Réforme de la protection de la vie privée dans le secteur privé en Ontario

Renforcer la protection de la vie privée dans le secteur privé pour les Ontariens à l'ère numérique

Contact : ccastets@uottawa.ca

Recommandations présentées par :

Céline Castets-Renard, Professeure à l'université d'Ottawa[1]
Titulaire de la chaire de recherche L'IA responsable à l'échelle mondiale
Coresponsable de l'Axe Relations Internationales, Action Humanitaire. Droits Humains à l'OBVIA

Anne-Sophie Hulin, Docteure de l'Université Paris II[2]
Chercheuse et Directrice adjointe du Centre Paul-André Crépeau de droit privé et comparé, Faculté de droit, McGill University
Membre de la Chaire de recherche sur L'IA responsable à l'échelle mondiale

Ariane Lamoureux
Étudiante en 3e année en licence de droit (LL.L.) à l'université d'Ottawa
Section de droit civil
&
Jessica Matte
Étudiante en 2e année en licence de droit (LL.L.) à l'université d'Ottawa
Section de droit civil

Ce rapport a été partiellement réalisé dans le cadre du cours de la professeure Céline Castets-Renard sur « *Le droit international et comparé du numérique* » de la Faculté de droit de l'Université d'Ottawa. Il nous fait plaisir de participer à cette consultation publique. Nous restons à l'écoute pour toute question ou discussion que vous souhaiteriez avoir avec nous.

---

[1] Céline Castets-Renard fut professeure à l'Université Toulouse Capitole (France) pendant 17 ans. Elle est titulaire d'une chaire de recherche *Law, Accountability and Social Trust in AI* financée par le gouvernement français au sein de *Artificial and Natural Intelligence Toulouse Institute* (ANITI). Elle fut 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 (droit européen, américain et canadien). Céline Castets-Renard a été auditionnée à deux reprises par l'assemblée nationale du Québec sur le projet de la loi 64 9 http://www.assnat.qc.ca/en/video-audio/archives-parlementaires/travaux-commissions/AudioVideo-86639.html) (sept. 2020) et sur les applications de traçage des contacts (http://www.assnat.qc.ca/fr/video-audio/archives-parlementaires/travaux-commissions/AudioVideo-85763.html) (août 2020).

[2] Anne-Sophie Hulin a fait sa thèse à Paris II sur « La philanthropie au profit des musées d'art : une étude de droit privé comparé » (France / États-Unis / Québec). (2019). Elle est spécialiste de la fiducie en droit québécois et du trust anglo-saxon.

1. Renforcement du consentement

Comparaison avec le RGPD en Europe et le projet de loi 64 au Québec qui prévoient tous deux des dispositions protectrices du consentement et encadrent les conditions de sa manifestation pour être valable.

RGPD art. 4.11 : Définition du consentement

> « consentement » de la personne concernée : toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement

RGPD, art. 7 : Conditions applicables au consentement

> 1. Dans les cas où le traitement repose sur le consentement, le responsable du traitement est en mesure de démontrer que la personne concernée a donné son consentement au traitement de données à caractère personnel la concernant.
> 2. Si le consentement de la personne concernée est donné dans le cadre d'une déclaration écrite qui concerne également d'autres questions, la demande de consentement est présentée sous une forme qui la distingue clairement de ces autres questions, sous une forme compréhensible et aisément accessible, et formulée en des termes clairs et simples. Aucune partie de cette déclaration qui constitue une violation du présent règlement n'est contraignante.
> 3. La personne concernée a le droit de retirer son consentement à tout moment. Le retrait du consentement ne compromet pas la licéité du traitement fondé sur le consentement effectué avant ce retrait. La personne concernée en est informée avant de donner son consentement. Il est aussi simple de retirer que de donner son consentement.
> 4. Au moment de déterminer si le consentement est donné librement, il y a lieu de tenir le plus grand compte de la question de savoir, entre autres, si l'exécution d'un contrat, y compris la fourniture d'un service, est subordonnée au consentement au traitement de données à caractère personnel qui n'est pas nécessaire à l'exécution dudit contrat.

Projet de loi 64 au Québec, art. 53.1

> Un consentement prévu à la présente loi doit être manifeste, libre, éclairé et être donné à des fins spécifiques. Il est demandé à chacune de ces fins, en termes simples et clairs, distinctement de toute autre information communiquée à la personne concernée. Lorsque celle-ci le requiert, il lui est prêté assistance afin de l'aider à comprendre la portée du consentement demandé.
>
> Le consentement ne vaut que pour la durée nécessaire à la réalisation des fins auxquelles il a été demandé.
>
> Un consentement qui n'est pas donné conformément à la présente loi est sans effet. ».

En outre, le RGPD (art. 8) et le projet de loi 64 du Québec prévoient des dispositions de protection spécifiques pour les mineurs.

Afin de renforcer les conditions de manifestation du consentement, nous recommandons :

- poser des conditions de qualité du consentement : manifestation d'une volonté, libre, spécifique, éclairée et univoque; ne pas faire dépendre l'exécution de services de l'obtention du consentement.
Des conditions de forme peuvent s'ajouter comme le fait d'imposer une déclaration ou un acte positif clair, bien distincte des autres consentements contractuels.

- poser des conditions de simplicité et clarté voire d'assistance pour s'assurer d'obtenir un consentement éclairé et une bonne compréhension de l'engagement :

- poser des règles de la charge de la preuve du consentement : il appartient au responsable de traitement de prouver qu'il a reçu le consentement;

- poser un droit de retrait du consentement. Poser aussi un droit à l'information sur l'existence de ce droit de retrait.
Le retrait doit être aussi simple à réaliser que le consentement à s'exprimer. Il peut par exemple s'exprimer suivant un parallélisme des formes ;

- poser une limite de validité du consentement en lien avec la finalité du traitement des renseignements personnels;

- poser une sanction en cas de non-respect de ces mesures tenant à l'invalidité du consentement qui aurait été obtenu en violation de ces obligations légales;

- poser une protection renforcée des mineurs.

Recommandations supplémentaires
Autres fondements de licéité des traitements de renseignements personnels au-delà du consentement
Le consentement est le principal fondement légal pour garantir la licéité des traitements de renseignements personnels. Or, le recueil du consentement n'est pas toujours possible ou facile voire n'est pas adapté à certaines situations.
Au-delà du consentement, il convient donc de poser d'autres fondements de licéité de licéité du traitement tenant par exemple à :
- l'exécution d'un contrat auquel la personne concernée est partie;
- le respect d'une obligation légale à laquelle le responsable du traitement est soumis;
- la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique;
- l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement :

les intérêts légitimes poursuivis par le responsable du traitement, à condition de garantir le respect des intérêts ou libertés et droits fondamentaux de la personne concernée et de préciser ce que pourraient être ces intérêts légitimes afin de poser un cadre et des limites.

Recommandations supplémentaires : renforcer les principes directeurs et les droits des personnes

Afin de compenser le fait que le consentement pourrait ne plus être le seul fondement de la licéité des traitements de renseignements personnels, il convient de renforcer d'autres dispositions de la loi tenant aux principes directeurs, droits des personnes concernées, consécration des données sensibles.

Renforcer et affirmer des principes directeurs

En contrepartie du fait que le consentement ne soit pas toujours exigé, il faut apporter d'autres garanties tenant en particulier aux principes directeurs qui encadrent les conditions de traitement des renseignements personnels :

- principe de licéité, loyauté, transparence;

- principe de limitation des finalités et précision des conditions d'un changement valable de finalité;

- principe de nécessité et minimisation des données;

- principe d'exactitude;

- principe de limitation de la conservation;

- principe d'intégrité et confidentialité.

des personnes concernées

Les droits de la personne concernée en cas d'utilisation des traitements automatiques

L'article 22 RGPD accorde 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 (c'est-à-dire produisant des effets négatifs). Ce droit est ambitieux et particulièrement protecteur à première vue. Cependant, il est assorti de trois larges exceptions en cas d'exécution d'un contrat, d'une exception légale ou de consentement de la personne, si bien qu'il est pratiquement vidé de son sens. Le risque est ici que à vouloir aller loin dans la protection, il faille prévoir de larges limitations du droit.

En conséquence, nous ne recommandons pas de consacrer ce droit de ne pas faire l'objet d'une décision automatisée, si cela conduit à prévoir trop d'exceptions et rend la prévision du droit plus compliquée pour les entreprises.

Nous recommandons de ne pas aller dans la même direction que l'Union européenne sur cette question.

En revanche, la prise de décision automatisée est aussi considérée par l'article 65.2 du projet de loi 64 au Québec et prévoit que :

« Un organisme public qui utilise des 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, en informer la personne concernée ». Le projet prévoit en outre que la personne concernée doit être informée des renseignements personnels utilisés pour rendre la décision si elle en fait la demande.

Nous recommandons de reconnaître aussi en Ontario le droit à l'information en cas d'utilisation de ce procédé de prise de décision automatique exclusivement. Nous recommandons aussi d'indiquer les renseignements personnels utilisés sans limiter ce droit à l'information à la demande de la personne concernée et de le faire systématiquement.

Plus encore, le projet de loi 64 accorde un droit à explication, dans la mesure où doivent aussi être indiquées les raisons, ainsi que les principaux facteurs et paramètres, ayant mené à la décision.
Nous recommandons de consacrer aussi ce droit à une explication individuelle qui est essentiel à la bonne compréhension des décisions algorithmiques et à leur acceptabilié sociale.

Enfin, le projet de loi 64 accorder un droit de faire rectifier les renseignements personnels utilisés pour rendre la décision automatisée. Ce droit de rectification est important mais nous recommandons d'aller plus loin en accordant un droit de contester la décision prise automatiquement, afin de respecter des garanties procédurales comme le principe du contradictoire.

Renforcer la protection par la création d'une catégorie de données sensibles
Alors que l'on constate que certains renseignements personnels sensibles ne font pas l'objet de protection, comme par exemple les renseignements personnels les données génétiques, les données biométriques et les données des syndicats et partis politiques, on sait que ce type de renseignements personnels sont pourtant particulièrement sensibles car de nature à créer des discriminations. Le RGPD et le projet de loi 64 prévoit de protéger tout particulièrement les données sensibles en posant par exemple des règles d'interdiction de traitement assorties d'exceptions.
Alors que l'article 9 du RGPD prévoit une liste exhaustive de données sensibles, le projet de loi 64 a adopté une autre approche.

L'article 9 du RGPD qualifie de données sensibles les données qui portent sur l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique.

Le projet de loi 64 prévoit aussi de créer une nouvelle catégorie de données sensibles. Une définition est donnée selon laquelle 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 a l'avantage de la souplesse mais risque de ne pas être opérationnelle et pas assez claire en pratique.

Pour éviter de créer de l'insécurité juridique pour les entreprises, nous recommandons de créer une nouvelle catégorie de données sensibles qui méritent d'être protégés davantage et de poser une énumération légale des renseignements personnels concernés.

2. Transparence et droit à l'information

Le respect de la transparence passe d'abord par l'octroi d'un droit à l'information et l'obligation pour le responsable de traitement de donner suite à l'exercice de ce droit.

Le droit à l'information est un droit cardinal, dans la mesure où les autres droits ne pourront être exercés si les personnes concernées ignorent que leurs données font l'objet d'un traitement. Les droits d'accès, opposition, portabilité ou effacement supposent avant toute chose le respect du droit à l'information.

Nous recommandons de garantir la transparence par l'exercice d'un droit à l'information et des communications
Le responsable du traitement doit fournir toute information concernant les droits des personnes concernées.

Quant à la forme de l'information : L'information doit être présentée d'une façon concise, transparente, compréhensible et aisément accessible, en des termes clairs et simples, en particulier pour toute information destinée spécifiquement à un enfant.
Les informations sont fournies par écrit ou par d'autres moyens y compris, lorsque c'est approprié, par voie électronique. La forme orale peut être retenue si la personne en fait la demande.
Les informations à communiquer aux personnes concernées peuvent être fournies accompagnées d'icônes normalisées afin d'offrir une bonne vue d'ensemble, facilement visible, compréhensible et clairement lisible.

Quant à la charge de la preuve de l'information, il appartient au responsable de traitement d'apporter la preuve qu'il a respecté le droit à l'information.
Sanction du défaut d'information : la loi doit prévoir une sanction en cas de défaut de l'information.

Contenu de l'information fournie : la loi devrait imposer au responsable du traitement de fournir des informations précises et énumérées dans la loi.
Devraient être fournis :
- l'identité et les coordonnées du responsable du traitement;
- les finalité du traitement, ainsi que la base juridique du traitement;
- les destinataires ou catégories de de destinataires des renseignements personnels;
la durée de conservation des renseignements personnels;
- l'existence des droits dont les droit d'accès aux renseignements personnels, le droit à la portabilité et à l'effacement;

- l’existence du droit de retirer le consentement;
- le droit d’introduire une plainte auprès du Commissaire à l’information et à la protection de la vie privée (CIPVP);

Renforcement de la transparence par l’octroi d’un droit d’accès
L’octroi d’un droit d’accès voire de rectification des données inexactes ou obsolètes permet d’assurer de la transparence et est facteur de confiance pour les personnes concernées par la collecte de leurs données.

3. Droit à la suppression / droit à la désindexation

L’article 17 du RGPD prévoit un droit à l'effacement («droit à l'oubli»). Cependant, le **droit** d'obtenir du responsable du traitement **l'effacement** de données à caractère personnel la concernant ne s’applique que dans certaines circonstances limitativement énumérées. Il n’existe donc pas de droit général à l’oubli. En outre, n’est pas spécialement considérée la désindexation des renseignements personnels dans les moteurs de recherche.

Compte tenu de ces limites, nous ne recommandons pas d’adopter le modèle européen de l’article 17.

En revanche, l’article 28.1 du projet de loi 64 prévoit que 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. ».

Ces dispositions nous paraissent équilibrées et plus protectrices des personnes.
Nous recommandons de suivre le modèle de l'article 28.1 du projet de loi 64 du Québec plutôt que l'article 17 du RGPD.

4. Droit à la portabilité des données

Alors que le projet de loi 64 du Québec ne prévoit pas de consacrer un droit à la portabilité, l'article 20 du RGPD consacre un tel droit.

Cependant, ce droit sert davantage aux entreprises qu'à la protection des personnes concernées. Il a en effet plus d'impact du point de vue du droit de la concurrence et doit avant tout servir à encourager la création de produits et services alternatifs.
Si ce droit est parfois présenté comme garantissant plus de contrôle et d'« empouvoierement » des personnes, cette hypothèse est illusoire. Au demeurant, ce droit risque d'être mal compris des personnes concernées donc nous ne recommandons pas de le consacrer dans une loi relative à la protection des renseignements personnels.

En revanche, si l'objectif principal est d'encourager la concurrence en matière numérique et permettre l'émergence de produits et services alternatifs aux géants américains de l'internet, il convient de prendre un plus grand nombre de mesures pour stimuler la concurrence et encourage l'innovation dans une loi dédiée et dans laquelle le droit à la portabilité trouvera une meilleure place.

5. Attribution des pouvoirs de surveillance, de conformité et d'application de la loi au Commissaire à l'information et à la protection de la vie privée (CIPVP)

Quelles que soient les mesures prises dans une future loi sur la protection des renseignements personnels, son efficacité sera nécessairement conditionnée par les capacités d'accompagnement, de surveillance et de sanction de l'autorité de contrôle, ce qui passe par l'octroi de larges pouvoirs et moyens renforcés, en particulier moyens humains et financiers. Les compétences, pouvoirs et moyens du CIPVP sont nécessaires à l'efficacité d'un régime de protection des renseignements personnels.

Nous recommandons que le commissaire doit être doté des pouvoirs de contrôle et de surveillance, ainsi que de sanctions élevées, mais aussi des pouvoirs d'aide pour permettre aux petites entreprises de se mettre en conformité avec la loi.
Une double mission doit donc être confiée tenant à :
- l'accompagnement, le conseil pour la mise en conformité
- le contrôle et la sanction en cas de non-conformité.

Cette approche duale de pédagogie et sanction est nécessaire à l'efficacité de la protection.

La dimension d'accompagnement doit se traduire concrètement par la mise en œuvre d'une boite à outils de conformité pour aider les entreprises à se conformer au texte. Tel sera par exemple le cas des codes de conduite, labels et certifications.
Les codes de conduite peuvent être élaborés par exemple par les parties prenantes d'un secteur d'activité (ex. commerce) et doivent ensuite être approuvés par le CIPVP. Enfin, il devient obligatoire après son adoption.
Cet exemple montre que les entreprises doivent être aidées pour la mise en conformité et la minimisation des risques pour les personnes.

Quant à la sanction, nous recommandons de poser des sanctions élevées pour que la protection des renseignements personnels soit prise au sérieux. Si en Europe la protection existe depuis 40 ans, elle est prise au sérieux seulement depuis l'adoption du RGPD et la consécration de sanctions élevées. Le Québec a prévu des sanctions aussi élevées.

Cependant, nous recommandons que les sanctions soient des montants maximum et il faudra naturellement prévoir des gradations dans la sanction et tenir compte des contextes, de la gravité des violations et des capacités financières des entreprises selon son chiffre d'affaire par exemple. Également, il faudra prévoir les conditions claires de déclenchement des sanctions d'un point de vue procédural.
Les sanctions ainsi prononcées sont des sanctions administratives qui devront être contestables devant le juge

6. Dépersonnalisation des renseignements personnels

Il est important de définir les concepts de dépersonnalisation. Le projet de loi 64 du Québec n'a pas répondu à cette difficulté, alors que le considérant 26 du RGPD a donné des éléments de réponse en distinguant la pseudonymisation et l'anonymisation.

L'anonymisation suppose une impossibilité d'identifier la personne, ce qui entraîne la sortie du champ d'application du régime de protection des données personnelles.
La pseudonymisation suppose que les données pseudonymisées (ex. un nom remplacé par un numéro) puissent permettre une identification que si des informations supplémentaires sont ajoutées.
L'article 4 du RGPD définit la «pseudonymisation» comme le traitement de données à caractère personnel de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable;

La pseudonymisation peut permettre ainsi une réidentification, plus ou moins difficile, longue et coûteuse. Il s'agit alors d'une mesure de sécurité pour protéger les données personnelles et le régime de protection continue de s'appliquer.

Le considérant 26 du RGPD prévoit que :

« Les données à caractère personnel qui ont fait l'objet d'une **pseudonymisation** et qui pourraient être attribuées à une personne physique par le recours à des informations supplémentaires devraient être considérées comme des informations concernant une personne physique identifiable.
Pour déterminer si une personne physique est identifiable, il convient de prendre en considération l'ensemble des moyens raisonnablement susceptibles d'être utilisés par le responsable du traitement ou par toute autre personne pour identifier la personne physique directement ou indirectement, tels que le ciblage.
Pour établir si des moyens sont raisonnablement susceptibles d'être utilisés pour identifier une personne physique, il convient de prendre en considération l'ensemble des facteurs objectifs, tels que le coût de l'identification et le temps nécessaire à celle-ci, en tenant compte des technologies disponibles au moment du traitement et de l'évolution de celles-ci.

Il n'y a dès lors pas lieu d'appliquer les principes relatifs à la protection des données aux informations anonymes, à savoir les informations ne concernant pas une personne physique identifiée ou identifiable, ni aux données à caractère personnel rendues **anonymes** de telle manière que la personne concernée ne soit pas ou plus identifiable ».

Nous recommandons de suivre ces définitions pour préciser les concepts de dépersonnalisation et de prendre en compte le risque de réidentification qui s'est accru dans le contexte du big data et de l'intelligence artificielle.

7. Champ d'application matériel de la loi

L'Ontario dispose déjà de lois sur l'accès à l'information et la protection de la vie privée, en particulier dans le secteur public et en matière de santé.

En outre, certaines entreprises relèvent de la compétence fédérale comme les banques, les compagnies aériennes, les compagnies de téléphone ou de radiodiffusion.

Dans le souci de prendre en compte le secteur non lucratif et les orgnisations caritatives et de bienfaisance, nous recommandons de choisir un large d'application pour couvrir l'ensemble du secteur privé, à l'exclusion des domaines d'activité pour lesquels il existe déjà une loi fédérale ou une loi ontarienne sectorielle.
La future loi du secteur privé devrait donc englober la part résiduelle de la protection des renseignements personnels.

Enfin, nous recommandons des activités de sensibilisation et pédagogie à l'égard du secteur privé non lucratif comme les organisations caritatives, des associations professionnelles, des syndicats et des partis politiques, qui n'ont pas encore la culture de protection des renseignements personnels, alors même qu'ils traitent de données particulièrement sensibles.