CI-134
2021-02-02
S. Mekki

Commission de l'éthique en science et en technologie
Québec

MÉMOIRE DE LA COMMISSION DE L'ÉTHIQUE EN SCIENCE ET EN TECHNOLOGIE

Consultations particulières sur le projet de loi nº 64, Loi modernisant des dispositions législatives en matière de protection des renseignements personnels

Présenté à la Commission des institutions
Assemblée nationale du Québec

Octobre 2020

Document préparé par
Jocelyn Maclure, D.Phil., président, CEST
Dominic Cliche, M.A., conseiller en éthique, CEST
Nathalie Torrès-Parent, B.A., conseillère en éthique, CEST

Direction
Sylvain Pelletier, M.A., secrétaire général, CEST

Commission de l'éthique en science et en technologie
888, rue Saint-Jean, bureau 555
Québec, QC
G1R 5H6
www.ethique.gouv.qc.ca

Table des matières

Présentation de la Commission de l'éthique en science et en technologie

La Commission de l'éthique en science et en technologie (CEST) est un organisme du gouvernement du Québec placé sous la responsabilité du ministre de l'Économie et de l'Innovation. Elle est composée de 13 membres, dont un président, nommés par le gouvernement.

Sa mission est de conseiller le ministre sur toute question relative aux enjeux éthiques liés à la science et à la technologie, ainsi que de susciter la réflexion sur ces enjeux éthiques. De façon générale, ses activités visent à informer, à sensibiliser et à organiser des débats autour des enjeux éthiques en science et en technologie. La CEST propose également des orientations susceptibles de guider les acteurs concernés dans leur prise de décision.

Contexte

Le projet de loi n^{o} 64, Loi modernisant des dispositions législatives en matière de protection des renseignements personnels, propose une mise à jour depuis longtemps attendue de l'encadrement visant à protéger la vie privée des Québécois. En effet, l'encadrement actuel repose sur des lois adoptées dans les années 1980 et 1990, qui s'avèrent mésadaptées au nouveau contexte généré par le développement rapide et l'adoption massive des technologies numériques. Pensons aux plateformes commerciales ou de prestation de services sur Internet, mais aussi à l'utilisation d'algorithmes d'intelligence artificielle et au traitement de données massives. C'est l'ensemble du cycle de vie des données qui est modifié par ce que certains appellent la « révolution numérique », ce qui ouvre sur de nouveaux risques et soulève de nouveaux enjeux : comment tirer parti des possibilités qu'ouvre l'analyse de grands ensembles de données tout en préservant la vie privée, l'autonomie et l'intégrité des personnes? Peut-on garantir l'anonymisation des données? Le consentement manifeste, libre, éclairé, spécifique et continu demeure-t-il l'outil privilégié pour assurer la collecte et l'usage acceptables et responsables des données portant sur les individus?

Dans le cadre de son avis *La ville intelligente au service du bien commun : lignes directrices pour allier l'éthique au numérique dans les municipalités au Québec,* la CEST formulait d'ailleurs comme recommandation que le gouvernement du Québec profite du renouvellement de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels et de la Loi sur la protection des renseignements personnels dans le secteur privé pour aborder les questions soulevées par l'utilisation des nouvelles technologies numériques par les administrations publiques[1].

[1] CEST (2017). La ville intelligente au service du bien commun : lignes directrices pour allier l'éthique au numérique dans les municipalités au Québec, gouvernement du Québec, p. 57. [En ligne] https://www.ethique.gouv.qc.ca/media/1043/ville_intelligente_a.pdf

Formulant le constat que la collecte et le traitement de données massives soulève en de nouveaux termes la question du consentement, la CEST soulevait une série de questions, tout aussi pertinentes dans le cadre d'une réflexion sur le projet de loi nº 64 :

- Est-il possible de réunir les conditions d'un consentement libre, éclairé et donné à des fins spécifiques pour des données collectées massivement et automatiquement?
- Les données fournies volontairement ou activement par les personnes le sont-elles suivant un consentement véritablement libre, éclairé et donné à des fins spécifiques? Pensons aux conditions d'utilisation et aux politiques de confidentialité, très longues et souvent difficiles à comprendre, que plusieurs acceptent sans lire, d'un simple clic.
- Est-il suffisant d'obtenir le consentement des personnes ou devrait-il y avoir d'autres mécanismes en place pour assurer l'acceptabilité de la collecte et du traitement des données?
- Plus on a recours aux données massives, plus elles sont d'emblée collectées dans l'optique d'un usage non initialement prévu, agrégées entre elles, soumises au forage (*data mining*), etc. C'est d'ailleurs l'un des éléments qui rendent les données massives attrayantes : la possibilité d'interroger de grands ensembles de données et de faire se recouper des données *a priori* disparates pour générer des connaissances nouvelles. Quelles devraient être les responsabilités des administrations publiques pour assurer l'équilibre entre les bénéfices organisationnels et sociaux, d'une part, et les droits et libertés individuels, d'autre part?
- Quelles fins seront jugées légitimes, notamment pour l'utilisation de ces données aux fins de conception et d'évaluation des politiques publiques?

Analyse

La CEST salue l'effort considérable réalisé par gouvernement par le dépôt du projet de loi nº 64 pour procéder à cette mise à jour, par exemple par le renforcement des pouvoirs de la Commission d'accès à l'information; par des pratiques plus claires concernant la communication des finalités présidant à la collecte et à l'utilisation de renseignements personnels; par l'ajout d'obligations relatives à la divulgation des incidents de confidentialité; par une meilleure définition de ce qui constitue un renseignement de nature sensible; par une meilleure prise en charge des enjeux soulevés par les projets de système d'information ou de prestation électronique de services, par les technologies permettant d'identifier, de localiser ou d'effectuer un profilage d'une personne, et par les systèmes permettant la prise de décision fondée sur un traitement automatisé des données.

En matière de gouvernance, prévoir la formation d'un comité sur l'accès à l'information et la protection des renseignements personnels ainsi qu'obliger la production d'une

évaluation des facteurs relatifs à la vie privée (EFVP) s'avèrent des pistes judicieuses pour renforcer un usage responsable des données.

Toutefois, des éléments du projet de loi soulèvent certains enjeux éthiques, qui sont examinés dans ce mémoire. La question sous-jacente à ces enjeux est celle de la conciliation des avantages associés à une plus grande mobilité des données, pour l'amélioration des services publics ou pour alimenter la recherche scientifique par exemple, avec une protection suffisante des renseignements personnels et de la vie privée. De manière plus spécifique, la CEST souhaite encourager les membres de la Commission des institutions à :

- Explorer la possibilité d'établir un régime particulier pour la recherche scientifique à des fins servant des intérêts collectifs;
- Affirmer le rôle du consentement comme mécanisme de régulation la plupart du temps *nécessaire*, mais *non suffisant* de la collecte, du partage et de l'utilisation des renseignements personnels;
- Remettre en question la dichotomie entre les renseignements personnels (identificatoires) et les autres renseignements pris en bloc, au regard des risques de réidentification des individus à partir de renseignement anonymisés ou dépersonnalisés et au regard des possibles usages illégitimes des renseignements, qu'il s'agisse de renseignements personnels ou non;
- Considérer d'inclure dans la loi un statut pour les renseignements inférés; et
- Réfléchir à la possibilité de définir plusieurs régimes d'encadrement des renseignements, à caractère personnel ou non, sur la base des types de renseignement et des finalités des usages qui peuvent en être fait.

1. Devrait-il y avoir un régime juridique particulier pour encadrer le partage et l'utilisation de renseignements personnels pour la recherche scientifique servant des intérêts collectifs?

Les lois actuelles protégeant les renseignements personnels font déjà, à juste titre, une distinction entre les organismes publics et privés. Dans un contexte où il convient d'explorer les façons dont une meilleure valorisation des données peut servir l'intérêt collectif, il apparaît judicieux de permettre d'abord à des institutions publiques, dont la mission est de contribuer à l'atteinte du bien commun, d'avoir un meilleur accès aux données. Le monde de la recherche scientifique universitaire est sans doute le milieu qui est le mieux positionné pour mettre à l'épreuve un nouveau cadre permettant à la fois la valorisation des données et la protection de la vie privée. D'une part, la recherche scientifique réalisée dans les établissements d'enseignement supérieur contribue au bien commun et est fortement encouragée par les pouvoirs publics. D'autre part, puisque les projets de recherche qui impliquent des sujets humains doivent être approuvés par un comité d'éthique de la recherche et, dans certains cas, par la Commission d'accès à l'information, le monde de la recherche universitaire a déjà une longue expérience en

matière d'application de règles visant la protection de la vie privée[2]. Comme le professeur de droit Pierre-Luc Déziel l'a affirmé lors de son audition devant la Commission des institutions[3], il serait opportun d'étudier la possibilité de créer un régime juridique spécifique pour encadrer le partage et l'utilisation de renseignements personnels à des fins de recherche scientifique. Cette expérience pourrait être riche en enseignements pour l'encadrement de l'accès aux données à la fois pour d'autres organismes publics et pour des entreprises privées.

Si une telle proposition était retenue, l'examen et le respect des normes encadrant les partenariats entre les chercheurs et l'industrie seraient nécessaires. Il serait aussi sage que le législateur mandate des organismes comme les Fonds de recherche du Québec, la Commission d'accès à l'information et la Commission de l'éthique en science et en technologie pour mener une analyse qui aurait pour but de proposer des modifications aux normes de l'éthique de la recherche afin de s'assurer que les projets de recherche n'impliquant pas directement des participants humains, mais posant néanmoins des risques pour la vie privée, soient évalués par des comités d'éthique de la recherche.

2. Le consentement, tel que maintenant balisé à l'intérieur du projet de loi nº 64, est-il en mesure d'assurer la collecte et l'usage acceptables et responsables des données portant sur les individus?

Il est à se demander si le consentement représente à lui seul un levier de protection des citoyens contre divers abus liés à la collecte de renseignements personnels. Certes, assurer le contrôle de l'individu sur ses données importe, ainsi que les conditions permettant d'exercer ce contrôle (information claire et simple à dispenser). Néanmoins, un recours systématique au consentement peut entrainer des effets pervers du fait, par exemple, de la multiplication de politiques de confidentialité à lire pour les individus.

On ne peut pas raisonnablement s'attendre à ce que les individus soient totalement responsables de la protection de leur vie privée et des données qu'ils transmettent. En tant que consommateurs, notamment, ils sont constamment sollicités pour donner leur consentement sur divers sujets. Le consommateur responsable idéal devrait lire attentivement tous ses contrats, toutes les conditions d'utilisation des plateformes, logiciels

---

[2] Conseil de recherches en sciences humaines du Canada, Conseil de recherches en sciences naturelles et en génie du Canada et Institut de recherche en santé du Canada (2018). *Énoncé de politique des trois conseils — EPTC2 : Éthique de la recherche avec des êtres humains*, Gouvernement du Canada, 247 p.
Voir aussi : Commission d'accès à l'information (2016). *Rétablir l'équilibre. Rapport quinquennal 2016*, Gouvernement du Québec, p. 111-120.

[3] *Consultations particulières et auditions publiques sur le projet de loi n° 64, Loi modernisant des dispositions législatives en matière de protection des renseignements personnels*, séance du jeudi 24 septembre 2020.

ou objets numériques qu'il utilise et comprendre tous les termes et tous les énoncés contenus dans ces politiques.

Par exemple, supposons que le consommateur responsable idéal veuille utiliser l'application photo d'une grande compagnie de vente en ligne. S'il est pleinement responsable, il devra lire attentivement un document juridique (rédigé en anglais) et maîtriser tous les termes techniques et légaux contenus dans le document[4]. Si le document compte plus d'une dizaine de pages, il lui faudra au moins une heure pour le lire (mais si le document a un indice de complexité élevé, il pourrait devoir y consacrer plus de temps)[5]. Ensuite, le consommateur responsable idéal pourrait avoir terminé de lire tous ces documents et, s'il accepte les clauses du contrat en toute connaissance de cause, utiliser cette application. Naturellement, dès que les documents juridiques seront mis à jour, le consommateur devra répéter l'exercice.

Cet idéal de la consommation responsable est inefficace et difficilement atteignable. Les consommateurs n'ont pas tous les mêmes connaissances techniques pour lire et comprendre des conditions d'utilisation détaillées. Et ceux qui disposent de ces connaissances ne devraient pas avoir à prendre une part déraisonnable de leur temps pour lire, apprendre et démêler tous les documents juridiques en cause. L'utilité collective l'oblige : la perte de temps et d'énergie résultant de la responsabilisation excessive des consommateurs et des commerçants crée plus de coûts que de bénéfices.

En ce sens, la protection de la vie privée devrait aussi passer par un encadrement des usages acceptables en amont par les autorités publiques. Par exemple, on peut saluer l'insertion dans la Loi sur la protection des renseignements personnels dans le secteur privé de l'article 9.1[6], selon lequel « une personne qui exploite une entreprise et qui recueille des renseignements personnels en offrant un produit ou un service technologique doit s'assurer que, par défaut, les paramètres de ce produit ou de ce service assurent le plus haut niveau de confidentialité, sans aucune intervention de la personne concernée. » Il est toutefois, possible de se questionner concernant la cohérence avec l'article 8.1 (prévu à l'article 99 du projet de loi n^{o} 64) selon lequel un utilisateur doit être informé, au moment de la collecte de ses renseignements personnels, des moyens pour **désactiver** les fonctions d'indentification, de localisation ou de profilage. Une véritable protection de la vie privée par défaut devrait plutôt exiger que ces fonctions soient limitées d'emblées et activées uniquement si le consommateur le désire.

---

[4] Pensons aux les licences logicielles tierces d'Amazon Photos, disponible à cette adresse : https://s3-us-west-2.amazonaws.com/customerdocumentation/Amazon+Photos/Third+Party+Licenses.html (page consultée le 16 avril 2019). Voir aussi Allhoff et Henschke (2018, p. 57).

[5] La complexité des conditions d'utilisation peut être mesurée de différentes manières. Par exemple, Luger, Moran et Rodden (2013) ont proposé un indice de complexité qui prend en compte le nombre de phrases, la longueur moyenne des phrases et le nombre de mots polysyllabiques. Selon cet indicateur, les conditions d'utilisation et les politiques de confidentialité de certaines entreprises sont plus complexes que des ouvrages classiques comme la *Bible*, *Guerre et Paix* ou *Les Misérables*.

[6] Voir l'article 100 du projet de loi no 64.

Ainsi, par-delà le consentement et la responsabilité individuelle, il s'avère judicieux de renforcer la responsabilité des institutions étatiques et des compagnies pour diminuer d'entrée de jeu les risques de préjudices difficiles à réparer. Cette idée peut se concrétiser par l'encadrement du développement même des technologies qui collectent des données. L'idée est d'imprégner leur conception du principe de respect de la vie privée (*privacy by design*). Les institutions étatiques et les entreprises devraient d'ailleurs être contraintes de respecter ce principe. Plus précisément, elles devraient être en mesure de justifier d'éventuelles violations de certains principes, dont la *prévention*, laquelle consiste à anticiper les événements qui peuvent compromettre la vie privée des utilisateurs et prévenir ces problèmes plutôt que de les corriger ou *une protection couvrant tout le cycle d'utilisation,* soit les mesures de protection et de sécurisation des données couvrent tout leur cycle de vie, pour la collecte, l'entreposage et la destruction des données.

À titre d'exemple, il est possible de se pencher sur l'encadrement les objets connectés et communiquant entre eux par l'entremise d'Internet[7]. Voici un exemple de développement numérique qui facilite énormément la collecte d'informations à propos de personnes (ou de groupes sociaux), quel que soit leur emplacement (incluant, notamment, leur domicile) et qui peuvent fournir une description directe de l'utilisateur (comme dans des images ou des enregistrements sonores). Bien que certaines de ces données ne sont pas considérées comme des données sensibles lorsqu'elles sont prises isolément, elles peuvent devenir potentiellement invasives et entrer en conflit avec le droit à la vie privée, lorsque mises en commun. Autrement dit, des données en apparence inoffensives peuvent être recoupées entre elles. Une fois recoupées, ces différentes données deviennent souvent sensibles, et y accéder compromet la vie privée des utilisateurs. Or, l'État pourrait jouer un rôle d'encadrement et mettre en place des politiques s'appliquant aux compagnies développant des objets connectés. Il est possible, par exemple, d'étudier la possibilité de créer un mécanisme de certification des objets connectés et de recommander aux futurs organismes de certification et aux professionnels impliqués dans le développement d'objets connectés d'établir des normes de sécurité appropriées pour les objets connectés. Le gouvernement pourrait aussi concentrer ses politiques publiques sur les usages acceptables des données collectées par des objets connectés.

3. Dans un contexte de données massives et d'IA, la protection de la vie privée devrait-elle être pensée par-delà la notion de protection des renseignements personnels?

Le projet de loi n^{o} 64 met l'accent sur la notion de renseignement personnels et sur les balises qui s'imposent pour encadrer la collecte, l'utilisation ou la communication de ce

[7] À cet effet, la CEST rendra public cet automne son avis *L'Internet des objets, la vie privée et la surveillance : balises éthiques et recommandations*, en supplément à son avis de 2008 sur les nouvelles technologies de surveillance et de contrôle à des fins de sécurité.

type de renseignements de manière à assurer la protection de la vie privée des individus. Cela s'avère cependant insuffisant pour protéger ce droit dans un contexte de données massives et d'intelligence artificielle. La protection de la vie privée devrait ainsi s'entendre de manière plus générale en termes de respect de l'autonomie, de l'intégrité et de la dignité des personnes, des principes qui sont au fondement de notre conception de la vie privée, mais qui la dépassent largement.

La CEST voudrait attirer l'attention de la Commission des institutions particulièrement sur un certain nombre de risques éthiques qui découlent de l'essor des technologies numériques, tels que :

- La quasi-impossibilité de garantir l'anonymat des données, même lorsque les procédures d'anonymisation ont été respectées;
- Les usages abusifs, dont des atteintes à la vie privée ou à la dignité de la personne, qui peuvent être faits de renseignements qui ne sont pourtant pas identificatoires;
- Les nouveaux savoirs de nature sensible à propos d'individus ou de sous-groupes de la population, pouvant être inférés par le recoupement de renseignements non identificatoires, ou de renseignements personnels mais qui ne sont pas sensibles.

Risques de réidentification des individus

Nous savons qu'il est relativement aisé de croiser des données *a priori* anonymes pour réidentifier des personnes. Pratiquement n'importe quelle donnée collectée ouvre la voie à des atteintes à la vie privée, à l'autonomie, à l'intégrité ou à la dignité de la personne.

Il s'agit d'un **risque qui subsiste même s'il y a eu en amont une dépersonnalisation ou anonymisation des données**. « Déjà en 1997, la chercheuse américaine Latanya Sweeney avait démontré qu'avec une combinaison de trois attributs démographiques, tels que le code postal, la date de naissance et le genre, il était possible d'identifier 87 % des Américains. En croisant une banque de données médicales, qui avaient été anonymisées et rendues publiques pour la recherche, avec le fichier des électeurs de la ville de Cambridge, elle avait également réussi à réidentifier un individu »[8]. Dans la même veine, « les chercheurs de l'Université catholique de Louvain, en Belgique, et de l'Imperial College of London, au Royaume-Uni, ont élaboré un algorithme d'apprentissage machine qui permet en quelque sorte d'estimer la probabilité d'identifier avec exactitude un individu parmi plusieurs milliards de personnes à partir d'une certaine combinaison d'attributs ou de caractéristiques. En utilisant leur méthode, ils démontrent que 99,98 % des Américains seraient correctement réidentifiés dans n'importe quelle base de données en utilisant 15 attributs démographiques »[9]. Comme le souligne le professeur d'informatique et titulaire

[8] Gravel, P. (2019). « Les données personnelles : un secret mal gardé », *Le Devoir*, 26 juillet 2019. [En ligne] https://www.ledevoir.com/societe/science/559444/un-secret-mal-garde
[9] Idem.

de la Chaire de recherche du Canada en analyse respectueuse de la vie privée et éthique des données massives, Sébastien Gambs, « 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'attributs »[10].

Plusieurs chercheurs mettent ainsi en doute la capacité des techniques d'anonymisation à assurer une protection optimale de la vie privée. Concrètement, cela pose problème au regard de l'article 28 du projet de loi nº 64, où il est proposé de modifier l'article 73 de la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (LADOPPRP) pour ajouter « ou l'anonymiser » après « détruire » : *Lorsque les fins pour lesquelles un renseignement personnel a été recueilli ou utilisé sont accomplies, l'organisme public doit le* ***détruire ou l'anonymiser****, sous réserve de la Loi sur les archives (chapitre A-21.1) ou du Code des professions (chapitre C-26)*. Or, ces deux opérations ne sont pas équivalentes sur le plan des risques résiduels : même les meilleurs pratiques d'anonymisation n'assurent pas qu'il soit par la suite impossible de réidentifier les individus.

Au regard des risques soulevés, il semble indiqué d'élargir le régime de protection au-delà des seuls renseignements personnels, pour **protéger également les renseignements dépersonnalisés ou anonymisés**. Actuellement, les renseignements dépersonnalisés ou anonymisés sont insuffisamment encadrés, puisqu'ils ne sont pas considérés comme des renseignements personnels. La formulation et l'application de règles particulières de protection pourraient être appropriées pour des données *qui ne sont pas* des renseignements personnels, mais dont le recoupement permet de réidentifier les personnes physiques et porter atteinte à leur vie privée. **Par exemple, une analyse des risques de réidentification pourrait être rendue légalement obligatoire avant le partage de tout ensemble de données concernant des personnes et ayant été anonymisées ou dépersonnalisées.**

Définition d'un « renseignement sensible »

Il est apprécié que le projet de loi nº 64 définisse la notion de renseignements à caractère sensible. Il est cependant à déplorer que cette catégorie ne soit comprise que comme un sous-ensemble des renseignements personnels : *un renseignement personnel est sensible lorsque, de par sa nature ou en raison du contexte de son utilisation ou de sa communication, il suscite un haut degré d'attente raisonnable en matière de vie privée* (article 12 du projet de loi, modifiant l'article 59 de la LADOPPRP).

Selon cette définition, la gradation est uniquement à l'intérieur du domaine des renseignements personnels et non des renseignements (ou des données) plus largement, alors que l'agrégation de données non personnelles peut produire des informations

[10] Idem.

personnelles ou sensibles et porter préjudice aux individus. Un exemple de cela se trouve dans la notion de renseignement inféré.

Les renseignements inférés

Un renseignement inféré est un savoir nouveau résultant du recoupement ou de l'analyse d'autres renseignements. À ce titre, le renseignement inféré ne peut pas être connu d'emblée et n'est pas soumis à l'encadrement prévu pour les renseignements dont il découle. Or, un tel renseignement peut être de nature sensible, même si les données utilisées pour l'inférer ne le sont pas. Pensons à un cas où l'analyse de données de navigation Internet permet d'inférer que l'utilisatrice est enceinte[11], ou à un autre cas où l'analyse de l'activité d'un individu sur un réseau social, telles que ses mentions « j'aime » sur Facebook, permet d'inférer son orientation sexuelle[12]. Avec les outils puissants que fournit l'intelligence artificielle, des données de prime abord anodines permettent d'inférer des savoirs très précis et sensibles, sur la base de corrélations établies à partir de très grands ensembles de données (données massives).

Par conséquent, il serait opportun que le projet de loi assure une protection des renseignements inférés, particulièrement pour ceux qui ont un caractère sensible de par le haut degré d'attente raisonnable en matière de vie privée qu'auraient les individus concernés par ces renseignements, ou de par les conséquences potentielles de leur utilisation sur l'autonomie, la dignité ou l'intégrité de la personne. De manière concrète, la loi pourrait définir certains types de savoirs, à haut degré de sensibilité, qu'il est interdit d'inférer à partir de renseignements collectés ou partagés, tels que, à titre d'exemple : l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses, la vie sexuelle ou l'orientation sexuelle d'une personne physique[13].

Au-delà de la nature du renseignement collecté, la prise en compte des effets qui découlent de leur utilisation

Il importe de couvrir des effets indésirables comme les effets discriminatoires découlant de jeux de données pourtant anonymisées. Ce n'est pas seulement le caractère personnel des données colligées qui peut s'avérer problématique, mais la finalité de leur usage et la traçabilité de leur cycle complet. Cela signifie de tenir compte des potentiels recoupements et agrégations des données et des risques éthiques de cette possibilité numérique.

Le projet de loi souligne, dans le nouvel article 63.9 de la LADOPPRP, prévu à l'article 14, que pour évaluer les risques de préjudice causés à une personne, un organisme doit

---

[11] Voir Hill, K. (2012). « How Target figured out a teen girl was pregnant before her father did », *Forbes*, 156 février 2012. [En ligne] https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/#5f6808de6668

[12] Voir Halliday, J. (2013). « Facebook users unwittingly revealing intimate secrets, study finds », The Guardian, 11 mars 2013. [En ligne] https://www.theguardian.com/technology/2013/mar/11/facebook-users-reveal-intimate-secrets

[13] Cette liste, non exhaustive et à titre d'exemple seulement, est inspirée directement de la définition d'une donnée sensible prévue à l'article 9 du *Règlement général de protection des données* (Europe).

considérer non seulement la sensibilité d'un renseignement concerné, mais *les conséquences appréhendées de son utilisation et la probabilité qu'il soit utilisé à des fins préjudiciables*. Toutefois, elle restreint une telle évaluation au préjudice causé à une personne *dont un renseignement personnel est concerné par un incident*.

Pourtant, le critère des renseignements personnels est limité pour dresser les contours d'un usage éthique des données. En effet, des pratiques de profilage à partir de données non identificatoires sont néanmoins susceptibles de porter préjudice à l'autonomie et à la dignité de membres de la population, des valeurs qui sont intimement liées à la notion de vie privée. Elles comportent le risque de renforcer des formes de stigmatisation et de profilage au sein de la population et donner lieu ainsi à un traitement inéquitable.

En vertu de cette idée, **la définition de profilage proposée dans le projet de loi devrait être modifiée**, puisqu'elle ne réfère qu'à des renseignements personnels : « 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 » (article 8.1, prévu à l'article 99 du projet de loi). Or, Il est tout à fait possible d'effectuer du profilage qui n'identifie à aucun moment une personne physique, mais qui aura des incidences sur des catégories de personnes dont les intérêts et les droits devraient néanmoins être protégés.

La formulation et l'application de règles particulières de protection pourraient être appropriées pour des données qui ne sont pas des renseignements personnels, mais dont le traitement peut entraîner également des préjudices pour les personnes physiques. Pensons à l'utilisation d'ensembles de données anonymisées pour établir un profil par quartier de manière à « optimiser » ou « préciser » des politiques de sécurité publique. Cela soulève un enjeu d'étiquetage ou de stigmatisation qui doit être pris en considération, ayant des répercussions sur les individus habitant ces quartiers et pouvant même mener à une forme de prophétie auto-réalisatrice (lorsqu'une politique est elle-même la cause des effets servant à en justifier la nécessité ou la légitimité). Cette utilisation des données à des fins de profilage devrait être soumise à un encadrement législatif ou réglementaire, que ce soit dans le cadre de ce projet de loi ou d'un autre, subséquent.

De même, la notion d'**incident de confidentialité** est uniquement attachée à la notion de renseignement personnel, alors que sont définies comme de tels incidents : « 1-l'accès non autorisé par la loi à un renseignement personnel, 2- l'utilisation non autorisée par la loi d'un renseignement personnel 3- la communication non autorisée par la loi d'un renseignement personnel 4- la perte d'un renseignement personnel ou toute autre atteinte à la protection d'un tel renseignement » (article 14 du projet de loi, insérant l'article 63.8) Ici encore, les effets préjudiciables de l'accès, de l'utilisation, de la communication ou de la perte de tout renseignement devraient pouvoir être pris en considération au moment de définir un incident de confidentialité.

La protection de la vie privée devrait s'entendre de manière plus générale en termes de respect de l'autonomie, de l'intégrité et de la dignité des personnes, des principes qui sont au fondement de notre conception de la vie privée, mais qui la dépassent largement. Ainsi, **les données inférées concernant une personne physique devraient être protégées**, comme le sont renseignements personnels, au regard des effets qu'elles génèrent.

À cet effet, il pourrait être attendu que les responsables de l'utilisation des données fournissent en amont une justification des inférences à effectuer. Il s'agirait d'étayer les raisons pour lesquelles les données choisies sont appropriées pour établir des inférences, ainsi que la pertinence des résultats inférés au regard de leur caractère moralement acceptable. Ils devraient aussi employer des méthodes éprouvées sur le plan de la fiabilité[14] et tenir compte des enjeux éthiques de l'accès à des données de qualité et exemptes de biais discriminatoires, de même que des risques de corrélations fallacieuses[15]. Au-delà du respect du critère de nécessité de la collecte, les données utilisées devraient, pour ainsi dire, faire l'objet d'une attention au regard de la légitimité de la finalité de leur traitement. Certes, comme le souligne l'Observatoire international sur les impacts sociétaux de l'IA et du numérique (OBVIA), « le critère de légitimité est déjà prévu par le droit québécois. Il requiert que toute entreprise ou organisation qui traite des renseignements personnels ait un intérêt légitime pour le faire ». Cependant, « la signification des termes légitimes et illégitimes demeure évidement largement subjective. Ainsi, pour que le critère de licéité arrive à encadrer adéquatement le traitement de renseignements personnels, il devrait y avoir des indications plus claires quant à ce que constitue une finalité interdite. »[16]

4. La prise en compte du cycle complet des données : baliser le partage des données et leurs usages ultérieurs

La CEST est sensible aux situations où il peut être acceptable de communiquer des renseignements personnels ou d'autres données à des fins qui justifient de passer outre l'obligation de consentement manifeste, libre, éclairé, donné à des fins spécifiques et en continu. Les bénéfices collectifs peuvent dépasser les risques et justifier des atteintes mineures aux principes d'autonomie et de protection de la vie privée. Cependant, cela doit se faire dans un contexte où l'encadrement est suffisant et où les personnes concernées sont bien informées des pratiques en vigueur.

---

[14] Wachter, S. & B. Mittelstadt (2019), « A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI », *Columbus Law Review*, nº 2, p. 1-131.
[15] Commissaire à l'information et à la protection de la vie privée de l'Ontario (2017), *Big Data Guidelines*, [En ligne] https://www.ipc.on.ca/resource/big-data-guidelines/
[16] OBVIA (2020), *Repenser la protection des renseignements personnels à la lumière des défis soulevés par l'IA – Document de réponse aux questions posées par la Commission d'accès à l'information du Québec dans le cadre de la consultation sur l'intelligence artificielle*. [En ligne] http://collections.banq.qc.ca/ark:/52327/bs4067010

Il serait pertinent que des mesures spécifiques soient prévues pour que soit visible et explicite l'information concernant la possibilité que le gouvernement fasse une utilisation secondaire des données que les citoyens lui confient, car les personnes concernées ne peuvent s'attendre raisonnablement à ce que leurs renseignements personnels soient communiqués puis utilisés sans leur consentement et potentiellement pour une autre finalité que celle pour laquelle elles les divulguent en premier lieu.

Les balises entourant la communication des renseignements personnels à des tiers pourraient être clarifiées davantage. Les situations pour lesquelles un aménagement dans la loi est prévu pour exempter les organisations de l'exigence d'obtenir le consentement doivent être raisonnables et justifiées. Par exemple, dans l'article 27 du projet de loi, ajoutant l'article 70.5, « *un renseignement personnel est communiqué par tout organisme public sans le consentement de la personne concernée à un gestionnaire de renseignements personnels lorsque la communication est nécessaire aux fins prévues à un décret pris en application de l'article 70.3 : Notamment, la planification, la gestion, l'évaluation ou le contrôle de ressources, de programmes ou de services gouvernementaux.* » Un flou réside cependant dans ce qui est entendu par les fins de planification, la gestion, l'évaluation ou le contrôle de ressources, de programmes ou de services gouvernementaux, une catégorie de fins susceptible d'englober une grande quantité d'usages différents. Le projet de loi n^{o} 64 pourrait apporter davantage de précision sur le point des usages secondaires des données permis sans le consentement des individus.

En parallèle, il est fait mention qu'un organisme peut communiquer des renseignements personnels sans le consentement des personnes pour des fins d'étude, de recherche ou de production statistique, avec des restrictions cependant (article 23 du projet de loi par l'insertion de l'article 67.2.1.) Le cas échéant, une ÉFVP doit précéder cette communication, laquelle pourra s'effectuer s'il est conclu notamment qu'il est déraisonnable d'exiger que la personne ou l'organisme obtienne le consentement des personnes concernées. Or, les éléments dont doit rendre compte l'EFVP contiennent plusieurs éléments laissant large place au jugement. D'une part, les interprétations risquent de varier d'un ministère, d'un organisme ou d'une entreprise à l'autre. **Une instance centrale permettant le partage des décisions et l'élaboration de bonnes pratiques pourrait aider à pallier ce problème.** D'autre part, la présence de membre éthiciens, par exemple par **l'inclusion du répondant en éthique de l'organisation au sein du comité sur la protection des renseignements personnels**, s'impose. Enfin, le rôle de la CAI pourrait être précisé en ce qui a trait à son pouvoir d'action sur l'entente qui lui est transmise, conformément à l'article 23 du projet de loi, introduisant l'article 67.2.3 suivant : « *L'organisme public qui communique des renseignements personnels conformément à l'article 67.2.1 doit préalablement conclure avec la personne ou l'organisme à qui il les transmet une* entente […], laquelle *est transmise à la Commission et entre en vigueur 30 jours après sa réception par celle-ci.* »

En outre, le projet de loi n^{o} 64 ne prévoit d'obligation de réaliser une EFVP que dans les cas où il y a collecte, utilisation ou communication de renseignements personnels. Or, une

EFVP pourrait être nécessaire pour des projets où il n'y a pas collecte, utilisation ou communication de renseignements personnels, mais où il existe néanmoins des risques relatifs à la vie privée (ou à d'autres valeurs liées, telle l'autonomie et la dignité de la personne), comme il a été souligné plusieurs fois dans le présent mémoire.