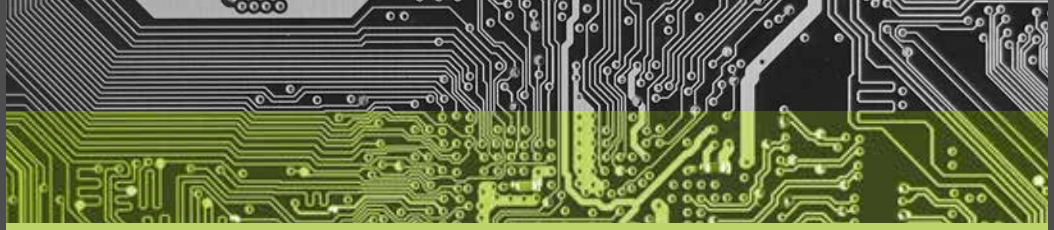

AVRIL 2018

FEUILLE-INFO
SUR LA TECHNOLOGIE

Les villes intelligentes et le droit à la vie privée

Les nouvelles technologies promettent d'aider les municipalités à mieux gérer l'environnement urbain et à fournir plus efficacement leurs services. Elles peuvent contribuer à rendre les collectivités plus agréables, durables et équitables. Bon nombre de ces technologies comportent la collecte et l'utilisation de grandes quantités de données, y compris de renseignements personnels. Les villes et autres municipalités qui utilisent ces technologies connectées sont souvent appelées des « villes intelligentes ».

Cette feuille-info destinée au grand public explique le concept de ville intelligente et son incidence possible sur la vie privée des particuliers

Le Bureau du commissaire à l'information et à la protection de la vie privée de l'Ontario (CIPVP) est un organisme indépendant qui surveille l'application de la *Loi sur l'accès à l'information municipale et la protection de la vie privée* (*LAIMPVP*). Cette loi protège la confidentialité des renseignements personnels en régissant leur collecte, leur utilisation et leur divulgation par les municipalités et les institutions municipales. Elle confère également aux particuliers le droit d'accéder aux renseignements personnels qui les concernent.

Le CIPVP a élaboré la présente feuille-info destinée au grand public pour expliquer la notion de ville intelligente et son incidence possible sur la vie privée des particuliers.

QUE SONT LES « VILLES INTELLIGENTES »?

Les villes intelligentes utilisent des technologies de collecte de données en vue d'améliorer la gestion et la prestation des services municipaux, d'appuyer la planification et l'analyse et de favoriser l'innovation au sein de la collectivité. En recueillant de grandes quantités de données, souvent en temps réel, les municipalités peuvent mieux évaluer la qualité et l'efficacité de leurs services. Par exemple, des données sur la

Information and Privacy Commissioner of Ontario
Commissaire à l'information et à la protection de la vie privée de l'Ontario

circulation automobile peuvent permettre de relever les endroits où il y a des bouchons et éclairer ainsi l'aménagement et le design urbain. Il est également possible d'associer les données recueillies et d'autres sources de données et d'utiliser la technologie de l'analytique pour découvrir des tendances et des liens dans de grands ensembles de données.

Il peut en résulter des mesures « intelligentes », par exemple :

- envoyer un signal aux éboueurs lorsque des détecteurs indiquent que des poubelles sont pleines;
- mettre en marche des dispositifs d'arrosage dans les parcs lorsque des détecteurs indiquent que le sol est sec;
- synchroniser les feux de circulation en fonction de la circulation automobile;
- diriger des véhicules autonomes vers des places de stationnement libres au moyen de données de localisation GPS.

Souvent, les renseignements que recueillent, utilisent, conservent et divulguent les villes intelligentes comprennent des renseignements personnels

QUELS SONT LES RENSEIGNEMENTS RECUEILLIS ET COMMENT SONT-ILS RECUEILLIS?

Souvent, les renseignements que recueillent, utilisent, conservent et divulguent les villes intelligentes comprennent des renseignements personnels. Par exemple, certaines technologies de ville intelligente recueillent des renseignements que contiennent les appareils mobiles des particuliers, notamment sur leurs allées et venues dans la ville.

Les municipalités peuvent aussi recueillir des renseignements personnels au moyen d'appareils qui lui appartiennent, comme des dispositifs d'enregistrement audio et vidéo ou des lecteurs de plaque d'immatriculation.

Les municipalités peuvent conclure des ententes de partage de renseignements avec des tiers, tels que des fournisseurs d'applis de téléphone intelligent, ou des entreprises qui installent et gèrent des détecteurs et des infrastructures de communication. En vertu de ces ententes, ces tiers peuvent être autorisés à recueillir et à utiliser des renseignements personnels pour leurs propres fins de même que pour les fins de la municipalité, ou être tenus de le faire.

À QUI APPARTIENNENT LES RENSEIGNEMENTS?

Les municipalités doivent s'assurer que les renseignements autres que les renseignements personnels que recueillent leurs partenaires du secteur privé sont accessibles au public. Elles peuvent le faire en s'assurant que, dans leurs contrats, elles ne cèdent pas la propriété de ces renseignements à ces partenaires, qui les utiliseraient à des fins commerciales.

Un service de police américain a retenu les services d'un fournisseur de logiciels pour recueillir et analyser des données sur des affaires criminelles et civiles. Lorsque leur contrat a pris fin, le service de police a perdu l'accès à une grande quantité de données et aux indications qu'il avait été possible d'obtenir grâce à elles, car le fournisseur de logiciels avait établi qu'il était titulaire de droits de propriété intellectuelle liés à ces données.

QUELLE PEUT-ÊTRE L'INCIDENCE DES VILLES INTELLIGENTES SUR LA VIE PRIVÉE?

La prudence est de mise pour éviter que les villes intelligentes ne deviennent des infrastructures de surveillance de masse

Lorsque les municipalités utilisent des technologies pour recueillir des renseignements personnels à quelque fin que ce soit, elles doivent se conformer à la *LAIMPVP*. Le concept de ville intelligente suscite différentes inquiétudes au sujet de cette conformité. En voici des exemples.

Collecte non autorisée de renseignements personnels et surveillance

La *LAIMPVP* autorise les municipalités à recueillir les renseignements personnels qui sont nécessaires au bon exercice d'activités autorisées par la loi. La collecte de renseignements personnels qui ne sont pas nécessaires au bon exercice de ces activités n'est pas permise.

Les technologies de ville intelligente permettent de recueillir des renseignements sur les résidents qui se livrent à leurs activités quotidiennes; elles pourraient donner lieu à la création de profils personnels décrivant les comportements, les intérêts et les interactions des particuliers, surtout si ces renseignements sont combinés à d'autres données.

Une grande ville européenne a installé des poubelles et des bacs de recyclage « intelligents » reliés à Internet, dotés sur les deux côtés de grands écrans vidéo diffusant des nouvelles, des renseignements et des publicités. Ces contenants captaient également les signaux des appareils sans fil des passants à leur insu; ces signaux pouvaient servir à les identifier et à retracer leurs déplacements. Au cours du premier mois de fonctionnement de ces appareils, plus d'un million d'appareils distincts ont été enregistrés. Devant les protestations du public, la ville a mis hors service ses « poubelles espionnes ».

Utilisation de renseignements personnels à des fins secondaires

La *LAIMPVP* limite l'utilisation des renseignements personnels. Ces limites s'appuient sur un principe fondamental de la protection de la vie privée selon lequel les renseignements personnels peuvent servir uniquement aux fins pour lesquels ils ont été obtenus ou à des fins compatibles, sauf dans des cas exceptionnels. Par exemple, des renseignements personnels recueillis aux fins de la prise de décisions en matière d'urbanisme ne doivent pas servir à exposer des particuliers à de la publicité ciblée, car cela représenterait une utilisation secondaire interdite aux termes de la *LAIMPVP*.

Les technologies connectées complexes des villes intelligentes peuvent être vulnérables aux pirates informatiques

> Les systèmes de détection de coups de feu sont une technologie de ville intelligente qui consiste à installer des micros sur les lampadaires afin de déceler les endroits où se produisent des coups de feu, lesquels sont signalés rapidement à la police. Or, ces micros peuvent aussi capter des conversations à des fins très différentes.

Divulgation non autorisée de renseignements personnels

La *LAIMPVP* oblige les municipalités de l'Ontario à prendre des mesures raisonnables pour prévenir la consultation et la divulgation non autorisées de renseignements personnels.

Comme toutes les technologies connectées complexes, les systèmes de ville intelligente sont vulnérables aux pirates informatiques. Plus les points de collecte et de traitement des renseignements et d'accès aux systèmes sont nombreux, plus le risque d'atteinte à la sécurité est élevé. Une atteinte à la vie privée peut également survenir à la suite de l'accès non autorisé à des renseignements personnels par des employés de la municipalité ou des tiers et de l'utilisation inappropriée de ces renseignements.

> Une ville canadienne ayant offert à ses résidents une appli pour se renseigner sur les horaires de ramassage des ordures, des matières à recycler et des résidus de jardin a découvert que la base de données de cette appli avait été piratée, révélant des renseignements personnels sur des milliers de résidents.

Certains souhaitent ardemment que des renseignements recueillis au moyen des technologies de ville intelligente soient accessibles au public afin de stimuler l'innovation dans les collectivités. Les municipalités doivent veiller à retirer tout renseignement personnel ou identificatoire des données qu'elles divulguent à des tiers ou qu'elles rendent publiques dans le cadre d'initiatives de données ouvertes.

COMMENT MINIMISER LES RISQUES POUR LA VIE PRIVÉE?

Il est possible de minimiser les risques et de protéger la vie privée des particuliers grâce à une planification et à une conception appropriées. Pour protéger la vie privée dans le cadre de projets de ville intelligente, les municipalités peuvent prendre notamment les mesures suivantes :

- Mener des **évaluations de l'incidence sur la vie privée et ainsi que des menaces et des risques**. Il s'agit là d'outils généralement reconnus pour relever les risques pour la vie privée et la sécurité et déterminer les mesures à prendre pour les réduire. Elles devraient être effectuées lors de la conception de nouvelles technologies et de nouveaux programmes comportant la collecte de renseignements personnels.
- Concevoir et utiliser la technologie selon une approche fondée sur la **minimisation des données**. Selon cette approche, les municipalités veillent à ce qu'elles et les tiers à qui elles font appel évitent de recueillir, d'utiliser, de conserver ou de divulguer des renseignements personnels s'ils peuvent utiliser d'autres renseignements aux mêmes fins. Dans tous les cas, il faut privilégier si possible des solutions de rechange qui ont moins d'incidence sur la vie privée pour atteindre les objectifs fixés.
- Lorsqu'il faut recueillir des renseignements personnels, veiller à en retirer dans les plus brefs délais tous les renseignements identificatoires. Dans la mesure du possible, les municipalités et leurs représentants devraient utiliser, conserver et divulguer uniquement des renseignements **anonymisés**.
- Mettre sur pied un programme de gestion de la protection de la vie privée et de l'accès à l'information comprenant des politiques et procédures de sécurité complètes, une surveillance rigoureuse des tiers et des politiques sur les mesures à prendre en cas d'attente à la vie privée. Ce programme doit également permettre aux particuliers d'exercer leur droit d'accéder aux renseignements personnels qui les concernent.
- **Mobiliser la collectivité et assurer la transparence** du projet afin que tous les citoyens comprennent son incidence possible sur eux et leurs possibilités de participation et d'expression de leur point de vue.
- Lorsque la loi l'exige, obtenir le **consentement** éclairé des particuliers dont les renseignements personnels pourraient être utilisés et divulgués, ou obliger les tiers concernés à l'obtenir. Dans la mesure du possible, les particuliers devraient avoir le choix de ne pas participer.

Il est possible de minimiser les risques et de protéger la vie privée grâce à une planification et à une conception appropriées

QUE FAIT LE CIPVP POUR PROTÉGER MA VIE PRIVÉE?

Le CIPVP est déterminé à protéger votre vie privée. Pour les municipalités et collectivités ontariennes, le concept des villes intelligentes représente de nouveaux défis et de nouvelles occasions à exploiter. Nous croyons qu'avec une planification attentive et la sensibilisation aux questions uniques que soulèvent les technologies de ville intelligente, il sera possible de recueillir et d'utiliser des renseignements personnels dans le respect de la vie privée. Le CIPVP collabore avec des chefs de file locaux et nationaux pour préconiser la transparence et assurer l'intégration de mesures de protection de la vie privée dans les initiatives de ville intelligente.

QUELS SONT MES DROITS EN VERTU DES LOIS ONTARIENNES SUR LA PROTECTION DE LA VIE PRIVÉE?

La collectivité où vivez est aussi la vôtre. Vous pouvez contribuer à orienter son avenir et à protéger vos renseignements personnels et votre vie privée.

Si vous avez des questions sur les renseignements personnels que recueille une municipalité ou leur utilisation, consultez son site Web ou communiquez avec elle pour obtenir de plus amples renseignements.

Pour obtenir une copie des renseignements qu'une municipalité détient à votre sujet, vous pouvez déposer une demande d'accès à l'information. Pour en savoir davantage sur la marche à suivre et sur ce que vous pouvez faire pour protéger votre vie privée, consultez le site Web du CIPVP à **www.ipc.on.ca**.

RESSOURCES SUPPLÉMENTAIRES

- **Que sont les renseignements personnels?**
- **Les mégadonnées et le droit à la vie privée**
- **Open Government and Protecting Privacy**

Information and Privacy Commissioner of Ontario
Commissaire à l'information et à la protection de la vie privée de l'Ontario