Chronique - Qu'est-ce qu'un renseignement personnel ? Le défi de qualifier les nouveaux types de renseignements

Eloïse GRATTON*

EYB2013REP1287 (approx. 15 page(s))

EYB2013REP1287

Repères, Janvier 2013

Eloïse GRATTON*
Chronique - Qu'est-ce qu'un renseignement personnel ? Le défi de qualifier les nouveaux types de renseignements

Indexation

COMMUNICATIONS ; TECHNOLOGIES DE L'INFORMATION ; INTERNET ; MÉDIAS SOCIAUX ; LOI CONCERNANT LE CADRE JURIDIQUE DES TECHNOLOGIES DE L'INFORMATION ; ACCÈS À L'INFORMATION ; PROTECTION DES RENSEIGNEMENTS PERSONNELS ; INTERPRÉTATION DES LOIS

TABLE DES MATIÈRES

Résumé

L'auteure traite de la définition de « renseignement personnel » que l'on retrouve dans les lois en matière de protection de renseignements personnels. Elle souligne le fait que cette dernière est mal adaptée aux nouvelles réalités technologiques (ainsi qu'aux défis que posent les nouvelles technologies d'Internet) et discute des interprétations ou solutions qui peuvent faire en sorte que ces lois demeureront efficaces compte tenu des technologies modernes.

INTRODUCTION

De nos jours, il existe un important volume de délocalisation informatique qui s'effectue à des vitesses plus grandes, atteignant des zones géographiques plus larges, transférant des données alphanumériques, audio, vidéo et autres types de données à un nombre encore plus grand d'intervenants[1]. Différents outils de suivi en ligne comme des témoins de connexion (*cookies*), des pixels espions ou des logiciels espions peuvent collecter des renseignements personnels, incluant les habitudes de navigation Web des utilisateurs (ou *clickstream data*), les sites Web visités, les commentaires diffusés en ligne ainsi que les recherches effectuées en ligne par ces derniers. Des renseignements peuvent aussi être collectés en lien avec les adresses IP. Les appareils mobiles peuvent divulguer leur emplacement de différentes façons : par des solutions basées sur un réseau, des solutions basées sur un combiné téléphonique (plusieurs téléphones utilisent maintenant des récepteurs GPS) ou par d'autres types de solutions hybrides[2], Les renseignements sur l'emplacement peuvent aussi être déduits, par exemple, à partir de l'adresse IP des terminaux et des points d'accès sans fil de type WiFi[3]. La technologie d'identification par radiofréquence IRF (« IRF »), qui consiste en un système d'étiquettes et de lecteurs qui peuvent être utilisés pour identifier et encoder une variété d'information, est de plus en plus utilisée[4]. On rencontre une variété grandissante d'autres méthodes et techniques de collecte comme les systèmes de péage routiers informatisés (par exemple EZ Pass), les systèmes de reconnaissance faciale, la biométrie et l'imagerie thermique.

Qu'est-ce qu'un renseignement personnel ? La réponse à cette question est cruciale puisque les lois en matière de protection de renseignements personnels (« LPRP ») ne régissent que les renseignements qu'elles qualifient de *personnels.* Le fait que certains renseignements soient *personnels* engendre certains droits pour les individus et des obligations pour les organisations. Par exemple, les individus ont le droit de connaître les renseignements personnels qui sont collectés à leur sujet ainsi que l'utilisation ou la divulgation qui en sera faite et ils ont le droit de consentir à de telles activités de manipulation des données. Les organisations qui gèrent des renseignements personnels ont l'obligation de protéger ces derniers au moyen de méthodes de sécurité appropriées, de s'assurer que les renseignements utilisés sont exacts, et d'autoriser les individus visés par ces renseignements à y accéder. Comme de nouveaux types de renseignements (adresses IP, données de localisation, etc.) ne sont pas toujours clairement visés par la définition générale de renseignement personnel que l'on retrouve dans les LPRP canadiennes (« renseignement concernant un individu identifiable ») et que de nouvelles méthodes d'identification sont de plus en plus disponibles, une analyse ou un réexamen de ce que constitue ou devrait constituer un renseignement concernant un individu identifiable est nécessaire.

Dans un premier temps, le présent article mettra en contexte l'adoption des LPRP. Dans un deuxième temps, on traitera des défis que posent ces nouvelles technologies et nouveaux types de renseignements eu égard à la nouvelle réalité du Web et à la définition traditionnelle de renseignement personnel. Enfin, on examinera différentes pistes de solution en vue de répondre à ces défis posés par les nouveaux types de renseignements.

I– L'ÉLABORATION DE LA DÉFINITION DE RENSEIGNEMENT PERSONNEL

Cette section traitera des origines et de l'historique menant à l'adoption des LPRP et de l'élaboration de la définition de renseignement personnel.

A. Les origines et l'historique de l'adoption des LPRP

Vers la fin des années 1960 et le début des années 1970, une quantité croissante de données concernant presque tous les citoyens étaient généralement enregistrées dans des dossiers automatisés ayant un rendement et des capacités de stockage encore plus grands que les dossiers traditionnels [5]. Évidemment, certains craignaient que cette technologie n'abandonne le contrôle de ces renseignements personnels aux entreprises qui contrôlaient les bases de données [6]. La façon d'aborder cette menace particulière a été résolue par la conceptualisation de la *vie privée* comme étant « le contrôle d'un individu sur ses renseignements personnels » [7]. Réglementer la façon dont les renseignements personnels pouvaient être collectés semblait nécessaire afin de prévenir l'utilisation de méthodes inadéquates ou un manque de transparence entourant la collecte des données, étant donné qu'il était beaucoup plus difficile pour un individu de prendre des moyens pour protéger ses intérêts personnels lorsqu'il s'agissait d'un système de données informatisées – si on le compare à un registre de données traditionnel [8]. Les principes relatifs à l'équité dans le traitement des données (aussi connus sous le nom de *Fair Information Practices*) ont été rédigés durant cette période, puis incorporés dans les LPRP.

Au Canada, la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE) a été introduite en 2000 et est entrée en vigueur pour le secteur privé en 2004 [9]. Le gouvernement fédéral peut exempter certaines entreprises ou activités dans les provinces canadiennes qui possèdent leur propre LPRP lorsque cette Loi est substantiellement similaire à la loi fédérale [10]. Le Québec a été la première province à adopter une LPRP avec la *Loi sur la protection des renseignements personnels dans le secteur privé* (la LPRPSP) [11] en 1993. Deux autres provinces, soit la Colombie-Britannique [12] et l'Alberta [13], ont édicté en 2003 des LPRP provinciales également reconnues comme étant essentiellement similaires à la LPRPDE.

B. L'élaboration de la définition de « renseignement personnel »

Dans les années 1970, au moment où la définition de *renseignement personnel* était en voie d'être établie, on en est arrivé à un consensus en Europe sur le fait que la seule définition possible de *renseignement personnel* aux fins des LPRP était : *toute donnée reliée à un individu identifié ou identifiable* [14]. Depuis les quarante dernières années, la même définition de *renseignement personnel* ou encore d'autres définitions très similaires ont été utilisées de façon répétitive dans d'autres instruments de politique transnationaux [15]. Des définitions identiques ou similaires sont également au coeur des LPRP que l'on retrouve à travers le monde, incluant l'Europe [16].

Au Canada, la LPRPDE définit le *renseignement personnel* comme étant tout renseignement *concernant un individu identifiable* [17]. Les LPRP de l'Alberta et de la Colombie-Britannique ont la même définition ou à tout le moins, des définitions très semblables [18]. Au Québec, la LPRPSP définit le *renseignement personnel* comme étant *tout renseignement qui concerne une personne physique et permet de l'identifier* [19]. Cette loi s'applique « à ces renseignements, quelle que soit la nature de leur support et quelle que soit la forme sous laquelle ils sont accessibles : écrite, graphique, sonore, visuelle, informatisée ou autre » [20]. Ainsi, quoique la majorité des LPRP canadiennes offre certaines exclusions, comme par exemple les données de contact d'affaires d'employés [21], les produits du travail (ou *work product*) [22] ou dans certains cas les données publiquement disponibles [23], il reste que le noyau de la définition est demeuré largement inchangé depuis que cette dernière a initialement été énoncée au début des années 1970. Avec les changements survenus au cours des dernières années sur le plan technologique, il est raisonnable de se questionner sur l'efficacité de cette définition dans le contexte d'Internet.

II– LES DÉFIS RÉSULTANT DES NOUVELLES TECHNOLOGIES

Cette section décrira dans un premier temps comment la notion d'« identifiable » peut créer certaines incertitudes. Dans un deuxième temps, une analyse sur le fait qu'il soit de plus en plus facile d'effectuer la corrélation de divers renseignements sera effectuée. Finalement, dans un dernier temps, nous examinerons les défis posés par différents types de nouveaux renseignements dans le but d'illustrer le genre de défi qui résulte de l'application de cette définition à de nouveaux types de renseignements.

A. L'incertitude quant à la notion d'« identifiable

En vertu de la définition de *renseignement personnel*, les renseignements ne sont couverts par les LPRP que s'ils permettent « d'identifier » un individu, ce qui est habituellement la norme pour l'établissement des limites appropriées des régimes de protection des données.

Par conséquent, la définition de *renseignement personnel* est plutôt vague puisqu'on ne sait pas toujours à quel moment un élément d'information est réputé « identifier » un individu [24]. Le Commissariat à la protection de la vie privée du Canada (CPVP) a récemment admis qu'il n'est pas toujours simple de déterminer si des renseignements constituent ou non des renseignements personnels en vertu de la LPRPDE [25].

Il est en effet souvent difficile de déterminer si certains types de renseignements générés sur Internet ou à travers d'autres nouvelles technologies sont inclus dans la définition actuelle puisque la notion « d'individu identifiable » peut être interprétée de diverses façons [26]. En Europe, le Groupe de travail de l'Article 29 a d'ailleurs effectué une analyse du concept de « donnée personnelle » après avoir observé que les pratiques courantes dans les états membres de l'UE suggéraient qu'il existait une incertitude à ce sujet, et plus précisément envers la notion d'individu « identifiable » [27].

Cette insécurité juridique (à savoir si un renseignement se qualifie ou non de « personnel ») est problématique pour les entreprises qui gèrent des renseignements personnels puisqu'elles ignorent si les renseignements qu'elles traitent constituent des renseignements personnels, auquel cas elles auraient l'obligation légale de se conformer aux LPRP applicables. Afin d'illustrer cette insécurité, il n'est pas toujours facile de décider quel type de ressources (en argent, en temps, en technologie, etc.) une entreprise doit utiliser pour déterminer ce qui constitue un renseignement « identifiable » ; où doit-on fixer les limites entre les renseignements personnels et les données anonymes, et comment savoir si les données doivent être évaluées seules ou si on doit plutôt tenir compte des autres données accessibles. Il existe aussi des enjeux quant à la détermination du moment où un renseignement relié à un appareil (pouvant être utilisé par un ou plusieurs individus) peut être qualifié de *renseignement personnel*. Enfin, il existe aussi une incertitude quant à la nécessité de la présence d'un lien « précis » entre un élément de renseignement et un individu pour que ce renseignement soit considéré comme étant identifiable au sens des LPRP.

Comme il a été discuté plus tôt, la notion d'individu « identifiable » a fait l'objet de plusieurs débats et controverses et elle est parfois même interprétée différemment selon les différentes juridictions (et parfois même à l'intérieur d'une même juridiction). En outre, alors que le système européen (contrairement au Canada) possède certains critères pour déterminer ce qui constitue une donnée « identifiable » au moyen du considérant 26 de la Directive 95/46/EC (« l'ensemble des moyens susceptibles d'être raisonnablement mis en oeuvre »), l'ensemble des cas s'attaquant à l'interprétation de l'article 2(a) de la Directive 95/46/EC (définition de *renseignement personnel*) conjointement avec le considérant 26 de la Directive 95/46/EC révèle que les tribunaux européens ont abordé cet enjeu de maintes façons, menant à des conclusions contradictoires et confuses [28].

B. La corrélation de plus en plus facile

Quoique l'agrégation et la corrélation de renseignements ne soient pas des activités nouvelles, leur puissance et leur portée ont augmenté au même rythme que les technologies d'Internet. De nouveaux algorithmes ont été développés afin de permettre l'extraction de renseignements à partir d'une grande quantité de renseignements collectés [29]. Les techniques et les capacités d'extraction de données atteignent de nouveaux degrés de sophistication si on les compare à celles qui existaient il y a à peine quelques années, ce qui a pour effet de générer des inquiétudes au sein de certains programmes ou initiatives impliquant la collecte massive de renseignements facilement accessibles [30]. La convergence de différentes technologies rend maintenant possible une collecte plus intrusive de renseignements et de nature beaucoup plus personnelle qu'auparavant [31].

Ce qui rend de plus en plus facile l'identification des individus en lien avec les renseignements en circulation est le fait qu'il y a un volume important de renseignements déjà en circulation. La capacité de stockage des ordinateurs a augmenté exponentiellement depuis l'avènement de l'ère informatique [32]. Il existe plus de 25,5 millions d'utilisateurs d'appareils mobiles au Canada [33] et 59,5 millions en France [34]. *The Economist* a récemment rapporté que la quantité totale de renseignements dans le monde croît de 60 % par année [35].

Avec l'avènement du Web 2.0, qui porte essentiellement sur ce pourquoi les individus utilisent les ordinateurs, la façon dont ils gèrent leurs renseignements personnels a subi un changement important [36]. En décembre 2009, plus de 350 millions de personnes à travers le monde utilisaient Facebook pour partager leur quotidien en ligne [37]. En février 2010, ce nombre d'utilisateurs a atteint 400 millions [38] et en juillet 2011, 500 millions [39]. Il y a plus de 40 milliards de photos seulement sur Facebook [40], plus de 3 milliards de photos sur le site Flickr.com [41] et on rapporte que les utilisateurs de YouTube téléchargent plus de 24 heures de vidéo par minute [42].

C. Illustration des défis : nouveaux types de renseignements

Avec les nouvelles technologies d'Internet, de nouveaux types de renseignements sont apparus et ces renseignements, plutôt que de référer à un individu identifiable, peuvent référer à un outil ou à un ordinateur. Ceci étant dit, il est parfois possible d'identifier l'utilisateur de façon indirecte. Le défi est donc d'être en mesure de déterminer dans quelles situations les renseignements doivent être considérés comme étant « personnels » ou « identifiables ». Dans les prochaines lignes, nous examinerons différents types de nouveaux renseignements afin de déterminer s'ils sont considérés comme étant des renseignements personnels au sens de la LPRPSP (Québec) et de la LPRPDE (fédérale), et les défis qu'ils posent soit dans la pratique ou encore sur le plan de la protection de la vie privée.

1. Adresse courriel et noms

Les adresses électroniques sont en général reconnues comme étant des renseignements personnels, que ce soit par la LPRPDE [43] (fédéral) ou la LPRPSP [44] du Québec. Toutefois, si on se fie à la définition littérale de *renseignement personnel* que l'on retrouve dans les LPRP, il n'est pas clair que ce renseignement soit toujours personnel. Par exemple, les auteurs Pierre Trudel, France Abran et Gabriel Dupuis suggèrent que pour qu'une adresse courriel puisse être qualifiée de renseignement personnel, elle se doit d'identifier un individu. Par conséquent, quoique l'adresse courriel pierre.trudel@umontreal se qualifie de renseignement personnel, on pourrait argumenter qu'une adresse courriel de type teacher@hotmail.com n'est pas un renseignement personnel [45].

Certains fournisseurs de services en ligne peuvent demander aux utilisateurs de créer un compte pour utiliser leurs services ; ils collecteront alors les noms d'usagers de ces utilisateurs. Dans l'affaire *Google/Viacom* qui a fait couler beaucoup d'encre [46], la cour américaine avait statué que les noms d'usagers n'étaient pas des renseignements personnels [47]. Toutefois, Orin Kerr, professeur de droit de la George Washington University, a émis l'opinion qu'il est dangereux de décider que ce type de renseignement n'est jamais un renseignement personnel puisque ce genre de renseignement peut au contraire être « identifiable », surtout si l'individu utilise son nom ou une partie de son nom dans son nom d'usager [48].

2. Adresse IP et donnée de type

Une adresse IP réfère à une connexion Internet. Même en utilisant une adresse IP dynamique, il est possible de faire un lien entre l'adresse IP et l'abonné qui a un service de connectivité Internet, au départ en utilisant une banque de données publique pour déterminer quel fournisseur de service Internet (FSI) détient l'adresse IP en question, et par la suite établir un lien entre le rapport du FSI (*log file*) et le nom de l'abonné à qui cette adresse IP a été assignée par le FSI à un moment donné. Cette adresse IP peut aussi être utilisée pour divulguer la position géographique de l'outil connecté à Internet, quoique ce renseignement ne soit pas toujours très précis [49].

En vertu de la LPRPDE, l'adresse de protocole Internet (IP) peut être considérée comme un renseignement personnel si elle peut être associée à un individu identifiable [50]. Par exemple, le CPVP a, dans une conclusion d'enquête, déterminé que des adresses IP recueillies par un FSI étaient des renseignements personnels puisque le FSI pouvait associer ces dernières à ses clients au moyen du numéro d'abonné.

Toutefois, la question de l'adresse IP est loin d'être résolue. En fait, bien que certains défenseurs de la vie privée européens soutiennent que les adresses IP devraient être qualifiées de renseignements personnels en vertu de la Directive 95/46/EC, d'autres fonctionnaires européens sont d'avis contraire. Les tribunaux et les autorités de réglementation de la Suède [51] et de l'Espagne [52] soutiennent que les adresses IP relèvent de la Directive 95/46/EC. En Allemagne [53] et au Royaume-Uni [54], un point de vue contraire est favorisé. Dans certains cas, à l'intérieur d'une même juridiction, soit celle de la France, les tribunaux ne s'entendent pas sur la question de savoir si les adresses IP sont des renseignements personnels. La position de la Cour d'appel de Paris, en avril et en mai 2007, était que les adresses IP ne représentaient pas des données personnelles [55]. En août 2007, la CNIL française a émis un communiqué de presse indiquant ses inquiétudes à propos de ces deux décisions et affirmant que les adresses IP devraient être considérées comme des *données personnelles* [56]. En mai 2008, la Cour d'appel de Rennes a statué sur le fait que les adresses IP sont effectivement des renseignements personnels [57]. En janvier 2009, la Cour de cassation a infirmé cette décision, déclarant que les adresses IP ne constituent pas des renseignements personnels [58]. En juin 2009, le Tribunal de Grande Instance de Paris a adopté une position voulant que les adresses IP soient effectivement des renseignements personnels [59]. En février 2010, la Cour d'appel de Paris, se ralliant à la position de la Cour de cassation, a déclaré que les adresses IP ne constituaient pas des renseignements personnels [60]. Cette analyse jurisprudentielle démontre que, bien que ces cas français aient eu à la base des faits très similaires, c'est l'interprétation littérale de la définition (stricte ou large) de *renseignement personnel* utilisée par les tribunaux français qui n'était pas uniforme, entraînant ainsi des décisions contradictoires sur le même sujet et ce, à l'intérieur d'une même juridiction. Ceci illustre bien le fait que la définition qui réfère à un « renseignement concernant un individu identifiable » n'est pas une bonne adéquation pour les nouveaux types de renseignements et la nouvelle réalité d'Internet.

3. Donnée de localisation et RFID

Un nouveau type de renseignement est la donnée de localisation. Elle peut être obtenue de diverses façons (réseau sans fil, GPS, WiFi, etc.) et permet d'identifier la localisation de l'outil ce qui, par déduction, permet de localiser son utilisateur [61]. Ce type de renseignement peut également divulguer la position géographique de l'utilisateur de l'outil et parfois même ses intérêts ou autres données sensibles. Par exemple, on pourrait présumer qu'un individu qui visiterait un centre d'aide aux victimes d'une maladie donnée serait probablement lui-même atteint de cette maladie, etc.

Au Canada, le CPVP a statué sur le fait que l'information de contrôle obtenue au moyen d'un système mondial de localisation (GPS) installé à l'intérieur d'un véhicule de travail constitue un renseignement personnel étant donné que cette information peut être associée à l'employé qui conduit le véhicule. Plus précisément, les employés sont *identifiables*, selon le CPVP, même s'ils ne sont pas *identifiés* en tout temps par les utilisateurs du système [62]. Aussi, la position du CPVP est que les renseignements obtenus grâce à des étiquettes d'identification par radiofréquence (IRF) en vue de suivre et de localiser les bagages, les produits de détail et les achats personnels peuvent constituer les renseignements personnels de tout individu identifiable associé à ces articles [63]. Au Québec, dans son article 43, la *Loi concernant le cadre juridique des technologies de l'information* [64] règlemente la collecte de ce genre de données de localisation en prohibant de lier un individu à un dispositif qui permet de savoir où il se trouve sans son consentement préalable.

Le problème de l'utilisation d'une interprétation trop étroite de la définition de renseignement personnel résulte du fait que ce genre de renseignement de localisation peut être utile pour la société. Par exemple, il y a quelques années, plusieurs entreprises américaines (dont la Intelligent Transportation Society of America [65]) avaient demandé au FCC [66] de leur permettre de suivre les déplacements physiques des utilisateurs de sans fil sur une certaine période de temps, sans devoir en informer lesdits utilisateurs [67]. Ces entreprises suggéraient qu'il puisse y avoir une certaine utilité pour elles de savoir qu'un individu associé à un certain profil (par exemple, appelons-le le profil ABC) vit à un endroit donné, travaille à un autre endroit et effectue un certain parcours à un moment précis de la journée. Ce genre de renseignement, même anonyme (au sens où le nom ou le numéro de téléphone de l'individu à qui un certain profil est attribué ne sont d'aucune utilité), pourrait avoir l'avantage de fournir aux ingénieurs chargés des questions de planification routière et du trafic, l'information utile leur permettant de planifier les routes en conséquence, de gérer la congestion routière et de pouvoir plus facilement rediriger le trafic en situation d'urgence. Ceci étant dit, déterminer à partir de quel moment des données de localisation sont dans les faits « identifiables » reste un défi à relever. Par exemple, les données de localisation peuvent être rendues anonymes dans le sens où le numéro de téléphone peut avoir été remplacé par un numéro de profil (par exemple le profil ABC). Toutefois, si les données de localisation sont collectées de façon précise et sur une longue période de temps, alors nous pourrions, à un certain point, être en mesure de déterminer que l'individu derrière le profil ABC, lequel passe ses nuits à un endroit précis (sa demeure) et ses journées à un autre endroit (lieu de travail ?), est en fait l'individu X, qui est alors identifiable.

4. Données biométriques

Au Québec, la *Loi concernant le cadre juridique des technologies de l'information*[68] réglemente les données de type biométriques à l'article 44 . La jurisprudence du Québec et du Canada semble adopter une interprétation large de renseignement personnel, afin d'y inclure toute forme de donnée biométrique. Par exemple, dans *Syndicat des travailleurs de Mométal* c. *Mométal Inc.*[69], un arbitre québécois a statué que le résultat binaire obtenu après la conversion algorithmique des mensurations de la main d'un salarié peut être considéré comme un renseignement personnel. Toutefois, il est intéressant de constater que l'on réfère ici à l'information du « salarié ». Il est clair que pour un employeur, ce genre de renseignement sera un renseignement personnel puisqu'il se sert précisément de ce renseignement pour identifier son employé. Toutefois, dans la situation où ce type de renseignement (résultat binaire obtenu après la conversion algorithmique des mensurations de la main d'un individu) se retrouve dans les mains d'un tiers qui n'a aucun autre renseignement pour faire une corrélation entre ce renseignement et un individu identifiable, il serait alors plus difficile d'argumenter qu'il s'agit en fait d'un renseignement personnel au sens des LPRP applicables.

Au fédéral, la position du CPVP est que les renseignements personnels dans le contexte technologique comprennent des formes de renseignements biométriques comme les empreintes digitales[70] et les empreintes vocales[71]. Toutefois, conscient du fait que ce type de renseignement n'est pas toujours nécessairement « identifiable », le CPVP souligne que l'empreinte vocale constitue un renseignement personnel, « même si elle révèle peu de choses sur une personne et que l'ampleur de ce qu'elle révèle variera selon la façon dont elle est utilisée »[72].

5. Contenu de recherches effectuées en ligne

D'autres types de renseignements peuvent aussi être collectés par les entreprises faisant affaires en ligne. Par exemple, les moteurs de recherche peuvent collecter, en plus des adresses IP, des données de type *clickstream*, le contenu des recherches effectuées et les préférences des utilisateurs[73]. Toutefois, ce genre de renseignement, même s'il n'est pas associé à un individu en particulier (par exemple à un nom, etc.) peut quand même en arriver à identifier un individu. Un exemple est la violation de la vie privée qui a eu lieu en août 2006 lorsque AOL Research a publié (divulgué publiquement à des fins de recherche) sur l'un de ses sites Web, un fichier texte compressé contenant vingt millions de mots-clés de recherche qui avaient été entrés dans le moteur de recherche d'AOL par plus de 650 000 utilisateurs AOL anonymes pendant une période de trois mois. Bien que ce ne soit pas tous les profils qui aient été « identifiants », étant donné le volume de données rendues accessibles (des millions de mots-clés de recherche entrés par plus de 650 000 utilisateurs AOL pendant une période de trois mois), le « potentiel » d'identifier certains utilisateurs était existant. Dans les faits, plusieurs de ces individus se sont avérés être identifiables, en raison de la combinaison des recherches effectuées par les individus en question[74]. Ceci illustre encore une fois la problématique associée à la notion de renseignement « identifiable » lorsque le volume de renseignements permet une corrélation permettant dans certains cas d'identifier l'individu derrière le profil.

III– DES PISTES DE SOLUTIONS

Plusieurs pistes de solutions ont été proposées par divers auteurs au cours des dernières années afin de s'assurer que les nouveaux renseignements personnels soient efficacement couverts par les LPRP. Par exemple, quoique certains proposent d'adopter une interprétation large afin de s'assurer que le plus grand nombre possible de renseignements soient couverts, d'autres proposent de réévaluer la notion d'« identifiabilité », ou encore d'adopter une interprétation qui respecterait le but ultime des LPRP.

A. Interprétation large

La définition de renseignement personnel est tellement large que presque n'importe quel renseignement peut être qualifié de *personnel*[75]. Tel que suggéré par Barbara McIsaac dans son ouvrage intitulé *The Law of privacy in Canada*: “In essence, almost any information in any form that can be attributed to an identified individual is caught by this expansive definition”[76]. Au fédéral, le CPVP joue un rôle important dans la détermination de ce qui constitue un renseignement personnel. La tendance est expansionniste, tel que suggéré par le CPVP dans son rapport annuel de 2001-2002 :

> The definition is deliberately broad, and in my findings I have tended to interpret it as broadly as possible. [...] I am inclined to regard information as personal even if there is the smallest potential for it to be about an identifiable individual.[77]

En 2011, dans son guide intitulé *A Privacy Handbook for Lawyers, PIPEDA and Your Practice*, le CPVP indique que : « as per relevant jurisprudence on the concept of “personal information”, a broad and expansive interpretation is in order »[78].

Selon la jurisprudence du secteur public fédéral, la définition de renseignement personnel donne également lieu à une interprétation large[79]. La définition de « renseignement personnel » indique que le renseignement est une information « concernant » un individu identifiable. Au sens de la jurisprudence fédérale, le terme « concernant » signifie non seulement que le renseignement en question porte sur un individu, mais aussi qu'il le touche ou qu'il peut y être associé[80]. Dans l'affaire *Gordon c. Canada (Ministre de la Santé)*[81], un renseignement concerne un « individu identifiable » lorsqu'il y a une possibilité sérieuse qu'un individu puisse être identifié au moyen du renseignement, que ce renseignement soit pris seul ou en combinaison avec d'autres renseignements disponibles. Ce genre d'interprétation est très large, peut-être même trop. D'ailleurs, Pierre Trudel et Karim Benyekhlef, qui ont été mandatés pour évaluer la LPRP du Québec dans le contexte d'Internet, quelques années après son adoption, ont également émis l'opinion que la définition de *renseignement personnel* était excessive dans le contexte d'Internet et que l'équilibre délicat entre la protection des renseignements personnels et la libre circulation des données n'avait pas encore été atteint[82]. Dans le contexte d'Internet et des nouvelles technologies, cette portée trop large (ou le fait que les LPRP soient « excessives ») crée un fardeau supplémentaire pour les entreprises et les fournisseurs de services en ligne qui sont avides de données. De surcroît, une définition excessive peut provoquer un système au sein duquel les entreprises et les joueurs de l'industrie subiront des coûts supplémentaires afin de se conformer aux LPRP, lesquelles lois n'ont aucun lien avec la protection des individus.

De plus, une interprétation large, en vertu de laquelle toutes ces nouvelles données ou profils seront considérés comme étant des renseignements personnels, implique alors des obligations pour les entreprises qui gèrent ces données et des droits pour les individus visés qui peuvent s'avérer problématiques à certains égards. Par exemple, il peut être difficile pour une entreprise qui collecte de nouveaux renseignements de donner accès à ces renseignements aux individus le requérant (les individus ayant un droit d'accéder à leurs renseignements personnels en vertu des LPRP) si ces renseignements n'ont pas encore été traités[83]. De plus, il peut s'avérer difficile pour une entreprise de divulguer ses politiques en matière de protection de renseignements personnels et d'obtenir les consentements nécessaires sans avoir identifié, au départ, les individus auxquels ces renseignements réfèrent.

B. Interprétation du terme « identifiable »

Plusieurs auteurs proposent des orientations possibles pour les enjeux mentionnés ci-dessus. Par exemple, dans certains de leurs travaux, Boštjan Bercic et Carlisle George ont examiné à quel point la connaissance des principes de conception des bases de données relationnelles peut nous aider à comprendre ce qui constitue ou non des *renseignements personnels*[84]. Patrick Lundevall-Unger et Tommy Tranvik, quant à eux, proposent une méthode pratique pour décider du statut juridique des adresses IP, un critère qui peut également s'appliquer à d'autres types de données[85]. Brièvement, la méthode proposée se divise en deux étapes : d'abord, un critère juridique en vertu duquel les moyens illicites de relier des « noms et visages » aux adresses IP ne sont pas pris en considération lorsqu'on évalue si les adresses IP sont des renseignements personnels (seules les méthodes légitimes d'identification devraient être à la base de ces décisions) ; et (ii) deuxièmement, un test « de raisonnabilité probable », qui évalue les coûts (en termes de temps, d'argent, d'expertise, etc.) associés à l'emploi de méthodes légitimes d'identification[86]. Dans un article plus récent, les professeurs Paul M. Schwartz et Daniel J. Solove soutiennent que l'approche actuelle concernant les « PII » (ou *informations personnellement identifiables*, notion très semblable à la définition de renseignement personnel) présente des lacunes et ils proposent une nouvelle approche nommée « PII 2.0 », qui représente la malléabilité des informations personnellement identifiables[87]. En partant d'une norme plutôt que d'une règle, PII 2.0 serait basée sur un continuum de « risque d'identification » et régirait les données reliées soit à un individu « identifié » ou « identifiable », faisant une distinction entre les deux catégories.

C. Nouvelle interprétation

Finalement, je désire apporter une autre contribution en formulant des recommandations sur cette notion d'individu « identifiable ». D'abord, je propose que la notion « d'individu identifiable » soit interprétée différemment selon l'objectif de l'activité de traitement des renseignements régie par les LPRP. La réglementation de la « divulgation » et de « l'utilisation » des renseignements personnels sert à des fins différentes – la protection contre les dommages subjectifs dans le premier cas (humiliation ou embarras en cas de divulgation) et la protection contre les dommages objectifs dans le second (dommage objectif pour l'individu, tel qu'un dommage financier, physique ou encore une certaine discrimination)[88]. Par conséquent, l'interprétation de la notion « d'identifiabilité » devrait varier en fonction de l'activité de traitement des données en jeu.

Lors de l'évaluation du *risque de dommage* relatif à la divulgation de renseignements personnels, nous devons interpréter cette notion à la lumière des deux autres critères qui sont pertinents lors de l'évaluation du dommage subjectif global suivant la divulgation : la nature « intime » des renseignements (plus les renseignements sont de nature intime, plus le risque de dommage est élevé), et leur « disponibilité » (moins ils étaient disponibles préalablement à la divulgation ou plus ils deviennent accessibles après celle-ci, plus le risque de dommage est élevé)[89]. Bien que le fait de savoir si les renseignements divulgués sont « identifiables » (plus ils sont identifiables à un individu unique, plus le risque de dommage est élevé), ce critère doit tenir compte des deux autres critères. Par exemple, plus le risque de dommage basé sur les critères précédents est élevé (données révélant des informations « intimes » qui n'étaient pas « accessibles » avant la divulgation), moins le lien entre les données et un individu identifiable devrait être contraignant pour que certains renseignements se qualifient de « personnels ». Si les renseignements divulgués ont comme résultat un très faible risque de dommage pour l'individu (les renseignements ne sont pas de nature « intime », ils ne sont pas « identifiables » à un individu unique ou à un petit groupe de personnes, et ils sont déjà très largement ou publiquement « disponibles »), ils ne devraient pas être qualifiés de *renseignements personnels* et leur divulgation devrait être exclue du champ d'application des LPRP.

Pour illustrer l'approche proposée, une entreprise qui envisage de divulguer des renseignements de nature « intime » qui ne sont pas facilement « accessibles » devrait considérer que ces renseignements sont des *renseignements personnels* même s'ils portent sur un petit groupe d'individus (comme « les cinq employés qui utilisent cet ordinateur ») au lieu de porter sur un seul individu. Ces renseignements (« intimes » et non « accessibles ») pourraient aussi être qualifiés de *renseignements personnels* même si le lien entre les renseignements et l'individu n'est pas du tout précis (par exemple, une adresse IP dynamique reliée à un ou deux appareils) et même si d'importantes sommes d'argent et d'efforts importants étaient requis pour établir un lien précis entre les renseignements et l'individu (ou le petit groupe sur lequel portent les données).

Lorsque des renseignements doivent être utilisés et que l'on veuille en arriver à déterminer s'ils doivent être qualifiés de *renseignements personnels*, je suggère que l'on tente de déterminer si les renseignements utilisés risquent d'avoir un impact sur l'individu et, le cas échéant, s'il s'agit d'un impact négatif (ou d'un impact qui peut créer un dommage objectif pour l'individu, tel qu'un dommage financier, physique ou encore une certaine discrimination)[90]. S'il n'y a aucun impact sur un individu ou encore si cet impact est positif, alors je maintiens que les renseignements ne devraient pas être qualifiés de renseignements personnels et devraient donc être utilisés sans autres restrictions, puisque ces renseignements n'étaient pas destinés à être couverts par les LPRP[91]. Dans le même sens, le fait que les renseignements (ou le profil) ne soient pas identifiables dans le sens où ils n'identifient pas un individu par son nom, je soutiens que si le profil non identifiable est utilisé de manière à créer un impact négatif sur l'individu derrière le profil (refus de service ou autre), alors ce profil, même non-identifiable au sens de la loi, devrait être considéré comme étant un *renseignement personnel*. D'ailleurs, il est intéressant de constater que dans le cadre de la réforme européenne en matière de protection de renseignements personnels qui a lieu depuis 2012, dans le même ordre d'idées, le Groupe de travail de l'article 29 a émis une opinion, en octobre 2012, dans laquelle il suggère de clarifier le fait que la notion de donnée personnelle doit également couvrir (en plus des renseignements qui réfèrent à un individu identifiable), *any information allowing a natural person to be singled out and treated differently*[92]. Ceci suggère en effet que la notion d'« identifiable » n'est pas toujours pertinente pour évaluer quels renseignements doivent être régis par les LPRP, avec la réalité du Web et le fait que les entreprises peuvent maintenant prendre des décisions sur la base de profils d'utilisateurs et ce, sans nécessairement connaître l'identité des utilisateurs derrière les profils.

CONCLUSION

La définition de renseignement personnel comme étant « tout renseignement qui réfère à un individu identifiable » comporte plusieurs incertitudes puisque le moment où un élément d'information est réputé identifier un individu n'est pas toujours clair, d'autant plus que la notion « d'individu identifiable » peut être interprétée de diverses façons. En effet, avec la réalité des nouvelles technologies et d'Internet, la notion de *renseignement personnel* doit être revue, dans la sens où avec les nouveaux types de renseignements incluant les adresses IP, profils, données de localisation ou données biométriques qui ne réfèrent pas toujours clairement à un individu « identifiable », les LPRP ne trouvent pas toujours application de façon claire. Diverses pistes de solutions proposées doivent être considérées afin de s'assurer que les nouveaux renseignements personnels soient efficacement couverts par les LPRP. Développer une interprétation commune de la définition de *renseignement personnel* équivaut à définir ce qui relève ou non du champ d'application des LPRP. Cette interprétation sera nécessaire pour en arriver à fournir un cadre utile à l'intérieur duquel les LPRP demeureront efficaces compte tenu des technologies modernes.

---

* Me Éloïse Gratton, une associée du cabinet McMillan, concentre sa pratique dans le domaine du droit des TI, de la protection des renseignements personnels et de la vie privée.

1. OECD, *Report on the Cross-Border Enforcement of Privacy Laws*, (Paris : OCDE, 2006), p. 8, en ligne : <http://www.oecd.org/dataoecd/17/43/37558845.pdf>.

2. Voir Éloïse GRATTON, *Internet and Wireless Privacy: A Legal Guide to Global Business Practices* (Toronto : CCH Canada, 2003), p. 29 à 32 incl.

3. Article 29 Data Protection Working Party, *Opinion 2/2010 on online behavioural advertising*, [2010] 00909/10/EN WP 171, p. 7.

4. Stephanie ALLEN, Gina CALCATERRA, Michael GRAY, Rahul NAIR, Sumit PAHWA et Edward ROBERTSON, *RFID Tagging: Final Report*, en ligne : <http://www.rahulnair.net/files/RFID_Final_Report.pdf>.

5. Assemblée parlementaire du Conseil de l'Europe, *Report on data processing and the protection of human rights*, Presented by Committee on Science and Technology (Rapporteur : Mr. Holst, Doc. 4472), 22 janvier 1980, à la Section II du Explanatory Memorandum, Section 2 intitulée « Reasons and objectives of the report », et par. 1 intitulé « reasons » ; Voir aussi le Rapport explicatif, Conseil de l'Europe Comité des Ministres, *Résolution (73) 22 relative à la protection de la vie privée des personnes physiques vis-à-vis des banques de données électroniques dans le secteur privé* (adoptée par le Comité des Ministres le 26 septembre 1973, lors de la 224e réunion des Délégués des Ministres), par. 21.

6. Home Office, Lord Chancellor's Office, Scottish Office (Chairman The Rt. Hon, Kenneth Younger), *Report of the Committee on Privacy*, presented to Parliament by the Secretary of State for the Home Department, the Lord High Chancellor and the Secretary of State for Scotland by Command of Her Majesty, Juillet 1972, p. 180, par. 582.

7. Alan F. WESTIN, *Privacy and Freedom* (New York: Atheneum, 1967).

8. Voir le Rapport explicatif, Conseil de l'Europe Comité des Ministres, *Résolution (73) 22 relative à la protection de la vie privée des personnes physiques vis-à-vis des banques de données électroniques dans le secteur privé* (adoptée par le Comité des Ministres le 26 septembre 1973, lors de la 224e réunion des Délégués des Ministres), aux p. 3 et 22.

9. *Loi sur la protection des renseignements personnels et les documents électroniques*, LC 2000, c 5.

10. Ces lois en matière de protection de renseignements personnels sont applicables à la place de la loi fédérale LPRPDE pour les questions intra-provinciales. De plus, certaines provinces ont adopté des lois qui visent plus spécifiquement la collection, l'utilisation et la divulgation de renseignements personnels dans certains secteurs spécifiques tels que le domaine de la santé. Ces lois spécifiques visant le secteur public existent également, quoiqu'elles ne soient pas analysées dans le présent article.

11. *Loi sur la protection des renseignements personnels dans le secteur privé*, L.R.Q., c. P-39.1.

12. *Personal Information Protection Act* (British Columbia), S.B.C. 2003, c. 63.

13. *Personal Information Protection Act* (Alberta), S.A. 2003, c. P-6.5.

14. Voir Chairman Sir Norman LINDOP, *Report of the Committee on Data Protection*, Presented to Parliament by the Secretary of State for the Home Department by Command of Her Majesty, Décembre 1978, Londres, p. 154, par. 18.27. Voir aussi le Rapport explicatif, Conseil de l'Europe Comité des Ministres, *Résolution (73) 22 relative à la protection de la vie privée des personnes physiques vis-à-vis des banques de données électroniques dans le secteur privé* (adoptée par le Comité des Ministres le 26 septembre 1973, lors de la 224e réunion des Délégués des Ministres), par. 12.

15. Voir les *Lignes directrices de l'OCDE sur la protection de la vie privée et les flux transfrontières de données de caractère personnel*, art. 1 b). Le « Privacy Framework » de l'APEC, à l'article 9, définit la notion de renseignement personnel comme étant « any information about an identified or identifiable individual ».

16. Plusieurs juridictions européennes ont adopté une définition de *renseignement personnel* qui est identique ou très similaire à celle de la Directive 95/46/EC, laquelle est similaire à la définition des LPRP canadiennes.

17. Toutefois, le nom et le titre d'un employé d'une organisation et les adresse et numéro de téléphone de son lieu de travail sont exclus de la définition. *Loi sur la protection des renseignements personnels et les documents électroniques*, L.C. 2000, ch. 5, par. 2(1).

18. Les lois en matière de protection de renseignements personnels de l'Alberta et de la Colombie-Britannique définissent la notion de *renseignement personnel* comme « any information about an identifiable individual ». Voir *Personal Information Protection Act* (Alberta), S.A. 2003, c. P-6.5, section 1(1)(k) et *Personal Information Protection Act* (British Columbia), S.B.C. 2003, c. 63, part 1, section 1.

19. *Loi sur la protection des renseignements personnels dans le secteur privé*, L.R.Q., c. P-39.1, section 2 .

20. LPRPSP, section 1 .

21. Voir par. 2(1) LPRPDE. En vertu de la Partie 1, s. 1 de la PIPA de la CB, l'information de type « contact information » est exclue de l'application de la loi.

22. En vertu de la Partie 1, s. 1 de la LPRP de la C.B. «work product information» est exclu de la définition de renseignement personnel.

23. Voir le Règlement précisant les renseignements auxquels le public a accès, SOR/2001-7, de la LPRPDE. Voir aussi la LPRP de l'Alberta à la Partie 2, Division 3, s. 14(e) et Partie 2, Division 4, s. 17. Voir aussi la LPRP de CB, Partie 4, s. 12(1)(e), Partie 5, s. 15(1)(3) et Partie 6, s. 18(1)(a).

24. Boštjan BERCIC et Carlisle GEORGE, « Identifying Personal Data Using Relational Database Design Principles » (2009) 17:3 International Journal of Law and Information Technology 233, p. 235.

25. Office of the Privacy Commissioner of Canada, *A Privacy Handbook for Lawyers, PIPEDA and Your Practice* (Ottawa: Office of the Privacy Commissioner of Canada, 2011), p. 2. “It is not always straightforward to determine whether or not information is *personal information* for the purposes of PIPEDA.”

26. Neil ROBINSON, Hans GRAUX, Maarten BOTTERMAN et Lorenzo VALERI, *Review of the European Data Protection Directive* (Santa Monica, CA: RAND Corporation, 2009), p. 27.

27. Art. 29 Data Protection Working Party, *Opinion 4/2007 on the concept of personal data*, [2007] 01248/07/EN WP 136, p. 3.

28. Pour une analyse détaillée des décisions sur ce sujet, voir : Patrick Lundevall-Unger et Tommy TRANVIK, « IP Addresses: Just a Number? » (2011) 19:1 International Journal of Law and Information Technology 53. Voir aussi la section 2.3.2 du présent qui développe sur cette question.

29. Voir James WALDO, Herbert S. LIN et Lynette I. MILLETT, Committee on Privacy in the Information Age, National Research Council, *Engaging Privacy and Information Technology in a Digital Age* (Washington, US: The National Academies Press, 2007), p. 2.

30. Comité consultatif de la convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, *Rapport sur l'application des principes de protection des données aux réseaux mondiaux de télécommunications. L'autodétermination informationnelle à l'ère de l'Internet : Éléments sur la réflexion sur la Convention no 108 destinés au travail futur du Comité consultatif*, Strasbourg, 18 novembre 2004, p. 24.

31. Dre . Teresa SCASSA et *al.*, *An Analysis of Legal and Technological Privacy Implications of Radio Frequency Identification Technologies*, Prepared for the Office of the Privacy Commissioner of Canada (28 avril 2005), p. 15, 28 et 29, en ligne : <http://www.library.dal.ca/law/Guides/FacultyPubs/Scassa/RFIDs_Report2(Single).pdf>.

32. James WALDO, Herbert S. LIN. et Lynette I. MILLET, eds., Committee on Privacy in the Information Age, National Research Council, *Engaging Privacy and Information Technology in a Digital Age* (Washington, US: The National Academies Press, 2007), p. 91 à 93 ; Voir aussi E. GROCHOWSKI et R.D. HALERN, « *Technological Impact of magnetic Hard Disk Drives on Storage Systems* », IBM Systems Journal $2(2): 338-346, Juillet 2003.

33. Le nombre d'abonnés au téléphone sans fil au Canada a atteint 25,5 millions à la fin de septembre 2011 selon les chiffres comptabilisés par le groupe Canadian Wireless Telecommunications Association (CWTA). Voir Hugh Thompson, « Latest numbers show Canada has over 25.5 million wireless customers » (16 janvier 2012), en ligne : digitalhome.ca <http://www.digitalhome.ca/2012/01/latest-numbers-show-canada-has-over-25-5-million-wireless-customers/>.

34. La France avait au total 59,543 millions d'abonnés au sans-fil en date du mois de décembre 2009. Voir <http://www.itu.int/ITU-D/icteye/Reporting/ShowReportFrame.aspx?ReportName=/WTI/CellularSubscribersPublic&ReportFormat=HTML4.0&RP_intYear=2009&RP_intLanguageID=1&RP_bitLiveData=False>.

35. *Id.*

36. Randal C. PICKER, « Competition and Privacy in Web 2.0 and the Cloud » (2008) U. of Chicago Law & Economics, Olin Working Paper No 414, p. 3.

37. Mark ZUCKERBERG, « An Open Letter from Facebook Founder Mark Zuckerberg » *Facebook Blog* (1er décembre 2009), en ligne : Facebook <http://blog.facebook.com/blog.php?post=190423927130>.

38. Erick SCHONFELD, « Privacy-Per-Post: Facebook Rolls Out Its New Privacy Settings » (9 décembre 2009), en ligne : Tech Crunch

<http://techcrunch.com/2009/12/09/facebook-privacy-per-post/>.

39. Paul SAWERS, « Could Facebook reach one billion users in 2011? » (10 juillet 2011), en ligne : thenextweb <http://thenextweb.com/socialmedia/2011/01/20/could-facebook-reach-one-billion-users-in-2011/>.

40. Peter FLEISCHER, « *The data deluge » Peter Fleischer: Privacy…?* (21 avril 2010), en ligne : <http://peterfleischer.blogspot.com/2010/04/data-deluge.html?spref=tw>.

41. Voir en ligne : <http://code.flickr.com/blog/2009/02/04/100000000-geotagged-photos-plus/>.

42. Peter FLEISCHER, « *The data deluge » Peter Fleischer: Privacy…?* (21 avril 2010), en ligne : <http://peterfleischer.blogspot.com/2010/04/data-deluge.html?spref=tw>.

43. Résumé de conclusions d'enquête en vertu de la LPRPDE n° 2005-297, *Courriels non sollicités pour fins de marketing*, 1er décembre 2004.

44. Québec : *C.F.* c. *Montréal (Ville de) (SPVM)*, 2008 QCCAI 92 (CanLII), par. 55 ; *Smith* c. *Teixeira*, 2009 QCCQ 3402, EYB 2009-214817 .

45. Voir Pierre TRUDEL, France ABRAN & Gabriel DUPUIS, *Analyse du cadre réglementaire québécois et étranger à l'égard du pourriel, de l'hameçonnage et des logiciels espions*, Rapport préparé pour la Direction des politiques du ministère des services gouvernementaux du Québec (Montréal : Chaire L.R. Wilson et CRDP, 2007), p. 55.

46. Pour les détails de cette poursuite, voir Miguel HELFT, « Judge Sides With Google in Viacom Video Suit » *The NY Times* (23 juin 2010), en ligne : <http://www.nytimes.com/2010/06/24/technology/24google.html>.

47. « Google Ordered To Turn Over All Personal YouTube Viewing Records To Viacom », en ligne : Search Engine World <http ://www.searchengineworld.com/google-search/3458026.htm>.

48. Matt HARTLEY, « YouTube told to hand over users' data » *Globe and Mail* (3 juillet 2008).

49. Art. 29 Data Protection Working Party, *Opinion 1/2008 on data protection issues related to search engines*, [2008] 00737/EN WP 148, p. 6.

50. Résumé de conclusions d'enquête en vertu de la LPRPDE #25, *Un radiodiffuseur accusé de recueillir des renseignements personnels avec son site Web*, 20 novembre 2001 ; Résumé de conclusions d'enquête en vertu de la LPRPDE #315, *Mesures de sécurité d'une société Internet et traitement d'une demande d'accès à l'information et d'une plainte relative à la protection des renseignements personnels mis en doute*, 9 août 2005 ; Résumé de conclusions d'enquête en vertu de la LPRPDE #319, *Mesures anti-pourriel du FSI contestées*, 3 novembre 2005 ; Résumé de conclusions d'enquête en vertu de la LPRPDE # 2009-010, *La commissaire adjointe recommande à Bell Canada d'informer les clients au sujet de l'inspection approfondie des paquets*, Septembre 2009. Voir aussi la *Soumission du Commissariat à la protection de la vie privée du Canada à l'intention du Conseil de radiodiffusion et des télécommunications canadiennes (CRTC)*, février 2009; Répliques finales du Commissariat à la protection de la vie privée du Canada à l'intention du Conseil de la radiodiffusion et des télécommunications canadiennes (CRCT), juillet 2009; la Politique réglementaire de télécom CRTC 2009-657 (par. 96-105).

51. John OATES, « Sweden: IP Addresses are Personal... Unless You're a Pirate » (18 juin 2009), en ligne : The Register <http://www.theregister.co.uk/2009/06/18/sweden_ip_law>.

52. AGENCIA ESPANOLA DE PROTECCION DE DATOS, Statement on search engines (2007), en ligne : <http://www.samuelparra.com/agpd/canaldocumentacion/recomendaciones/common/ pdfs/declaracion_aepd_buscadores_en.pdf>. Selon l'opinion de la *Spanish Data Protection Agency*, les moteurs de recherche traitent des « renseignements personnels », en se basant entre autres sur des décisions antérieures sur les adresses IP.

53. Voir le post de Jeremy MITTMA, « German Court Rules That IP Addresses Are Not Personal Data » (17 octobre 2008), en ligne : Proskauer Privacy Law Blog <http://privacylaw.proskauer.com/2008/10/articles/european-union/german-court-rules-that-ip-addresses-are-not-personal-data>. En même temps, Peter SCHARR, le commissaire à la vie privée de l'Allemagne mentionnait que sa position en janvier 2008 était qu'une adresse IP devait être considérée comme un renseignement personnel. Voir : Aoife WHITE, « IP Addresses Are Personal Data, E.U. Regulator Says », *Washington Post* (22 janvier 2008), D01.

54. Information Commissioner's Office, *Personal Information online, Code of Practice*, U.K., Juillet 2010, p. 9-10.

55. CA Paris, 27 avril 2007, N° 06/02334 ; CA Paris, 15 mai 2007, N° 06/01954 : « L'adresse IP ne permet pas d'identifier la ou les personnes qui ont utilisé cet ordinateur puisque seule l'autorité légitime pour poursuivre l'enquête (police ou gendarmerie) peut obtenir du fournisseur l'accès d'identité de l'utilisateur. »

56. Commission nationale de l'information et des libertés (France), « L'adresse IP est une donnée à caractère personnel pour l'ensemble des CNIL européennes » (2 août 2007), en ligne : CNIL <http://www.cnil.fr/la-cnil/actu-cnil/article/article/ladresse-ip-est-une-donnee-a-caractere-personnel-pour-lensemble-des-cnil-europeennes/>.

57. CA Rennes, 22 mai 2008, N° 07/01495.

58. Cass. crim., 13 janvier 2009, N° 08-84088.

59. Trib. gr. inst. Paris, 24 juin 2009, *Jean-Yves Lafesse et autres* c. *Google et autres* : « Le tribunal considère que l'adresse IP est un renseignement personnel puisqu'elle correspond à un numéro fourni par un fournisseur d'accès à internet identifiant un ordinateur connecté au réseau ; elle permet d'identifier rapidement à partir de services en ligne gratuits le fournisseur d'accès du responsable du contenu qui délient obligatoirement les données nominatives du responsable du contenu, c'est-à-dire son adresse et ses coordonnées bancaires. »

60. CA Paris, 1er février 2010, *Cyrille S. c. Sacem*.

61. Voir Éloïse GRATTON, *Internet and Wireless Privacy: A Legal Guide to Global Business Practices* (Toronto: CCH Canada, 2003), p. 29 à 32.

62. 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*, 9 novembre 2006.

63. L'identification par radiofréquence (IRF) en milieu de travail : Recommandations de règles de pratique : Document de consultation, mars 2008, en ligne : http://www.privcom.gc.ca/information/pub/rfid_f.pdf.

64. L.R.Q., c. C-1.1.

65. Public/private partnership serving as a utilized Federal Advisory Committee to the U.S. Department of Transportation, Educational and scientific research organization created in 1991 for the purpose of fostering the development and deployment of intelligent transportation systems.

66. Federal Communication Commission des États-Unis.

67. Before the Federal Communications Commission, Washington D.C., In the Matter of the Petition of the Cellular Telecommunications and Internet Association Regarding

Proposed Location Information Privacy Principles, WT Docket Nº 01-72, INTELLIGENT TRANSPORTATION SOCIETY OF AMERICA, Reply Comments (April 24, 2001), 16 pages, p. 7.

68. L.R.Q., c. C-1.1.

69. DTE 2001T-919 (T.A.).

70. Rapport de conclusions d'enquête de la Commissaire à la protection de la vie privée, *Enquête concernant le Law School Admission Council*, 29 mai 2008.

71. *Wansink* c. *TELUS Communications Inc.* (CFA), 2007 CFA 21.

72. Précité, note 70.

73. *Ibid*.

74. Voir Nate ANDERSON, « AOL releases search data on 500,000 users (updated) » (7 août 2006), online: ARS technica <http://arstechnica.com/uncategorized/2006/08/7433/>.

75. Boštjan BERCIC et Carlisle GEORGE, « Identifying Personal Data Using Relational Database Design Principles » (2009) 17:3 International Journal of Law and Information Technology 233 at 235: “The criteria are met if it applies to a concrete individual, for example: the mere fact that an individual is wearing a red shirt can constitute an item of personal data.”

76. Barbara McISAAC et *al.*, *The Law of Privacy in Canada* 4-7 (2011); See Jeffrey A. KAUFMAN, ed., *Privacy law in the private sector: an annotation of the legislation in Canada* (Aurora: Canada Law Book, 2007), p. 15: “It is, therefore, important to note at the outset that the definition of ‘personal information' [in PIPEDA] is extremely broad” ; Voir aussi Stephanie PERRIN et al., *The personal information protection and electronic documents act: an annotated guide* (Toronto: Irwin Law, 2001) p. 54: “The definition in the Act is limitless in terms of what can be information about an identifiable individual.”

77. Office of the Privacy Commissioner of Canada, *Annual Report to Canada 2001-2002* (Ottawa: Office of the Privacy Commissioner of Canada, 2003) at Part Two, “Report on the Personal Information Protection and Electronic Documents Act, The Definition of Personal Information”. Voir aussi *Gordon* v. *Canada (Health)*, 2008 FC 258 (CanLII) et *Wyndowe* c. *Rousseau*, 2008 FCA 39 (CanLII).

78. Office of the Privacy Commissioner of Canada, *A Privacy Handbook for Lawyers, PIPEDA and Your Practice* (Ottawa: Office of the Privacy Commissioner of Canada, 2011) p. 2 “Information will be ‘about' an individual when it is not just the subject of that individual, but also relates to or concerns the individual.”

79. *Dagg* c. *Canada (Ministre des Finances*), [1997] 2 R. S. C. REJB 1997-01528, dissidents, 403, par. 68 ; *Canada (Commissaire à l'information)* v. *Canada (Bureau canadien d'enquête sur les accidents de transport et de la sécurité des transports*), 2006 CAF 157 ; *Canada (Commissaire à l'information)* c. *Canada (Commissaire de la Gendarmerie royale du Canada)*, [2003] 1 R. S. C. 66, 2003 CSC 8, REJB 2003-38212 , par. 23)

80. *Canada (Commissaire à l'information)* v. *Canada (Bureau canadien d'enquête sur les accidents de transport et de la sécurité des transports)*, 2006 CAF 157.

81. *Gordon* c. *Canada (Ministre de la Santé)*, 2008 CF 258 (CanLII). Cette affaire découle de l'application de la *Loi sur l'accès à l'information*, L.R., 1985, ch. A-1 qui incorpore la définition de « renseignement personnel » de la *Loi sur la protection des renseignements personnels*, L.R.C. 1985, ch. P-21, qui est pratiquement identique à celle de la LPRPDE.

82. Pierre TRUDEL et Karim BENYEKHLEF, « Approches et stratégies pour améliorer la protection de la vie privée dans le contexte des inforoutes », dans *Mémoire présenté à la Commission de la Culture de l'Assemblée nationale dans le cadre de son mandat sur l'étude du rapport quinquennal de la Commission d'accès à l'information* (Montréal : CRDP, Université de Montréal, 1997), p. 3.

83. Comité consultatif de la convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel, *Rapport sur l'application des principes de protection des données aux réseaux mondiaux de télécommunications, L'autodétermination informationnelle à l'ère de l'Internet*, Éléments sur la réflexion sur la Convention no 108 destinés au travail futur du Comité consultatif, Strasbourg, 18 novembre 2004, p. 34.

84. Boštjan BERCIC et Carlisle GEORGE, *Identifying Personal Data Using Relational Database Design Principles*, International Journal of Law and Information Technology Vol. 17 Nº 3, Oxford University Press 2008.

85. Patrick LUNDEVALL-UNGER et Tommy TRANVIK, « IP Addresses: Just a Number? » (2011) 19:1 International Journal of Law and Information Technology 53.

86. *Id*., p. 6.

87. Paul M. SCHWARTZ et Daniel J. SOLOVE, « The PII Problem: Privacy and a New Concept of Personally Identifiable Information » (2011) 86 *N.Y.U. Law Review* 1814.

88. Ryan CALO, “The Boundaries of Privacy Harm” (2011) 86:3 Indiana Law Journal 1131.

89. Éloïse GRATTON, *Redefining “personal information” in the Context of the Internet*, Thèse de doctorat en droit en vue de l'obtention du diplôme LL.D. (Université de Paris II et Université de Montréal), 30 octobre 2012, p. 289 et s.

90. *Id*., p. 388 et s.

91. *Id*.

92. Voir la p. 5 de l'opinion suivante : Article 29 Working Party, Opinion 08/2012 providing further input on the data protection reform discussions, 5 octobre 2012, en ligne : http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp199_en.pdf.

Date de dépôt : 16 janvier 2013