



ROBIC

+ DROIT
+ AFFAIRES
+ SCIENCES
+ ARTS

AVOCATS, AGENTS DE BREVETS ET DE MARQUES DE COMMERCE
DEPUIS 1892

GÉOLOCALISATION ET APPLICATIONS MOBILES: MODE D'EMPLOI POUR UNE GÉOLOCALISATION ÉLOIGNÉE DES PROBLÈMES JURIDIQUES!

VINCENT BERGERON ET THOMAS GAGNON-VAN LEEUWEN *

ROBIC, LLP

AVOCATS ET AGENTS DE BREVETS ET DE MARQUES DE COMMERCE

1. Introduction: la géolocalisation à l'ère des mégadonnées et des données ouvertes
2. Le droit d'auteur dans les données géographiques
 - a) Existence du droit d'auteur
 - i) *L'objet du droit d'auteur : la compilation de données*
 - ii) *L'originalité*
 - iii) *Les données géographiques comme compilation originale*
 - b) Violation du droit d'auteur dans le cadre de l'utilisation de données géographiques
 - c) Impact des amendements récents à la LDA
 - d) Licences relatives aux données géographiques
3. Protection de la vie privée
 - a) Introduction
 - b) Cadre législatif : vie privée et protection de renseignements personnels
 - i) *Secteur public*
 - ii) *Secteur privé*
 - c) Les données de géolocalisation comme renseignement personnel
 - d) Limites à la collecte, l'utilisation, la divulgation et la conservation de renseignements personnels : le consentement et autres principes
 - i) *Le consentement*
 - ii) *Au-delà du consentement*
 - iii) *Divulgation des renseignements personnels sans consentement*
 - iv) *Communication exigée par assignation, mandat ou ordonnance*
 - v) *Communication à une institution gouvernementale*
4. Conclusion

© CIPS 2015.

* Avocat et agent de marques de commerce, Vincent Bergeron est un des associés de ROBIC, S.E.N.C.R.L., un cabinet multidisciplinaire d'avocats, d'agents de brevets et d'agents de marques de commerce; Thomas Gagnon-Van Leeuwen est avocat dans le même cabinet. Publié dans *Développements récents en propriété intellectuelle 2015*, Service de la Formation continue du Barreau du Québec (Cowansville, Blais, 2015). Publication 447.

ROBIC, S.E.N.C.R.L.
www.robic.ca
info@robic.com

MONTRÉAL
1001, Square-Victoria - Bloc E - 8^e étage
Montréal (Québec) Canada H2Z 2B7
Tél.: +1 514 987-6242 Téléc.: +1 514 845-7874

QUÉBEC
2828, boulevard Laurier, Tour 1, bureau 925
Québec (Québec) Canada G1V 0B9
Tél.: +1 418 653-1888 Téléc.: +1 418 653-0006

1. Introduction: la géolocalisation à l'ère des mégadonnées et des données ouvertes

Que ce soit Uber¹ qui déplace chaque jour des milliers de personnes du point A au point B ou des montres intelligentes qui tracent le parcours précis du jogging de ceux et celles qui les portent, les applications mobiles et autres plateformes numériques guident et accompagnent aujourd'hui nos moindres déplacements. Waze, une application mobile de navigation «communautaire» qui permet aux conducteurs de se rendre à destination en évitant les embouteillages grâce aux données partagées par l'ensemble des utilisateurs du service². La Société de transport de Laval permet de son côté à ses usagers de voir l'emplacement précis de ses autobus en temps réel³, et la Société de transport de Montréal compte implanter un système similaire sous peu⁴. Au-delà du transport, des milliers d'images «géomarquées» sont partagées sur Instagram et Facebook, indiquant l'endroit précis où elles ont été prises.

Ces données de géolocalisation s'inscrivent dans le contexte des mégadonnées («*big data*»), cette quantité phénoménale de données qui existe au sujet des objets et personnes qui nous entourent. Les entreprises privées, que ce soit les géants de la technologie comme Apple et Google, ou les commerçants, assureurs ou développeurs d'applications mobiles, détiennent plus d'informations à propos de leurs clients et utilisateurs que jamais, voire même plus que les gouvernements dans certains cas.

En même temps, le mouvement en faveur de l'externalisation ouverte (le «*crowdsourcing*»), des données ouvertes et des villes intelligentes met à la disposition des concepteurs d'applications et de services mobiles une mine d'or de données ayant le potentiel d'améliorer la qualité de vie des citoyens et l'interaction de ces derniers entre eux et avec leur environnement. À Boston, à titre d'exemple, l'application Street Bump utilise l'accéléromètre du téléphone des automobilistes pour détecter les nids de poule et transmettre leur emplacement en temps réel aux

1. «Uber, anciennement UberCab, est une entreprise technologique qui développe et exploite des applications mobiles de mise en contact d'utilisateurs avec des conducteurs réalisant des services de transport» [note de l'éditeur tirée de Wikipédia].

2 Waze, en ligne : <<https://www.waze.com/fr/>>.

3 STL, « Fonctionnement de STL Synchro », en ligne : <<http://www.stl.laval.qc.ca/fr/nouveaux-usagers/fonctionnement-stl-synchro/>>.

4 STM, « iBUS », en ligne : <<http://www.stm.info/fr/a-propos/grands-projets/ibus>>.

autorités municipales⁵. Plus près de chez nous, les villes de Montréal⁶ et de Québec⁷ promeuvent activement leurs initiatives de villes intelligentes.

Mais qu'en est-il de la façon dont les données de géolocalisation sont encadrées par le droit? Quelle est la route à prendre lorsque vient le temps d'innover et concevoir une application mobile dont le cœur du fonctionnement repose sur la géolocalisation? Le présent article vise d'abord à démystifier les notions de droit d'auteur et de vie privée applicables au monde des applications mobiles utilisant la géolocalisation, qui sont des notions qui doivent être au cœur du développement d'applications par les entreprises technologiques.

Dans un premier temps, cet article examine comment le droit d'auteur encadre l'utilisation de données géographiques nécessaires au fonctionnement des applications et des services basés sur la géolocalisation. Le droit d'auteur existe-t-il dans de telles bases de données et, si oui, à quelles conditions? Est-ce qu'intégrer des données trouvées sur le web dans son application peut constituer de la contrefaçon? Qu'en est-il des licences conférées par les différents organismes et sociétés sur certaines bases de données?

Dans un deuxième temps, cet article explore la protection de la vie privée des utilisateurs, dans un monde où les données de localisation ont une valeur sans précédent pour l'État et les entreprises privées. Il examine les données de géolocalisation comme «renseignements personnels», décrit les meilleures pratiques à adopter pour s'assurer de respecter la législation en la matière et aborde finalement certaines des circonstances dans lesquelles les données peuvent être divulguées à des tiers.

2. Le droit d'auteur dans les données géographiques

a) Existence du droit d'auteur

En droit européen, les bases de données sont protégées par un droit *sui generis* («de son propre genre»)⁸. En l'absence d'un tel droit au Canada, il faut se tourner vers le droit d'auteur, qui traite notamment de la protection accordée aux données dans certaines circonstances.

⁵ Street Bump, en ligne : <<http://www.streetbump.org/about>>.

⁶ Ville de Montréal, « Montréal, ville intelligente et branchée », en ligne : <<http://villeintelligente.montreal.ca>>.

⁷ Ville de Québec, « Québec, ville intelligente », en ligne : <https://www.ville.quebec.qc.ca/ville_intelligente/>.

⁸ Directive (CE) n° 96/9 du Parlement européen et du Conseil du 11 mars 1996 concernant la protection juridique des bases de données, *J.O.C.E.*, L.77, 23 mars 1996, p 20.

Lorsqu'on pense à une œuvre protégée par droit d'auteur, la première chose qui vient en tête est rarement une base de données géographiques. On associe souvent le droit d'auteur à l'expression artistique ou à la protection des programmes informatiques. Alors, on peut se demander de quelle façon le droit d'auteur s'applique à des données qui, pourrait-on dire, ne font que décrire la réalité objective qui nous entoure : les coordonnées de telle rue, le vélo libre-service le plus proche ou le tracé d'un sentier.

La réponse se trouve dans ce que le droit d'auteur peut viser : le droit d'auteur ne protège pas les données géographiques *en soi*, mais il est susceptible de protéger la forme qu'elles prennent lorsqu'elles sont arrangées, suivant certaines conditions.

i) L'objet du droit d'auteur : la compilation de données

Pour revenir aux principes fondamentaux, la *Loi sur le droit d'auteur* (ci-après la «LDA») protège les œuvres originales⁹. Dans l'arrêt *CCH Canadienne Ltée c Barreau du Haut-Canada*, la Cour suprême rappelle que «la protection du droit d'auteur ne s'étend pas aux données»¹⁰. Le droit d'auteur ne protège pas les faits ou les idées, mais bien leur expression dans une œuvre¹¹. Les données géographiques doivent donc être exprimées sous la forme d'une œuvre visée par le droit d'auteur.

Les données géographiques sont souvent représentées sous forme de graphiques, de cartes ou de plans, qui sont tous susceptibles d'être protégés à titre d'«œuvre artistique», telle que définie à l'article 2 LDA¹² :

«œuvre artistique» Sont compris parmi les oeuvres artistiques les peintures, dessins, sculptures, oeuvres architecturales, gravures ou photographies, les oeuvres artistiques dues à des artisans ainsi que les graphiques, cartes, plans et compilations d'oeuvres artistiques.

[Soulignements ajoutés]

Si la protection accordée à une carte pose relativement peu de problèmes – il est clair, par exemple, qu'on ne peut simplement reproduire sans autorisation les cartes de Google Maps – les bases de données soulèvent des questions plus épineuses. Nous nous attarderons principalement au droit d'auteur qui peut exister dans les bases de données, car c'est sous cette forme que les données géographiques sont

⁹ *Loi sur le droit d'auteur*, LRC 1985, c C-42, art 5 [LDA].

¹⁰ *CCH Canadienne Ltée c Barreau du Haut-Canada*, [2004] 1 RCS 339, 2004 CSC 13 au para 22 [CCH].

¹¹ *Ibid* au para 8.

¹² LDA, *supra* note 9, art 2.

le plus souvent susceptibles d'être utilisées dans le cadre d'applications mobiles et de plateformes numériques.

Une base de données composée de données géographiques pourrait être protégée par le droit d'auteur à titre de compilation. La compilation est définie ainsi à l'article 2 *LDA* :

«compilation» Les oeuvres résultant du choix ou de l'arrangement de tout ou partie d'oeuvres littéraires, dramatiques, musicales ou artistiques ou de données.

[Soulignements ajoutés]

Dans une compilation, le droit d'auteur vise le choix ou l'arrangement des composantes d'une compilation et non les composantes elles-mêmes, comme l'explique la Cour suprême dans l'arrêt *CCH*¹³ :

Une compilation consiste dans la présentation, sous une forme différente, d'éléments existants. Celui qui l'effectue n'a aucun droit d'auteur sur les composantes individuelles. Cependant, il peut détenir un droit d'auteur sur la forme que prend la compilation. [TRADUCTION] «Ce ne sont pas les divers éléments qui sont visés par le droit d'auteur, mais bien leur agencement global qui est le fruit du travail du demandeur».

[Soulignements dans l'original; références omises]

Bref, il faut retenir qu'en vertu de la *LDA*, les données brutes ne peuvent être protégées en soi : c'est plutôt leur choix ou leur arrangement dans une base de données qui sera potentiellement protégée par droit d'auteur.

ii) L'originalité

Toute œuvre, pour être protégée par le droit d'auteur, doit être «originale»¹⁴. La jurisprudence en matière de droit d'auteur a longtemps oscillé entre deux conceptions de l'originalité : l'une, plus large, récompense l'effort et le labeur nécessaire à la conception de l'œuvre, alors que l'autre, plus restreinte, nécessite de la créativité¹⁵. Depuis l'arrêt *CCH*, le droit d'auteur canadien se situe entre ces deux extrêmes : une œuvre est originale si elle est «le produit de l'exercice du talent et du jugement d'un auteur»¹⁶. La Cour suprême définit le critère ainsi¹⁷ :

¹³ *CCH*, *supra* note 10 au para 33.

¹⁴ *LDA*, *supra* note 9, art 5(1).

¹⁵ Voir notamment *CCH*, *supra* note 10 au para 15.

¹⁶ *Ibid* au para 25.

J'entends par talent le recours aux connaissances personnelles, à une aptitude acquise ou à une compétence issue de l'expérience pour produire l'œuvre. J'entends par jugement la faculté de discernement ou la capacité de se faire une opinion ou de procéder à une évaluation en comparant différentes options possibles pour produire l'œuvre. Cet exercice du talent et du jugement implique nécessairement un effort intellectuel. L'exercice du talent et du jugement que requiert la production de l'œuvre ne doit pas être négligeable au point de pouvoir être assimilé à une entreprise purement mécanique. Par exemple, tout talent ou jugement que pourrait requérir la seule modification de la police de caractères d'une œuvre pour en créer une «autre» serait trop négligeable pour justifier la protection que le droit d'auteur accorde à une œuvre «originale».

[Soulignements ajoutés]

Si ce critère a le mérite d'être un compromis équilibré entre l'effort et la créativité, son application à des situations concrètes a donné lieu à bien des difficultés, particulièrement dans le cas des compilations de données.

En théorie, pour qu'une compilation soit originale, c'est le choix ou l'arrangement des composantes (comme les données) – et non leur collecte, leur création ou leur découverte – qui doit être le produit de l'exercice du talent et du jugement de l'auteur. Cependant, en pratique, la ligne est mince entre, par exemple, la collecte et la compilation de données. Dans la décision récente *Geophysical Services Incorporated c Office Canada-Nouvelle-Écosse des hydrocarbures extracôtiers* (ci-après «GSI»), la Cour fédérale a examiné le droit d'auteur applicable à des données sismiques concernant le sous-sol marin au large des côtes de la Nouvelle-Écosse, utilisées dans le cadre de l'exploitation pétrolière¹⁸. Au stade de la demande d'injonction interlocutoire, la Cour s'est limitée à confirmer qu'il n'y a pas de droit d'auteur dans les données comme telles, mais que l'existence du droit d'auteur dans la compilation soulève une question sérieuse¹⁹ :

[24] Il ne saurait y avoir de droit d'auteur sur des données sismiques ou géophysiques. Le droit d'auteur ne peut porter que sur l'analyse des compilations de ces données.

¹⁷ *Ibid* au para 16.

¹⁸ *Geophysical Service Incorporated c Office Canada-Nouvelle-Écosse des hydrocarbures extracôtiers*, 2014 CF 450 [GSI].

¹⁹ *Ibid* aux paras 24 à 26. Voir aussi *ResourceEye Services Inc v Atrum Coal Groundhog Inc*, 2015 BCSC 821 aux paras 39 à 42, citant GSI et ajoutant : « raw data such as was provided by the plaintiff to West Hawk is incapable of attracting the protection of copyright ».

[25] La demanderesse signale que, sur ce point, la preuve consiste en un seul paragraphe de l'affidavit produit par GSI, où le déposant laisse entendre que les employés de GSI font preuve [TRADUCTION] «de discernement, de circonspection, de créativité, de savoir, d'efforts et d'imagination».

[26] Malgré la minceur de la preuve produite par la demanderesse et les éléments de preuve tendant à indiquer qu'une autre entité a participé aux travaux livrés à l'Office, j'estime que, du point de vue de la demanderesse, on peut tout au plus dire que la propriété du droit d'auteur soulève au moins une question sérieuse, étant donné l'ensemble de faits démontrant que GSI est bien propriétaire des données en question et qu'elle a joué un rôle majeur dans leur collecte et leur compilation.

[Soulignements ajoutés; références omises]

On voit autant le critère actuel du talent et du jugement que les anciens critères de créativité et d'effort dans les arguments de GSI à l'effet que ses employés ont fait preuve «de discernement, de circonspection, de créativité, de savoir, d'efforts et d'imagination». Cependant, on voit aussi que la Cour parle de «propriété» des données, même s'il ne peut y avoir de droit d'auteur dans les données elles-mêmes. De plus, la Cour mentionne le rôle que GSI a joué dans la «collecte» des données, mais il n'est pas clair si elle parle ici des données elles-mêmes ou du choix et de l'arrangement des données qui est protégeable à titre de compilation.

Ces défis se retrouvent couramment dans la jurisprudence concernant les compilations de données. Dans l'arrêt *Télé-Direct (Publications) Inc c American Business Information, Inc*, la Cour d'appel fédérale a jugé qu'il n'existait pas de droit d'auteur dans la compilation de renseignements sur des abonnés dans un annuaire téléphonique, car le choix et l'arrangement de données étaient mécaniques et évidents²⁰. Quoique cet arrêt précède *CCH* et le critère de l'exercice de talent et de jugement, il est encore cité avec approbation²¹.

Lorsque le choix ou l'arrangement des composantes d'une compilation résultent de leurs fonctions, les tribunaux hésitent à reconnaître l'originalité. Dans la décision récente *Distrimedic Inc c Dispill Inc*, la Cour fédérale a jugé que la sélection et l'arrangement de renseignements sur des feuilles d'étiquettes pour médicaments ne constituaient pas une compilation originale²² :

²⁰ *Télé-Direct (Publications) Inc c American Business Information, Inc*, [1998] 2 RCF 22, 1997 CanLII 6378 (CAF) [Télé-Direct].

²¹ Voir notamment *Distrimedic Inc c Dispill Inc*, 2013 CF 1043 au para 323 [Distrimedic]; *GSI*, supra note 18 au para 24.

²² *Distrimedic*, supra note 21 au para 325. Voir aussi *Bonnette c Entreprise Dominion Blue Line Inc*, 2005 QCCA 342 aux paras 46, 56, 69 [Bonnette].

[L]es formules et les autres œuvres résultant d'une compilation d'éléments ne sont pas considérées comme possédant un degré suffisant d'originalité lorsque la sélection des éléments faisant partie de l'œuvre est dictée par la fonction et/ou par les exigences de la loi et que leur disposition en une forme concrète d'expression n'est pas originale.

Ce principe a récemment trouvé application dans la décision *Denturist Group of Ontario c Association des denturologistes du Canada*²³. La Cour fédérale a jugé que des codes numériques associés à des actes médicaux et utilisés à des fins d'assurance médicale ne constituaient pas une compilation originale susceptible de protection:

[74] Il n'y a aucun doute que les codes à cinq chiffres sont de nature fonctionnelle, comme l'a admis M. Vout au nom des défenderesses en contre-interrogatoire. De plus, les descriptions des services associés aux codes sont aussi principalement de nature fonctionnelle. En outre, les codes à cinq chiffres et les descriptions des services qui y sont associées sont exigés par les assureurs et les tiers fournisseurs de services, afin que tous les denturologistes en Ontario puissent être payés pour les services fournis aux patients. Les codes, ainsi qu'ils ont été modifiés au fil du temps, ont constamment été utilisés à partir des années 1970 jusqu'à aujourd'hui, selon les besoins, par les denturologistes peu importe que ceux-ci soient ou non membres de l'ADC ou de la DAO. Les compagnies d'assurances acceptent un seul ensemble de codes pour effectuer les paiements aux denturologistes, ce qui fait des codes à cinq chiffres une norme professionnelle et une nécessité pour que les denturologistes soient remboursés par les compagnies d'assurances et les tiers fournisseurs de services.

[75] Je n'estime pas qu'il y a suffisamment d'originalité ou de talent et de jugement pour justifier l'existence d'un droit d'auteur relativement à de simples codes numériques à cinq chiffres et/ou aux descriptions fonctionnelles des services de denturologie qui sont associées à ces codes.

[Soulignements ajoutés]

Certaines décisions illustrent la difficulté de distinguer une compilation et les données dont elle est composée. Dans *B & S Publications Inc v Max-Contacts Inc*, la Cour du *Queen's Bench* de l'Alberta a jugé qu'un droit d'auteur existait dans des données comme telles concernant des compagnies d'exploration et de production de pétrole,

²³ *Denturist Group of Ontario c Association des denturologistes du Canada*, 2014 CF 989.

vu le talent et le jugement exercés par le demandeur dans la collecte de l'information²⁴ :

I am of the opinion that the data relating to the exploration and production companies as researched and presented by the plaintiff is capable of and by itself of being copyrighted, owing in part to the criteria used to select the names by the plaintiff, the research done on its currency and accuracy, and its categorization. The design layout and format of the works comprising the Index and the Field Guide are also original and unique works deserving of copyright.

[Soulignements ajoutés]

Un raisonnement similaire a été repris par la Cour d'appel du Québec dans *Gahel c Corporation Xprima.com*²⁵. La Cour a jugé que le droit d'auteur existait dans les données obtenues à partir de tests réalisés par l'appelant sur des motocyclettes quant à la consommation d'essence et l'accélération sur un quart de mile, car elles étaient l'expression d'une idée et résultaient de l'exercice du talent et du jugement de l'appelant²⁶.

Ces décisions sont à première vue contraires au principe selon lequel le droit d'auteur existe seulement dans la compilation de données, et non dans les données elles-mêmes. Comme l'explique l'auteure Teresa Scassa, il est difficile de départager les données et le choix ou l'arrangement de ces données²⁷ :

The key may lie in understanding what an original selection of facts is. Copyright law protects an "original selection" of facts, independent of any original arrangement. In the case of the *Oil and Gas Index [B & S Publications Inc. v Max-Contacts Inc]*, it is possible to argue that the court found it to be an original selection of facts. The copyright extended to the facts themselves since independent creation would necessarily involve copying the core protectable expression in the work: the selection.

Autrement dit, lorsque les données *elles-mêmes* résultent d'une sélection ou d'un choix nécessitant du talent et du jugement, elles risquent d'être protégées à titre de compilation. Il s'agit là d'une interprétation incongrue avec les dispositions de la LDA, qui semble malgré tout trouver application dans la jurisprudence.

²⁴ *B & S Publications Inc. v Max-Contacts Inc.*, 2001 CarswellAlta 69 au para 52, [2001] AJ No 143, 287 AR 201 [B & S].

²⁵ *Gahel c Corporation Xprima.com*, 2008 QCCA 1264 [Gahel].

²⁶ *Ibid* aux paras 43-47.

²⁷ Teresa Scassa, « Original Facts : Skill, Judgment, and the Public Domain » (2006) 51 RD McGill 253 à la p 262, en ligne : <http://lawjournal.mcgill.ca/userfiles/other/6736036-1224868339_Scassa.pdf>.

iii) Les données géographiques comme compilation originale

Dans le cas qui nous occupe, la compilation de données géographiques résulte souvent de l'exercice du talent et du jugement. Dans un ouvrage de 1993 sur les enjeux juridiques liés à la géomatique, des auteurs expliquent la latitude laissée aux créateurs de fichiers géomatiques²⁸ :

[O]n pourrait prétendre que la géomatique ne fait qu'énumérer des coordonnées géographiques et qu'en conséquence, on ne répond pas au critère d'originalité. Ce serait là se méprendre sur la nature du droit d'auteur et sur celle de la géomatique. En ce qui a trait à la géomatique, il faut préciser que les phénomènes géographiques que l'on veut représenter ne sont pas aussi objectifs que l'on pourrait le croire. Ainsi, si les coordonnées d'une ville, d'un pont ou d'une montagne semblent statiques, elles varieront cependant en fonction du système de référence utilisé.

Par exemple, le Canada a utilisé jusqu'en 1990 le Système de référence nord-américain de 1927 (NAD 27), mais depuis lors, on utilise plutôt celui de 1983 (NAD 83). Ce nouveau système permet de rectifier les coordonnées de repères géodésiques de façon à éliminer les erreurs et distorsions dues à la mauvaise représentation de la forme de la terre. Les experts qui créent les fichiers géomatiques doivent donc tenir compte d'une foule de paramètres.

Un autre exemple vise à illustrer la latitude laissée au créateur d'un fichier géomatique. Tout le monde a sa petite idée sur ce qu'est un lac. Or, ce mot peut avoir un sens différent pour un spécialiste du ministère de l'Environnement qui s'intéresse à l'habitat, notamment aux lieux de reproduction des poissons, et qui aura tendance à inclure les zones humides adjacentes et pour un promoteur immobilier qui veut développer un site enchanteur le long d'un lac, mais qui voudrait bien pouvoir éliminer un marécage d'où se dégage au printemps une nuée de moustiques.

Il demeure que l'originalité de chaque compilation dépend des faits de chaque cas d'espèce. Pensons, par exemple, à une municipalité qui publierait sur son site web un inventaire des immeubles vacants sur son territoire sous la forme d'un ensemble de données contenu dans un fichier informatique : les données seraient organisées de façon à associer des coordonnées géographiques (latitude et longitude) à un immeuble désigné par son adresse postale ainsi que le nom et les coordonnées de son propriétaire. On peut se demander si un tel arrangement de données est «original» au sens de la LDA. Certes, on peut considérer que la *collecte* de ces

²⁸ René Côté et al., *La géomatique : ses enjeux juridiques*, Québec, Publications du Québec, 1993 aux pp 64-65.

données a nécessité l'exercice de talent et de jugement (par exemple, la détermination des coordonnées géographiques de chaque immeuble en fonction de sa vacance ou non). Cependant, ces considérations ne sont pas pertinentes pour déterminer si le *choix et l'arrangement* des données nécessitent l'exercice de talent et de jugement, faisant de la compilation une œuvre originale protégée par droit d'auteur.

Si une chose est certaine, malheureusement, c'est que le droit dans ce domaine reste incertain! Les auteures Teresa Scassa et Elizabeth Judge résument ainsi dans quelles circonstances les compilations de données géographiques sont plus susceptibles d'être protégées par le droit d'auteur²⁹ :

Thus, raw data are not copyrightable subject matter, but data can be compiled or graphically represented and the original contributions in those products can qualify as 'original expressions' that come within copyright's scope. In simple terms, a factual datum, such as that an individual resides at a given address, does not qualify for copyright protection, but if a group of those facts were part of a compilation and the selection or arrangement was original, the choices making up the original selection or arrangement can be copyrightable. Additionally, graphic representations of data, such as 'drawings, maps, charts, plans, [and] photographs' are eligible for copyright protection as artistic works provided they are original.

[...]

However, it is clear that the originality must lie in the 'selection or arrangement' of the data and that the protection 'shall not extend to the data or material itself'. What might constitute an original 'selection' of data under Canadian law is unclear, but it is likely that a data set, particularly a 'whole of universe' data set, that is ordered chronologically, numerically or alphabetically and where the entire data set is provided without selection, would not contain sufficient originality in its arrangement to attract copyright. The fact that a set of geospatial data is the product of expensive, complex and labour-intensive processes will not suffice to make it original. The cost and work involved in compiling data do not render it protectable in copyright law, as the Supreme Court of Canada has expressly rejected the 'sweat of the brow' approach to originality in copyright law. Where, however, the data are analyzed and compiled through an exercise of skill and judgement, sufficient originality to ground copyright may be found. For compilations, that originality will lie in the author's selection and arrangement of the data.

[Soulignements ajoutés; références omises]

²⁹ Teresa Scassa et Elizabeth Judge, « Intellectual property and the licensing of Canadian government geospatial data: an examination of GeoConnections' recommendations for best practices and template licences » (2010) 54:3 *Le Géographe canadien* 366 à la p 370.

Bref, le droit d'auteur existe dans le choix ou l'arrangement de données géographiques si ceux-ci résultent de l'exercice de talent et de jugement de la part de l'auteur. Dans l'absence d'une réponse claire, il est prudent de présumer que la plupart des bases de données géographiques résultent du choix ou d'arrangement original des données, et que le droit d'auteur protège ce choix ou cet arrangement original, au vu de la jurisprudence applicable. Reste maintenant à voir dans quelles circonstances il y a violation de ce droit d'auteur.

b) Violation du droit d'auteur dans le cadre de l'utilisation de données géographiques

La question de savoir s'il y a violation de droit d'auteur dans une compilation est aussi épineuse, sinon plus, que l'existence même du droit d'auteur. Pour nos fins, la clé est de déterminer si une «partie importante» de la compilation a été reproduite.

En effet, l'article 27 LDA définit la violation du droit d'auteur comme l'accomplissement non autorisé d'un acte que seul le titulaire du droit d'auteur a le droit d'accomplir³⁰. Les droits exclusifs du titulaire sont énumérés à l'article 3 LDA, lesquels incluent notamment le droit de «produire ou reproduire la totalité ou une partie importante de l'œuvre». La personne qui reproduit une partie importante d'une œuvre sans l'autorisation du titulaire viole donc le droit d'auteur.

La violation comporte deux éléments essentiels : les œuvres doivent être substantiellement similaires – autrement dit, la deuxième doit reproduire une partie importante de la première – et la défenderesse doit avoir eu accès à l'œuvre de la demanderesse³¹. En effet, si l'œuvre de la demanderesse a été créée indépendamment à partir de sources communes ou d'idées conventionnelles, cela constitue une défense à la violation du droit d'auteur, puisqu'il s'agirait d'une ressemblance fortuite³².

Pour déterminer ce qu'est une «partie importante» de l'œuvre, il faut examiner ce que le droit d'auteur protège. Dans l'arrêt récent *Cinar Corporation c Robinson*, la Cour suprême a récemment énoncé le principe ainsi³³ :

On détermine ce qui constitue une partie importante en fonction de l'originalité de l'œuvre qui doit être protégée par la *Loi sur le droit d'auteur*. En règle générale, une partie importante d'une œuvre est

³⁰ LDA, *supra* note 9, art 27(1).

³¹ *Philip Morris Products SA c Malboro Canada limitée*, 2010 CF 1099 au para 315 [*Philip Morris*], conf sur ce point par 2012 CAF 201 au para 119, autorisation de pourvoi à la CSC refusée, 35001(21 mars 2013).

³² *Ibid* au para 320.

³³ *Cinar Corporation c Robinson*, [2013] 3 RCS 1168, 2013 CSC 73 au para 26.

une partie qui représente une part importante du talent et du jugement de l'auteur exprimés dans l'œuvre.

Autrement dit, l'analyse de ce qu'est une partie importante de l'œuvre exclut «toute partie de l'œuvre qui n'est pas protégée par le droit d'auteur»³⁴.

Dans le cas d'une compilation, il faut donc analyser si une partie importante du choix ou de l'arrangement des composantes a été reproduite : c'est le choix ou l'arrangement que le droit d'auteur protège, pas les composantes elles-mêmes³⁵. Dans l'arrêt *Robertson c Thomson Corp*, la Cour suprême a statué que le choix original peut constituer à lui seul une partie importante d'une compilation protégée par droit d'auteur, en l'occurrence un journal : «le choix original peut constituer, à lui seul, une partie importante d'un journal, dans la mesure où l'on conserve l'essence du journal, c.-à-d. ce qui confère au recueil l'originalité requise pour qu'un droit d'auteur s'y rattache»³⁶.

Dans l'arrêt *Édutile Inc c Assoc. pour la protection des automobilistes*, c'est l'arrangement des composantes d'une compilation qui était une «partie importante» de l'œuvre³⁷. La Cour d'appel fédérale a jugé qu'un guide d'achat de voitures usagées était protégé par le droit d'auteur du fait qu'il juxtaposait deux colonnes d'informations de façon originale; la Cour a jugé que la reproduction de ces colonnes juxtaposées était une violation du droit d'auteur³⁸ :

Il m'apparaît évident que l'APA s'est approprié une «partie importante», [voire] l'essence même de l'oeuvre d'Édutile au sens où l'entend la jurisprudence. En termes de quantité, l'essentiel des guides de l'APA et d'Édutile tient en la présentation sur chaque page d'une colonne décrivant le marché «Vente Privé» flanquée d'une colonne décrivant le marché «Valeur Détail». En termes de qualité et de nature, ce qui distinguait nettement le guide d'Édutile et ce qu'a nettement repris à son compte le guide de l'APA, c'est justement cette même présentation.

À l'inverse, on ne viole généralement pas le droit d'auteur dans une compilation en n'utilisant que ses composantes, comme des données, sans reproduire leur choix ou arrangement. Par exemple, dans la récente décision *GSI* mentionnée précédemment, une autorité gouvernementale avait publié sur son site Internet une figure tracée à partir de données sismiques obtenues de différentes sources, dont notamment certaines données de la demanderesse *GSI* qui avaient servi à élaborer

³⁴ *Philip Morris*, *supra* note 31 au para 318.

³⁵ *CCH*, *supra* note 10 au para 33.

³⁶ *Robertson c Thomson Corp.*, [2006] 2 RCS 363, 2006 CSC 43.

³⁷ *Édutile Inc c Assoc pour la protection des automobilistes*, [2000] 4 RCF 195, 2000 CanLII 17129 (CAF).

³⁸ *Ibid* au para 37.

environ 8.4% du tracé³⁹. La Cour fédérale a jugé qu'il n'y avait pas eu de violation de droit d'auteur⁴⁰ :

[L]a similarité objective entre l'œuvre contrefaite et l'œuvre protégée par le droit d'auteur ou, du moins, une part substantielle de cette œuvre, semble insuffisante pour que l'on conclue que la figure 5.5 constitue une copie, une reproduction ou une adaptation de l'œuvre protégée par le droit d'auteur.

[...]

Compte tenu de l'apport relativement réduit des données recueillies par la demanderesse au tracé de la figure 5.5, des opérations importantes de manipulation et de remaniement des données effectives par l'Office, et du fait que la grande majorité des données provenaient d'autres sources, j'estime que la figure 5.5 n'est pas une reproduction ou une adaptation violant le droit d'auteur de GSI.

Dans ce cas, l'utilisation de données parmi d'autres dans la confection d'un tracé ne peut pas violer le droit d'auteur dans une compilation de données. En effet, cette utilisation ne reproduit pas le choix ou l'arrangement des données, soit la «partie importante» de la compilation protégée par le droit d'auteur.

Reste qu'en pratique, la ligne est mince entre la protection d'une compilation et des données elles-mêmes. Dans les décisions *B & S*⁴¹ (information sur des compagnies pétrolières) et *Gahel*⁴² (résultats de tests routiers de motos) mentionnées précédemment, il semble que les tribunaux aient jugé que la reproduction d'une partie importante des données elles-mêmes constituait une violation du droit d'auteur. Par exemple, la Cour d'appel du Québec dans *Gahel* statue d'abord qu'il ne saurait y avoir de droit d'auteur sur des données mesurées par l'auteur, mais rajoute ensuite que fournir systématiquement les mêmes données viole le droit d'auteur dans la compilation⁴³ :

[54] La situation de l'appelant est à rapprocher de celle de l'appelante dans l'arrêt *Édutile Inc. c. L'Association pour la protection des automobilistes (APA)*. Comme dans cette affaire, l'appelant a recueilli des données sur lesquelles il ne saurait y avoir de droit d'auteur puisqu'elles sont fondées sur des idées conventionnelles largement répandues (par exemple, le couple ou l'accélération d'une moto) et qu'elles sont de l'ordre du fait. Cela dit, l'expression ou la concrétisation que reçoivent ces idées par le *Guide* est quant à elle originale. Toutes les compilations ne présentent pas un caractère

³⁹ *GSI*, *supra* note 18 aux paras 10-15.

⁴⁰ *Ibid* aux paras 28, 32.

⁴¹ *B & S*, *supra* note 24 aux paras 51-53.

⁴² *Gahel*, *supra* note 25.

⁴³ *Ibid* au para 54.

d'originalité, mais certaines si. Fournir systématiquement les mêmes données-étalons (qui n'existent pas sous cette forme dans le domaine public) afin de rendre possible une comparaison entre modèles de motocyclettes est un aspect de la compilation réalisée par l'appelant que l'on peut qualifier d'innovateur. Plagier ces données constitue une atteinte au droit d'auteur.

[Soulignements ajoutés; références omises]

Encore une fois, le droit dans ce domaine est incertain : quoiqu'on puisse considérer que c'est contraire aux principes de droit d'auteur, il semble que la reproduction d'une partie importante de données contenues dans une compilation de données puisse constituer une violation du droit d'auteur en vertu de la jurisprudence. Les auteurs Scassa et Judge font état de l'incertitude du droit quant aux compilations de données géographiques⁴⁴ :

Even if a data compilation were to be protected, copyright law would provide recourse only against an unauthorized reproduction of all or a substantial part of the original expression, that is, the selection or arrangement, and not the data itself. If the underlying data were mined so as to present certain data in a new arrangement, there would likely be no copyright infringement, as there would be no copying of the protected original expression in the selection or arrangement. The new selection or arrangement would not only be unlikely to infringe any copyright, but, if original, would be protected. In an area so replete with uncertainty, it will often be difficult to determine the existence or scope of any copyright in a data set.

[Soulignements ajoutés; références omises]

Du point de vue du droit d'auteur, utiliser des données géographiques disponibles publiquement afin de les présenter, compiler ou organiser à sa manière ne violerait pas le droit d'auteur de la compilation de données puisqu'il ne reproduit pas une partie importante du choix et de l'arrangement des données. Cette situation est analogue aux faits de la décision *GSI*, dans laquelle l'autorité publique a utilisé quelques données sismiques pour produire un tracé⁴⁵. Ceci dit, il existe également des nuances entre la «propriété» des données à proprement parler et le droit d'auteur applicable à celles-ci ou à leur arrangement sous forme de compilation. Nous y reviendrons plus loin.

À l'inverse, une application mobile ou un site web qui reproduit substantiellement le choix ou l'arrangement des données dans une compilation ou l'expression de ces

⁴⁴ Scassa et Judge, « Intellectual property and the licensing of Canadian government geospatial data », *supra* note 29, à la p 371.

⁴⁵ *GSI*, *supra* note 18.

données sur une carte, avec le résultat que les deux sont substantiellement similaires, viole fort probablement le droit d'auteur.

L'incertitude du droit dans ce domaine peut donner lieu à des situations complexes. Par exemple, l'auteure Scassa fait état d'un litige aux États-Unis concernant les données relatives aux horaires d'autobus⁴⁶ :

A flurry of disputes has recently erupted in the United States over public transit data. These disputes raise interesting questions about the nature of "facts" and their protection under copyright law. In some cases, the disputes have arisen in contexts where public transit authorities have contracted with a company called NextBus. NextBus uses proprietary algorithms to crunch data from transit timetables with data harvested from GPS systems installed on buses and that communicate with electronic readers at set points along routes. The result is prediction data — predictions about when the next bus is likely to arrive at any given stop. The information is made available to transit riders, and the goal is to improve their public transit experience. In a number of American cities that have launched NextBus services, entrepreneurial individuals have created iPhone applications which harvest and make the prediction data accessible to iPhone users in a format more convenient to them than the web-based NextBus interface. NextBus claims copyright in its prediction data; the application developers insist that the information is "fact" and in the public domain. At least one transit company has muddied the waters by asserting rights in the underlying transit timetable data. The disputes that have arisen over the rights in the underlying data offer a good illustration not only of the uncertainties of copyright law in this area, but also of the dynamic and likely contentious area into which we are moving regarding data, innovation and copyright.

Cette situation illustre bien comment l'innovation rend complexe l'application du droit d'auteur. Dans ce scénario, les sociétés de transport conçoivent des horaires d'autobus; NextBus crée une valeur ajoutée en générant des données qui prédisent l'arrivée des autobus; et des développeurs d'applications mobiles créent une nouvelle valeur ajoutée en présentant les données de NextBus sous forme plus conviviale. À chaque étape du scénario, les acteurs apportent leur propre contribution et revendiquent des droits afin de récompenser leurs efforts, créativité, talent et jugement.

Dans un tel contexte, il est donc primordial d'encadrer les droits et obligations de chaque partie convenablement, dont notamment par le biais de licences détaillées, afin d'éviter les litiges potentiels. Dans l'exemple de NextBus, les sociétés de

⁴⁶ Teresa Scassa, « Copyright Reform and Fact Based Works » dans Michael Geist, dir, *From "Radical Extremism" to "Balanced Copyright" : Canadian Copyright and the Digital Agenda*, Toronto, Irwin Law, 2010, 571 aux pp 586-587, en ligne : <<http://www.ruor.uottawa.ca/handle/10393/19633>>.

transport publiaient les données relatives à l'horaire sous licence⁴⁷. En effet, la plupart des données géographiques disponibles publiquement sont sujettes à des licences, le sujet que nous abordons plus bas.

c) Impact des amendements récents à la LDA

Avant de passer aux licences, il est pertinent de mentionner deux dispositions ajoutées à la LDA lors des amendements apportés à la loi en 2012, qui peuvent avoir des implications pour l'utilisation de données géographiques⁴⁸.

La première est l'interdiction de contourner des mesures techniques de protection pour accéder à une œuvre. Les articles 41 et 41.1 LDA prévoient que la personne qui contourne une telle mesure s'expose aux mêmes sanctions que la personne qui viole le droit d'auteur⁴⁹. Une « mesure technique de protection » est définie comme « [t]oute technologie ou tout dispositif ou composant qui, dans le cadre normal de son fonctionnement [...] contrôle efficacement l'accès à une œuvre [...] et est autorisé par le titulaire du droit d'auteur »⁵⁰.

Ainsi, une personne qui contourne une mesure technique de protection pour accéder à une compilation de données protégées et accomplir un acte qui n'aurait pas constitué une violation du droit d'auteur – par exemple, parce que l'utilisation des données en question n'aurait pas constitué la reproduction d'une partie importante du choix ou de l'arrangement des données dans la compilation – contreviendrait tout de même à la LDA.

La deuxième disposition pertinente est l'exception à la violation du droit d'auteur pour le contenu non commercial généré par l'utilisateur, prévue à l'article 29.21 LDA. Une personne physique peut, sans violer le droit d'auteur, utiliser une œuvre protégée et disponible publiquement (ce qui pourrait inclure une compilation de données) pour créer une nouvelle œuvre, à condition de respecter les critères suivants :

- d) la nouvelle œuvre n'est utilisée qu'à des fins non commerciales;
- e) la source de l'œuvre originale est indiquée;
- f) la personne croit raisonnablement que l'œuvre originale n'est pas contrefaite; et
- g) l'utilisation ou la diffusion de la nouvelle œuvre n'a pas d'effet négatif important sur l'œuvre originale.

⁴⁷ *Ibid.*

⁴⁸ *Ibid* aux pp 591 à 596.

⁴⁹ LDA, *supra* note 9, arts 41, 41.1.

⁵⁰ LDA, *supra* note 9, art 41.

Si cette exception peut permettre à des utilisateurs de faire des *mash-ups* de cartes et données géographiques dans certains cas, elle ne peut s'appliquer aux concepteurs d'applications mobiles qui désirent utiliser des données dans des logiciels à des fins commerciales, même si ces logiciels sont distribués à titre gratuit. Cette exception est donc d'une utilité limitée.

d) Licences relatives aux données géographiques

La LDA prévoit que le titulaire du droit d'auteur peut permettre à des tiers, par licence, d'accomplir des actes qui constitueraient autrement une violation du droit d'auteur⁵¹. Quoique le droit d'auteur qui existe réellement dans les compilations de données géographiques soit incertain, les bases de données et les services de cartographie disponibles sur le web font généralement l'objet de licences.

Par ailleurs, le fait de rendre accessibles des données sur Internet au moyen de licences règle de façon plutôt simple l'incertitude relative au droit d'auteur. En effet, les données amassées par une personne ou entité sont généralement confidentielles et non disponibles publiquement. Il est donc difficile pour quiconque d'y accéder et de pouvoir les utiliser, qu'elles soient des données brutes ou encore des données arrangées sous forme de compilation suite à un exercice de talent et de jugement.

Lorsqu'une personne ou entité prend la décision de rendre les données qu'elle détient disponibles au public, elle peut convenir de termes de licence sous lesquels elle rendra ces données disponibles, que ce soit pour des utilisations commerciales ou non. En procédant ainsi, les utilisateurs potentiels des données doivent consentir aux termes de la licence, et sont ainsi liés contractuellement quant à l'utilisation des données.

Au Canada comme ailleurs dans le monde, le mouvement vers les données ouvertes («*open data*») a poussé les gouvernements et autorités publiques à rendre disponibles des données sujettes à des licences dites «ouvertes». Par exemple, l'initiative du gouvernement du Canada, GeoGratis⁵², est régie par la «Licence du gouvernement ouvert – Canada»⁵³. Le gouvernement du Québec⁵⁴, ainsi que les

⁵¹ LDA, *supra* note 9, art 13(4).

⁵² Ressources naturelles Canada, « Données gratuites – GéoGratis », en ligne : <<http://www.rncan.gc.ca/sciences-terre/geographie/information-topographique/donnees-gratuites-geogratis/11043>>.

⁵³ Gouvernement du Canada, « Licence du gouvernement ouvert – Canada », <<http://ouvert.canada.ca/fr/licence-du-gouvernement-ouvert-canada>>.

⁵⁴ Gouvernement du Québec, « Licence », en ligne : <<http://www.donnees.gouv.qc.ca/?node=/licence>>.

villes de Montréal⁵⁵ et de Québec⁵⁶, ont chacun leurs portails de données ouvertes dont l'utilisation est assujettie à des licences.

Outre les autorités publiques, de nombreux utilisateurs peuvent bâtir ensemble une base de données : c'est le principe de l'externalisation ouverte, ou «*crowdsourcing*». Dans cette catégorie, OpenStreetMap fournit des données de cartographie bâties «par une communauté de cartographes bénévoles qui contribuent et maintiennent les données des routes, sentiers, cafés, stations ferroviaires et bien plus encore, partout dans le monde»⁵⁷. Ceux qui utilisent ces données doivent respecter les modalités de la licence applicable⁵⁸.

Bref, contrairement aux mythes qui sont parfois répandus, ce n'est pas parce que des données sont «ouvertes» qu'elles sont libres de droits. Même les licences ouvertes imposent certaines modalités à respecter. Par exemple, la licence des données de la Ville de Québec, basée sur le modèle «Paternité 4.0 International» de *Creative Commons*, prévoit que ceux qui utilisent les données doivent notamment mentionner (i) la source des données, (ii) si elles ont été modifiées et (iii) le fait qu'elles sont visées par une licence publique⁵⁹.

Par ailleurs, il importe de rappeler qu'une licence ne confère pas de droit d'auteur sur les données ou les logiciels qui font l'objet de la licence⁶⁰ : ce n'est pas parce qu'une licence revendique un droit d'auteur que celui-ci existe réellement. Cependant, ceux qui utilisent les données tout en respectant les modalités de la licence évitent d'être poursuivis pour violation du droit d'auteur ou pour violation des termes contractuels de la licence. Les licences constituent donc des solutions pratiques à l'incertitude du droit dans le domaine.

En somme, un entrepreneur technologique qui désire créer un nouveau logiciel ou une nouvelle application devrait toujours s'assurer d'utiliser une banque de données géographiques pour laquelle il a légalement eu les droits d'accès, et pour laquelle il détient suffisamment de droits, par licence ou autrement, pour en faire l'utilisation dans le cadre de son logiciel ou son application.

3. Protection de la vie privée

⁵⁵ Ville de Montréal, « Licence », en ligne : <<http://donnees.ville.montreal.qc.ca/licence-2014/>>.

⁵⁶ Ville de Québec, « Licence », en ligne : <<http://donnees.ville.quebec.qc.ca/licence.aspx>>.

⁵⁷ OpenStreetMap, en ligne : <<http://www.openstreetmap.org/about>>.

⁵⁸ OpenStreetMap, « Droit d'auteur et licence », en ligne : <<http://www.openstreetmap.org/copyright>>.

⁵⁹ Ville de Québec, « Licence », *supra* note 56, art 3.

⁶⁰ Teresa Scassa, « Legal issues with volunteered geographic information » (2013) 57(1) *Le Géographe canadien* 1 à la p 3.

a) Introduction

En novembre 2014, une journaliste du site *BuzzFeed News* raconte qu'elle utilise une voiture opérée par le service de covoiturage Uber pour se rendre aux bureaux de cette populaire entreprise à New York, afin de réaliser une entrevue avec un dirigeant. Alors qu'elle débarque de son véhicule, le dirigeant lui souhaite la bienvenue : «Vous voici, dit-il, en pointant son téléphone mobile. Je vous suivais» («*There you are, I was tracking you*»)⁶¹. Selon des anciens employés d'Uber, un outil interne appelé «*God view*» permettait aux employés de l'entreprise de suivre en temps réel les déplacements des utilisateurs du service⁶². À l'époque, Uber n'avait pas publié de politique de confidentialité. En réponse à la controverse, Uber a assuré sur son blogue que ses employés n'ont accès aux données de géolocalisation concernant ses chauffeurs et ses utilisateurs que pour un nombre limité de «fins commerciales légitimes»⁶³.

L'exemple est extrême, certes, mais il montre bien que les applications mobiles et les services basés sur la géolocalisation ont des implications sérieuses pour la vie privée de leurs utilisateurs. De plus en plus, nos moindres activités et déplacements sont suivis, compilés et enregistrés sous forme de données de géolocalisation, souvent grâce aux appareils mobiles qui nous accompagnent dans notre vie quotidienne.

Parmi les domaines où les services basés sur la géolocalisation sont omniprésents, mentionnons le transport et le bien-être.

Le domaine du transport met évidemment à profit la géolocalisation pour faciliter nos déplacements quotidiens. Outre le service de covoiturage Uber, qui cause actuellement une onde de choc dans l'industrie du taxi à travers la planète, pensons à Waze, cette application mobile de navigation «communautaire» qui permet aux conducteurs de se rendre à destination en évitant les embouteillages grâce aux données partagées par l'ensemble des utilisateurs du service en temps réel⁶⁴.

La géolocalisation fait également partie intégrante du domaine du bien-être et de la santé, surtout avec l'apparition des appareils électroniques vestimentaires (ou «*wearables*») comme le bracelet FitBit ou la montre Apple Watch⁶⁵. Par exemple, le

⁶¹ Johana Bhuiyan et Charlie Warzel, « "God View": Uber Investigates Its Top New York Executive For Privacy Violations », *BuzzFeed News* (18 novembre 2014) en ligne : <<http://www.buzzfeed.com/johanabhuiyan/uber-is-investigating-its-top-new-york-executive-for-privacy>>.

⁶² *Ibid.*

⁶³ « Uber's Data Privacy Policy » (18 novembre 2014), *Uber Newsroom* (blogue), en ligne : <<http://newsroom.uber.com/2014/11/ubers-data-privacy-policy/>>.

⁶⁴ Waze, en ligne : <<https://www.waze.com/fr/>>.

⁶⁵ Voir, par exemple, Éloïse Gratton, « Health-tracking bracelets and privacy issues » (20 décembre 2014), *Privacy & IT Law* (blogue), en ligne : <<http://www.eloisegratton.com/blog/2014/12/20/health-tracking-bracelets-and-privacy-issues/>>.

bracelet FitBit et les applications qui l'accompagnent enregistrent et compilent toutes les activités effectuées dans une journée comme le nombre de pas, les calories brûlées, ou encore la distance et le trajet parcourus lors d'une course⁶⁶. L'application mobile RunKeeper suit spécifiquement les trajets de course à pied, vélo ou randonnée⁶⁷. Souvent, ces applications encouragent les utilisateurs à partager leurs trajets et leurs statistiques sur les réseaux sociaux, ce que plusieurs n'hésitent pas à faire afin d'obtenir des messages d'encouragement ou d'approbation de la part de leurs pairs.

Plus généralement, les réseaux sociaux eux-mêmes encouragent les utilisateurs à partager leur localisation. Combien de photos partagées sur Instagram sont «géomarquées», permettant de connaître l'emplacement de l'utilisateur et de ses amis? Pensons aussi aux utilisateurs de Facebook qui indiquent se trouver à l'aéroport avant de s'envoler pour une semaine de vacances, gâchant ainsi la journée de leurs amis encore cloués au travail pour de longues heures. Souvent, les paramètres de confidentialité des réseaux sociaux sont tels que les messages et photos sont visibles au public par défaut.

Ces services ont en commun qu'ils génèrent une quantité phénoménale de données de géolocalisation concernant leurs utilisateurs. Qu'en est-il du cadre législatif qui encadre la collecte, l'utilisation et la communication de ces données?

b) Cadre législatif : vie privée et protection de renseignements personnels

Au Canada, la protection de la vie privée revêt un aspect constitutionnel en raison de la protection contre les fouilles, perquisitions et saisies abusives prévue à l'article 8 de la *Charte canadienne des droits et libertés*⁶⁸ : «Chacun a droit à la protection contre les fouilles, les perquisitions ou les saisies abusives». Au Québec, la vie privée est plus explicitement protégée comme un droit fondamental en vertu de l'article 5 de la *Charte des droits et libertés de la personne*, qui prévoit que «[t]oute personne a droit au respect de sa vie privée»⁶⁹.

Au-delà de son aspect constitutionnel, la protection de la vie privée est encadrée par la législation en matière de protection des renseignements personnels, autant dans le secteur public que le secteur privé.

⁶⁶ FitBit, « Découvrez une application tout-en-un adaptée à tous », en ligne : <<https://www.fitbit.com/fr/app>>.

⁶⁷ RunKeeper, en ligne : <<http://runkeeper.com/>>.

⁶⁸ *Charte canadienne des droits et libertés*, partie I de la *Loi constitutionnelle de 1982*, constituant l'annexe B de la *Loi de 1982 sur le Canada* (R-U), 1982, c 11, art 8.

⁶⁹ *Charte des droits et libertés de la personne*, RLRQ c C-12, art 5.

i. Secteur public

Les institutions gouvernementales détiennent une quantité phénoménale de renseignements personnels sur nous : du numéro d'assurance sociale aux revenus, en passant par les informations sur la santé.

Au niveau fédéral, la *Loi sur la protection des renseignements personnels*⁷⁰ encadre la collecte, l'usage et la communication des renseignements personnels par les institutions fédérales :

4. Les seuls renseignements personnels que peut recueillir une institution fédérale sont ceux qui ont un lien direct avec ses programmes ou ses activités.

[...]

7. À défaut du consentement de l'individu concerné, les renseignements personnels relevant d'une institution fédérale ne peuvent servir à celle-ci :

- a) qu'aux fins auxquelles ils ont été recueillis ou préparés par l'institution de même que pour les usages qui sont compatibles avec ces fins;
- b) qu'aux fins auxquelles ils peuvent lui être communiqués en vertu du paragraphe 8(2).

8. (1) Les renseignements personnels qui relèvent d'une institution fédérale ne peuvent être communiqués, à défaut du consentement de l'individu qu'ils concernent, que conformément au présent article.

L'article 8(2) prévoit de nombreuses exceptions qui permettent la communication de renseignements personnels sans le consentement de l'individu, notamment «aux fins auxquelles ils ont été recueillis ou préparés par l'institution» ou «aux fins qui sont conformes avec les lois fédérales ou ceux de leurs règlements qui autorisent cette communication»⁷¹.

Ces exceptions sont particulièrement pertinentes à la lumière de la législation récente en matière de sécurité nationale. Le controversé projet de loi C-51 a reçu la sanction royale en juin 2015, devenant la *Loi antiterroriste de 2015*⁷² et édictant la *Loi sur la communication d'information ayant trait à la sécurité du Canada*. Cette loi crée une autorisation large et vague de partage de renseignements «à l'égard d'activités portant atteinte à la sécurité du Canada»⁷³ entre plusieurs institutions

⁷⁰ *Loi sur la protection des renseignements personnels*, LRC 1985, c P-21.

⁷¹ *Ibid*, art 8(2)a)-b).

⁷² *Loi antiterroriste de 2015*, LC 2015, c 20.

⁷³ *Loi sur la communication d'information ayant trait à la sécurité du Canada*, art 5, telle qu'édictée par la *Loi antiterroriste de 2015*, *supra* note 72.

fédérales, incluant l'Agence du revenu du Canada⁷⁴. Le Commissaire à la protection de la vie privée du Canada et plusieurs experts ont exprimé la préoccupation que cette loi ouvre la porte à la collecte, l'utilisation et la conservation des renseignements personnels disproportionnés quant aux objectifs visés⁷⁵.

Au Québec, la protection des renseignements personnels détenus par les organismes publics dans l'exercice de leur fonction est régie par la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*⁷⁶. La loi précise que les renseignements personnels sont confidentiels⁷⁷, sauf exception, et encadre leur collecte, utilisation, communication, conservation et destruction⁷⁸. La loi prévoit aussi un droit d'accès et de rectification aux renseignements personnels⁷⁹.

Outre ces lois générales, des lois spécifiques peuvent imposer des limites plus strictes à la communication de renseignements personnels plus sensibles. Pensons, par exemple, aux renseignements concernant la santé : la *Loi sur l'assurance maladie*⁸⁰ va au-delà de la législation plus générale et interdit la communication («révélation») de tout renseignement obtenu pour l'exécution de la loi, sauf dans des cas exceptionnels⁸¹.

Bien que ce cadre législatif puisse apparaître bien loin des considérations de base du concepteur d'applications technologiques utilisant le géolocalisation, il n'est pas farfelu de penser que les organismes publics fédéraux ou provinciaux puissent avoir des besoins pour le développement de logiciels utilisant la géolocalisation et combinant également d'autres renseignements personnels faisant partie des banques de données gouvernementales. Il est donc important de garder en tête que des règles particulières s'appliquent à de tels cas.

⁷⁴ *Ibid*, annexe 3.

⁷⁵ Daniel Therrien, « Le commissaire Therrien soulève des préoccupations liées au projet de loi C-51 », *Commissariat à la protection de la vie privée du Canada* (6 mars 2015), en ligne : https://www.priv.gc.ca/media/nr-c/2015/oped_150306_f.asp; Kent Roach et Craig Forcese, « Stumbling Toward Total Information Awareness: The Security of *Canada Information Sharing Act* » (2015) 12(7) *Canadian Privacy Law Review* 65, en ligne : http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2622703.

⁷⁶ *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, RLRQ c A-2.1, chap 3, arts 53 à 102.1.

⁷⁷ *Ibid*, art 53.

⁷⁸ *Ibid*, arts 63.1 et suiv.

⁷⁹ *Ibid*, arts. 83 à 102.1.

⁸⁰ *Loi sur l'assurance maladie*, RLRQ c A-29.

⁸¹ *Ibid*, arts 63 à 68.2.

ii. Secteur privé⁸²

Si l'État a toujours détenu énormément d'informations sur ses citoyens, les entreprises qui offrent des services et des applications mobiles, surtout basés sur la géolocalisation, détiennent plus de données concernant les utilisateurs que jamais. Après tout, quoique cela puisse paraître anecdotique, certaines entreprises détiennent tellement d'informations sur leurs clients qu'elles sont apparemment maintenant capables de prédire que leurs clientes sont enceintes avant qu'elles le sachent elles-mêmes⁸³!

La *Loi sur la protection des renseignements personnels et les documents électroniques*⁸⁴ fédérale (ci-après «LPRPDE») s'applique notamment «à toute organisation à l'égard des renseignements personnels [...] qu'elle recueille, utilise ou communique dans le cadre d'activités commerciales»⁸⁵. Cette loi fédérale s'applique partout au Canada, non seulement à l'égard des entreprises fédérales, sauf dans la mesure où une loi provinciale déclarée «essentiellement similaire» s'applique⁸⁶. C'est le cas du Québec, de la Colombie-Britannique et de l'Alberta⁸⁷.

Au Québec, la protection des renseignements personnels dans le secteur privé est régie par la *Loi sur la protection des renseignements personnels dans le secteur privé*⁸⁸ (ci-après la *LPRPSP*). La loi précise l'application des articles 35 à 40 CcQ en matière de protection des renseignements personnels et vise la personne qui exploite une entreprise⁸⁹.

Ayant été déclarée «essentiellement similaire», la *LPRPSP* s'applique donc à l'exclusion de la *LPRPDE* «à l'égard de la collecte, de l'utilisation et de la

⁸² Pour un exposé complet de la législation applicable au secteur privé, voir l'excellent article de Eloïse Gratton et Frédérick Néron, « Bris de sécurité informationnelle : étapes à suivre et gestion des risques », dans Service de la formation continue du Barreau du Québec, *Les 20 ans de la Loi sur la protection des renseignements personnels dans le secteur privé*, vol 392, Cowansville, Éditions Yvon Blais, 2014, aux pp 118-122, en ligne : <<http://edoctrine.caij.qc.ca/developpements-recents/392/368214302>>.

⁸³ Charles Duhigg, « How Companies Learn Your Secrets », *The New York Times Magazine* (16 février 2012), en ligne : <<http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html>>.

⁸⁴ *Loi sur la protection des renseignements personnels et les documents électroniques*, LC 2000, c 5 [LPRPDE].

⁸⁵ *Ibid*, art 4.

⁸⁶ *Ibid*, art 26(2)b).

⁸⁷ *Personal Information Protection Act*, SBC 2003, c. 63; *Personal Information Protection Act*, SA 2003, c P-6.5. Au Manitoba, la *Loi sur la protection des renseignements personnels et la prévention du vol d'identité*, CPLM c P33.7 n'est pas en vigueur.

⁸⁸ *Loi sur la protection des renseignements personnels dans le secteur privé*, RLRQ c P-39.1 [LPRPSP].

⁸⁹ *Ibid*, art 1, al 1; arts 35-40 CcQ.

communication de renseignements personnels qui s'effectuent à l'intérieur de la province de Québec» (soulignements ajoutés)⁹⁰. C'est donc la *LPRPDE* fédérale qui régit la collecte, l'utilisation et la communication interprovinciales ou internationales de renseignements personnels⁹¹, alors que la *LPRPSP* s'applique seulement aux activités effectuées à l'intérieur du Québec. Considérant la nature souvent interprovinciale et internationale des renseignements utilisés sur les réseaux sociaux et les applications mobiles, la *LPRPDE* trouvera toutefois application dans la plupart des cas.

Puisque les applications mobiles et les services offerts sur Internet impliquent généralement que des données qui circulent hors des frontières provinciales et nationales, nous nous concentrerons sur les exigences de la *LPRPDE*, tout en mentionnant les dispositions de la *LPRPSP* lorsque cela est pertinent. La *LPRPDE* a d'ailleurs été amendée de façon significative en juin 2015⁹²; nous mentionnerons ces amendements au fil de notre analyse.

Finalement, outre la législation en matière de protection des renseignements personnels, certaines lois peuvent prévoir des règles spécifiques liées à la protection de la vie privée. Au Québec, le deuxième alinéa de l'article 43 de la *Loi concernant le cadre juridique des technologies de l'information* (ci-après la «*LCJTI*») prévoit que⁹³ :

À moins que la loi le prévoie expressément en vue de protéger la santé des personnes ou la sécurité publique, nul ne peut exiger qu'une personne soit liée à un dispositif qui permet de savoir où elle se trouve.

Cet article a rarement été mentionné en jurisprudence, tout comme le reste de la *LCJTI* malheureusement, quoiqu'il ait été invoqué par des employés ayant subi des sanctions de la part de leurs employeurs suite aux informations recueillies à partir du système GPS de leur véhicule de travail⁹⁴. Considérant que certains employeurs fournissent à leurs employés des appareils mobiles avec des applications qui utilisent

⁹⁰ Décret d'exclusion visant des organisations de la province de Québec, DORS/2003-374.

⁹¹ *Lawson c Accusearch Inc*, [2007] 4 RCF 314, 2007 CF 125 au para 51 : « la *LPRPDE* confère compétence à la commissaire à la protection de la vie privée de mener enquête sur des plaintes portant sur la circulation transfrontalière de renseignements personnels », du moment qu'il existe un lien avec le Canada.

⁹² *Loi modifiant la Loi sur la protection des renseignements personnels et les documents électroniques et une autre loi en conséquence*, LC 2015, c 32 [*Loi modifiant la LPRPDE*].

⁹³ *Loi concernant le cadre juridique des technologies de l'information*, RLRQ c C-1.1, art 43, al 2 [*LCJTI*].

⁹⁴ Luc Beaulieu et Philippe Levac, « Les litiges qui découlent de l'usage des nouvelles technologies en contexte d'emploi : quelques réflexions et perspectives des employeurs » dans Conférence des arbitres du Québec, (auteur collectif), *Mes amis Facebook, moi et mon emploi : l'arbitrage de grief à l'ère des réseaux sociaux*, Montréal, Wilson et Lafleur, 2012, aux pp 113-115, en ligne : <<http://edoctrine.cajj.qc.ca/wilson-et-lafleur-livres/85/469440017>>.

la fonction de localisation des appareils, on peut se demander si cet article sera appelé à jouer un rôle plus important dans la protection de la vie privée dans les années à venir.

c) Les données de géolocalisation comme renseignement personnel

Avant d'examiner les obligations imposées par la législation en matière de protection de renseignements personnels, il faut d'abord s'attarder à la notion de «renseignement personnel». En effet, les données de géolocalisations sont-elles des «renseignements personnels» au sens de la loi?

La *LPRPDE* définit «renseignement personnel» comme «tout renseignement concernant un individu identifiable»⁹⁵, une définition similaire à celle de la *LPRPSP*⁹⁶. Suivant les directives publiées par le Commissariat à la vie privée du Canada (ci-après «CVPC»), cette définition doit recevoir une interprétation large et libérale⁹⁷ :

Selon la jurisprudence portant sur la notion de «renseignements personnels», une interprétation large et libérale s'impose. Des renseignements «concernent» une personne non seulement lorsqu'ils portent sur celle-ci, mais aussi lorsqu'ils lui touchent ou qu'ils peuvent y être associés⁹⁸. Une personne est «identifiable» lorsqu'il y a de fortes possibilités que celle-ci puisse être identifiée à l'aide de cette information, seule ou en combinaison avec des renseignements d'autres sources⁹⁹.

Les données de géolocalisation, dans la plupart des cas, entrent dans cette définition. Quoiqu'un emplacement géographique en soi ne porte pas sur une personne (contrairement à son nom ou son numéro d'assurance sociale, par exemple), il est généralement possible de l'associer à un individu identifiable. En effet, les données de géolocalisation – comme de nombreuses autres données – sont souvent liées à un identifiant unique ou au compte d'un utilisateur¹⁰⁰. Par

⁹⁵ *LPRPDE*, *supra* note 84, art 2 « renseignement personnel ».

⁹⁶ *LPRPSP*, *supra* note 88, art 2 : « Est un renseignement personnel, tout renseignement qui concerne une personne physique et permet de l'identifier. »

⁹⁷ Commissariat à la vie privée du Canada, « La *LPRPDE* et votre pratique – Guide sur la protection de la vie privée à l'intention des avocats », en ligne : <https://www.priv.gc.ca/information/pub/gd_phl_201106_f.asp>.

⁹⁸ *Canada (Commissaire à l'information) c Canada (Bureau d'enquête sur les transports)*, 2006 CAF 157; *Dagg c Canada (Ministre des Finances)*, [1997] 2 RCS 403.

⁹⁹ *Gordon c Canada (Santé)*, 2008 CF 258.

¹⁰⁰ Voir, par exemple, *Rapport de conclusions en vertu de la LPRPDE no 2013-017 : Apple est sommée de fournir davantage de précisions sur l'utilisation et la communication des identifiants uniques d'appareils aux fins de la publicité ciblée*, 2013 CanLII 96099 (CVPC) au para 35.

exemple, selon la politique de confidentialité de l'application Waze, toutes les données sur un utilisateur sont associées à un identifiant unique même si l'utilisateur n'a pas créé de compte¹⁰¹.

Considérant que les appareils mobiles sont généralement utilisés par une seule personne, les renseignements qui concernent un appareil peuvent souvent être associés à un individu¹⁰². Suite à une plainte formulée contre Google, le CVPC a récemment conclu que la position d'un appareil mobile est un renseignement qui peut être associé à un individu, seul ou avec d'autres renseignements auxquels Google a accès, et donc constituer un renseignement personnel¹⁰³. Le CVPC avait déjà conclu en 2006 que des données provenant d'un GPS installé dans les véhicules de travail d'employés constituent des renseignements personnels, car «un lien peut être établi entre les renseignements recueillis et les employés qui conduisent les véhicules»¹⁰⁴.

Si les données de géolocalisation peuvent paraître inoffensives, elles ont le potentiel de révéler des détails intimes et sensibles¹⁰⁵. Comme le mentionne le Groupe de travail «Article 29» sur la protection des données de la Commission européenne, les données de géolocalisation peuvent constituer un profil sur une personne qui révèle ses habitudes de vie et les lieux qu'elle fréquente¹⁰⁶ :

This allows the providers of geolocation based services to gain an intimate overview of habits and patterns of the owner of such a device and build extensive profiles. From a pattern of inactivity at night, the sleeping place can be deduced, and from a regular travel pattern in the morning, the location of an employer may be deduced.

¹⁰¹ Waze, « Privacy Policy » (dernière modification le 28 juin 2015), <<https://www.waze.com/fr/legal/privacy>>.

¹⁰² Éloïse Gratton, « Dealing with Canadian and Quebec Legal Requirements in the Context of Trans-border Transfers of Personal Information and Cloud Computing Services », dans Service de la formation continue du Barreau du Québec, *Développements récents en droit de l'accès à l'information et de la protection des renseignements personnels – les 30 ans de la Commission d'accès à l'information*, vol. 358, Cowansville, Éditions Yvon Blais, 2012 aux pp 18-19, en ligne : <<http://edoctrine.caij.qc.ca/developpements-recents/358/368100901>>.

¹⁰³ *Rapport de conclusions en vertu de la LPRPDE no 2014-008: Le fait qu'un utilisateur accorde des « autorisations » à une application ne signifie pas, en soi, qu'il consent à la collecte, à l'utilisation et à la communication de renseignements personnels – Nous encourageons Google à donner plus de précisions aux utilisateurs pour éviter toute interprétation erronée*, 2014 CanLII 77274 (CVPC) aux paras 64-65.

¹⁰⁴ *Résumé de conclusions d'enquête en vertu de la LPRPDE #351 : Examen de l'utilisation des renseignements personnels recueillis au moyen d'un système mondial de localisation*, 2006 CanLII 42313 (CVPC).

¹⁰⁵ Voir généralement Teresa Scassa et Anca Sattler, « Location-Based Services and Privacy » (2011) 9 CJLT 99 aux pp 109 à 113.

¹⁰⁶ Article 29 Data Protection Working Party, « Opinion 13/2011 on Geolocation services on smart mobile devices » (16 mai 2011), en ligne : <http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp185_en.pdf>.

The pattern may also include data derived from the movement patterns of friends, based on the so-called social graph.

A behavioural pattern may also include special categories of data, if it for example reveals visits to hospitals and religious places, presence at political demonstrations or presence at other specific locations revealing data about for example sex life. These profiles can be used to take decisions that significantly affect the owner.

À titre d'illustration du phénomène, les auteures Éloïse Gratton et Elisa Henry donnent l'exemple d'une personne qui se trouverait à un endroit X au moment où une parade de la fierté gaie se déroule à cet endroit : on peut en tirer des conclusions – exactes ou erronées – sur son orientation sexuelle¹⁰⁷. Pensons aussi à un utilisateur de l'application RunKeeper qui partagerait les trajets de ses courses à pied : non seulement les trajets risquent de révéler où cette personne demeure, mais ils permettent de prédire qu'elle se trouvera à tel moment à tel endroit, probablement essoufflée et écoutant de la musique à l'aide de son appareil mobile. Selon la vitesse du coureur et la durée du trajet, on pourra même tirer des conclusions sur l'état de santé général d'une personne. Ce genre de scénario soulève évidemment des inquiétudes au niveau de la sécurité. Plus simplement, un utilisateur de l'application Waze peut désigner des favoris qui indiquent que, par exemple, un emplacement X est sa résidence, un renseignement que Waze collecte et conserve¹⁰⁸. En sachant que l'utilisateur quitte sa résidence en direction du travail, l'entreprise sait alors que la résidence est potentiellement vide à ce moment.

À l'ère des mégadonnées (les «*big data*»), les données de géolocalisation peuvent révéler encore plus de détails lorsqu'elles sont combinées à d'autres données, comme le mentionnent les auteurs Teresa Scassa et Michael Dertubide :¹⁰⁹

Information that seems trivial, irrelevant, or not particularly personal can, if mined and matched with other data, be used to create profiles of individuals that are of much greater concern than any of the individual pieces of data.

Dans un récent document de recherche sur les métadonnées, le CPVC donne des exemples évocateurs de ce que peuvent révéler les données de géolocalisation¹¹⁰ :

¹⁰⁷ Éloïse Gratton et Elisa Henry, *Practical Guide to E-Commerce and Internet Law*, Markham, Ont., LexisNexis Canada, 2015, à la p 286.

¹⁰⁸ Waze, « Privacy Policy » (dernière modification le 28 juin 2015), <<https://www.waze.com/fr/legal/privacy>>.

¹⁰⁹ Teresa Scassa et Michael Dertubide, *Electronic Commerce and Internet Law in Canada*, 2^e éd, Toronto, CCH Canadian Limited, 2012, aux pp 123-124.

¹¹⁰ Commissariat à la protection de la vie privée au Canada, « Métadonnées et vie privée : un aperçu technique et juridique » (Octobre 2014), en ligne : <https://www.priv.gc.ca/information/research-recherche/2014/md_201410_f.asp>.

Des études ou expériences réalisées au fil des années ont montré le caractère extrêmement sensible et unique des données de géolocalisation, notamment :

- En 2010, le site Web «I Can Stalk U» (<http://icanstalku.com>) a vu le jour. Ce site aujourd'hui fermé analysait les photos affichées en ligne, pour trouver les étiquettes de géolocalisation (métadonnées de localisation) et il indiquait ensuite l'emplacement précis associé au message tweeté;
- En 2012, le programmeur d'antivirus John McAfee a été arrêté au Guatemala après qu'une photo géolocalisée eut révélé l'endroit où il se trouvait;
- En 2013, des chercheurs ont publié l'étude intitulée «Unique in the Crowd: The privacy bounds of human mobility», montrant qu'il suffisait de disposer de quatre points spatio temporels choisis de façon aléatoire pour identifier un individu.

[Références omises.]

L'auteure Éloïse Gratton propose une approche basée sur le risque de préjudice pour déterminer ce que constitue un renseignement personnel : le risque qu'un préjudice résulte de l'utilisation, la collecte ou de la communication du renseignement est un facteur à considérer dans l'application de la législation en matière de protection de renseignements personnels¹¹¹ :

I am proposing a new method of interpreting the notion of personal information, which would be taking into account the ultimate purpose behind the adoption of data protection laws in order to ensure that only data that were meant to be covered by these laws will in fact be covered. I maintain that the idea is to aim for a level of generality which corresponds with the highest level goal that the lawmakers wished to achieve. I argue that the ultimate purpose of these laws is broader than protecting the privacy rights of individuals, as it is to protect individuals against the risk of harm that may result from the collection, use or disclosure of their information and that when determining whether certain information qualifies as personal, this risk of harm should be taken into account. This proposed interpretation may also be useful when dealing with and having to qualify new types of information, as discussed below.

[Soulignements ajoutés]

¹¹¹ Éloïse Gratton, « Dealing with Canadian and Quebec Legal Requirements in the Context of Trans-border Transfers of Personal Information and Cloud Computing Services », *supra* note 102, à la p 17.

Cette approche peut également permettre de déterminer à quel point un renseignement est *sensible*, eu égard à trois critères : (i) s'il identifie un individu, (ii) s'il est de nature intime, et (iii) s'il a été rendu accessible à des tiers et, dans ce cas, l'étendue de son accessibilité¹¹² :

I maintain that in assessing the sensitivity of certain information (for instance, upon this information being disclosed), we should evaluate the information in light of three very specific criteria: namely whether the data is "identifiable" to an individual, is of an "intimate" nature, and whether it has been made "available" to others and the extent of its availability. Basically, the sensitivity of the data can be determined by the sum of the risk of harm resulting from the "identifying" aspect of the data (the more identifying to a unique individual, the greater the risk of harm), the "intimate" nature of the data (the more intimate, the greater the risk of harm upon this information being disclosed), and the "availability" of the data (the less available it was pre-disclosure, and the more available it will be post-disclosure, the greater the risk of harm) upon this data being disclosed. These criteria may be useful for organizations attempting to assess the sensitivity of the information that they are processing and transferring.

La nature sensible d'un renseignement est un facteur à considérer si le consentement à sa collecte, son utilisation et sa communication est valable, comme nous le verrons dans la prochaine partie.

Appliquant ce cadre aux données de géolocalisation, on peut considérer que les données de géolocalisation, comme discuté plus haut, (i) sont souvent liées à un individu, à moins qu'elles n'aient été dépersonnalisées; (ii) qu'elles peuvent révéler des détails intimes de notre vie; et (iii) que l'étendue de leur accessibilité à des tiers dépend d'à quel point l'utilisateur les a rendues publiques : si elles sont demeurées privées, si elles ont été partagées entre un cercle restreint de contacts sur les réseaux sociaux, ou si elles sont accessibles à tous. Dans la plupart des cas, des données de géolocalisation seront donc considérées comme des renseignements personnels sensibles.

d) Limites à la collecte, l'utilisation, la divulgation et la conservation de renseignements personnels : le consentement et autres principes

La législation en matière de renseignements personnels pose plusieurs limites à la collecte, l'utilisation, la divulgation et la conservation de renseignements personnels. Les entreprises soumises à la *LPRPDE* doivent se conformer aux obligations de

¹¹² *Ibid*, aux pp 20-21.

l'annexe 1 de la loi¹¹³, qui énonce 10 grands principes : (1) responsabilité, (2) détermination des fins de la collecte des renseignements, (3) consentement, (4) limitation de la collecte, (5) limitation de l'utilisation, de la communication et de la conservation, (6) exactitude, (7) mesures de sécurité, (8) transparence, (9) accès aux renseignements personnels, et (10) possibilité de porter plainte à l'égard du non-respect des principes. Nous nous concentrerons d'abord sur le consentement avant d'aborder quelques autres de ces principes.

i) Le consentement

Le consentement est au cœur de la protection de la vie privée¹¹⁴ : l'organisation qui collecte, utilise et communique des renseignements personnels doit s'assurer d'obtenir le consentement de l'intéressé¹¹⁵. Cette exigence a d'ailleurs été renforcée par les récents amendements à la *LPRPDE*, qui prévoit maintenant que :

[L]e consentement de l'intéressé n'est valable que s'il est raisonnable de s'attendre à ce qu'un individu visé par les activités de l'organisation comprenne la nature, les fins et les conséquences de la collecte, de l'utilisation ou de la communication des renseignements personnels auxquelles il a consenti¹¹⁶.

Au Québec, la *LPRPSP* prévoit que le consentement «doit être manifeste, libre, éclairé et être donné à des fins spécifiques», et «ne vaut que pour la durée nécessaire à la réalisation des fins pour lesquelles il a été demandé»¹¹⁷.

Pour que le consentement soit éclairé, les «fins auxquelles des renseignements personnels sont recueillis doivent être déterminées par l'organisation avant la collecte ou au moment de celle-ci» (principe 4.2 de la *LPRPDE*)¹¹⁸, qui doit en aviser l'utilisateur (principe 4.2.3)¹¹⁹.

Ces dispositions imposent aux entreprises le fardeau d'identifier clairement les fins de la collecte et d'aviser les utilisateurs de leurs applications clairement et en termes compréhensibles la façon dont leurs renseignements personnels seront collectés¹²⁰.

¹¹³ *LPRPDE*, *supra* note 84, art 5(1).

¹¹⁴ *Wansink c TELUS Communications Inc*, [2007] 4 RCF 368, 2007 CAF 21 au para 21 (le consentement est la « pierre d'assise » de la *LPRPDE*).

¹¹⁵ *LPRPDE*, *supra* note 84, ann 1, principe 4.3.

¹¹⁶ *Ibid*, art 6.1.

¹¹⁷ *LPRPSP*, *supra* note 88, art 14, al 1.

¹¹⁸ *LPRPDE*, *supra* note 84, ann 1, principe 4.2.

¹¹⁹ *Ibid*, ann 1, principe 4.2.3.

¹²⁰ *Scassa et Sattler*, *supra* note 105, à la p 118.

Ces fins devraient être limitées à celle «qu'une personne raisonnable estimerait acceptables dans les circonstances»¹²¹.

Concrètement, les entreprises qui collectent et utilisent des renseignements personnels avisent leurs utilisateurs de la collecte des renseignements personnels au moyen d'une politique de confidentialité (aussi appelée «déclaration de confidentialité» ou «politique relative à la vie privée»). Cette politique devrait notamment préciser quels renseignements personnels et quelles données sont collectés, comment ils seront utilisés et dans quelles circonstances ils seront communiqués à des tiers¹²².

Pour respecter les exigences de la loi en matière de consentement et de détermination des fins de la collecte, une politique de confidentialité devrait être rédigée en langage clair et être précise, tout en étant concise et facile à lire, notamment en s'adaptant au public cible de l'application¹²³. Par exemple, le CVPC a reproché à un réseau social pour adolescents d'avoir une politique de confidentialité rédigée dans un langage technique qui ne tenait pas compte de son public cible de jeunes¹²⁴. Sur la question de la langue, nous avons remarqué que de nombreuses applications mobiles distribuées au Canada ne publient pas de politique de confidentialité en français, même si elles sont disponibles pour les utilisateurs québécois. Au Québec, une telle pratique constitue une violation de la *Charte de la langue française*¹²⁵.

La forme que prend un consentement valable dépend des circonstances. La *LRPPDE* prévoit que le consentement peut être obtenu de différentes façons : il peut être explicite ou implicite, positif («opt-in») ou négatif («opt-out»)¹²⁶. Pour évaluer si le consentement est valable, il faut tenir compte de la sensibilité des renseignements¹²⁷ et des attentes raisonnables des utilisateurs¹²⁸. Les données de géolocalisation, considérant les détails intimes qu'elles ont le potentiel de révéler sur la vie intime des utilisateurs, devraient généralement être traitées comme sensibles. Quant aux attentes des utilisateurs, tout dépend du contexte. Au niveau

¹²¹ *LPRPDE*, supra note 84, art 5(3).

¹²² Commissariat à la protection de la vie privée du Canada, « Lignes directrices en matière de consentement en ligne » (Mai 2014) à la p 7, en ligne : <https://www.priv.gc.ca/information/guide/2014/gl_oc_201405_f.pdf>.

¹²³ Voir notamment Gratton et Henry, *Practical Guide to E-Commerce and Internet Law*, supra note 107, à la p 24.

¹²⁴ *Rapport des conclusions en vertu de la LPRPDE no 2012-001 : Nexopia, site de réseautage social pour jeunes, a enfreint la loi canadienne sur la protection des renseignements personnels*, section 2, para 61, en ligne : <https://www.priv.gc.ca/cf-dc/2012/2012_001_0229_f.asp>.

¹²⁵ *Charte de la langue française*, RLRQ c C-11, art 51.

¹²⁶ *LPRPDE*, supra note 84, ann 1, principe 4.3.7.

¹²⁷ *Ibid*, ann 1, principes 4.3.4 et 4.3.6.

¹²⁸ *Ibid*, ann 1, principe 4.3.5.

de la collecte, on peut s'attendre à ce qu'une application de navigation comme Waze collecte la localisation précise d'un téléphone, mais on s'étonnerait sans doute qu'un simple jeu de carte pour téléphone mobile collecte ces mêmes données¹²⁹. Au niveau de l'utilisation des données recueillies, on peut raisonnablement s'attendre à ce que Waze utilise les données collectées pour fournir un service de navigation efficace, mais certains pourraient s'étonner que ces mêmes données servent à fournir une publicité ciblée sur la localisation de leur téléphone¹³⁰. Bref, plus les renseignements sont sensibles et plus la collecte, l'utilisation et/ou la communication s'éloignent des attentes raisonnables des utilisateurs, plus le consentement de l'utilisateur devra être positif et explicite.

Si une politique de confidentialité simple et complète est essentielle, obtenir un consentement manifeste et éclairé à l'ère des applications mobiles requiert souvent plus que simplement publier cette politique sur son site Internet et présumer que les utilisateurs de l'application iront la lire. Comme l'explique le CVPC, les utilisateurs prennent rarement le temps de lire une politique de confidentialité¹³¹ :

Le défi consiste à montrer aux utilisateurs, de manière créative et intelligible, à quoi servent réellement les renseignements personnels les concernant. Somme toute, personne ne veut lire 20 pages de politiques sur la protection des renseignements personnels sur un petit écran.

Certaines fonctionnalités des appareils mobiles peuvent aider, mais tout dépend du contexte. Par exemple, au moment où une application mobile tente d'accéder aux données de géolocalisation d'un appareil mobile, les systèmes d'exploitation comme iOS et Android obligent maintenant les utilisateurs à consentir à cet accès au moyen d'une autorisation dite «juste-à-temps». Cependant, dans le cadre d'une plainte formulée contre Google, le CVPC a déterminé que cette simple autorisation *en soi* ne constitue pas un consentement à la collecte, l'utilisation et la divulgation des renseignements personnels, car «les autorisations ne décrivent pas la collecte, l'utilisation ou la communication de renseignements personnels par Google, mais

¹²⁹ Pourtant, le site PrivacyGrade fait état de plusieurs applications mobiles, notamment des jeux, qui collectent les données de localisation alors que les utilisateurs ne s'y attendraient raisonnablement pas : « This privacy model measures the gap between people's expectations of an app's behavior and the app's actual behavior. By expectations, we mean what people think an app does versus what it actually does. For example, according to studies we have conducted, most people don't expect games like Cut the Rope to use location data, but many of them actually do (this is true for Android as of May 2015) ». PrviacyGrade, « FAQ », en ligne : <<http://privacygrade.org/faq>>.

¹³⁰ Voir notamment Scassa et Sattler, *supra* note 105 aux pp 118-119.

¹³¹ Commissariat à la protection de la vie privée du Canada, « Une occasion à saisir : Développer des applis mobiles dans le respect du droit à la vie privée » (Octobre 2012) à la p 8, en ligne : <https://www.priv.gc.ca/information/pub/gd_app_201210_f.pdf>.

indiquent plutôt les données et les fonctions de l'appareil mobile que l'application est autorisée à consulter»¹³².

Par ailleurs, le fait de refuser l'accès aux services de géolocalisation pourrait, dans certains cas, donner l'impression erronée à l'utilisateur que l'application ne collecte pas de données de géolocalisation. Par exemple, Uber précise dans sa politique de confidentialité que les données de localisation précises des parcours effectués sont collectées à partir de l'appareil mobile du chauffeur même si le client a refusé que l'application Uber ait accès aux services de localisation de son propre appareil¹³³ :

Lorsque vous utilisez les Services pour un transport ou une livraison, nous collectons des données de localisation précises concernant le parcours à partir de l'application Uber utilisée par le Chauffeur. [...]

De plus, le fait de désactiver sur votre mobile l'application nous permettant de collecter vos données précises de localisation ne limitera pas notre capacité de collecter les données de localisation de votre parcours depuis le mobile d'un Chauffeur, ni notre capacité à obtenir votre localisation approximative à partir de votre adresse IP.

Cependant, une demande d'autorisation ou une notification «juste-à-temps» peut être un outil parmi d'autres pour obtenir un consentement valable de la part de l'utilisateur, car elle permet à l'utilisateur de prendre une décision au moment clé, soit avant ou au moment de la collecte de données¹³⁴. Pour rendre le consentement plus éclairé, le CVPC recommande que les notifications «juste-à-temps» incluent de l'information sommaire sur la manière dont les données seront utilisées, tout en fournissant un lien vers de l'information plus détaillée pour les utilisateurs qui désirent en savoir plus¹³⁵. Ce genre d'avis «multicouche» permet à l'utilisateur d'accéder à des couches d'information de plus en plus détaillées, tout en étant avisé des points principaux dès le moment où la collecte de renseignements personnels a lieu¹³⁶.

¹³² *Rapport de conclusions en vertu de la LPRPDE no 2014-008: Le fait qu'un utilisateur accorde des « autorisations » à une application ne signifie pas, en soi, qu'il consent à la collecte, à l'utilisation et à la communication de renseignements personnels – Nous encourageons Google à donner plus de précisions aux utilisateurs pour éviter toute interprétation erronée*, 2014 CanLII 77274 (CVPC) au para 68.

¹³³ Uber, « Déclaration de confidentialité applicable aux utilisateurs » (en vigueur le 15 juillet 2015), en ligne : <<https://www.uber.com/legal/privacy-proposed/users/fr>>.

¹³⁴ *LPRPDE*, *supra* note 84, ann 1, principe 4.2.3 : les utilisateurs doivent être informés des fins de la collecte des renseignements « avant la collecte ou au moment de celle-ci ».

¹³⁵ Commissariat à la protection de la vie privée du Canada, « Lignes directrices en matière de consentement en ligne », *supra* note 122 à la p 9.

¹³⁶ The Center for Information Policy Leadership, « Ten steps to develop a multilayered privacy notice », en ligne :

Finalement, si un aspect significatif concernant la collecte, l'utilisation et la communication des renseignements personnels est modifié après que l'utilisateur ait donné son consentement, l'entreprise devrait l'aviser du changement et obtenir son consentement de nouveau¹³⁷.

ii. Au-delà du consentement

Même en obtenant un consentement libre et éclairé des utilisateurs, les développeurs d'applications mobiles n'ont pas carte blanche pour récolter, utiliser ou communiquer des renseignements personnels comme bon leur semble. Les développeurs doivent s'assurer de respecter les autres principes de la *LPRPDE*.

Nonobstant le consentement libre et éclairé des utilisateurs, on ne peut «recueillir, utiliser ou communiquer des renseignements personnels qu'à des fins qu'une personne raisonnable estimerait acceptables dans les circonstances»¹³⁸. Selon le principe 4.4.2 de la *LPRPDE*, «[o]n doit restreindre tant la quantité que la nature des renseignements recueillis à ce qui est nécessaire pour réaliser les fins déterminées»¹³⁹. Par exemple, il ne serait pas raisonnable de demander le numéro d'assurance sociale d'une personne pour lui permettre de «géomarquer» une photographie prise au sommet d'un observatoire à l'aide d'une application mobile.

De plus, on ne peut pas conserver indéfiniment les renseignements recueillis : «On doit restreindre tant la quantité que la nature des renseignements recueillis à ce qui est nécessaire pour réaliser les fins déterminées»¹⁴⁰ et «détruire, effacer ou dépersonnaliser les renseignements personnels dont on n'a plus besoin aux fins précisées»¹⁴¹.

On doit également protéger les renseignements personnels «au moyen de mesures de sécurité correspondant à leur degré de sensibilité»¹⁴², une obligation liée aux limites quant à leur collecte et à leur conservation. En effet, une collecte et conservation excessive de renseignements augmente le risque de préjudice aux

<https://www.hunton.com/files/Publication/37a71d77-14c4-4361-a62b-89f67feb544f/Presentation/PublicationAttachment/e7ffca9d-da66-4ed6-a445-f8fdc0b97e22/Ten_Steps_whitepaper.pdf>.

¹³⁷ *LPRPDE*, *supra* note 84, ann 1, principe 4.3.1; Scasser et Sattler à la p 118.

¹³⁸ *Ibid*, art 5(3).

¹³⁹ *Ibid*, ann 1, principe 4.4.2.

¹⁴⁰ *Ibid*, ann 1, principe 4.5.

¹⁴¹ *Ibid*, ann 1, principe 4.5.3.

¹⁴² *Ibid*, ann 1, principe 4.7.

individus concernés advenant un bris de sécurité informationnel¹⁴³. Personne n'est à l'abri d'un bris de sécurité potentiellement dévastateur : la faille Heartbleed en 2014 a touché autant des réseaux sociaux tels Facebook et Instagram que l'Agence du revenu du Canada¹⁴⁴. Depuis les modifications apportées à la *LPRPDE* en juin 2015, les organisations doivent d'ailleurs aviser le CVPC et les individus touchés de toute atteinte aux mesures de sécurité s'il est raisonnable de croire que «l'atteinte présente un risque réel de préjudice grave à l'endroit d'un individu»¹⁴⁵.

Ultimement, l'organisation est «responsable des renseignements personnels dont elle a la gestion»¹⁴⁶. Cette responsabilité s'étend aux renseignements confiés à des tiers aux fins de traitement : à l'ère des applications mobiles et de l'infonuagique («*cloud computing*»), les données nécessaires au bon fonctionnement des applications peuvent être traitées par des tiers et stockées dans des serveurs à différents endroits dans le monde. Par exemple, Uber indique dans sa politique de confidentialité qu'elle peut partager les données qu'elle collecte, incluant les données de localisation, avec «les fournisseurs, consultants, partenaires marketing et autres prestataires de services qui ont besoin d'accéder à ces informations afin de réaliser un travail pour [son] compte».

Si c'est le cas, «[l']organisation doit, par voie contractuelle ou autre, fournir un degré comparable de protection aux renseignements qui sont en cours de traitement par une tierce partie»¹⁴⁷. L'organisation qui communique des renseignements personnels à un fournisseur de service devrait donc prévoir par contrat les obligations du fournisseur quant à la sécurité des renseignements communiqués et pourrait également prévoir un droit de surveillance et de vérification pour s'assurer que le fournisseur respecte ses engagements¹⁴⁸.

¹⁴³ Voir notamment Scassa et Dertubide, *Electronic Commerce and Internet Law in Canada*, *supra* note 109 à la p 172 : « The obligation to safeguard data is, of course, closely linked to the obligations on organizations to limit their collection of data to only that which is required for the purposes for which it is sought, and to limit the retention of such data to the period in which it remains necessary for those purposes. Excessive collection and undue retention of data can only increase the risk to individuals in the event of a data security breach ».

¹⁴⁴ Christine Bureau, « La faille Heartbleed démystifiée », ICI Radio-Canada (12 avril 2014), en ligne : <<http://ici.radio-canada.ca/nouvelles/societe/2014/04/11/007-heartbleed-definition-changer-mot-passe-questions.shtml>>.

¹⁴⁵ *LPRPDE*, *supra* note 84, art 10.1, telle que modifiée.

¹⁴⁶ *Ibid*, ann 1, principe 4.1.

¹⁴⁷ *Ibid*, ann 1, principe 4.1.3.

¹⁴⁸ Voir généralement Éloïse Gratton, « Dealing with Canadian and Quebec Legal Requirements in the Context of Trans-border Transfers of Personal Information and Cloud Computing Services », *supra* note 102, aux pp 36 à 39.

iii. *Divulgence des renseignements personnels sans consentement*

Bien que le consentement des utilisateurs soit généralement nécessaire pour récolter, utiliser ou communiquer des renseignements personnels, la *LPRPDE* prévoit plusieurs exceptions qui permettent aux entreprises de déroger à cette règle générale¹⁴⁹.

iv. *Communication exigée par assignation, mandat ou ordonnance*

Comme nous l'avons vu plus haut, il y a plus de données de géolocalisation qui existent que jamais à propos des utilisateurs des nouvelles technologies. Considérant les détails que ces données peuvent révéler sur les activités de chacun (l'endroit où se situait une personne à un moment donné et les personnes avec qui elle était), elles ont le potentiel de devenir une preuve fort pertinente pour trancher un litige.

À la fin 2014, il a été rapporté qu'une demanderesse, dans une action en responsabilité délictuelle en Alberta, allait soumettre en preuve des données de son bracelet FitBit afin de démontrer l'incapacité partielle causée par une blessure¹⁵⁰. Dans ce cas, le consentement ne pose pas problème : la demanderesse dépose elle-même ces données en preuve. Mais qu'en serait-il si la partie défenderesse avait voulu obtenir de telles données de la part d'un tiers au litige, comme une entreprise qui fournit une application mobile?

La *LPRPDE* prévoit qu'une entreprise peut divulguer un renseignement personnel à l'insu de l'intéressé et sans son consentement si la communication¹⁵¹ :

est exigée par assignation, mandat ou ordonnance d'un tribunal, d'une personne ou d'un organisme ayant le pouvoir de contraindre à la production de renseignements ou exigée par des règles de procédure se rapportant à la production de documents.

L'assignation qui émane d'un avocat ne suffit pas pour remplir cette exception. Par exemple, dans le cadre de procédures en divorce, une banque ne peut pas communiquer de l'information financière sur l'un de ses clients à l'avocat de son ancienne conjointe, suite à une assignation de celui-ci¹⁵². Pour que la

¹⁴⁹ *LPRPDE*, supra note 84, art 7.

¹⁵⁰ Parmy Olson, « Fitbit Data Now Being Used In The Courtroom », *Forbes* (16 novembre 2014), en ligne : <<http://www.forbes.com/sites/parmyolson/2014/11/16/fitbit-data-court-room-personal-injury-claim/>>.

¹⁵¹ *LPRPDE*, supra note 84, art 7(3)c).

¹⁵² *Résumé de conclusions d'enquête en vertu de la LPRPDE no 2002-96 : Une banque a indûment communiqué des renseignements personnels; rejet de l'exception en vertu de l'alinéa 7(3)c*, Commissariat à la vie privée du Canada, en ligne : <<https://www.priv.gc.ca/cf-dc/2002/cf->

communication soit permise dans ce contexte, il faudrait qu'un tribunal ait rendu une ordonnance suite à la requête de l'avocat.

Cette disposition peut trouver application dans le contexte du piratage d'œuvres en ligne, comme l'a récemment démontré l'affaire *Voltage Pictures LLC c John Doe*¹⁵³. Voltage Pictures, titulaire du droit d'auteur sur le film *The Hurt Locker*, voulait obtenir l'identité des abonnés du fournisseur de service Internet TekSavvy associés aux adresses IP prétendument impliquées dans le téléchargement du film à l'aide du protocole BitTorrent. Sans une ordonnance d'un tribunal, TekSavvy n'aurait pas pu communiquer ces renseignements sans violer la *LPRPDE*. La Cour fédérale, appliquant les principes établis par la Cour d'appel fédérale dans *BMG Canada Inc c Doe*¹⁵⁴, a ordonné à TekSavvy de communiquer les renseignements personnels à Voltage Pictures, tout en établissant des balises visant à atteindre un équilibre entre le droit à la vie privée des utilisateurs d'Internet et les droits des titulaires de droit d'auteur¹⁵⁵.

De façon similaire, on peut imaginer que la localisation d'une personne à un moment précis – une information connue de l'entreprise qui fournit une application mobile – pourrait revêtir une importance capitale dans le cadre d'un litige. Pensons à une réclamation d'assurance suite à un incendie suspect : si l'assuré s'est rendu sur les lieux de l'incendie à l'aide d'une voiture Uber, l'assureur a intérêt à obtenir de Uber les données concernant cet utilisateur. Au contraire, si l'assuré se déplaçait à l'autre extrémité de la ville avec une voiture Uber au moment de l'incendie, il pourrait décider de déposer en preuve les données de son parcours Uber. Ainsi, l'omniprésence des services de géolocalisation dans la vie de tous les jours résulte en une masse de données qui, dans certains cas, ont le potentiel de jouer un rôle important dans de nombreux litiges, dans les années à venir.

Les amendements de juin 2015 à la *LPRPDE* introduisent de nouvelles exceptions qui, dans certains cas, pourraient éviter aux demandeurs éventuels de s'adresser à un tribunal pour obtenir la communication de renseignements personnels. Le nouvel article 7(3)d.1) vise la communication qui :

est faite à une autre organisation et est raisonnable en vue d'une enquête sur la violation d'un accord ou sur la contravention au droit fédéral ou provincial qui a été commise ou est en train ou sur le point de l'être, s'il est raisonnable de s'attendre à ce que la communication effectuée au su ou avec le consentement de l'intéressé compromettrait l'enquête¹⁵⁶.

dc_021203_2_f.asp>, cité dans Scassa et Deturbide, *Electronic Commerce and Internet Law in Canada*, *supra* note 109 à la p 154.

¹⁵³ *Voltage Pictures LLC c John Doe*, 2014 CF 161.

¹⁵⁴ *BMG Canada Inc c Doe*, 2005 CAF 193.

¹⁵⁵ *Voltage Pictures*, *supra* note 153 au para 133.

¹⁵⁶ *LPRPDE*, *supra* note 84, art 7(3)d.1).

[Soulignements ajoutés]

Le terme «accord» («*agreement*» dans sa version anglaise) vise potentiellement n'importe quel contrat, donnant à cette exception une portée très large et facilitant considérablement l'échange de renseignements personnels entre entreprises privées. Selon certains¹⁵⁷, cette exception va à l'encontre des enseignements des tribunaux concernant les balises à imposer à la communication de renseignements personnels d'utilisateurs, tant dans le contexte civil comme l'affaire *Voltage Pictures* que le contexte criminel, que nous examinerons maintenant.

v. **Communication à une institution gouvernementale**

Des questions similaires surgissent évidemment dans le contexte criminel et de sécurité nationale : les données de géolocalisation qui existent à propos des utilisateurs d'applications mobiles représentent une mine d'or pour les forces de l'ordre et les services de renseignements comme le Service canadien du renseignement de sécurité.

L'une des exceptions les plus controversées à la *LPRPDE* est son article 7(3)c.1), qui permet aux entreprises de communiquer un renseignement personnel, à l'insu de l'intéressé et sans son consentement, «à une institution gouvernementale [...] qui a demandé à obtenir le renseignement en mentionnant la source de l'autorité légitime étayant son droit de l'obtenir» pour des fins d'application du droit¹⁵⁸.

La Cour suprême s'est récemment penchée sur cette disposition dans l'arrêt *R c Spencer*¹⁵⁹. Se fondant sur cette exception, la police avait demandé à un fournisseur de services Internet de lui fournir l'identité d'une abonnée dont l'adresse IP avait été utilisée pour consulter de la pornographie juvénile¹⁶⁰. La police n'avait pas tenté d'obtenir une ordonnance de communication (l'équivalent d'un mandat de perquisition)¹⁶¹. L'accusé a demandé l'exclusion de la preuve au motif qu'il y avait eu violation de son droit à la protection contre les fouilles et perquisitions abusives prévu à l'article 8 de la *Charte canadienne*¹⁶².

¹⁵⁷ Voir notamment Michael Geist, « Fixing the Digital Privacy Act: My Bill S-4 Appearance Before the Industry Committee », *Michael Geist* (blogue), 11 mars 2015, en ligne : <<http://www.michaelgeist.ca/2015/03/fixing-digital-privacy-act-bill-s-4-appearance-industry-committee/>>.

¹⁵⁸ *LPRPDE*, *supra* note 84, art 7(3)c.1).

¹⁵⁹ *R c Spencer*, [2014] 2 RCS 212, 2014 CSC 43.

¹⁶⁰ *Ibid* au para 11.

¹⁶¹ *Ibid*.

¹⁶² *Charte canadienne*, *supra* note 68, art 8.

La Cour a reconnu qu'il existe une attente raisonnable de vie privée à l'égard de l'identité de l'abonnée¹⁶³:

La communication de ces renseignements permettra souvent d'identifier l'utilisateur qui mène des activités intimes ou confidentielles en ligne en tenant normalement pour acquis que ces activités demeurent anonymes. La demande faite par un policier visant la communication volontaire par le [fournisseur de services Internet] de renseignements de cette nature constitue donc une fouille.

La Cour a ensuite examiné la notion de «source de l'autorité légitime» centrale à l'exception de l'article 7(3)c.1) de la *LPRPDE*¹⁶⁴. Il ne s'agit pas d'une ordonnance ou d'un mandat de perquisition, puisque ces cas sont prévus à l'article 7(3)c) discuté précédemment. Mais il faut plus qu'une simple requête de la part de la police, comme c'était le cas dans *Spencer*. Selon la Cour¹⁶⁵ :

Cette notion peut désigner le pouvoir conféré par la common law aux policiers de poser des questions portant sur des éléments qui ne font pas l'objet d'une attente raisonnable en matière de vie privée. Elle peut renvoyer au pouvoir de la police d'effectuer une fouille ou une perquisition sans mandat dans des circonstances contraignantes ou dans des cas où une loi qui n'a rien d'abusif le permet.

S'il reste à clarifier cette notion, on peut retenir de l'arrêt *Spencer* deux leçons importantes. Premièrement, la police ou les services de renseignements, lorsqu'ils formulent une demande à une entreprise privée pour la communication de renseignements personnels, doivent s'appuyer sur quelque chose d'autre que leur simple statut d'institution gouvernementale: un pouvoir conféré par la *common law* ou une loi raisonnable. Plus fondamentalement, autant sous l'angle de la protection constitutionnelle de la *Charte canadienne* que celui de la protection des renseignements personnels, des données collectées dans le cadre de l'utilisation de nouvelles technologies ont d'importantes conséquences pour la vie privée des utilisateurs.

Dans tous les cas, l'entrepreneur technologique qui conçoit et opère une application mobile faisant la collecte, l'utilisation et la communication de renseignements personnels doit maîtriser le cadre juridique qui s'applique à de telles activités, de façon à éviter des violations importantes des droits de ses utilisateurs.

4. Conclusion

¹⁶³ *Spencer*, *supra* note 159 au para 66.

¹⁶⁴ *Ibid* au para 71.

¹⁶⁵ *Ibid*.

Le fil directeur qui émerge de notre exposé est sans doute que l'utilisation de la géolocalisation dans les applications mobiles soulève des questions juridiques nuancées aux réponses parfois incertaines, autant sous l'angle du droit d'auteur que sous l'angle de la protection de la vie privée. Du côté du droit d'auteur, la protection accordée aux compilations de données géographiques dépend véritablement de chaque cas d'espèce, selon le choix et l'arrangement original des données. Pour ce qui est de la vie privée, ce qui constitue un consentement éclairé à la collecte, l'utilisation et la communication de renseignements sur la géolocalisation des utilisateurs demeure un défi de taille pour les entreprises technologiques.

Le droit n'évolue parfois pas aussi rapidement que l'innovation dans le secteur des technologies de l'information, qui nous confère des bénéfices inespérés tout en entraînant certains risques nouveaux. Il n'est pas étonnant que le droit s'adapte parfois mal à des situations que le législateur et les tribunaux, autant que les citoyens, n'auraient pas pu imaginer il y a dix ou quinze ans.

Heureusement, l'innovation n'est pas limitée aux entreprises technologiques : des solutions juridiques pratiques permettent de combiner innovation et certitude juridique. Par exemple, les entreprises technologiques peuvent utiliser des ensembles de données disponibles sous licences en respectant les modalités qui s'y rattachent et ainsi éviter l'ambiguïté du droit d'auteur. De plus, les solutions technologiques comme les notifications et les avis « multicouches » peuvent aider les entreprises à respecter leurs obligations en matière de protection de renseignements personnels tout en n'assommant pas leurs utilisateurs avec des politiques de confidentialité incompréhensibles.

Il n'en demeure pas moins qu'il est parfois difficile d'éviter les mauvais tournants en naviguant à travers les règles juridiques qui encadrent la géolocalisation à l'ère des applications mobiles et des réseaux sociaux. Une chose est certaine : il est préférable de pécher par excès de prudence, afin d'éviter de se retrouver géolocalisé au Palais de justice le plus près!



ROBIC + DROIT
+ AFFAIRES
+ SCIENCES
+ ARTS

ROBIC, S.E.N.C.R.L.
www.robic.ca
info@robic.com

MONTREAL
1001, Square-Victoria - Bloc E - 8^e étage
Montréal (Québec) Canada H2Z 2B7
Tél.: +1 514 987-6242 Téléc.: +1 514 845-7874

QUÉBEC
2828, boulevard Laurier, Tour 1, bureau 925
Québec (Québec) Canada G1V 0B9
Tél.: +1 418 653-1888 Téléc.: +1 418 653-0006

ROBIC, S.E.N.C.R.L.
www.robic.ca
info@robic.com

MONTRÉAL
1001, Square-Victoria - Bloc E - 8^e étage
Montréal (Québec) Canada H2Z 2B7
Tél.: +1 514 987-6242 Téléc.: +1 514 845-7874

QUÉBEC
2828, boulevard Laurier, Tour 1, bureau 925
Québec (Québec) Canada G1V 0B9
Tél.: +1 418 653-1888 Téléc.: +1 418 653-0006

ROBIC, S.E.N.C.R.L.
www.robic.ca
info@robic.com

MONTRÉAL
1001, Square-Victoria - Bloc E - 8^e étage
Montréal (Québec) Canada H2Z 2B7
Tél.: +1 514 987-6242 Téléc.: +1 514 845-7874

QUÉBEC
2828, boulevard Laurier, Tour 1, bureau 925
Québec (Québec) Canada G1V 0B9
Tél.: +1 418 653-1888 Téléc.: +1 418 653-0006

ROBIC, S.E.N.C.R.L.
www.robic.ca
info@robic.com

MONTRÉAL
1001, Square-Victoria - Bloc E - 8^e étage
Montréal (Québec) Canada H2Z 2B7
Tél.: +1 514 987-6242 Téléc.: +1 514 845-7874

QUÉBEC
2828, boulevard Laurier, Tour 1, bureau 925
Québec (Québec) Canada G1V 0B9
Tél.: +1 418 653-1888 Téléc.: +1 418 653-0006

ROBIC, S.E.N.C.R.L.
www.robic.ca
info@robic.com

MONTRÉAL
1001, Square-Victoria - Bloc E - 8^e étage
Montréal (Québec) Canada H2Z 2B7
Tél.: +1 514 987-6242 Téléc.: +1 514 845-7874

QUÉBEC
2828, boulevard Laurier, Tour 1, bureau 925
Québec (Québec) Canada G1V 0B9
Tél.: +1 418 653-1888 Téléc.: +1 418 653-0006