Assemblée nationale du Québec

Commission des institutions

Consultations particulières et auditions publiques au sujet

Québec, le 28 septembre 2020

1. Mémoire déposé par :

Céline Castets-Renard
Professeure à l'Université d'Ottawa, Faculté de droit civil
Chaire de Recherche *L'intelligence artificielle Responsable à l'échelle mondiale*

Céline Castets-Renard est coresponsable de l'Axe « Relations Internationales, Action Humanitaire Droits Humains » au sein de l'Observatoire International sur les Impacts Sociétaux de l'IA et du Numérique (OBVIA), financé par le FRQSC.

Elle fut professeur d'Université en France pendant 17 ans et est titulaire d'une chaire de recherche *Law & AI* financé par le gouvernement français au sein de l'*Artificial and Natural Intelligence Toulouse Institute* (ANITI). Elle fut également chercheuse invitée à la *Fordham Law School* (*Center of Law and Information Policy*) et *Yale Law School* (*Internet Society Project*) (2017-2019).

Elle est spécialiste de droit du numérique, droit des données personnelles et vie privée, droit de l'intelligence artificielle dans une perspective comparative de droit européen, américain et canadien.

2. Résumé de l'intervention

La protection des renseignements personnels présente des caractéristiques au Canada et au Québec qui les positionnent entre deux systèmes légaux de protection de la vie privée aux États-Unis et de protection des données personnelles dans l'Union européenne. Ce constat invite à faire du droit comparé pour trouver des sources d'inspiration, tout en tenant compte des particularités du Québec. Le droit est en effet le reflet d'une société et de sa culture dont il ne doit pas être déconnecté.

Dans le contexte du projet de loi 64 et de la réforme des lois sur la protection des renseignements personnels, nous souhaitons contribuer au débat en concentrant la réflexion sur deux enjeux principaux auxquels tout législateur souhaitant réformer aujourd'hui une législation sur la protection de renseignements personnels est confronté :

- La prise en compte des évolutions technologiques ;
- La nécessité de renforcer la protection des personnes face au développement de l'économie numérique et de la marchandisation des données, tout en préservant un équilibre à l'égard des différents acteurs.

3. Exposé général

1er enjeu : la prise en compte des évolutions technologiques

Certaines dispositions du projet de loi 64 tendent à tenir compte de certaines pratiques rendues possibles par les technologies disponibles aujourd'hui.
On note des points forts et des points d'amélioration de la législation.

LES POINTS FORTS

- les techniques d'identification, localisation et profilage
- les techniques permettant la prise de décision automatisée.

1) Recours à une technologie comprenant des fonctions permettant de l'identifier, de la localiser ou d'effectuer un profilage

Le projet de loi 64 envisage d'encadrer la collecte de 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.
Pour ce faire, le projet de loi pose

- une **obligation d'information préalable** du recours à une telle technologie;
- une obligation **d'offrir des moyens pour désactiver** les fonctions permettant d'identifier, de localiser ou d'effectuer un profilage.

Ce type de technologies permet en effet de collecter des données personnelles qui peuvent être intimes et sensibles sans que la personne concernée en est conscience le plus souvent.

2) Décision fondée exclusivement sur le traitement automatisé : nouveaux droits

Le projet de loi 64 pose que l'utilisation de renseignements personnels, afin que soit rendue une **décision fondée exclusivement sur un traitement automatisé** de ceux-ci doit, au moment de la décision ou avant, faire l'objet d'une information auprès de la personne concernée.

Il doit aussi, à la demande de la personne concernée, l'informer :

> 1° des renseignements personnels utilisés pour rendre la décision;
> 2° des raisons, ainsi que des principaux facteurs et paramètres, ayant mené à la décision;
> 3° de son droit de faire rectifier les renseignements personnels utilisés pour rendre la décision ».

Cette disposition se rapproche de l'article 22 du RGPD. Cependant, les droits consacrés diffèrent puisque le RGPD consacre le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage, produisant des effets

juridiques la concernant ou l'affectant de manière significative de façon similaire. Il s'agit ici de poser un droit à l'information et un droit à l'explication individuelle qui n'existe pas en tant que tel dans le RGPD et dont l'interprétation fait l'objet d'une controverse doctrinale.

Le droit de rectifier et de reconsidérer les renseignements personnels utilisés paraît être une solution intéressante pour lutter contre certains risques sociaux liés à certains systèmes d'intelligence artificielle qui se sont par exemple révélés racistes ou sexistes.

LES POINTS D'AMELIORATION

- Définition des renseignements sensibles et traitement de données massives
- Augmentation des fonctions et pouvoirs de la CAI

1) Définition des renseignements sensibles et traitement de données massives

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. ».

Cette définition est intéressante et même séduisante au premier abord car elle présente des qualités de souplesse et d'adaptation,
Le problème est qu'elle est floue et risque de générer des problèmes d'interprétation, alors que cette catégorie de données est nouvelle et doit faire l'objet d'une protection renforcée.
Dans le contexte technologique de traitement massif de données qui est aujourd'hui banalisé, il risque d'être difficile de tenir compte de la nature et *a fortiori* du contexte d'utilisation des données, s'agissant possiblement de certaines données noyées dans une masse.
Dans un tel contexte, il n'est déjà pas facile de distinguer des renseignements personnels de ceux qui ne le sont pas et penser qu'il sera aisé d'interpréter les données pour repérer celles qui seraient sensibles paraît peu réaliste.
Il est également difficile d'assurer la protection des données sensibles qui sont énumérées comme à l'article 9 du RGPD donc le flou de leur qualification risque de porter atteinte à la protection.

Recommandation 1 : *il est recommandé au législateur de préciser la catégorie des données sensibles si on souhaite véritablement créer cette catégorie de données et leur accorder une protection renforcée.*

2) Augmentation des dotations financières de la CAI

De nouveaux pouvoir sont accordés à la CAI tenant en particulier au pouvoir d'étude, de donner des avis et de prononcer des sanctions renforcées.
Il ne sert à rien de renforcer la protection de la loi, en particulier les sanctions, et de renforcer les pouvoirs d'une autorité de contrôle si on n'augmente pas aussi les dotations financières nécessaires pour lui permettre d'assurer ses missions anciennes et nouvelles, *a fortiori* pour faire face à la toute-puissance des géants américains du numérique.

La protection des renseignements personnels ne peut être prise au sérieux par les grandes entreprises du numérique s'il n'existe pas une autorité suffisamment forte pour jouer le rôle de gendarme. Les exemples en Europe et aux États-Unis le confirment.

Recommandation 2 : *il est recommandé au législateur d'aller plus loin dans les pouvoirs et missions de la CAI pour assurer son statut d'indépendance et surtout de la doter des moyens financiers et ressources humaines nécessaires à la mise en œuvre de la réforme.*

2e enjeu : la nécessité de renforcer la protection des personnes face au développement de l'économie numérique et de la marchandisation des données, tout en préservant un équilibre à l'égard des différents acteurs.

Si le RGPD semble avoir servir de modèle pour l'adoption de certaines mesures de durcissement, notamment des sanctions, il faut comprendre que le RGPD comporte des règles dures à l'égard des géants du numérique mais aussi des mécanismes d'assouplissement permettant une interprétation *in concreto* des situations et de tenir compte des toutes les parties prenantes. Le RGPD est un texte de loi « omnibus » qui s'applique à la matière civile et commerciale dans les secteurs privé et public mais comporte des outils pour tenir compte des petites entreprises et des petits organismes publics.
Il ne semble pas que le législateur québécois est suffisamment introduit de mécanismes de souplesse permettant de conserver un niveau élevé de protection tout en tenant compte de la situation des acteurs privés et publics.

Mécanismes de souplesse

Plusieurs mécanismes d'assouplissement et de personnalisation de la loi (appréciation in concreto) pourraient être introduits.

1) **La souplesse tenant aux sanctions**

Les sanctions élevées du RGPD ont amplement inspiré le projet de loi 64 qui prévoit des sanctions jusqu'à 25 millions de dollars ou 4% du CA mondial.
Ces sanctions paraissent utiles pour que la protection des renseignements personnels soit prises au sérieux. Le Québec n'est pas si isolé en Amérique du nord et il est arrivé à la *Federal Trade Commission* aux États-Unis de prononcer des sanctions élevées envers les géants de l'internet.
Ex. sanction de 170 millions de dollars en 2019 contre Youtube sur le fondement de la loi COPPA (Children's Online Privacy Protection Act).

Au demeurant, il s'agit là de montant maximum et il ne s'agit pas de les appliquer à des situations où les risques pour la vie privée ne seraient pas élevés. Dans l'UE ces montants n'ont pas encore été prononcés mais la menace doit être prise au sérieux. Un certain nombre de facteurs seront pris en compte dans le prononcé des sanctions et notamment la gravité de la violation.
Le régime des sanctions tel que prévu par la loi 64 doit donc être maintenu.

2) **Mesures d'accompagnement des entreprises et petits organismes publics**

Le RGPD est très lourd et complexe et le législateur européen a prévu des mesures d'accompagnement de *soft law* (droit souple) pour aider les petites entreprises et organismes publics à se mettre en conformité
Une partie normative essentielle du RGPD tient aux lignes directrices, codes de conduite, certifications, outils de conformité qui ont été créés par les autorités nationales de protection et par Commissaire européen à la protection des données personnelles.

Si le législateur québécois veut adopter une législation suffisamment efficace, il doit aussi penser à aider les petites entreprises à se mettre en conformité avec l'aide de la CAI qui doit être doté des moyens et pouvoirs de le faire.

3) **La prise en compte de l'impact sur les « droits et libertés fondamentales » des personnes concernées**

Certaines dispositions contraignantes du RGPD ne s'appliquent que s'il existe un risque d'atteinte aux « droits et libertés fondamentales » des personnes concernées.
Tel est par exemple le cas de la notification des failles de sécurité ou encore de l'étude d'impact sur la protection des données personnelles qui ne doit être réalisée que s'il existe un risque d'atteindre ces droits.
Le projet de loi 64 impose l'évaluation des facteurs relatifs à la vie privée pour tout projet de système d'information ou de prestation électronique de service impliquant des renseignements personnels, ce qui peut paraître lourd et pas systématiquement nécessaire.

Il faut noter que le RGPD est fondé sur la protection des droits fondamentaux (articles 7 et 8 de la Charte des droits fondamentaux de l'UE), ce qui n'est pas nécessairement l'approche du droit québécois mais mérite réflexion.

- **4) Critères d'appréciation *in concreto***

Le RGPD dispose à plusieurs reprises que les règles posées doivent être respectées

> « Compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques », le responsable du traitement et le sous-traitant mettent en œuvre les mesures techniques et organisationnelles appropriées.

- **5) Le consentement dans une approche globale**

Le consentement n'est pas le seul fondement légal pour garantir la licéité du traitement de données personnelles. Il n'est qu'un fondement parmi d'autres. En revanche, la protection des personnes concernées est garantie par d'autres règles comme les droits accordés aux personnes concernées et surtout le respect des principes directeurs (principes de licéité, nécessité, finalité, minimisation des données et conservation limitées) (art. 5).
Ces principes sont de nature à compléter la protection et peuvent s'avérer parfois plus efficaces pour protéger efficacement la personne que le consentement donné dans un contexte numérique.

Recommandation 3 : *introduire des mécanismes de souplesse et d'accompagnement dans la mise en œuvre des nouvelles règles tout en maintenant les exigences élevées de protection.*

Je remercie la Commission de me donner cette occasion d'ouvrir la discussion et la coopération entre les députés et les experts indépendants.