuette, M.Sc. Analyste, « Les demandes d'autorisation à la Commission d'accès à l'information: comment améliorer la qualité des demandes? », https://www.cai.gouv.qc.ca/documents/CAI_PR_20141107_LR.pdf

bénéfices attendus de la recherche sont clairement d'intérêt public », comme le recommande la CAI dans son Rapport quinquennal 2016⁵⁴.

5. Droit au déréférencement ou à l'oubli⁵⁵

Le droit introduit à l'article 28.1 de la LPRPSP semble viser tant le déréférencement d'un moteur de recherche que le droit à l'effacement. Avec le déréférencement, le contenu original reste inchangé et demeure accessible en utilisant d'autres critères de recherche que les nom et prénom de la personne. Le droit à l'effacement, de son côté, est particulièrement drastique puisqu'il signifie en principe que les informations ne seront plus disponibles à l'issue d'une quelconque recherche.

Le droit à l'effacement est une question délicate, encore peu débattue au Québec. En Europe, ce droit est régi par l'article 17 du RGPD et inclut, par interprétation des tribunaux, le droit au déréférencement⁵⁶.

Plusieurs voient dans ce droit une menace à la liberté de presse et à la liberté d'expression⁵⁷. Pour Reporters Committee for Freedom of the Press, « La norme applicable au principe du « droit à l'oubli » désormais reconnu dans l'Union européenne est [traduction] « vague, ambiguë et inutile » et nuisible pour le régime de la liberté d'expression dans son ensemble⁵⁸ ».

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 net⁵⁹. On peut aussi craindre que les entreprises privées acceptent le retrait

⁵⁴ La Commission d'accès à l'information recommandait l'abandon de l'autorisation préalable, mais proposait de conditionner la demande à la démonstration que : « La divulgation et l'utilisation des renseignements personnels par le chercheur dans le cadre de sa recherche ne sont pas préjudiciables aux personnes concernées par les renseignements et les bénéfices attendus de la recherche sont clairement dans l'intérêt public », voir « Rapport quinquennal 2016 », p.170.

⁵⁵ Article 113 du PL64. « 28.1. La personne concernée par un renseignement personnel peut exiger d'une personne qui exploite une entreprise qu'elle cesse la diffusion de ce renseignement ou que soit désindexé tout hyperlien rattaché à son nom permettant d'accéder à ce renseignement par un moyen technologique, lorsque la diffusion de ce renseignement contrevient à la loi ou à une ordonnance judiciaire.

Elle peut faire de même, ou encore exiger que l'hyperlien permettant d'accéder à ce renseignement soit réindexé, lorsque les conditions suivantes sont réunies: 1° la diffusion de ce renseignement lui cause un préjudice grave relatif au droit au respect de sa réputation ou de sa vie privée; 2° ce préjudice est manifestement supérieur à l'intérêt du public de connaître ce renseignement ou à l'intérêt de toute personne de s'exprimer librement; 3° la cessation de la diffusion, la réindexation ou la désindexation demandée n'excède pas ce qui est nécessaire pour éviter la perpétuation du préjudice.

Dans l'évaluation des critères du deuxième alinéa, il est tenu compte, notamment : 1° du fait que la personne concernée est une personnalité publique; 2° du fait que la personne concernée est mineure; 3° du fait que le renseignement est à jour et exact; 4° de la sensibilité du renseignement; 5° du contexte dans lequel s'effectue la diffusion du renseignement; 6° du délai écoulé entre la diffusion du renseignement et la demande faite en vertu du présent article; 7° si le renseignement concerne une procédure criminelle ou pénale, de l'obtention d'un pardon ou de l'application d'une restriction à l'accessibilité des registres des tribunaux judiciaires.

Les articles 30, 32 et 34 s'appliquent à une demande faite en vertu du présent article, avec les adaptations nécessaires. »

⁵⁶ FASKEN, « Bulletin La portée (extra) territoriale du RGPD : le droit à l'oubli », 29 novembre 2019,

<https://www.fasken.com/fr/knowledge/2019/11/the-extra-territorial-scope-of-the-gdpr/>

⁵⁷ « Le droit à l'oubli constitue un danger pour la liberté de presse et la liberté d'expression, et il n'est aucunement applicable au Canada », Journalistes canadiens pour la liberté d'expression, Association canadienne des journalistes, Centre For Free Expression, Journaux canadiens, Le Devoir, La Presse, Fédération professionnelle des journalistes du Québec, Buzzfeed Canada, National NewsMedia Council, magazine NOW, « Mémoire concernant la consultation sur la réputation en ligne du Commissariat à la protection de la vie privée du Canada », août 2016,

https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/completed-consultations/consultation-on-online-reputation/submissions-received-for-the-consultation-on-online-reputation/or/sub_or_24/

⁵⁸ The Reporters Committee for Freedom of the Press, « Mémoire soumis dans le cadre de la consultation sur la réputation en ligne du Commissariat à la protection de la vie privée du Canada », août 2016. https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/completed-consultations/consultation-on-online-reputation/submissions-received-for-the-consultation-on-online-reputation/or/sub_or_23/

⁵⁹ « Les décisions relatives au contenu rédactionnel doivent être prises par les éditeurs, et non par des entreprises de technologies. Google ne peut pas et ne devrait pas décider quels sont les renseignements auxquels le public peut avoir accès ou non », Journalistes canadiens pour la liberté d'expression, *op.cit.*

de renseignements sans trop se poser de questions, afin d'éviter les contestations. Comme le souligne ARTICLE 19, « en pratique, les intermédiaires ont une tendance bien connue à supprimer ou déréférencer aussi des contenus licites par peur d'engager leur responsabilité. Cela a finalement un effet paralysant sur la liberté d'expression⁶⁰ ».

Selon le Groupe de travail sur la protection des données personnelles du Barreau du Québec, il appartient aux tribunaux d'évaluer si un renseignement contrevient à la loi ou s'il constitue une atteinte à la réputation ou la vie privée : « [...] la décision de supprimer un hyperlien dans des résultats de recherche doit découler d'une décision judiciaire. Le seul fait qu'une personne se sente inconfortable en raison de la disponibilité d'une information qui circule licitement dans l'espace public ne saurait en aucun cas être une justification pour supprimer de l'information licitement disponible en ligne. Il faut qu'un juge indépendant statue sur la légalité d'une information⁶¹ ».

Pour la LDL la désindexation ou la suppression d'information des plateformes numériques ne devraient pas être prises à la légère. Certes, des abus sont commis qui mettent en cause la réputation, la dignité et la vie privée des personnes. Mais des recours existent déjà en droit civil, en droit criminel⁶² et dans les lois de protection des données personnelles⁶³.

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 LDL réserve-t-elle son jugement sur cette question. En revanche, nous convenons qu'une protection particulière devrait s'appliquer pour les enfants.

« Pour les enfants, la possibilité de remodeler leur identité au fil du temps est essentielle à ces processus et leur capacité de se réinventer dépend dans une certaine mesure du caractère éphémère de l'information. Ils devraient donc être en mesure de faire évoluer leur identité et leurs opinions sans être à jamais liés à des renseignements caducs à propos d'eux-mêmes ou de points de vue qui ne sont plus les leurs⁶⁴ ».

Nous souscrivons donc à la proposition du Groupe de travail sur la protection des données personnelles du Barreau du Québec en faveur d'un droit à l'effacement se limitant aux enfants :

⁶⁰ ARTICLE 19, « Le « droit à l'oubli » : sans oublier la liberté d'expression », 2016, [https://www.article19.org/data/files/medialibrary/38318/R2BF-Fr-\[pages\].pdf](https://www.article19.org/data/files/medialibrary/38318/R2BF-Fr-[pages].pdf). Le BC Freedom of Information and Privacy Association note de son côté: "(...) companies are often risk-averse, and may err towards censorship to protect themselves. Private companies will act to protect their own bottom lines. While this does at times align with the public interest—providing services for which there is a demand, for example—this is not the same as specifically working for the public." BC Freedom of Information and Privacy Association, "Submission to Consultation on Online Reputation (FIPA). Office of the Privacy Commissioner of Canada", août 2016, https://www.priv.gc.ca/en/about-the-opc/what-we-do/consultations/completed-consultations/consultation-on-online-reputation/submissions-received-for-the-consultation-on-online-reputation/or/sub_or_13/

⁶¹ Barreau du Québec, Groupe de travail sur la protection des données personnelles, « RÉFLEXION SUR UNE RÉFORME DE L'ACCÈS À L'INFORMATION ET DE LA PROTECTION DES DONNÉES PERSONNELLES », p.6, <https://www.barreau.qc.ca/media/1667/rapport-reflexion-acces-information-protection-donnees.pdf>

⁶² « Nous prétendons que les statuts en matière de protection de la vie privée, la common law et les lois créant des délits pour atteinte à la vie privée, et les dispositions du Code criminel contribuent déjà à protéger la capacité des personnes à gérer l'utilisation de leurs renseignements personnels et à préserver leur réputation, mais que les lois ne peuvent pas régler tous les problèmes de société », Freedom of Information and Privacy Association de la Colombie-Britannique, « Mémoire présenté au Commissariat à la protection de la vie privée du Canada dans le cadre de la consultation sur la réputation en ligne », août 2016, août 2016, https://www.priv.gc.ca/fr/a-propos-du-commissariat/ce-que-nous-faisons/consultations/consultations-terminees/consultation-sur-la-reputation-en-ligne/memoires-recus-dans-le-cadre-de-la-consultation-sur-la-reputation-en-ligne/or/sub_or_13/

⁶³ Le CPVP rappelle : « En ce qui a trait au déréférencement, le Commissariat estime que la LPRPDE s'applique au référencement du contenu en ligne et à l'affichage des résultats de recherche par les moteurs de recherche. Par conséquent, les moteurs de recherche sont tenus de respecter les obligations leur incombant en vertu de la Loi. Ils doivent notamment permettre aux individus de contester le caractère exact, à jour et complet des résultats d'une recherche lancée au moyen de leur nom », « Projet de position du Commissariat sur la réputation en ligne », https://www.priv.gc.ca/fr/a-propos-du-commissariat/ce-que-nous-faisons/consultations/consultations-terminees/consultation-sur-la-reputation-en-ligne/pos_or_201801/

⁶⁴ Yun Li-Reilly (Université Harvard), « Le droit à l'oubli des enfants. Mémoire présenté au Commissariat à la protection de la vie privée du Canada dans le cadre de la consultation sur la réputation en ligne », août 2016, https://www.priv.gc.ca/fr/a-propos-du-commissariat/ce-que-nous-faisons/consultations/consultations-terminees/consultation-sur-la-reputation-en-ligne/memoires-recus-dans-le-cadre-de-la-consultation-sur-la-reputation-en-ligne/or/sub_or_26/

« Le Groupe de travail propose, à l’instar du Comité permanent de l’accès à l’information, de la protection des renseignements personnels et de l’éthique de la Chambre des communes, de permettre aux jeunes d’obtenir l’effacement ou le déréférencement de données personnelles qui ont été produites lorsque ces personnes étaient mineures. Ainsi, nous proposons la mise en place d’un encadrement du droit à l’effacement inspiré du modèle mis en place dans l’Union européenne limité au droit des jeunes d’obtenir l’effacement de renseignements qu’ils ont mis en ligne⁶⁵ ».

6. Communication de renseignements personnels à l’extérieur du Québec⁶⁶

Le transfert de RP hors du Québec sera assujéti à une évaluation des facteurs relatifs à la vie privée⁶⁷. La communication pourra s’effectuer si l’évaluation démontre que le renseignement bénéficierait d’une protection équivalente à celle prévue aux lois québécoises.

Il en est de même lorsque l’OP ou l’entreprise 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 tel renseignement.

Le ministre responsable publiera dans la *Gazette officielle* une liste d’États dont le régime juridique encadrant les renseignements personnels équivaut aux principes de protection des renseignements personnels applicables au Québec. En quelque sorte, une liste de « tiers pays sûrs » du renseignement personnel...

Dans le cas des RP détenus par les OP et ministères, la décision récente du gouvernement du Québec de faire appel au secteur privé pour le stockage de ces données est particulièrement inquiétante. Les renseignements « sensibles » seraient conservés en infonuagique gouvernementale (environ 20 %) tandis que les données jugées moins critiques (80 %) seraient stockées chez des fournisseurs privés⁶⁸.

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 contrat⁶⁹. Le cas échéant, les données des Québécois-es seraient à la merci de la législation américaine, notamment le *CLOUD ACT*⁷⁰ et le *Foreign Intelligence Surveillance Act*⁷¹.

Le ministre délégué à la Transformation numérique gouvernementale, Éric Caire, a dit vouloir contrer cette menace par le biais de clauses contractuelles; la firme décrochant le contrat d’hébergement devrait garantir

⁶⁵ Barreau du Québec. Groupe de travail sur la protection des données personnelles, *op.cit.*, p. 5.

⁶⁶ Articles 27 et 103 du PL 64.

⁶⁷ « Cette évaluation devra tenir compte de la sensibilité du renseignement; de la finalité de son utilisation; des mesures de protection dont le renseignement bénéficierait; du régime juridique applicable dans l’État où ce renseignement serait communiqué, notamment son degré d’équivalence par rapport aux principes de protection des renseignements personnels applicables au Québec », Article 70.1 LAI et 17 LPRPSP.

⁶⁸ Jocelyne Richer, « Gestion informatique: Québec confiera le stockage de ses données au privé », *Le Soleil*, 4 février 2019, <https://www.lesoleil.com/actualite/politique/gestion-informatique-quebec-confiera-le-stockage-de-ses-donnees-au-privé-2d427ed8ae2b430b7772a88f62d9cfce>

⁶⁹ Michel Girard, « Legault, Caire et Dubé dans les nuages », *Journal de Montréal*, 1^{er} juin 2019, « Confier au secteur privé l’hébergement des données gouvernementales représente évidemment une mine d’or pour les géants de l’infonuagique (cloud computing), tels IBM, Amazon, Microsoft, Google ou autres multinationales du merveilleux monde de l’Internet. Ce sont eux, les géants de l’informatique, qui ont les moyens de répondre aux appels d’offres en cette matière », <https://www.journaldemontreal.com/2019/06/01/legault-caire-et-dube-dans-les-nuages>

⁷⁰ Clarifying Lawful Overseas Use of Data Act (*CLOUD Act*)

⁷¹ « Ottawa estime que le principal risque pour la souveraineté des données canadiennes est la loi américaine sur la surveillance des renseignements étrangers (Foreign Intelligence Surveillance Act) et le pouvoir de Washington d’obliger une organisation soumise à la loi américaine à remettre des données qu’elle détient, peu importe l’emplacement des données et sans en informer le Canada », La Presse canadienne, « Inquiétudes face au transfert de données de Statistique Canada sur l’infonuagique », *Radio-Canada*, 12 janvier 2020, <https://ici.radio-canada.ca/nouvelle/1469886/infonuagique-statistique-canada-questions-securite-donnees>

que les données bénéficieront d'un niveau de protection équivalent à celui prévu à la LAI. Cette solution est d'une portée limitée, car, comme le rappelle le CPVP, « ...aucun contrat ne peut avoir préséance sur les lois d'une autre administration. Les ententes contractuelles (...) n'offrent donc qu'une protection limitée contre une loi étrangère qui est incompatible avec leurs dispositions⁷² ».

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-Unis⁷³. **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.**⁷⁴

On peut se demander ce qui adviendra de la communication de RP à des organismes ou entreprises américaines compte-tenu de cette décision? Ce pays apparaîtra-t-il malgré tout à la liste d'États disposant d'un « régime équivalant de protection » ?

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.

7. Biométrie

La reconnaissance faciale offre un bel exemple des risques que présente le développement incontrôlé et chaotique de systèmes basés sur l'IA. Certains corps policiers utilisent ou auraient déjà utilisé cette technologie au pays⁷⁵. Le Service de police de la Ville de Montréal déclarait récemment ne pas l'utiliser, ajoutant qu'il pourrait y avoir recours en mandatant un tiers⁷⁶!

Les photos utilisées pour mettre au point la plus connue de ces applications proviendraient des réseaux sociaux⁷⁷. La reconnaissance faciale servirait aussi dans certains centres commerciaux à des fins de marketing⁷⁸. La commercialisation de cette technologie pourrait s'étendre bientôt à d'autres secteurs⁷⁹.

Il est à souligner que cette technologie de reconnaissance des individus n'est pas que « faciale », elle s'intéresse autant à l'allure, au comportement ou à l'habillement des personnes surveillées. Les individus ne sont pas tant

⁷² Commissariat à la protection de la vie privée, « Consultation sur la circulation aux fins de traitement – Document de discussion révisé », avril 2019, <https://www.priv.gc.ca/fr/a-propos-du-commissariat/ce-que-nous-faisons/consultations/consultations-terminees/consultation-sur-les-transferts-aux-fins-de-traitement/>

⁷³ C-311/18, Data Protection Commissioner c. Facebook Ireland Ltd and Maximilian Schrems (l'arrêt Schrems II). Voir https://edpb.europa.eu/news/news/2020/statement-court-justice-european-union-judgment-case-c-31118-data-protection_en

⁷⁴ BLG avocats, Perspectives, « L'arrêt « Schrems II » : répercussions sur les ententes impliquant le traitement de données à caractère personnel en dehors de l'EEE », 30 juillet 2020, <https://www.blg.com/fr/insights/2020/07/schrems-impacts-on-agreements-involving-processing-personal-data>

⁷⁵ 3 Gagnon, Charles-Antoine, « Le SPO a déjà expérimenté un outil de reconnaissance faciale », *Le Droit*, 24 février 2020, <https://www.ledroit.com/actualites/justice-et-faits-divers/le-spo-a-deja-experimente-un-outil-de-reconnaissance-faciale-c42e84e649af176165e20eb536123117>

⁷⁶ « L'organisation n'exclut toutefois pas, dans des situations particulières et exceptionnelles, de recourir aux services d'une tierce partie possédant ce type de technologie pour faire avancer une enquête d'envergure, en s'assurant toujours de mener ses opérations et ses enquêtes dans le respect de toutes les lois en vigueur », 24H Montréal, « Reconnaissance faciale: Les élus obtiennent une réponse du SPVM... après six mois », 30 juin 2020, <https://www.24heures.ca/2020/06/29/reconnaissance-faciale--les-elus-obtiennent-une-reponse-du-spvm-apres-six-mois>

⁷⁷ « Google, Facebook et Twitter mettent en demeure Clearview AI », *Radio-Canada*, 6 février 2020, <https://ici.radio-canada.ca/nouvelle/1509484/clearview-ai-intelligence-artificielle-reconnaissance-faciale>

⁷⁸ Pierre Couture, « Reconnaissance faciale : les consommateurs épiés à leur insu dans les commerces », *Journal de Québec*, 11 mai 2019, <https://www.journaldequebec.com/2019/05/11/souriez-on-vous-surveille-par-la-reconnaissance-faciale>

⁷⁹ Marie-Claude Malboeuf et Fanny Lévesque, « Reconnaissance faciale: indignation et inquiétude à Québec et à Ottawa », *La Presse*, 28 février 2020, <https://www.lapresse.ca/actualites/politique/2020-02-28/reconnaissance-faciale-indignation-et-inquietude-a-quebec-et-a-ottawa>

ciblés pour ce qu'ils font que pour ce qu'ils sont. Cette surveillance est d'autant plus inquiétante alors que certains groupes racisés sont victimes de discrimination systémique de la part des forces policières. Les auteurs d'un rapport de 2019 sur les interpellations policières à Montréal écrivaient :

Aussi, il faut tenir compte du fait que le profilage criminel, fondé sur la prédiction, s'appuie sur des éléments liés directement ou indirectement à l'appartenance « raciale » (la couleur de peau, certes, mais également l'habillement, la démarche, la gestuelle corporelle ou tout simplement le lieu de résidence), ce qui peut avoir pour effet d'accentuer les disparités raciales existantes. C'est pourquoi il est nécessaire de dévoiler et de comprendre les forces structurelles et systémiques qui encouragent la production de discriminations raciales⁸⁰.

Ces outils de surveillance battent en brèche le droit à la vie privée et à l'anonymat, tout en rendant possible le profilage discriminatoire. Ils semblent pourtant se développer sans contrôle, malgré l'existence au Québec de certaines balises légales⁸¹ qui sont, de toute évidence, inefficaces ou non respectées.

Le CPVP et les commissaires de quelques provinces viennent de lancer une enquête pancanadienne soulignant leurs « préoccupations croissantes quant à l'utilisation de la reconnaissance faciale⁸² ». La situation est telle que même les géants du Web réclament maintenant des balises légales⁸³.

Ce dossier met en lumière l'urgence de revoir l'encadrement légal sur cette question⁸⁴. Pourtant le PL 64 effleure à peine le sujet. Tout au plus modifie-t-il l'article 45 de la Loi concernant le cadre juridique des technologies de l'information; un préavis de soixante jours à la CAI s'appliquera désormais avant la mise en service d'une banque de caractéristiques ou de mesures biométriques. Actuellement, aucun délai de divulgation n'est fixé.

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.

8. Notification obligatoire d'incident de confidentialité des données⁸⁵

Tout incident de confidentialité présentant un risque de préjudice sérieux devra être signalé à la CAI. La personne concernée devra aussi en être avisée. **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.**

⁸⁰ Armony, Victor et al., « Les interpellations policières à la lumière des identités racisées, Analyse des données du Service de Police de la Ville de Montréal (SPVM) et élaboration d'indicateurs de suivi en matière de profilage racial, Rapport final remis au SPVM », août 2019, p. 8, https://spvm.qc.ca/upload/Rapport_Armony-Hassaoui-Mulone.pdf

⁸¹ L'article 45 de la Loi concernant le cadre juridique des technologies de l'information (L.R.Q. c. C-1.1) prévoit : « La création d'une banque de caractéristiques ou de mesures biométriques doit être préalablement divulguée à la Commission d'accès à l'information. De même, doit être divulguée l'existence d'une telle banque qu'elle soit ou ne soit pas en service. La Commission peut rendre toute ordonnance concernant de telles banques afin d'en déterminer la confection, l'utilisation, la consultation, la communication et la conservation y compris l'archivage ou la destruction des mesures ou caractéristiques prises pour établir l'identité d'une personne. La Commission peut aussi suspendre ou interdire la mise en service d'une telle banque ou en ordonner la destruction, si celle-ci ne respecte pas ses ordonnances ou si elle porte autrement atteinte au respect de la vie privée ».

⁸² Malboeuf et Lévesque, *op.cit.*

⁸³ Agence France-Presse, « Microsoft refuse à la police l'accès à sa technologie de reconnaissance faciale », *Le Devoir*, 12 juin 2020, « Lors d'un discours à Bruxelles, Sundar Pichai, le patron du groupe, avait expliqué que Google ne fournirait pas de service clé en main de reconnaissance faciale tant que des règles et garde-fous n'étaient pas mis en place par les autorités », <https://www.ledevoir.com/monde/etats-unis/580704/microsoft-refuse-a-la-police-l-acces-a-sa-technologie-de-reconnaissance-faciale>

⁸⁴ *Ibid.* « Pour Dominic Martin, spécialiste de l'éthique de l'intelligence artificielle et de la gestion de l'éthique en entreprise, « il faut fixer les conditions d'utilisation et instaurer des moyens de contrôle, parce que la reconnaissance faciale a le potentiel de mener à des écarts éthiques importants ». Le professeur Pierre Trudel note quant à lui : « Le potentiel d'intrusion est considérable. Le législateur doit courir pour faire du rattrapage, car il y a un défaut affligeant d'encadrement. »

⁸⁵ Articles 14 et 95 du PL 64.

Cela 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. Sans compter que celles-ci sont souvent les mieux placées pour agir en vue de limiter les dégâts.

Depuis des années, les fuites de RP se multiplient au Québec et au Canada : Desjardins, Capital One, Revenu Québec, Industrielle Alliance, Trans Union, Équifax, ministère de l'Éducation, RAMQ, etc. 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 prévention⁸⁶.

Le projet de loi répond à ce fléau par une hausse substantielle des sanctions pénales⁸⁷, l'attribution à la CAI d'un pouvoir d'ordonnance provisoire, d'un droit de poursuite en matière pénale⁸⁸ et du pouvoir d'infliger des sanctions administratives sévères en cas d'infraction à la loi⁸⁹. 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.

Le verrou de sécurité, prévu par le projet de loi 53⁹⁰ et permettant aux consommateurs et consommatrices de bloquer les informations contenues dans leur dossier aux agences de crédit, est une autre mesure importante. Ce verrou doit être accessible gratuitement.

Un débat s'impose par ailleurs en vue d'établir des modes d'identification et d'authentification des personnes qui soient à la fois sécuritaires et respectueux des droits humains⁹¹.

Finalement, le PL64 énonce expressément un droit de poursuite civile pour le préjudice résultant d'une atteinte illicite à un droit conféré par la loi⁹². Cela pourrait faciliter les recours collectifs en cas de fuite de renseignement et autres bris de confidentialité. Une difficulté majeure demeure toutefois : la preuve d'un préjudice. Un vol d'identité ou une fuite de renseignements engendrent des risques, mais qui ne se réaliseront souvent que beaucoup plus tard. Il peut donc devenir ardu de prouver un lien entre l'incident de sécurité et le dommage⁹³.

⁸⁶ Vérificatrice générale du Québec, « Rapport du Vérificateur général du Québec à l'Assemblée nationale pour l'année 2020-2021 », juin 2020, « Le contrôle des activités du personnel de la RAMQ et de Retraite Québec ayant des accès informatiques privilégiés est insuffisant par rapport à l'importance de ces accès et aux conséquences possibles d'une mauvaise utilisation de ceux-ci », https://www.vgq.qc.ca/Fichiers/Publications//rapport-annuel//163/vgq_tome-juin2020_ch02_web.pdf

Voir aussi concernant les fuites à Revenu Québec <https://www.journaldequebec.com/2019/08/10/donnees-personnelles-on-est-mal-barre>

⁸⁷ « Ainsi, une personne morale qui contrevient à la loi est passible d'une amende de 15 000 \$ à 25 000 000 \$ ou du montant correspondant à 4 % du chiffre d'affaires mondial de l'exercice financier précédent si ce dernier montant est plus élevé », Article 91 LPRPSP.

⁸⁸ Article 92 LPRPSP.

⁸⁹ La CAI serait habilitée à imposer des sanctions d'un montant maximum de 10 000 000 \$ ou, si ce montant est supérieur, le montant correspondant à 2 % du chiffre d'affaires mondial de l'exercice financier précédent.

⁹⁰ Projet de loi n° 53, Loi sur les agents d'évaluation du crédit. Article 90.12 LPRPSP

<http://www.assnat.qc.ca/fr/travaux-parlementaires/projets-loi/projet-loi-53-42-1.html?appelant=MC>

⁹¹ « On est encore dépendant du numéro d'assurance sociale et de sa date de naissance ; [les gens] peuvent ouvrir un compte en banque avec ces informations-là, on l'a encore vu récemment avec la vague de fraudes de la Prestation canadienne d'urgence », citation d'Éric Parent, PDG de la firme de cybersécurité EVA Technologies dans *La Presse*, « Vol de données chez Desjardins, la catastrophe, un an trop tard », 19 juin 2020, <https://www.lapresse.ca/affaires/entreprises/2020-06-19/vol-de-donnees-chez-desjardins-la-catastrophe-un-an-plus-tard>

⁹² Article 152 du PL 64 : « 93.1 à moins que le préjudice ne résulte d'une force majeure, la personne qui exploite une entreprise qui conserve un renseignement personnel est tenue de la réparation du préjudice résultant d'une atteinte illicite à un droit conféré par la présente loi ou par les articles 35 à 40 du Code civil. En outre, lorsque l'atteinte est intentionnelle ou résulte d'une faute lourde, le tribunal accorde des dommages-intérêts punitifs d'au moins 1 000 \$ ».

⁹³ « En effet, s'il est établi en jurisprudence qu'un demandeur n'a pas besoin de démontrer avoir été personnellement victime d'un vol d'identité pour intenter une action, il faut tout de même que celle-ci vise un dommage indemnifiable. Or, la possession non autorisée de renseignements personnels par des tiers ne constitue pas en soi un tel préjudice, non plus que des dommages futurs,

9. 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. Le consentement peut impliquer le dévoilement de la vie privée de tiers. Et l'utilisation massive de données servir à la manipulation politique. Comme le souligne à juste titre l'auteur Philippe de Grosbois : « [...] C'est en envisageant la protection de la vie privée comme un enjeu collectif plutôt que comme le fruit d'ententes individuelles qu'il sera véritablement possible d'avancer⁹⁴ ».

Le PL64 ne répond pas à cette problématique.

Transparence et reddition de compte

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. Le professeur Pierre Trudel note à cet égard : « Hormis des obligations de surmultiplier les mentions et « conditions d'utilisation », les lois n'imposent pratiquement pas d'exigences de transparence et de reddition de comptes quant à la façon dont les entreprises génèrent de la valeur avec les données de tout un chacun⁹⁵ ».

Le Groupe de travail sur la protection des données personnelles du Barreau du Québec résume bien les défauts de l'approche individuelle à l'ère du Big-data :

[...] la création de valeurs par le truchement de procédés d'analyse des gisements massifs de données (Big data) peut engendrer des risques aussi bien pour les individus que pour l'ensemble de la collectivité. De tels enjeux ne sauraient être pris en charge simplement en faisant consentir en amont tous ceux qui, consciemment ou non, produisent des données. (...) Il faut une réglementation conséquente avec les caractéristiques inhérentes des traitements massifs de données⁹⁶.

L'utilisation de l'IA à des fins décisionnelles soulève aussi des enjeux collectifs⁹⁷. De nombreux cas prouvent que des vices de conception ou l'utilisation de données historiquement biaisées peuvent conduire l'algorithme à reproduire, voire aggraver, des attitudes et comportements discriminatoires⁹⁸. Selon AccessNow, ces biais seraient la règle plutôt que l'exception⁹⁹.

Un exemple des risques que présente la décision automatisée nous est venu récemment du Royaume-Uni. En raison de la pandémie, des milliers d'étudiant-e-s n'ont pu passer leur examen de fin d'année. Un algorithme a été chargé d'attribuer une note présumée aux élèves. Devant des résultats biaisés, favorisant les élèves en

hypothétiques ou de peu de gravité », Philippe Buist, « Fuite de renseignements personnels : pourquoi Equifax s'en tire-t-elle à bon compte? », *Le blogue SOQUIJ*, 14 novembre 2019, <https://blogue.soquij.qc.ca/2019/11/14/autorisations-dactions-collectives-en-matiere-de-fuites-de-renseignements-personnels-frequentes-mais-pas-automatiques/>

⁹⁴ de Grosbois, Philippe, « Les batailles d'Internet : assauts et résistances à l'ère du capitalisme numérique », 2018, p.156.

⁹⁵ Pierre Trudel, « Renseignements personnels: les vraies urgences », *Le Devoir*, 18 février 2020, <https://www.ledevoir.com/opinion/chroniques/573151/renseignements-personnels-les-vraies-urgences>

⁹⁶ Barreau du Québec. Groupe de travail sur la protection des données personnelles, « RÉFLEXION SUR UNE RÉFORME DE L'ACCÈS À L'INFORMATION ET DE LA PROTECTION DES DONNÉES PERSONNELLES », <https://www.barreau.qc.ca/media/1667/rapport-reflexion-acces-information-protection-donnees.pdf>

⁹⁷ « Pour demeurer compatibles avec le respect des droits fondamentaux, les processus d'évaluation des personnes doivent reposer sur de solides garanties de transparence et de reddition de comptes », Pierre Trudel, « En Chine et ici », *Le Devoir*, 8 octobre 2019, <https://www.ledevoir.com/opinion/chroniques/564299/le-credit-social-en-chine-et-ici>

⁹⁸ Nathalie Collard, « Nos robots seront-ils machos? », *La Presse*, 29 mai 2019, <https://www.lapresse.ca/societe/201905/29/01-5227959-nos-robots-seront-ils-machos.php>

⁹⁹ « Unfortunately, biased data and biased parameters are the rule rather than the exception. Because data are produced by humans, the information carries all the natural human bias within it », Access Now, "Human rights in the age of artificial intelligence", novembre 2018, p.12, <https://www.accessnow.org/cms/assets/uploads/2018/11/AI-and-Human-Rights.pdf>

provenance des écoles privées, le gouvernement a dû annuler l'exercice et s'en remettre aux estimations des professeurs pour la notation¹⁰⁰.

Les algorithmes de personnalisation peuvent conduire les individus à s'enfermer dans leurs certitudes et miner la capacité de mener des débats publics éclairés. La « quantification de soi » et autres capteurs de données personnelles peuvent compromettre les principes de mutualisation des risques (en assurances notamment) et de solidarité sociale. Les chambres d'écho¹⁰¹ des réseaux sociaux peuvent, quant à elles, amoindrir la circulation de l'information et la diversité d'opinions et mener à de la manipulation. En outre, des algorithmes mal calibrés peuvent entretenir - voire aggraver - des pratiques discriminatoires.

Cela démontre l'importance de la transparence dans l'utilisation des algorithmes. Leur fonctionnement logique devrait être divulgué publiquement et de façon proactive. C'est ce que la Commission nationale de l'informatique et des libertés inclut dans le principe de loyauté :

[...] alors que dans la loi Informatique et Libertés, l'information est un droit qui peut éventuellement être mobilisé par l'individu auprès du responsable de l'algorithme, avec le principe de loyauté, cette information doit d'emblée être diffusée à destination de la communauté des utilisateurs. Il n'est pas question ici de droit des utilisateurs, mais d'obligation des plateformes algorithmiques. Dans cette mesure, la loyauté semble à même de constituer une réponse au problème de l'asymétrie entre les responsables des algorithmes et les utilisateurs¹⁰².

Un système d'audit indépendant pourrait garantir que les algorithmes utilisés respectent la loi et sont exempts de biais discriminatoires¹⁰³.

Bien collectif

Les données que détiennent les organismes publics et les ministères constituent un bien collectif : « Par exemple, les données massives produites par l'ensemble des faits et gestes survenant dans notre système de santé sont des ressources collectives. En postulant que la valeur qu'elles permettent de générer revient à l'entreprise qui obtient le « consentement libre et éclairé » des individus, on dépossède la collectivité d'une ressource essentielle¹⁰⁴ ».

Ce bien collectif suscite la convoitise. Les GAFAM (Google, Apple, Facebook, Amazon, Microsoft), de même que d'autres entreprises pharmaceutiques et technologiques investissent de plus en plus le domaine médical¹⁰⁵.

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

¹⁰⁰ Radio-France international, « Royaume-Uni: face à la fronde, le gouvernement recule sur la notation du baccalauréat », 19 août 2020, <https://www.rfi.fr/europe/20200819-royaume-uni-face-fronde-gouvernement-recule-notation-bac>

¹⁰¹ « Quant aux « chambres d'écho », ce sont des amplificateurs, des « bulles de filtrage » qui font qu'un individu n'est exposé qu'à certaines informations auxquelles il adhère a priori », Antoine Char, « Anatomie des fausses nouvelles dans le cyberspace », *Le Devoir*, 12 janvier 2019. <https://www.ledevoir.com/opinion/idees/545373/anatomie-des-fausses-nouvelles-dans-le-cyberspace>

¹⁰² CNIL, « Comment permettre à l'Homme de garder la main ? Rapport sur les enjeux éthiques des algorithmes et de l'intelligence artificielle », 15 décembre 2017, p.50. <https://www.cnil.fr/fr/comment-permettre-lhomme-de-garder-la-main-rapport-sur-les-enjeux-ethiques-des-algorithmes-et-de>

¹⁰³ *Ibid.* « Développer l'audit des algorithmes de manière à contrôler leur conformité à la loi et leur loyauté est une solution fréquemment évoquée pour assurer leur loyauté, leur responsabilité et, plus largement, leur conformité à la loi ».

¹⁰⁴ Pierre Trudel, « La valeur de nos données de santé », *Le Devoir*, 25 août 2020, <https://www.ledevoir.com/opinion/chroniques/584714/la-valeur-de-nos-donnees-de-sante>

¹⁰⁵ « Partenariats avec des établissements hospitaliers, mise à disposition d'infrastructures cloud, développement d'appli santé embarquées dans les enceintes et montres connectées... Les initiatives stratégiques dans le secteur de la santé se multiplient parmi les acteurs leaders de l'économie numérique et des fournisseurs d'infrastructures informatiques », *Mydigitalweek*, « LES STRATÉGIES DES GAFAM ET DES BIGTECH DANS LA SANTÉ », 22 février 2020, <https://mydigitalweek.com/les-strategies-des-gafam-et-des-bigtech-dans-la-sante/>

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 privée¹⁰⁶ ».

La déclaration récente du ministre de l'Économie et de l'Innovation, M. Fitzgibbon, est pour le moins préoccupante. Qualifiant de mine d'or les données que détient la Régie de l'assurance maladie du Québec (RAMQ), il ajoutait que « La stratégie du gouvernement, c'est carrément de vouloir attirer les pharmas, quelques pharmas, à venir jouer dans nos platebandes, profiter de ça. Et je pense qu'on a une chance incroyable d'y arriver¹⁰⁷ ».

Cette annonce du ministre 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 commun¹⁰⁸. Comme l'affirment des chercheurs des secteurs public et universitaire: « [...] des balises sont nécessaires, et face aux récentes dérives d'usages inappropriés des données par des entreprises privées (ex. Cambridge Analytica), la rhétorique aveugle de l'accès ubiquitaire, ou libre accès, aux données personnelles convient de moins en moins, plus particulièrement si la compréhension de la notion de bien commun n'est pas partagée socialement ».

Conclusion

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 que dans le reste du 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*¹⁰⁹ ».

L'essor du modèle économique fondé sur la surveillance a conduit deux entreprises (Google et Facebook) à contrôler une architecture de surveillance sans précédent dans l'histoire de l'humanité. (...) le modèle économique fondé sur la surveillance est incompatible avec le droit à la vie privée et constitue une menace grave pour une série d'autres droits humains¹¹⁰.

Les géants du Web (GAFAM : Google, Apple, Facebook, Amazon, Microsoft) ne sont du reste plus seuls sur la patinoire; de nombreuses autres entreprises adoptent aujourd'hui ce modèle d'affaires : « ... des annonceurs aux courtiers en données, en passant par les start-up et les entreprises en dehors du secteur technologique qui cherchent à développer ou à réorienter leurs activités pour monétiser les données personnelles¹¹¹ ». Cette logique de surveillance et d'extraction de données s'étend maintenant au monde réel par le biais des objets connectés¹¹². Un rapport soumis en 2014 au Forum économique mondial indiquait :

¹⁰⁶ Organisation des Nations Unies, Soixante-quatorzième session, 36e & 37e séances plénières, matin & après-midi. 29 octobre 2019. « Troisième Commission: le respect des données médicales et le versement de réparations pour l'esclavage dominant le débat », <https://www.un.org/press/fr/2019/agshc4276.doc.html>

¹⁰⁷ Bernard Barbeau, « Les données de la RAMQ pour appâter les pharmaceutiques », *Radio-Canada*, 20 août 2020, <https://ici.radio-canada.ca/nouvelle/1728106/pierre-fitzgibbon-compagnies-pharmaceutiques-donnees-medicales-mila>

¹⁰⁸ Ces chercheurs notent aussi : « Pour les chercheurs du secteur public et des universités, où la recherche est valorisée, le bien commun vise notamment à favoriser le bien-être et la santé des citoyens. Il vise également le maintien d'une société libre et démocratique, où il y a un juste équilibre entre l'intérêt personnel et collectif, en permettant de concilier vie privée et recherche en santé publique », Louise Ringuette, Bryn Williams-Jones, Victoria Doudenkova, « Au nom du bien commun, vos renseignements de santé peuvent être utilisés sans votre consentement », *The conversation*, 25 avril 2019, <https://theconversation.com/au-nom-du-bien-commun-vos-renseignements-de-sante-peuvent-etre-utilises-sans-votre-consentement-114267>

¹⁰⁹ Shoshana Zuboff, « Un capitalisme de surveillance », *Le Monde diplomatique*, janvier 2019, <https://www.monde-diplomatique.fr/2019/01/ZUBOFF/59443>

¹¹⁰ Amnistie internationale, « LES GÉANTS DE LA SURVEILLANCE LE MODÈLE ÉCONOMIQUE DE FACEBOOK ET GOOGLE MENACE LES DROITS HUMAINS (EXTRAITS) », 2019, <https://www.amnesty.org/download/Documents/POL3014042019FRENCH.pdf>

¹¹¹ *Ibid.*

¹¹² « De la bouteille de vodka « intelligente » au thermomètre rectal connecté, les produits destinés à interpréter, suivre, enregistrer et communiquer des données prolifèrent ». Shoshana Zuboff, *op.cit.*

What did we search for? What did we read? Where did we go? With whom do we associate? What do we eat? What do we purchase? In short, almost any imaginable human interaction can be captured and studied within the realm of big data¹¹³.

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 socialisée¹¹⁴ ». Un encadrement s'impose 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.

¹¹³ Beñat Bilbao-Osorio, Soumitra Dutta et Bruno Lanvin, « The Global Information Technology Report 2014. Rewards and Risks of Big Data », World economic Forum, 2014, http://www3.weforum.org/docs/WEF_GlobalInformationTechnology_Report_2014.pdf

¹¹⁴ Pierre Henrichon, « Big Data : Faut-il avoir peur de son nombre? », 2020, p.180.

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 paraît 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'entière 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 déferencement 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.