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

DOCUMENT DE DISCUSSION

1 Recueillir l'avis des Ontariens

Protéger la vie privée et soutenir l'économie de l'innovation de l'Ontario

Pour poursuivre le mandat de l'innovation numérique, le ministère des Services gouvernementaux et des Services aux consommateurs (MSGSC) cherche à combler les lacunes du cadre législatif de l'Ontario sur la protection de la vie privée, et à établir des règles exhaustives et actualisées qui protègeront les droits à la vie privée et accroîtront la confiance dans les services numériques. En nous penchant sur des sujets essentiels ayant trait à la réglementation de la protection de la vie privée, et en tenant compte de l'avis des Ontariens, nous sommes déterminés à créer une solution à l'échelle de l'Ontario pour répondre aux défis actuels liés à la protection de la vie privée. Elle sera adaptée à la taille et à la complexité de l'Ontario, et constituera un levier d'innovation pour les entreprises, associations et autres organismes ontariens.

Pour entamer le dialogue à ce sujet avec les Ontariens, nous avons ciblé plusieurs sujets ayant influencé les réglementations sur la protection de la vie privée à travers le monde. Votre avis nous aidera à déterminer dans quelle mesure ces sujets s'appliquent au secteur privé de l'Ontario. Nous voulons que les Ontariens aient un meilleur accès à leurs données personnelles et un plus grand contrôle sur celles-ci lorsqu'ils interagissent avec des entreprises et organismes privés : pour être mieux informés de la façon dont leurs renseignements personnels sont utilisés et des conditions qu'ils acceptent lorsqu'ils les fournissent; pour être en mesure de retirer leur consentement et de récupérer leurs données plus facilement; pour s'assurer que les entreprises ontariennes assureront leur confidentialité même en cas d'utilisation de nouvelles technologies et de modèles d'affaires numériques. Outre la protection des renseignements personnels des Ontariens, nous voulons également nous assurer que toute nouvelle mesure de protection de la vie privée n'est pas un fardeau inutile pour les entreprises, ou ne freine pas la croissance et la prospérité de l'écosystème de l'innovation de l'Ontario.

COMMENT PARTICIPER.

Réponse formelle
Si vous êtes un organisme, un expert juridique ou un expert technique, et souhaitez nous soumettre une réponse formelle sur ce Registre, vous pouvez soumettre votre réponse à access.privacy@ontario.ca.

Sondage
Vous pouvez également soumettre votre avis et vos suggestions par le biais de notre sondage en ligne. Répondez au sondage.

Consultation avec les secteurs d'activité, les experts techniques et les parties prenantes impactées
En outre, nous consulterons les secteurs d'activité, les experts et les autres parties prenantes impactées en ce qui concerne les aspects juridiques, techniques et opérationnels de la modernisation de la protection de la vie privée pour un monde numérique.

La période de consultation pour cette proposition se terminera le **16e octobre 2020**.

2 La protection de la vie privée en Ontario : 2020

Les données à l'ère numérique : La nécessité de la protection de la vie privée

Les technologies et services numériques ont permis l'innovation, mais comportent de nouveaux risques tels que les atteintes à la protection des données, l'usurpation d'identité, la surveillance et la vente de données commerciales. Les entreprises collectent désormais un plus grand nombre de renseignements auprès de leurs clients, y compris leur emplacement géographique, leurs communications personnelles et leurs préférences d'achat. Ces évolutions ont rendu les choses plus complexes pour les Ontariens afin d'exercer un contrôle sur la collecte, l'utilisation et la divulgation de leurs renseignements personnels. Nous devons nous assurer que la transformation numérique se fait d'une manière qui permet de tirer les bénéfices de l'innovation centrée sur les données, tout en réduisant les risques pour la vie privée des Ontariens.

Ces changements dans le paysage numérique ont globalement provoqué une baisse de la confiance du public dans la protection de la vie privée. Le commissaire actuel à la protection de la vie privée du Canada et auteur du sondage auprès des Canadiens sur la protection de la vie privée de 2018-2019 indique que 92 % des répondants étaient plus ou moins préoccupés par la protection de leurs renseignements personnels. Les

Ontariens ont exprimé des préoccupations similaires dans le récent sondage sur la protection des consommateurs et lors des consultations sur la stratégie en matière de données de 2019. La pandémie de COVID-19 a mis en évidence l'importance et le besoin urgent de services numériques, pour lesquels la confiance dans la collecte, le traitement et le stockage des données reste un obstacle à une adoption par les utilisateurs et à une utilisation efficace.

Lois et tendances en matière de protection de la vie privée : L'Ontario, le Canada et d'autres pays dans le monde

Actuellement, la province de l'Ontario ne possède pas de réglementation concernant la protection de la vie privée dans le secteur privé. Les lois provinciales actuelles[1] régissent uniquement la collecte, l'utilisation et la divulgation des renseignements personnels par des institutions gouvernementales et certains fournisseurs de soins de santé. Pour le secteur privé, l'Ontario s'appuie plutôt sur une loi fédérale, à savoir la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE). Cependant, les provinces de l'Alberta, du Québec et de la Colombie-Britannique ont choisi d'adopter des lois sur la protection de la vie privée adaptées au secteur privé. Au début de l'année 2020, le Québec a par exemple adopté le projet de loi nº 64, qui renforce également les droits à la vie privée et les exigences en la matière applicables aux organismes publics et privés.

En 2018, la Commission européenne a adopté le Règlement général sur la protection des données (RGPD), qui a considérablement renforcé les mesures de protection de la vie privée dans l'Union européenne en introduisant des exigences plus strictes en matière de consentement, de transparence et d'application de la loi, et donné un plus grand contrôle aux particuliers sur leurs données personnelles. Depuis lors, de nombreux pays et territoires à travers le monde ont mis à jour leurs cadres législatifs pour s'harmoniser avec cette nouvelle norme mondiale. Le gouvernement fédéral du Canada a indiqué son intention de moderniser la LPRPDE, mais à ce jour, aucune modification importante n'a été apportée.

Examiner les domaines d'amélioration pour l'Ontario

La série de sujets de discussion relatifs à la protection de la vie privée est énumérée ci-dessous, et chacun des sujets est expliqué plus en détail à la section suivante. Ces

[1] *Loi sur l'accès à l'information et la protection de la vie privée (FIPPA), Loi sur l'accès à l'information municipale et la protection de la vie privée (MFIPPA,* et *Loi sur la protection des renseignements personnels sur la santé* (*PHIPA)*

sujets concernent les principaux domaines que le gouvernement étudie pour élaborer une loi ontarienne sur la protection de la vie privée et sont les suivants :

1. une plus grande **transparence** pour les particuliers, donnant aux Ontariens plus de détails sur la façon dont leurs renseignements personnels sont utilisés par les entreprises et les organismes;

2. des dispositions claires sur le **consentement**, permettant aux particuliers de révoquer leur consentement à tout moment, et adoptant un modèle « à option d'adhésion » pour les utilisations secondaires de leurs renseignements personnels;

3. le droit pour les particuliers de demander la **suppression ou désindexation** de leurs renseignements personnels, sous réserve des restrictions applicables (ce droit est aussi connu sous le nom d'« effacement » ou de « droit à l'oubli »);

4. le droit pour les particuliers d'obtenir leurs données dans un format numérique standard et **portable**, leur donnant ainsi une plus grande liberté pour changer de fournisseur de services sans perdre leurs données (ce droit s'appelle la « portabilité des données »);

5. l'attribution de 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) pour appuyer la conformité à la loi, y compris le pouvoir d'imposer des sanctions si nécessaire;

6. la mise en place d'exigences et de possibilités d'utilisation de données qui ont été **dépersonnalisées et tirées** de renseignements personnels, dans un souci de clarté de l'applicabilité des mesures de protection de la vie privée;

7. l'élargissement du **champ d'application** de la loi afin d'inclure les organisations non commerciales, y compris les organismes sans but lucratif, les organismes de bienfaisance, les syndicats et les partis politiques;

8. la création d'un cadre législatif établissant un régime juridique plus moderne concernant la protection de la vie privée, qui permettrait un éventail de mécanismes d'appui de la conformité comme l'établissement de **fiducies de données** pour le partage de données respectant la protection de la vie privée.

3 Principaux domaines à réformer

Les sujets ci-dessous concernent les nouveaux domaines de réflexion pour l'Ontario sur la base des exigences légales mises en place dans d'autres territoires, et auxquels font face de nombreuses entreprises canadiennes dans l'exercice de leurs activités à l'échelle mondiale. Même s'ils ne constituent ni une liste exhaustive ni une approche définitive, ces sujets visent à orienter le débat.

Plus de consentement et de transparence

Au Canada, les lois sur la protection de la vie privée dans le secteur privé s'appuient sur le consentement des consommateurs comme étant le principal outil juridique pour la collecte et l'utilisation de leurs renseignements personnels. Les entreprises sont tenues de publier les détails relatifs à la collecte des données des consommateurs et leurs pratiques en matière d'utilisation dans des politiques sur les services et dans des déclarations de confidentialité. Toutefois, ces politiques et déclarations sont rédigées dans un jargon juridique très dense, qui semble souvent obscur pour les particuliers lorsqu'ils s'inscrivent à de nouveaux services, ce qui les dissuade d'aller plus loin. La fréquence de collecte ajoute souvent à la confusion du public : les renseignements personnels sont collectés de façon si régulière et automatique qu'on ne peut s'attendre à ce que les clients donnent leur consentement chaque fois que leurs renseignements personnels sont collectés.

Pour relever ces défis, le gouvernement réfléchit actuellement à la refonte des normes relatives au consentement et à la transparence, et envisage d'autres modèles qui dotent les Ontariens de meilleurs outils pour prendre des décisions avisées au sujet de leurs fournisseurs de services, et exercer un plus grand contrôle sur la collecte, l'utilisation et la divulgation de leurs renseignements personnels. L'Ontario envisage les options suivantes :

- Demander aux entreprises de fournir des renseignements précis et en langage clair sur l'utilisation des renseignements personnels : en indiquant quels sont les renseignements personnels collectés, comment ils sont collectés, comment ils sont utilisés, et à quels tiers ces renseignements seront communiqués. Grâce à des exigences claires en matière de transparence, les particuliers comprendraient quand et comment leurs renseignements personnels sont collectés, et ne devraient donner leur consentement que pour les collectes, utilisations et divulgations de renseignements personnels n'entrant pas dans le champ d'application des pratiques décrites par l'entreprise.

- Clarifier les exigences en matière de consentement tout en clarifiant les exceptions au consentement. Il y a des cas où le consentement individuel n'est pas nécessaire, possible ou approprié, notamment dans les cas où les données collectées ont été « dépersonnalisées » ou « tirées » (voir les définitions et la discussion à ce sujet ci-dessous) et utilisées au profit du particulier ou du bien public général (p. ex. à des fins de recherche ou d'innovation). Ces exceptions seraient également envisagées lors de l'examen du sujet global du consentement et de la transparence, et de son application à l'Ontario.

- Pour toutes les autres collectes, utilisations et divulgations de renseignements personnels, l'entreprise devrait obtenir un consentement affirmatif, démontrable, éclairé et univoque. Demander aux particuliers d'« adhérer » à la collecte, à l'utilisation ou à la divulgation serait l'option par défaut la plus respectueuse des principes de protection de la vie privée. Des dispositions améliorées en matière de consentement et de transparence ne permettraient pas aux entreprises de collecter des renseignements sans condition, mais permettraient un accord et une entente plus explicites entre les particuliers et leurs fournisseurs de services.

Droits sur les données : L'effacement et la portabilité

Le RGPD adopte une approche fondée sur les droits en matière de protection de la vie privée, et a introduit de nouveaux concepts de droits numériques que d'autres pays ont adoptés. Certains de ces droits numériques existent déjà dans la loi canadienne sur la protection de la vie privée, comme la possibilité d'accéder à ses renseignements personnels ou de les corriger, ou la possibilité de retirer son consentement afin d'empêcher qu'une entreprise ne les utilise. Toutefois, certains droits numériques ne sont pas accessibles aux Ontariens à l'heure actuelle. Deux des plus importants de ces droits sont la « portabilité des données » et l'« effacement des données ».

Effacement des données

Aussi connu sous le nom de « droit à l'oubli », le droit à l'effacement des données permet aux particuliers de demander aux entreprises de désindexer (retirer des résultats de recherche ou des références en ligne) ou de supprimer leurs renseignements personnels lorsqu'elles n'ont plus besoin de fournir un service. Ce principe peut s'appliquer lorsque le particulier a retiré son consentement pour que l'entreprise utilise ses renseignements personnels, ou lorsque l'utilisation des renseignements personnels était illégale dès le départ. Ce droit est de plus en plus important à l'ère des services numériques, car il permet aux particuliers de gérer plus directement la protection de leur vie privée et leur réputation.

Même dans les pays où il a été mis en œuvre, le droit à l'effacement n'est pas illimité, et une solution à l'échelle de l'Ontario veillerait à ne pas élargir de façon excessive le champ d'application de cette exigence de manière à permettre sa mise en œuvre par les entreprises. Dans le RGPD, par exemple, le droit à l'effacement ne s'applique pas lorsque les données sont nécessaires pour exercer le droit à la liberté d'expression, respecter une obligation légale, effectuer une tâche dans l'intérêt public, ou dans l'exercice d'une autorité officielle. Ce droit peut également être limité pour des raisons d'intérêt public, y compris la santé publique, l'archivage, la recherche scientifique, historique ou statistique, ou pour l'établissement, l'exercice ou la défense de droits légaux.

Portabilité des données

Le droit à la portabilité des données permet aux Ontariens d'accéder à leurs renseignements personnels. Il permet notamment aux particuliers de demander que leurs renseignements personnels leur soient fournis dans un format ouvert et accessible. = La portabilité des données donnera aux particuliers un plus grand degré de contrôle sur leurs données personnelles. Cela signifie qu'un particulier aurait le droit d'extraire toutes ses données personnelles auprès d'une entreprise ou d'un organisme (par exemple, une plateforme de médias sociaux) et de les transférer sous une forme structurée, facilement utilisable et possiblement normalisée vers une plateforme différente qui offre un service similaire.

La portabilité des données permet aux consommateurs de « voter avec leurs pieds ». Un autre fournisseur de services peut offrir de meilleures mesures de protection de la vie privée ou de meilleurs services. Cela permet de créer une plus grande concurrence entre les fournisseurs de services, favorise de nouveaux biens et services innovants, et donne aux particuliers la possibilité de changer plus facilement de fournisseur de services sans perdre l'accès à ses données personnelles.

Surveillance, application de la loi et amende

La réglementation en matière de protection de la vie privée n'est efficace que si elle est respectée. Divers outils peuvent être utilisés pour aider et inciter les organisations à respecter la réglementation. Par exemple, le mandat du CIPVP peut être élargi pour lui permettre de fournir des conseils et des orientations aux petites organisations. Le CIPVP occupe une position unique qui lui permet de travailler de manière constructive avec le secteur privé, comme c'est déjà le cas avec les institutions publiques, afin de proposer les meilleures pratiques visant à rendre les organisations plus efficaces en matière de protection de la vie privée.

Les stratégies relatives à la conformité peuvent viser aussi bien l'éducation, la recherche, l'orientation et les services-conseils que les bacs à sable réglementaires. La pandémie de COVID-19 a contraint de nombreuses entreprises à numériser des services du jour au lendemain, sans mettre en place une architecture solide pour la protection de la vie privée et la cybersécurité. Un régime efficace de protection de la vie privée n'adopterait pas une approche « unique », mais définirait différentes stratégies pour les petites, moyennes et grandes organisations, et inciterait au respect des règles en donnant des exemples positifs, en défendant les meilleures pratiques et en favorisant les solutions novatrices.

Cette approche proactive et positive de la conformité serait certes préférable, mais une boîte à outils réglementaire ne serait pas complète sans la capacité de faire appliquer la loi. Les sanctions constituent un moyen pour le CIPVP de faire respecter la loi. L'une des principales caractéristiques de la réforme de la protection de la vie privée dans d'autres pays est le pouvoir d'un organisme de surveillance de rendre des ordonnances à l'encontre des organisations qui enfreignent la loi et d'imposer des amendes dans les cas graves de non-conformité. En Europe, ces amendes peuvent atteindre 20 millions d'euros, soit 4 % du chiffre d'affaires annuel d'une entreprise.

Ce pouvoir d'imposer des ordonnances et des amendes est généralement absent du régime canadien d'application de la loi sur la protection de la vie privée. Le commissaire à la protection de la vie privée du Canada est actuellement habilité à enquêter sur des plaintes et à émettre des recommandations non contraignantes ainsi que des rapports publics sur les pratiques d'une organisation en matière de protection de la vie privée. En attendant, le CIPVP peut rendre des ordonnances exécutoires à l'égard de la LAIPVP, la LAIMPVP (uniquement pour l'accès) et la LPRPS (pour l'accès et la vie privée). En l'absence d'une loi sur le secteur privé en Ontario, ces pouvoirs de rendre des ordonnances ne s'étendent pas à la collecte, l'utilisation ou la divulgation de renseignements personnels par des organisations du secteur privé.

Il est essentiel de renforcer le régime d'application de la loi pour moderniser les mesures de protection de la vie privée. Par exemple, le fait de permettre au CIPVP de rendre des ordonnances exécutoires relatives à la protection de la vie privée aux organisations garantirait que ces organisations respectent le droit à la vie privée des personnes. Imposer des amendes selon une grille de sanctions devrait renforcer la confiance du public envers l'application de la loi et donc de favoriser les bonnes pratiques en matière de protection de la vie privée chez les acteurs commerciaux. Une surveillance et une responsabilité accrues pourraient également permettre au CIPVP de traiter les plaintes du public, de lancer des enquêtes, d'exiger des organisations qu'elles signalent les infractions importantes à la vie privée ou de prendre des mesures publiques en réponse aux enquêtes sur la vie privée.

Application aux organisations non commerciales

La loi fédérale sur la protection de la vie privée, la LPRPDE (*Loi sur la protection des renseignements personnels et les documents électroniques*) s'applique aux organisations qui collectent, utilisent ou communiquent des renseignements personnels dans le cadre d'activités commerciales. Si une organisation effectue des transactions liées à la vente, à l'échange de marchandises ou à la location, elle doit se conformer à la LPRPDE. La loi fédérale ne s'applique toutefois pas aux autres catégories de renseignements personnels, tels que les renseignements personnels des employés, les données génétiques, les données biométriques, qui ne sont pas liés aux activités commerciales d'une organisation (certaines exceptions incluent les organisations sous réglementation fédérale comme les banques, les compagnies aériennes, les compagnies de téléphone ou de radiodiffusion).

Ainsi, beaucoup d'organisations présentes en Ontario ne sont actuellement soumises à aucune loi sur la protection de la vie privée. Il s'agit notamment des organisations à but non lucratif, des organisations caritatives, des associations professionnelles, des syndicats et des partis politiques. Il s'agit là d'une lacune importante dans le cadre de la protection de la vie privée au Canada. L'Alberta, la Colombie-Britannique et le Québec ont tous introduit des lois sur la protection de la vie privée dans le secteur privé de portée plus large, qui s'appliquent à toutes les organisations qui recueillent, utilisent et communiquent des renseignements personnels.

Dans le cadre d'une réforme de la protection de la vie privée dans le secteur privé, la portée et l'application des protections sont des éléments importants à prendre en considération. Il apparaît essentiel dans tout régime moderne de protection de la vie privée que les renseignements personnels de nature sensible soient protégés, qu'ils soient détenus par une entreprise commerciale ou par un organisme à but non lucratif. Des règles cohérentes pour tous les types d'organisations du secteur privé contribueraient à garantir une protection uniforme de la vie privée.

Renseignements personnels dépersonnalisés, données tirées de renseignements personnels

L'économie moderne de l'innovation est alimentée par des données dépersonnalisées, qui ne sont pas très différentes de la façon dont le pétrole a alimenté l'économie du 20^{e} siècle. Les données « dépersonnalisées » sont des données personnelles qui ont été regroupées de manière à empêcher la reconnaissance des données personnelles de quiconque se trouvant dans le lot. Les méthodes de dépersonnalisation comprennent la suppression des « éléments d'identification » (p. ex., les noms, les numéros d'identification), le recours au brouillage de l'information (p. ex., l'indication

d’une tranche d’âge au lieu de l’âge exact), et la suppression ou le regroupement des renseignements sur les personnes dont les données sont atypiques ou dont la taille des cellules est petite (p. ex., lorsque moins de cinq personnes ont le même code postal).

Les données « tirées » de renseignements personnels sont des données que les entreprises peuvent avoir sur les clients et qui n’ont pas été directement fournies par le client. Ce type de données (telles que les évaluations) réutilise des renseignements personnels qui ont été fournis précédemment, ainsi que d’autres comportements enregistrés (tels que les habitudes de navigation sur le web). Par exemple, les entreprises peuvent classer les clients en fonction de leurs habitudes d’achat observées, ou obtenir d’autres indications sur les habitudes de chacun.

Au Canada, ce type de données ne s’inscrit pas parfaitement dans le cadre de la protection de la vie privée. Il n’existe pas un ensemble de règles claires sur la manière dont les organisations doivent gérer les renseignements personnels dépersonnalisés ou les données tirées de renseignements personnels. Par souci de clarté vis-à-vis des organisations et pour inspirer confiance à la population, la province de l’Ontario pourrait envisager de définir plus précisément ces concepts dans la loi et d’établir des lignes directrices bien définies sur la manière dont les règles de protection de la vie privée s’appliquent à ces types de données. Étant donné que l’utilisation de données dépersonnalisées réduit le risque d’atteinte à la vie privée, nous examinerons les moyens de promouvoir l’amélioration et le déploiement de ces pratiques dans le secteur privé, par exemple en incitant les entreprises à concevoir des applications protégeant la vie privée ou en soutenant la création de nouvelles normes techniques.

Permettre le partage des données pour l’innovation, tout en protégeant la vie privée

Les lois sur la protection de la vie privée fixent des limites sur la manière dont les organisations peuvent échanger des renseignements personnels. Ces limites sont certes importantes, mais elles représentent souvent un défi pour la recherche et l’innovation. Les réserves de données peuvent entraver l’innovation puisqu’elles réduisent le nombre de groupes ou de secteurs autorisés à utiliser les données pour élaborer de nouvelles idées ou améliorer les services.

Les nouveaux modèles de gouvernance des données — où les renseignements personnels, les renseignements personnels dépersonnalisés ou les données regroupées peuvent être échangés entre différents acteurs ou secteurs — pourraient contribuer à stimuler l’innovation pour le bien public ou pour un intérêt commun entre des organisations bien précises. En réunissant des données provenant de différents

secteurs et acteurs, il est possible de les exploiter à de nouvelles fins dans l'intérêt public.

Parfois appelés « fiducies de données », ces nouveaux modèles de gouvernance des données permettent aux organisations de désigner une personne comme gardien ou gestionnaire des données, de convenir d'un ensemble de règles standard pour le partage des données et de garantir que toute personne ayant accès à la fiducie utilise les données conformément à ces règles. Si le concept des fiducies de données est encore relativement nouveau, l'établissement de lignes directrices, de principes ou de normes pour l'utilisation de ces fiducies peut ouvrir de nouveaux modèles de partage de données pour la protection de la vie privée, la promotion de la collaboration, le développement économique et des solutions innovantes aux problèmes de société.

La confidentialité de vos données est importante

Nous vous demandons de nous faire part de vos commentaires pour nous permettre de mieux comprendre les préoccupations des Canadiens en matière de protection des renseignements personnels et la meilleure façon de répondre à ces préoccupations, que ce soit au moyen d'une politique, d'une loi ou d'un règlement.

Ces renseignements seront utilisés par le ministère des Services gouvernementaux et des Services aux consommateurs pour nous aider à élaborer un cadre de protection de la vie privée pour l'Ontario qui répond à vos besoins.

Si vous donnez votre adresse courriel, elle ne sera pas associée à vos commentaires et ne sera utilisée que pour vous tenir au courant de cette initiative et vous informer des consultations à venir. Votre adresse courriel ne sera pas ajoutée aux listes de diffusion ni communiquée à des tiers, sauf dans les cas autorisés par la loi.

Pour toute question concernant l'utilisation des renseignements recueillis sur cette page, veuillez communiquer avec nous :

Chef de l'Unité des stratégies et des politiques relatives à l'accès à l'information et à la protection de la vie privée
Ministère des Services gouvernementaux et des Services aux consommateurs
Direction de la conservation des documents, de l'accès à l'information et de la protection de la vie privée pour la FPO
134 Ian Macdonald Blvd.
Toronto (Ontario)
M7A 2C5