Explicatif : Données de localisation

La possibilité de savoir où un individu se trouvait, se trouve à l'heure actuelle ou pourrait se trouver est très alléchante pour divers organismes privés ou publics, dont les spécialistes en marketing, les compagnies de télécommunications, les urbanistes, les corps policiers ou les responsables de la santé publique. La valeur des données de localisation est commerciale ou sociale, voire les deux, et varie selon la méthode de leur collecte, les organismes qui s'y intéressent et le but qu'elles pourraient servir. Les distinctions — si importantes dans les lois sur la protection de la vie privée — qui prévalaient entre les secteurs public et privé s'estompent de plus en plus, les organismes publics achetant les données recueillies par le secteur privé ou s'associant à ce dernier. Il en résulte diverses préoccupations liées à la protection de la vie privée des individus dont les données sont en cause.

Les données de localisation sont de plus en plus faciles à recueillir grâce à l'ubiquité des téléphones intelligents que nous transportons tous. Un nombre croissant d'applications fait appel à la localisation GPS et aux technologies sans fil Wi-Fi et Bluetooth utilisées par ces appareils pour déterminer notre emplacement exact à un moment donné. Ces données de localisation, que l'on peut facilement recueillir n'importe quand en temps réel, permettent désormais de suivre nos déplacements à la trace, de notre maison à notre bureau, en passant par la maison de notre grand-mère, l'épicerie, l'église, la clinique, bref, tous ces endroits qui jalonnent notre vie. Ces données peuvent donc révéler des particularités de notre comportement, les liens que nous entretenons, nos convictions religieuses ou notre état de santé. Il s'agit là de renseignements de nature sensible et personnelle.

Les usages que l'on fait des données de localisation sont nombreux :

- Les applications de navigation assistée par ordinateur font appel aux données GPS des téléphones intelligents pour évaluer la congestion routière et la durée des déplacements;
- Les applications d'entraînement physique font aussi appel à ces données GPS pour calculer les distances parcourues et la vitesse de déplacement à pied, à vélo ou à la course;
- Les réseaux sociaux permettent à leurs usagers de « faire rapport » en indiquant leur emplacement, et permettent aux concepteurs d'utiliser des interfaces de programmation d'applications pour que les usagers interagissent avec leurs sites;
- Les magasins physiques peuvent utiliser les signaux Wi-Fi ou Bluetooth qu'émet notre téléphone pour nous suivre à la trace au moyen de l'identifiant MAC (contrôle d'accès au support) de ce dernier. Ces données peuvent facilement être reliées à notre nom ou à notre adresse, entre autres, et servir par la suite à nous proposer en ligne des publicités ciblées en fonction des magasins où nous sommes allés ou des produits que nous avons longuement étudiés en magasin.

La seule façon dont nous pourrions être mis au courant de ces usages est souvent au moyen de ces interminables documents que sont les conditions générales d'utilisation ou les politiques

de protection des renseignements personnels. Les usagers ne lisant presque jamais ces documents, et ceux qui le font se heurtant souvent à des formulations vagues qui ne permettent de déterminer ni les renseignements qui sont recueillis ni les communications ou usages qui en sont faits, la situation est donc problématique. En d'autres termes, même si un usager consent à ce que ses données de localisation soient recueillies, ce consentement n'a aucune valeur. L'usager se voit donc privé de presque tout contrôle ou pouvoir de négociation face aux organismes qui recueillent, utilisent ou communiquent ses données.

Les recherches effectuées jusqu'ici n'ont permis de découvrir aucune preuve de l'efficacité de l'anonymisation des données de localisation. À titre illustratif, une étude du MIT fréquemment citée rapporte que le recoupement de deux vastes échantillons de données dépersonnalisées, l'un provenant d'un opérateur de téléphonie mobile et l'autre d'une compagnie de transport, a permis d'identifier les usagers dans 17 % des cas sur la base d'une semaine de données et dans plus de 55 % des cas pour un mois de données. Selon les chercheurs, la combinaison de ces données avec des traces GPS permettrait d'identifier jusqu'à 95 % des usagers en recourant à moins d'une semaine de données. [i] Étant donné l'importance de ce risque, les données de localisation devraient donc être jugées de nature sensible et traitées en conséquence.

Partenariats publics-privés, législation sur la vie privée et données de localisation

Secteur privé : la loi fédérale canadienne sur la protection de la vie privée dans le secteur privé, la *Loi sur la protection des renseignements personnels et les documents électroniques*, s'applique à la collecte de renseignements personnels dans le cadre d'activités commerciales partout au pays, sauf en Alberta, en Colombie-Britannique et au Québec, ces trois provinces disposant de leur propre loi substantiellement similaire en la matière. Le commissariat à la vie privée du Canada affiche sur son site Web un document explicatif sur cette loi fédérale.

Secteur public : il existe un certain nombre de lois qui s'appliquent aux municipalités, aux provinces, aux territoires et aux organismes de compétence fédérale. Si des données de localisation doivent être recueillies dans le cadre d'un partenariat public-privé, il faut déterminer la loi pertinente et les obligations en matière de reddition de comptes qui en découlent. À titre d'exemple, le commissariat ontarien à l'information et à la protection de la vie privée s'est penché sur les préoccupations soulevées par un projet de ville intelligente, énoncées dans la fiche informative Les Villes intelligentes et le droit à la vie privée. On y apprend notamment le bien-fondé d'un bon modèle de gérance permettant de trancher au bénéfice de la population entre les impératifs commerciaux et les intérêts publics dans les données.

Données de localisation et modèles de gérance des données

Les modèles de gérance des données ne répondent pas à toutes les préoccupations en matière de vie privée que soulève la collecte de données de localisation. Ces modèles ne sont pas destinés à remplacer les pratiques exemplaires d'un consentement éclairé à la collecte, à l'utilisation, à la communication et à la conservation de données. Ils visent plutôt à atténuer les risques pour la vie privée que fait peser une collecte nécessaire et proportionnée de ces

données à des fins qui sont dans l'intérêt public. La réponse à la question de savoir si les bénéfices possibles de la collecte de données de localisation l'emportent sur les risques qu'elle fait peser pour la vie privée varie selon les situations et cette question doit être soigneusement évaluée. Il est même possible qu'il faille légiférer en la matière.

---

[i] Kondor, Dániel & Hashemian, Behrooz & Montjoye, Yves-Alexandre & Ratti, Carlo. (2017). *Towards matching user mobility traces in large-scale datasets. IEEE Transactions on Big Data*. PP. 10.1109/TBDATA.2018.2871693.

[ii] Voir par exemple la fiche ISO/IEC 20889:2018 *Terminologie et classification des techniques de dé-identification de données pour la protection de la vie privée*.