SOUMISSION AU COMITÉ PERMANENT DE LA CHAMBRE DES COMMUNES RESPONSABLE DE L'ACCÈS À L'INFORMATION, DE LA PROTECTION DES RENSEIGNEMENTS PERSONNELS ET DE L'ÉTHIQUE

Par Paige Backman et Aaron Baer, du cabinet d'avocats Aird & Berlis, s.r.l.[1]

Avril 2017

Nous accueillons donc favorablement l'occasion qui nous est offerte de faire part d'un point de vue au Comité permanent de la Chambre des communes responsable de l'accès à l'information, de la protection des renseignements personnels et de l'éthique (ETHI) eu égard à cette étude de la Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE).[2]

L'ETHI, conjointement avec le Commissariat à la protection de la vie privée du Canada, a le défi de trouver le juste équilibre entre : (i) permettre à des organisations de recueillir, d'utiliser et de divulguer des renseignements personnels pour des intérêts commerciaux légitimes; et (ii) de protéger les droits des personnes quant à leurs renseignements personnels qui sont utilisés par d'autres à des fins commerciales. Les lois sur la protection des renseignements personnels, de même que la mise en vigueur et l'application de celles-ci, ont des incidences tangibles considérables à la fois sur les entreprises et sur les personnes.

La rapidité des progrès technologiques depuis la mise en place de la LPRPDE en l'an 2000, est ahurissante et ces avancées ont constitué les façons dont les entreprises ont créé et continuent de créer de nouveaux modèles d'affaires, afin de tirer profit de ces nouvelles technologies. Par conséquent, cela représente une évolution tout aussi importante quant aux moyens de communication utilisés par les personnes grâce à la technologie; la nature et la portée du recueil, de l'agrégation, de la ré-identification, de l'utilisation, de la divulgation et de la vente des renseignements personnels; la manière dont les entreprises peuvent commercialiser les renseignements au sujet des personnes; et les répercussions sur les personnes découlant de tout ce qui précède.

Il s'avère essentiel que la LPRPDE soit modernisée et, de ce fait, qu'elle tienne compte des modèles d'affaires nouvellement créés et émergents, tout en s'adaptant afin de répondre au comportement des personnes en travaillant avec ces nouveaux modèles d'affaires. Cela ne se produira pas en apportant des changements subtils en marge de ce que prévoit la loi.

Lorsque la LPRPDE a été présentée en l'an 2000, moins de 30 % des Canadiens et Canadiennes avaient un téléphone cellulaire. [3] Les téléphones cellulaires les plus couramment

---

[1] Paige Backman, partenaire et coprésidente du Groupe responsable de la confidentialité et de la sécurité des données, au sein du cabinet d'avocats Aird & Berlis, s.r.l. et directrice de la fondation Knowledgeflow Cybersécurité (touchant la cybersécurité). Aaron Baer, associé et membre du Groupe responsable de la confidentialité et de la sécurité des données, au sein du cabinet d'avocats Aird & Berlis, s.r.l.

[2] *Loi sur la protection des renseignements personnels et les documents électroniques*, L.C. 2000, ch. 5, Annexe 1 [*LPRPDE*].

[3] Association canadienne des télécommunications sans fil, rapport quant aux statistiques des abonnés de 2000 à 2004, disponible en ligne à l'adresse suivante : <https://www.cwta.ca>.

utilisés étaient alors de marques Nokia et Motorola, [4]ayant des capacités très limitées, malgré le fait que Research in Motion (maintenant Blackberry) avait, à l'époque, récemment présenté son premier appareil, le BlackBerry 850. [5] En 2007, Apple a lancé son premier iPhone. En 2014, 55 % des Canadiens et des Canadiennes possèdent un téléphone intelligent. Aujourd'hui, plus de 76 % des Canadiens et des Canadiennes ont un téléphone intelligent. [6] Le iPhone et l'évolution d'autres téléphones intelligents et d'appareils mobiles ont fondamentalement changé la façon dont les personnes interagissent avec les entreprises et aussi la nature et la portée des renseignements recueillis au sujet des personnes.

Les téléphones intelligents, les appareils mobiles, les appareils ménagers intelligents, les voitures intelligentes, les technologies portables et le reste de l'Internet des objets a fait augmenter de façon considérable le nombre de renseignements personnels qui sont recueillis; la nature, la portée et le caractère délicat des renseignements personnels; de même que les utilisations de telles informations à des fins commerciales. Cela a également entraîné des défis significatifs et substantiels quant à la mise en pratique de la LPRPDE pour de tels nouveaux modèles d'affaires et ces nouvelles façons de faire.

La LPRPDE a été adoptée en se fondant sur les principes permettant d'accorder une certaine souplesse quant à sa mise en pratique et pour favoriser l'évolution de la technologie. Bien que la présentation des lois sur la protection de la vie privée au Canada il y a plus d'une décennie en se servant de principes généraux ait peut-être été l'approche prudente à adopter à cette époque, l'évolution de la technologie et les pratiques commerciales ont eu pour conséquence de se questionner sérieusement à savoir si la LPRPDE assure une protection efficace des droits des personnes.

Bien que nous puissions proposer de faire des amendements à certaines autres parties de la LPRPDE, aux fins de notre soumission, nous avons identifié trois éléments clés auxquels des modifications devraient être apportées à la LPRPDE : (i) Cadre du consentement; (ii) Personnes mineures; et (iii) Droit d'effacement. Même si nous ne présenterons pas de recommandations quant aux pouvoirs d'application du Commissariat à la protection de la vie privée du Canada, nous terminerons en faisant part de quelques commentaires à ce sujet.

1. Consentement - Cadre pour rationaliser et pour cibler des renseignements importants

A) Le statu quo

Un consentement valable s'avère la base pour la LPRPDE et pour toutes les lois sur la protection de la vie privée. Afin de déterminer la validité du consentement, la LPRPDE fournit les éléments suivants auxquels il faut satisfaire : Toute personne doit être **informée et consentir** au recueil, à l'utilisation et à la divulgation de renseignements personnels (sauf

[4] « Gartner Dataquest indique que les ventes mondiales de téléphones cellulaires en 2001 sont à la baisse pour la première fois de l'histoire de l'industrie », *Tech-Insider* (le 11 mars 2002), disponible en ligne à l'adresse suivante : <www.tech-insider.org>.
[5] Taylor Martin, « L'évolution du téléphone intelligent », *Pocketnow* (le 28 juillet 2014), disponible en ligne à l'adresse suivante : <www.pocketnow.com>.
[6] « Comportement associé au téléphone intelligent au Canada et les conséquences pour les marchands en 2016 », *Catalyst Canada*, disponible en ligne à l'adresse suivante : <www.catalyst.ca>.

lorsque cela serait jugé inapproprié). Les organisations doivent déployer des efforts **raisonnables pour veiller à ce qu'une personne soit avisée des fins** pour lesquelles les renseignements seront utilisés et ces fins **doivent être énoncées d'une manière qu'une personne puisse raisonnablement comprendre, à savoir comment les informations seront utilisées ou divulguées**. Une organisation **ne devra pas, à titre de condition de la fourniture d'un produit ou d'un service,** exiger qu'une personne donne son consentement pour le recueil, l'utilisation ou la divulgation de renseignements **autres que pour ce qui est nécessaire pour réaliser les fins légitimes et explicitement stipulées.** [7] De plus, le consentement est considéré comme étant valable seulement s'**il est raisonnable de s'attendre à ce qu'une personne, envers qui les activités de l'organisation sont dirigées, puisse comprendre la nature, l'objet et les conséquences du recueil, de l'utilisation ou de la divulgation des renseignements personnels visés par le consentement**.

On pourrait avancer que l'évolution des modèles d'affaires et des façons de faire, en plus de la manière dont les personnes interagissent avec ces modèles d'entreprises, ont entraîné l'échec de satisfaire un grand nombre, sinon tous ces éléments reliés à la notion de consentement. Les nouvelles pratiques commerciales sont fondées sur un grand nombre de données recueillies en temps réel, par le biais de notre engagement en ligne, de nos téléphones, de nos montres, de nos voitures et de nos maisons et nous avons évolué d'une manière qui fait qu'une personne moyenne ignore complètement ce qui en est et n'est pas en mesure de saisir ou de comprendre les implications. Le mode d'interaction entre les personnes (de tout âge et de tout segment démographique) et les pratiques commerciales représentent des défis supplémentaires pour veiller à ce que les personnes puissent raisonnablement comprendre comment leurs informations seront utilisées ou divulguées. Cela constitue également des défis pour établir que les personnes, envers qui les activités de l'organisation sont dirigées, sont en mesure de comprendre la nature, l'objet et les conséquences du recueil, de l'utilisation ou de la divulgation des renseignements personnels visés par le consentement. On peut également ajouter qu'en raison du manque de clarté quant à la définition des « fins commerciales légitimes », il est impossible de savoir exactement quand une organisation doit offrir une option positive quant au droit de renonciation, en ce qui a trait aux pratiques qui vont au-delà de ce qui est nécessaire pour réaliser une fin légitime.

La plupart des organisations se fient aux politiques de confidentialité afin d'obtenir le consentement des personnes. Généralement, les politiques de confidentialité sont affichées dans les sites Web ou encore liées à des formulaires de demande en ligne et ont une longueur qui varie entre quelques pages et plus de 30 pages complètes. Sur un appareil mobile, cela représente tout un défi en soi.

Sans avoir de discussion à savoir si le contenu de telles politiques est approprié ou non, de nombreuses études ont démontré que les politiques de confidentialité, telles qu'elles sont actuellement rédigées et utilisées, s'avèrent un moyen inefficace de communiquer des informations, d'offrir un choix ou d'obtenir un consentement valable auprès des personnes. Par exemple, un article de l'Université York, paru en 2016, a estimé à quel point les personnes ignorent réellement les politiques de confidentialité lorsqu'elles adhèrent à un site fictif de réseautage social.[8] Soixante-quatorze pour cent des personnes ont passé outre la politique de

[7] *LPRPDE, supra* note 1, s 4.3.

[8] Jonathan A. Obar & Anne Oeldorf-Hirsch, « Le plus grand mensonge véhiculé dans Internet : Ignorer les politiques de confidentialité et les politiques régissant les conditions d'utilisation des services de réseautage social » (document présenté

confidentialité, préférant plutôt choisir « l'option rapide » pour s'inscrire au site. L'étude a également démontré que, parmi les 26 % des personnes qui ont tenté de consulter la politique de confidentialité, la durée moyenne consacrée à la lecture de celle-ci était seulement 73 secondes, alors que la vitesse de lecture d'un adulte moyen aurait nécessité au moins 30 minutes pour lire ces informations.

Les résultats de cette étude correspondent à nos observations. La plupart des politiques de confidentialité sont des documents volumineux, chargés de jargon juridique et de dispositions avec lesquels la majorité des lecteurs ne sont pas familiers. Par souci de divulgation, les conditions sont énoncées d'une manière exhaustive dans les politiques de confidentialité. La plupart de celles-ci font référence à des pratiques auxquelles une organisation devrait pouvoir se fier quant au consentement implicite. L'ajout de ces conditions essentielles augmente le nombre de pages des documents traitant des politiques de confidentialité, nécessite du temps et cela détourne l'intérêt et l'attention des pratiques liées au traitement des informations qui sont, soit complémentaires aux pratiques touchant le traitement des informations de base ou encore qui décrivent les utilisations ou les communications secondaires des renseignements personnels pour lesquelles un consentement exprès devrait être obtenu.

De plus, nous nous permettons d'ajouter qu'en raison de la multitude de personnes à qui s'adressent les politiques de traitement des informations par une organisation en particulier, une compréhension de ce à quoi s'attendrait une personne raisonnable dans les circonstances (soit une exigence de consentement) s'avère une question difficile à répondre. Les modèles d'affaires impliqueront souvent la participation de personnes mineures et de jeunes adultes, de même que de personnes âgées. Les modèles d'affaires suscitent la participation de personnes qui possèdent une assez bonne compréhension des pratiques modernes liées au traitement des informations, de même que de personnes qui ont une compréhension très limitée (ou nulle) des pratiques modernes liées au traitement des informations. Par conséquent, il est permis de se demander s'il est raisonnable de s'attendre à ce que toutes ces personnes, envers qui les activités de l'organisation sont dirigées, puissent comprendre la nature, l'objet et les conséquences du recueil, de l'utilisation ou de la divulgation des renseignements personnels visés par le consentement. Toutes les personnes à qui s'adressent les pratiques d'une organisation peuvent être des personnes raisonnables et pourtant, chaque personne peut en venir à une conclusion différente quant à ce qui consiste en une fin légitime pour le recueil, l'utilisation et / ou la divulgation de leurs renseignements personnels.

Il en résulte donc qu'il s'avère extrêmement discutable de savoir si les personnes fournissent un consentement éclairé à une organisation quant à ses pratiques légitimes liées au traitement des informations. Cela constitue un enjeu à la fois pour les organisations et pour les personnes. Les organisations qui se fient aux politiques de confidentialité pourraient avoir un faux sentiment de sécurité en pensant qu'elles ont obtenu le consentement requis. On pourrait également soutenir que les personnes ne reçoivent pas les informations nécessaires, d'une manière qui leur permettrait de comprendre raisonnablement comment leurs renseignements personnels seront utilisés ou divulgués ou que certaines pratiques liées au traitement des informations vont au-delà des exigences requises pour répondre à une fin légitime.

---

lors de la 44ème Conférence de recherche au sujet des communications, des informations et de la politique pour l'utilisation d'Internet 2016, le 30 septembre 2016), disponible en ligne à l'adresse suivante : <https://ssrn.com/abstract=2757465>.

Il serait irréaliste d'affirmer que nous puissions trouver une approche qui saura satisfaire toutes les personnes, de tous les segments démographiques. Cependant, nous nous permettons de suggérer que l'utilisation d'un cadre adéquat pour le consentement et la clarté des informations entourant certains concepts (comme les bases sur lesquelles reposent le consentement et ce qui est considéré comme étant une fin commerciale légitime), accorderont aux entreprises la possibilité d'avoir une plus grande certitude d'avoir établi le consentement requis et de fournir aux personnes des informations utiles sur lesquelles elles pourront se baser pour donner leur consentement.

B) Nos recommandations

Bien que de nombreuses recommandations pourraient s'avérer appropriées pour résoudre les problèmes mentionnés ci-haut, nos recommandations mettront l'accent sur l'importance de fournir une plus grande certitude quant aux pratiques commerciales pour lesquelles un consentement pourrait être implicite, des politiques de confidentialité énoncées dans des textes plus courts, une attention aux personnes quant aux pratiques liées au traitement des informations qui s'éloignent des pratiques de base liées au traitement des informations et nous nous efforcerons de fournir des options utiles quant aux pratiques liées au traitement des informations relatives à des fins secondaires.

Plus précisément, nous recommandons l'adoption du cadre suivant quant au consentement :

1. Définir les pratiques liées au traitement des informations pour lesquelles un consentement pourrait être implicite et énoncer le même principe dans un code type. Vous trouverez ci-joint quelques suggestions quant aux conditions à ajouter dans ce code type, à l'Annexe 1.

L'adoption d'un code type qui fait état des pratiques de base liées au traitement des informations permettrait de clarifier les pratiques liées au traitement des informations sur lesquelles les organisations peuvent se fier quant au consentement implicite. Cela permettra aux organisations d'abréger les politiques de confidentialité de façon significative, en se référant simplement au code type, plutôt que d'avoir à répéter ces mêmes politiques. Les organisations (généralement les organisations de moins grande envergure) qui se servent des informations uniquement d'une façon qui est saisie par le code type, pourraient simplement se référer au code type et celles-ci n'auraient pas besoin d'augmenter les coûts et les ressources afin d'en créer un pour leur entreprise.

Dans la mesure où les pratiques d'une organisation liées au traitement des informations diffèrent d'un tel code type, les politiques de confidentialité de l'organisation mettraient l'accent sur ces pratiques complémentaires. Avoir des politiques de confidentialité qui mettent l'accent sur des pratiques complémentaires permettrait de fournir une plus grande assurance que les personnes sont au courant de l'utilisation de ces pratiques et cela offrirait un meilleur soutien quant à la capacité de l'organisation à se fier au consentement d'une personne de la même manière.

Par exemple, si le code type englobait la possibilité de transférer des renseignements personnels vers un partenaire de la chaîne d'approvisionnement *au Canada* et qu'une organisation avait recours à des partenaires de la chaîne d'approvisionnement aux *États-Unis*, la politique de confidentialité pourrait ainsi attirer l'attention sur le fait que l'exploitation de l'organisation nécessite également le transfert des renseignements personnels vers des

partenaires de la chaîne d'approvisionnement aux États-Unis. Une telle disposition, qui devient plus importante compte tenu du récent climat politique, ne serait plus difficile à trouver dans un long document au sujet de la politique de confidentialité; celle-ci serait plutôt très évidente en lisant le document et cela augmenterait la probabilité que la personne qui lit le document donne son consentement en étant vraiment bien informée.

2. Exiger le consentement exprès quant à ces pratiques liées au traitement des informations qui diffèrent de celles indiquées dans le code type ou qui s'ajoutent à celles-ci.

Les organisations qui intègrent des pratiques liées au traitement des informations qui diffèrent de celles indiquées dans le code type ou qui s'ajoutent à celles-ci (nous faisons référence à celles-ci comme étant des pratiques liées au traitement des informations complémentaires), seraient tenues d'établir ces pratiques liées au traitement des informations d'une manière clairement exprimée dans une politique de confidentialité et elles devraient obtenir un consentement exprès d'une façon vérifiable pour de telles pratiques complémentaires.

3. Distinguer les pratiques liées au traitement des informations relatives à des fins secondaires de celles à des fins non secondaires, énoncées dans les politiques de confidentialité et fournir une option clairement indiquée et facilement accessible quant au droit de renonciation pour chacune des fins secondaires.

Actuellement, les fins secondaires se trouvent souvent parmi toutes les autres pratiques liées au traitement des informations dans les documents au sujet des politiques de confidentialité et elles semblent indiquer une « acceptation » de tout ou rien. Nous recommandons donc que les conditions énoncées dans une politique de confidentialité relative à des pratiques complémentaires soient établies dans des sections distinctes :

> (i) les pratiques liées au traitement des informations qui, bien que celles-ci peuvent possiblement différer de celles indiquées dans le code type, soient raisonnablement nécessaires quant aux produits et aux services pour lesquels une personne fait une demande auprès d'un fournisseur; et
>
> (ii) les pratiques liées au traitement des informations relatives à des fins secondaires.

Un exemple d'une fin secondaire serait le transfert des informations à des tiers à des fins de marketing. En ce qui concerne ces pratiques liées au traitement des informations relatives à des fins secondaires, une option quant au droit de renonciation pour de telles fins secondaires devrait être clairement énoncée et facilement accessible aux personnes qui lisent le document. Si de telles fins secondaires ont été communiquées dans un environnement en ligne, l'option quant au droit de renonciation pourrait être fournie directement à côté de chacune des fins secondaires énoncées et pour lesquelles une action est requise, d'une manière facilement accessible (comme par exemple, une case pour indiquer une option quant au droit de renonciation, située directement à côté de chacune des fins secondaires).

4. Dans chaque cas où un consentement exprès est requis et a été obtenu, une copie de la politique de confidentialité devrait être fournie à la personne qui a donné son consentement exprès, dans un format qui puisse être conservé par celle-ci (par exemple, par message courriel ou par la poste, à une adresse précisée). L'exigence de « fournir » une copie des conditions qu'une personne est tenue de respecter s'inscrit dans le même ordre d'idée que de nombreuses lois sur la protection du consommateur au Canada.

2. Personnes mineures

A) Le statu quo

Actuellement, la LPRPDE exige qu'un consentement soit considéré comme étant valable uniquement s'il est raisonnable de s'attendre à ce qu'une personne, envers qui les activités de l'organisation sont dirigées, puisse comprendre la nature, l'objet et les conséquences du recueil, de l'utilisation ou de la divulgation des renseignements personnels visés par le consentement. Cela constitue le lien le plus étroit quant à une protection légale que la LPRPDE octroie aux personnes mineures.

Une étude menée en 2014 auprès de jeunes Canadiens et Canadiennes a démontré que 24 % des élèves de 4ème année et que plus de 50 % des élèves de 7ème année avaient leur propre téléphone cellulaire.[9] Les élèves de 4ème année ont généralement entre 9 et 10 ans. Les élèves de 7ème année ont généralement entre 12 et 13 ans. Bien entendu, les jeunes Canadiens et Canadiennes ne se limitent pas seulement à des téléphones cellulaires pour avoir accès à Internet. L'accès à Internet est largement accessible aux jeunes Canadiens et Canadiennes par l'entremise d'ordinateurs portables, de tablettes, de consoles de jeux et de technologies portables et, dans l'ensemble, cet accès à Internet ne relève pas de la supervision de leurs parents.

La disponibilité croissante de l'accès à Internet qui s'offre aux jeunes Canadiens et Canadiennes représente des préoccupations au sujet de la protection des renseignements personnels. Un rapport publié récemment par le Commissaire à l'enfance pour l'Angleterre (Commissaire) a souligné les inquiétudes croissantes quant aux renseignements personnels que les jeunes fournissent à des organisations. [10] Le commissaire a évalué les conditions générales d'Instagram, qui est un site utilisé par 56 % des jeunes âgés de 12 à 15 ans et par 43 % des jeunes âgés de 8 à 11 ans en Angleterre. Les conditions générales d'Instagram comportaient 17 pages et comprenaient plus de 5000 mots, rédigées dans un langage complexe et employant une structure de phrases dépassant de loin la capacité de compréhension d'un jeune moyen. Il n'a pas été surprenant de constater que, lorsqu'on leur demande de lire les conditions générales, les jeunes se sentent frustrés et confus.[11]

Bien que les jeunes Canadiens et Canadiennes soient doués en ce qui a trait à la technologie, ils leur manquent souvent les connaissances et la compréhension requises pour donner un consentement éclairé pour le recueil, l'utilisation et la divulgation de leurs renseignements personnels. Les jeunes Canadiens et Canadiennes sont moins susceptibles de reconnaître les implications à court et à long terme des choix qu'ils font en ligne, y compris le partage de leurs renseignements personnels. L'impact des choix faits par des personnes mineures dans l'environnement en ligne peut causer des dommages à court et à long terme aux personnes mineures.

B) Nos recommandations

---

[9] Valerie Steeves, « Les jeunes Canadiens et Canadiennes dans un monde branché, 3ème cycle », *la vie en ligne : MediaSmarts* (2014), disponible en ligne à l'adresse suivante : <http://mediasmarts.ca/ycww>.

[10] Royaume-Uni, Groupe de travail du Commissaire à l'enfance se penchant sur la question de grandir à l'ère numérique, *Grandir à l'ère numérique*, (Londres : Commissaire à l'enfance, janvier 2017).

[11] *Ibid* à 8.

Nous recommandons donc que les organisations soient tenues d'obtenir un **consentement vérifiable** auprès d'un parent ou d'un tuteur des personnes âgées de moins de 16 ans, afin de recueillir, d'utiliser ou de divulguer leurs renseignements personnels dans le cadre de leurs activités commerciales. Toute méthode employée pour obtenir un consentement vérifiable devrait être raisonnablement délibérée, compte tenu de la technologie disponible, afin de veiller à ce que la personne qui donne le consentement soit bien le parent ou le tuteur légal de l'enfant.

Même si l'âge de 16 ans ne constitue pas un chiffre magique, cet âge est conforme aux lois du pays, de même qu'aux lois internationales, comme, entre autres, le **Règlement général sur la protection des données** (RGPD) de l'Union européenne, qui entrera en vigueur en mai 2018 et pour lequel le Canada doit proposer une protection comparable.

La loi sur la protection des renseignements personnels sur la santé, de l'Ontario, 2004 exige, dans la plupart des cas, le consentement d'un parent ou d'un tuteur pour le recueil, l'utilisation ou la divulgation des renseignements personnels quant à la santé d'un enfant âgé de moins de 16 ans.[12] Le RGPD exige également le consentement d'un parent ou d'un tuteur quant aux pratiques liées au traitement des informations auxquelles s'applique le RGPD lorsqu'un enfant est âgé de moins de 16 ans.[13]

La Children's Online Privacy Protection Rule *de la Federal Trade Commission des États-Unis* (COPPA) exige que les organisations déploient *des efforts raisonnables pour obtenir un consentement parental vérifiable*, en tenant compte de la technologie disponible. Toute méthode employée pour obtenir un consentement parental vérifiable doit être raisonnablement délibérée, compte tenu de la technologie disponible, afin de veiller à ce que la personne qui donne le consentement soit bien le parent ou le tuteur légal de l'enfant. D'une manière similaire à COPPA, le RGPD exige également que les organisations déploient des efforts raisonnables pour vérifier que le consentement a bien été fourni par le parent ou le tuteur légal de l'enfant, en tenant compte de la technologie disponible. [14]

3. Droit d'effacement

(a) Statu quo :

Selon l'American Academy of Child and Adolescent Psychiatry, plus de 60 % des jeunes âgés de 13 à 17 ans ont au moins un profil dans un site de réseau social et nombreux d'entre eux consacrent plus de deux heures par jour à parcourir des sites de réseautage social. [15] La CBC a indiqué que, selon un ratissage pour la protection de la vie privée impliquant des organisations responsables de la mise en vigueur de mesures dans 21 pays lors duquel on a étudié 1494 applications et sites Web, comme des sites de jeux, des sites éducatifs et de

[12] L.C. 2004, ch. 3, Annexe A.
[13] CE, *Règlement de la commission (CE) 679/2016 en date du 4 mai 2016 au sujet de la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données et pour abroger la directive 95/46/CE (Règlement général sur la protection des données)*, [2016] JO, L 119/1 à 8 [*Règlement CE*].
[14] *Règlement CE, supra* note 16 à 8.
[15] American Academy of Child & Adolescent Psychiatry, « Le réseautage social et les enfants », N° 100, février 2017.

médias sociaux, hébergés par des organisations bienveillantes à l'égard des enfants, telles que des musées et des zoos[16] :

- 67 % des sites Web et des applications ayant fait partie de l'étude recueillent des renseignements personnels, comme des noms, des photos, des adresses et des numéros de téléphone ou par le biais d'une fonction de clavardage. Parmi les principaux contrevenants, on retrouve les sites Web consacrés à la musique.
- 51 % d'entre eux indiquent qu'ils pourraient divulguer des renseignements personnels à un tiers à des fins publicitaires ou autres.
- 71 % d'entre eux n'offraient aucun moyen simple de supprimer les renseignements indiqués dans un compte.
- 58 % d'entre eux dirigeaient parfois des enfants vers d'autres sites, souvent par l'entremise de concours ou de publicités, y compris vers certains sites qui ne conviennent pas du tout à des enfants, comme des sites Web assurant la promotion de sites de rencontre et de boissons alcoolisées.

Le Commissaire à la protection de la vie privée, M. Daniel Therrien, a conclu qu'un « trop grand nombre de concepteurs de sites recueillent des renseignements personnels qui sont d'une nature particulièrement délicate, comme des photos, des vidéos et des informations quant à la localisation d'enfants et, souvent, ils permettent la diffusion de ces données publiquement... »

Il existe des avantages significatifs pour les enfants et les jeunes quant à l'engagement dans les médias sociaux, notamment le développement de nouveaux liens sociaux avec des pairs partageant des intérêts similaires et le développement et l'expression de leur identité individuelle. Les conséquences liées à une erreur de jugement d'une personne mineure ou encore le jugement d'une autre personne (y compris les entreprises et d'autres personnes), qui impliquent des renseignements au sujet d'une personne mineure, peuvent avoir des effets importants à court et à long terme tant sur la personne mineure que sur la société. Plus souvent, nous remarquons qu'une présence en ligne peut mener à ou être le point central de l'intimidation en ligne; ce qui peut avoir une incidence significative tant au plan de la santé physique que de la santé mentale de la personne mineure et entraîner des conséquences à long terme pour la personne mineure et aussi pour la société.

Outre les enjeux très réels et significatifs liés aux dommages infligés, tant au plan physique que mental, à une personne mineure, que cela soit dû à une erreur de jugement ou simplement être le résultat d'une pratique commerciale, le partage des renseignements relatifs à une personne mineure peut avoir un impact sur la capacité de la personne mineure à décrocher ou à conserver un emploi et cela peut mener à une exploitation de la personne mineure par des adultes prédateurs.

En ce qui a trait à notre recommandation en réponse à cet enjeu, nous intégrons, par référence, les données établies à la section qui précède immédiatement, intitulée « Personnes mineures ». Un important pourcentage d'enfants âgés entre 9 et 12 ans ont leur propre téléphone intelligent et communiquent avec d'autres personnes dans un environnement en ligne, en se servant de diverses plateformes commerciales.

---

[16] CBC News souligne que : « *La plupart des applications et des sites Web pour les enfants recueillent et partagent des renseignements personnels. Le ratissage pour la protection de la vie privée a pu déterminer que de nombreuses photos, vidéos et informations quant à la localisation sont diffusées publiquement* ».*,* le 3 septembre 2015, http://www.cbc.ca/news/technology/most-kids-apps-websites-collect-and-share-personal-information-1.3214213

Notre recommandation soulignant l'exigence d'obtenir le consentement du parent ou du tuteur légal pour des jeunes et des enfants âgés de moins de 16 ans, fait état de la participation du parent ou du tuteur légal à un moment donné. Toutefois, nous devons également aborder le sujet du partage continu des informations, de même que l'utilisation des renseignements concernant des personnes mineures dans le cadre d'activités commerciales qui ont lieu tout au long de l'engagement d'un enfant ou d'un jeune dans l'environnement en ligne.

Bien que nous souhaitions que les parents et les tuteurs légaux d'enfants de cette catégorie d'âge supervisent en tout temps l'utilisation d'Internet de leurs enfants, de même que leur partage de renseignements en ligne, lorsque des enfants âgés de 9 à 12 ans ont leur propre téléphone intelligent et appareil mobile, nous devons accepter le fait que la supervision d'un adulte pour ces enfants s'avère limitée. La supervision des jeunes âgés de 13 ans et plus est encore moins plausible. Nous ne pouvons ignorer cette réalité ni le fait que certaines entreprises ciblent les enfants et les jeunes, mais pourtant nous devons essayer de protéger nos enfants et nos jeunes pour les même raisons et d'une manière qui soit conforme à la protection que nous offrons à nos enfants et à nos jeunes dans d'autres secteurs du droit.

(b) Recommandations :

Nous recommandons fortement que le droit d'effacement soit mis en vigueur, relativement aux personnes mineures, lorsque leurs renseignements personnels ont été recueillis, utilisés ou divulgués dans la cadre d'activités commerciales. [17]

Dans le cadre de l'éducation générale de nos enfants, nous croyons qu'il s'avère important d'encourager nos enfants et nos jeunes à apprendre à se servir des ressources disponibles en ligne et aussi d'apprendre à participer à un environnement en ligne. Toutefois, nous devons également fournir un mécanisme visant à protéger cette tranche d'âge très vulnérable de notre société. Le droit d'effacement (ou encore le droit d'être oublié) de la façon dont celui-ci s'applique aux personnes mineures est non seulement un avantage à court terme pour la personne mineure, mais également pour l'impact à long terme sur la personne mineure et sur l'ensemble de la société.

Nous soulignons que l'Union européenne, par l'entremise du RGPD, soutient également la nécessité accrue du droit d'effacement lorsque cela touche les renseignements personnels d'une personne mineure. « *Ce droit s'avère pertinent, surtout dans les cas où la personne qui a fourni les données a transmis son consentement en tant qu'enfant et qu'elle ne comprend pas bien les risques qu'impliquent le traitement des informations et qu'elle désire par la suite, retirer de telles données personnelles, tout particulièrement dans Internet. La personne qui a fourni les données devrait avoir la possibilité de faire valoir ce droit, en dépit du fait qu'il ou elle ne soit plus un enfant* ».

Plus précisément, nous faisons les recommandations suivantes et d'une manière conforme au RGPD :

[17] Dans nos soumissions, nous employons l'expression personne mineure, afin de référer aux personnes n'ayant pas encore atteint l'âge de la majorité légale, d'une manière générale; cependant, nous employons le mot enfants pour faire référence aux personnes qui ont moins de 13 ans et nous utilisons le terme jeunes pour identifier les personnes ayant entre 13 ans et l'âge de la majorité légale.

Les personnes dont les renseignements personnels, qui sont sujets à la LPRPDE (recueillis, utilisés ou divulgués dans le cadre d'activités commerciales) et qui sont ou qui ont été recueillis, utilisés et / ou divulgués lorsque la personne était mineure, devraient avoir le droit (en plus de ses parents ou tuteurs légaux), de faire supprimer de tels renseignements personnels, sans retard excessif, sauf dans les circonstances suivantes : (i) l'utilisation ou la divulgation de tels renseignements est requis afin de répondre à des obligations légales ou statutaires, y compris des exigences gouvernementales ou une ordonnance d'un tribunal; ou (ii) pour la constatation, l'exercice ou la défense d'un droit en justice.

Dans la mesure où de tels renseignements personnels ont été divulgués ou transférés à un tiers ou que ceux-ci ont été rendus publics autrement, l'organisation qui a initialement recueilli les informations, de même que toutes les parties qui se servent ou qui communiquent de tels renseignements, devraient prendre des mesures raisonnables, notamment l'utilisation de technologie raisonnablement disponible, afin de supprimer toutes les copies et tous les liens vers de tels renseignements personnels.

4. Mise en vigueur

Nous avons procédé à la révision de nombreuses soumissions quant à l'élargissement des pouvoirs d'application du Commissariat à la protection de la vie privée du Canada (Commissaire à la protection de la vie privée). Nous reconnaissons et nous apprécions les objectifs visés par ceux qui désirent élargir les pouvoirs d'application du Commissaire à la protection de la vie privée et aussi le fait que ces pouvoirs accrus seraient conformes aux pouvoirs d'application d'autres juridictions.

Bien que nous ne proposerons pas de recommandations entourant des pouvoirs d'application précis, pour les fins de la discussion à ce sujet, nous suggérons fortement qu'il s'avère important de se rappeler que les principes généraux sur lesquels est fondée la LPRPDE, malgré le fait que ceux-ci permettent d'avoir une certaine souplesse, ils créent une grande incertitude quant aux obligations de l'organisation concernant les questions de conformité. Sans une plus grande certitude entourant les exigences de conformité sous la directive de la LPRPDE, il sera injuste et hautement préjudiciable d'imposer des pénalités et des amendes supplémentaires à de telles organisations. Sans cette précision supplémentaire, les organisations pourraient être exposées d'une manière injuste à recevoir des amendes, des pénalités et des ordonnances du tribunal, en dépit du fait qu'elles agissent de bonne foi, afin de se conformer aux exigences de la LPRPDE.

Bien que nous ne contestions pas une augmentation des pouvoirs d'application, nous recommandons fortement, qu'avant d'accroître les pouvoirs d'application, une plus grande certitude et plus de détails concernant les obligations de conformité soient fournis quant à la LPRPDE. Comme il est mentionné plus haut, il s'avère essentiel d'avoir une plus grande précision quant à l'obtention du consentement requis (que celui-ci soit implicite ou exprès, provenant de personnes mineures ou adultes, etc.). Nous croyons que le cadre pour le consentement recommandé ci-haut peut aider dans cette mesure, bien qu'une autre directive réglementaire puisse également s'avérer nécessaire. Par exemple, selon les détails précis établis dans les règles finales entourant les exigences relatives à des atteintes à la sécurité des données, il pourrait être nécessaire d'avoir plus de précisions à ce sujet.

Si l'objectif est d'encourager une conformité aux exigences de la LPRPDE et non simplement de prendre des mesures punitives, une clarté vraisemblablement plus grande quant à ces points essentiels sera donc dans le meilleur intérêt de tous.

Conclusion

La tâche à laquelle l'ETHI est confronté est de taille, mais elle est extrêmement importante. Nous vous félicitons pour le temps et l'effort que vous avez consacrés à moderniser la LPRPDE et pour veiller à ce que les amendements apportés à celle-ci soient pertinents et bénéfiques pour atteindre ses objectifs établis. L'effort déployé pour arriver à moderniser la LPRPDE et pour veiller à ce que les protections qu'elle confère soient pertinentes et bénéfiques ne sera pas sans difficultés. Cependant, les décisions de ne pas moderniser la LPRPDE ou d'amender la LPRPDE d'une manière qui ne donnerait pas de protections réelles, tant pour les entreprises que pour les personnes, auront également un coût.

Nous espérons que notre soumission aura une certaine utilité. Bien que nous ayons limité les changements que nous proposons à trois éléments clés, il nous fera plaisir de discuter avec vous de ceux-ci ou de toute autre modification proposée quant à la LPRPDE dans l'avenir.

Annexe 1
Code type

Vous trouverez ci-après une liste de termes proposés, qui pourraient faire partie du code type :

Objectifs visés par le recueil et l'utilisation de renseignements personnels :

Une organisation (« organisation ») peut se fier au consentement implicite d'une personne lorsque l'organisation recueille et se sert des renseignements personnels pour les fins énoncées ci-après :

a) pour établir et pour maintenir des liens commerciaux responsables avec la personne et pour fournir des services d'une manière continue;
b) pour communiquer avec la personne pour l'informer de changements, d'améliorations ou pour lui faire part d'avis similaires, en rapport avec les produits et les services de l'organisation;
c) à des fins établies dans les ententes conclues entre la personne et l'organisation;
d) pour comprendre les besoins des personnes;
e) pour mettre au point, pour améliorer, pour mettre en marché ou pour fournir des produits et des services; et
f) pour répondre à des exigences légales ou réglementaires, y compris pour protéger ou pour défendre un intérêt juridique.

Objectifs visés par la divulgation de renseignements personnels et le transfert d'informations :

Une organisation (« organisation ») peut se fier au consentement implicite d'une personne lorsque l'organisation divulgue des renseignements personnels pour les fins énoncées ci-après :

a) pour fournir les produits et / ou les services pour lesquels une personne a soumis une demande;
b) pour établir et pour maintenir des liens commerciaux responsables avec la personne;
c) pour respecter les conditions des ententes conclues entre la personne et l'organisation; et
d) pour répondre à des exigences légales ou réglementaires, y compris pour protéger ou pour défendre un intérêt juridique.

Il arrive parfois que l'organisation transfère des renseignements personnels à d'autres entités, notamment à des entités affiliées ou à des entreprises indépendantes (« fournisseurs de services »), qui accomplissent certaines fonctions au nom de l'organisation, comme l'exécution des commandes, le traitement des données, les services de comptabilité et d'administration, le service à la clientèle et les services de technologie de l'information, y compris, sans s'y limiter, les services d'hébergement et de stockage des données. Dans ces types de cas, l'organisation exige que ces fournisseurs de services ne se servent pas et ne divulguent pas les renseignements personnels des personnes à des fins autres que celles demandées par l'organisation.

De temps à autre, il se peut que l'organisation ait à fournir des renseignements personnels en réponse à une ordonnance d'un tribunal, à une assignation à comparaître, dans le cadre d'une enquête gouvernementale ou conformément à toute autre exigence légale. L'organisation se réserve également le droit de signaler aux autorités policières, toute activité que l'organisation considère, en toute bonne foi, être illégale. Une organisation peut communiquer certains renseignements personnels lorsque celle-ci juge que cela s'avère raisonnablement nécessaire, afin de protéger les droits, les biens et la sécurité d'autrui et aussi de l'organisation.

Remarque aux enfants

Une organisation n'accepte pas volontiers des renseignements personnels soumis par des enfants mineurs ou les concernant, sans le consentement du parent ou du tuteur légal de l'enfant. Nous encourageons les parents et les tuteurs à passer du temps avec les enfants et à assurer une surveillance de leurs activités en ligne. Veuillez protéger la vie privée de votre enfant en lui enseignant de ne jamais fournir de renseignements personnels en ligne sans vous en aviser et obtenir votre consentement.