Commissariat
à la protection de
la vie privée du Canada

Consentement et protection de la vie privée

Document de discussion sur les améliorations possibles au consentement sous le régime de la *Loi sur la protection des renseignements personnels et les documents électroniques*

Préparé par le Groupe des politiques et de la recherche du Commissariat à la protection de la vie privée du Canada

Table des matières

30, rue Victoria, 1er étage, Gatineau (Québec) K1A 1H3 • Sans frais : 1-800-282-1376 • Télécopieur : (819) 994-5424 • ATS : (819) 994-6591
www.priv.gc.ca • Suivez-nous sur Twitter : @priveeprivacy

Introduction

Le consentement est considéré comme la pierre angulaire de la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE)[1]. Afin de pouvoir recueillir, utiliser et communiquer les renseignements personnels d'un individu en toute légitimité dans le cadre d'activités commerciales, les organisations doivent obtenir son consentement. En l'absence de consentement, elles ne peuvent traiter les renseignements personnels que dans certains cas bien précis. La LPRPDE repose sur un cadre neutre sur le plan technologique composé de dix principes – dont le consentement – assez souples pour s'appliquer dans divers environnements. Toutefois, la technologie et les modèles d'affaires ont évolué considérablement depuis la rédaction de la LPRPDE et l'on craint que cette évolution n'ait une incidence sur les mécanismes de protection des renseignements personnels et ne remette en question la faisabilité de l'obtention d'un consentement valable.

De fait, le Commissariat à la protection de la vie du Canada a tenu en 2015 des discussions en vue d'établir ses priorités pour la protection de la vie privée. Certains intervenants ont alors mis en doute la viabilité à long terme du modèle de consentement dans un écosystème caractérisé par l'ampleur et la complexité de la circulation de l'information et l'omniprésence de l'informatique. La LPRPDE a été adoptée avant l'avènement de technologies comme le téléphone intelligent et l'infonuagique et des modèles d'affaires reposant sur un accès illimité aux renseignements personnels et aux processus automatisés. Les intervenants ont fait écho à un débat mondial plus vaste sur le rôle du consentement dans les régimes de protection de la vie privée, débat qui a pris de l'ampleur alors que les avancées dans l'analyse des mégadonnées et la prédominance croissante de la collecte de données par l'Internet des objets commencent à imprégner fortement nos activités quotidiennes.

Certains préconisent un assouplissement des exigences en matière de consentement pour la collecte de renseignements personnels et souhaitent que l'on mette plutôt l'accent sur la reddition de comptes, l'utilisation éthique des renseignements personnels ou une approche axée sur le risque[2]. D'après eux, [traduction] « il devient de plus en plus difficile, voire impossible, pour le citoyen ordinaire de comprendre comment nos renseignements personnels sont utilisés dans cet environnement. Dès lors, il est de plus en plus irréaliste de s'attendre à ce que les individus jouent un rôle actif en décidant eux-mêmes comment leurs renseignements personnels seront utilisés de façon systématique[3] ».

D'autres, en revanche, estiment que l'on devrait prendre des mesures afin de renforcer le consentement, notamment accroître la transparence et mettre en place des mécanismes qui resserrent le contrôle individuel. Pour reprendre leurs paroles, [traduction] « en éliminant le consentement de l'équation, on risque de saper les protections, libertés et droits individuels fondamentaux[4] ».

Le Commissariat a décidé d'examiner de plus près le modèle de consentement dans le cadre de ses travaux portant sur la priorité stratégique de l'économie des renseignements personnels. En réponse aux préoccupations soulevées par des particuliers et des organisations, nous nous sommes engagés à déterminer et à analyser les améliorations que l'on pourrait apporter au modèle de consentement. Le présent document de discussion donne un aperçu du paysage, des enjeux clés et

des solutions éventuelles pour stimuler le dialogue et solliciter des suggestions afin d'améliorer ou de remplacer le modèle de consentement actuel.

Nous encourageons le lecteur à garder à l'esprit le rôle des différents acteurs – particuliers, organisations, organismes de réglementation et législateurs – lorsqu'il examinera les avantages relatifs des diverses solutions possibles que nous avons présentées. En procédant à une évaluation pour déterminer la solution ou la combinaison de solutions optimales pour résoudre le dilemme du consentement, il est important de se rappeler qui est le mieux placé pour utiliser les outils proposés et à qui ils servent. À terme, le but consiste à mieux protéger la vie privée des individus.

Pourquoi donner son consentement?

Dans la LPRPDE, le consentement représente un moyen pour les individus de protéger leur vie privée en exerçant un contrôle sur leurs renseignements personnels – il s'agit de déterminer quels renseignements personnels les organisations peuvent recueillir, comment elles peuvent les utiliser et à qui elles peuvent les communiquer. Dans *Privacy and Freedom*, son ouvrage majeur publié en 1967, le professeur Alan Westin affirme que la vie privée fait partie intégrante de l'autonomie personnelle, qui est à la base de notre système démocratique. D'après lui, [traduction] « dans les sociétés démocratiques, les gens ont profondément foi dans le caractère unique de l'individu, sa dignité et sa valeur […] et dans la nécessité de maintenir les mécanismes sociaux qui protègent son individualité sacrée[5] ».

Selon la définition proposée par M. Westin, la notion de vie privée renvoie à la volonté des individus de choisir librement quelle proportion d'eux-mêmes ils dévoileront aux autres. L'idée selon laquelle la protection de la vie privée consiste à exercer un contrôle sur ses propres renseignements personnels a été reprise dans un rapport publié en 1972 par le Groupe d'étude sur l'ordinateur et la vie privée du ministère des Communications et du ministère de la Justice, qui a jeté les bases de la législation canadienne sur la protection des renseignements personnels. En ce qui concerne la notion de vie privée dans le contexte de l'information, les auteurs du rapport affirment : « toute information concernant une personne constitue essentiellement sa propriété et il lui revient de décider si elle la communiquera ou si elle la conservera pour elle-même. […] Elle pourra décider de mettre l'information à la disposition des autres en contrepartie de certains avantages, […] mais n'en exercera pas moins un contrôle de base sur ce qui arrive à l'information et sur l'accès à cette dernière[6] ». Le juge Gérard La Forest, de la Cour suprême du Canada, a confirmé ce principe une vingtaine d'années plus tard en reprenant les propos de M. Westin pour affirmer que « la notion de vie privée est au cœur de celle de la liberté dans un État moderne. […] Fondée sur l'autonomie morale et physique de la personne, la notion de vie privée est essentielle à son bien-être[7] ».

Le respect de l'autonomie individuelle se trouvait en toile de fond de la rédaction de la LPRPDE. Non seulement l'autonomie individuelle est à la base du principe du consentement, mais aussi elle figure dans d'autres aspects du droit. Par exemple, les législateurs ont décidé de ne pas établir de distinction entre les données « sensibles » et les autres types de données. D'après eux, [traduction] « il est extrêmement difficile de déterminer *a priori* ce qu'est une donnée sensible, car les gens ont généralement une opinion différente quant aux données qu'ils considèrent comme particulièrement sensibles et les réponses peuvent varier d'un contexte à l'autre. On a donc jugé plus sûr de laisser aux personnes concernées le soin de décider ce qui est sensible et dans quelles circonstances, en leur permettant d'exercer le contrôle sur leurs renseignements personnels en vertu du principe du consentement[8] ».

Sans mentionner expressément le respect de la vie privée ou la protection des renseignements personnels, la *Charte canadienne des droits et libertés* assure une protection de la vie privée en vertu de l'article 7 (droit à la

30, rue Victoria, 1er étage, Gatineau (Québec) K1A 1H3 • Sans frais : 1-800-282-1376 • Télécopieur : (819) 994-5424 • ATS : (819) 994-6591
www.priv.gc.ca • Suivez-nous sur Twitter : @priveeprivacy

vie, à la liberté et à la sécurité de sa personne) et de l'article 8 (droit à la protection contre les fouilles, les perquisitions ou les saisies abusives). Dans *Information and Privacy Commissioner of Alberta c. Travailleurs et travailleuses unis de l'alimentation et du commerce, section locale 401*[9], la Cour suprême du Canada a statué que la législation sur la protection des renseignements personnels a un statut quasi constitutionnel en raison des intérêts importants qu'elle protège.

Consentement sous le régime de la LPRPDE

La LPRPDE a pour objet d'établir les règles régissant la collecte, l'utilisation et la communication des renseignements personnels de manière à prendre en compte à la fois le droit des individus à la confidentialité de leurs renseignements personnels et la nécessité pour les organisations de recueillir, d'utiliser ou de communiquer ce type de renseignements à des fins qu'une personne raisonnable estimerait acceptables dans les circonstances[10].

La LPRPDE exige que la collecte, l'utilisation et la communication des renseignements personnels se fassent au su et avec le consentement de l'intéressé. Les organisations sont tenues d'informer les personnes concernées de la nature des renseignements personnels qu'elles recueillent, de la façon dont elles ont l'intention d'utiliser ou de communiquer cette information ainsi que des fins de la collecte, de l'utilisation ou de la communication pour que les individus puissent décider de donner ou non leur consentement. Le but est de permettre à l'individu d'exercer un contrôle sur la façon dont ses renseignements personnels seront recueillis, utilisés et communiqués.

Pour qu'un consentement soit considéré comme valable sous le régime de la LPRPDE, les personnes concernées doivent bien comprendre ce qui sera recueilli, comment leurs renseignements personnels seront utilisés et à qui ils seront communiqués. Le consentement de l'intéressé n'est valable que s'il est raisonnable de s'attendre à ce qu'un individu visé par les activités de l'organisation comprenne la nature, les fins et les conséquences de la collecte, de l'utilisation ou de la communication des renseignements personnels auxquelles il consent[11].

Tout en reconnaissant la nécessité pour les organisations de recueillir, d'utiliser ou de communiquer des renseignements personnels à des fins raisonnables, la LPRPDE prévoit plusieurs exceptions à l'obligation d'informer l'individu et d'obtenir son consentement compte tenu du fait que l'obtention du consentement n'est pas forcément appropriée dans toutes les circonstances. Par exemple, l'information pourra être utilisée ou communiquée sans consentement dans une situation d'urgence mettant en danger la vie, la santé ou la sécurité d'une personne ou bien lorsque la recherche du consentement de l'intéressé pourrait compromettre une enquête portant sur la violation d'un accord ou une infraction à la loi. Ces exceptions reconnaissent que le consentement individuel et l'autonomie qu'il protège ne priment pas sur les autres intérêts, mais qu'il doit plutôt y avoir un juste équilibre entre la protection de la vie privée et les valeurs concurrentes que pourrait bafouer le consentement individuel[12]. En ce sens, comme nous l'expliquons ci-après, la LPRPDE reconnaît déjà les limites inhérentes au principe du consentement et elle les prend en compte. Certaines obligations prévues par la loi s'appliquent même si le consentement n'est pas exigé. Par exemple, le paragraphe 5(3) de la LPRPDE limite les fins de la collecte, de l'utilisation ou de la communication des renseignements personnels par une organisation à celles « qu'une personne raisonnable estimerait acceptables dans les circonstances ». Cette disposition aide à protéger les individus contre la collecte, l'utilisation et la communication inappropriées de leurs renseignements personnels même s'ils y consentent ou dans les cas où le consentement n'est pas exigé[13]. Tous les autres principes énoncés dans la LPRPDE, par exemple les mesures de sécurité et la responsabilité, continuent aussi de s'appliquer même si le consentement n'est pas exigé.

En vertu de la LPRPDE, l'organisation doit expliquer de manière claire et transparente les fins auxquelles les renseignements personnels d'un individu seront recueillis, utilisés ou communiqués. Elle doit obtenir le consentement avant de recueillir ce type de renseignements ou au moment de leur collecte, de même que chaque fois qu'elle souhaite utiliser à une nouvelle fin des renseignements déjà recueillis. L'organisation ne peut refuser de fournir un produit ou un service à un individu parce qu'il ne consent pas à la collecte, à l'utilisation ou à la communication de renseignements *autres* que ceux nécessaires pour réaliser une fin légitime et expressément indiquée. Parallèlement, elle devrait informer l'intéressé des conséquences du retrait de son consentement, en particulier s'il s'agit du consentement à la collecte, à l'utilisation ou à la communication de ses renseignements personnels qui sont indispensables pour obtenir le service qu'il commande.

La LPRPDE reconnaît que la forme de consentement peut varier en fonction du degré de sensibilité des renseignements et des attentes raisonnables de l'individu. Le consentement explicite est la forme de consentement la plus appropriée et la plus respectueuse à utiliser généralement. Il est obligatoire dans le cas des renseignements sensibles[14]. Le consentement implicite peut être acceptable dans certaines circonstances strictement définies[15].

Le rôle du consentement ailleurs dans le monde

1) Union européenne

Au sein de l'Union européenne (UE), le droit à la protection des données et le droit à la vie privée sont deux droits de la personne distincts reconnus par la *Charte des droits fondamentaux de l'Union européenne*, le Traité sur le fonctionnement de l'Union européenne et deux instruments juridiques du Conseil de l'Europe, auxquels sont parties tous les États membres de l'UE.

La directive 95/46 de l'UE relative à la protection des données (Directive de l'UE) régit le traitement des données à caractère personnel dans les secteurs public et privé. Elle vise deux grands objectifs : protéger le droit fondamental de la personne concernée à exercer un contrôle sur les données à caractère personnel la concernant, et assurer la libre circulation des données à caractère personnel sur le marché intérieur.

En vertu de l'article 6 de cette directive, les données à caractère personnel doivent « être collectées pour des finalités déterminées, explicites et légitimes » et « ne pas être traitées ultérieurement de manière incompatible avec ces finalités ». Elles doivent aussi être « adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et pour lesquelles elles sont traitées ultérieurement » et « exactes et, si nécessaire, mises à jour ». À de nombreux égards, ces dispositions sont comparables au paragraphe 5(3) de la LPRPDE.

Dans les limites de l'article 6, le consentement de la personne concernée constitue l'un des six fondements juridiques qui légitiment le traitement des données à caractère personnel. Cet article prévoit en outre que le traitement peut être effectué s'il est nécessaire à l'exécution d'un contrat, au respect d'une obligation légale imposée au responsable du traitement, à la sauvegarde de l'intérêt vital de la personne concernée, à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement ou à la réalisation de l'intérêt légitime poursuivi par le responsable du traitement, à condition que ne prévalent pas l'intérêt ou les droits et libertés fondamentaux de la personne concernée. Le consentement ne constitue pas le fondement juridique privilégié pour le traitement des données. Il est plutôt mentionné sur un pied d'égalité avec les autres fondements juridiques susmentionnés. Les États membres de l'UE, qui ont également leur propre législation nationale sur la protection de la vie privée, reconnaissent le

30, rue Victoria, 1er étage, Gatineau (Québec) K1A 1H3 • Sans frais : 1-800-282-1376 • Télécopieur : (819) 994-5424 • ATS : (819) 994-6591
www.priv.gc.ca • Suivez-nous sur Twitter : @priveeprivacy

consentement comme fondement juridique pour le traitement, mais l'importance qu'ils lui accordent varie d'un pays à l'autre[16].

Lorsque le traitement licite des données à caractère personnel repose sur le consentement, celui-ci doit être donné de manière explicite et être une « manifestation de volonté, libre, spécifique et informée[17] » témoignant des choix de l'individu. De plus, la personne doit donner son consentement de façon non équivoque et explicite dans certaines circonstances. Ainsi, un consentement explicite est requis pour le traitement de certaines catégories de données à caractère personnel, par exemple celles qui révèlent l'origine ethnique et les opinions politiques ainsi que les données génétiques. En outre, les individus ont le droit de retirer leur consentement au traitement des données qui les concernent.

Le nouveau *Règlement général sur la protection des données* (RGPD), qui devrait entrer en vigueur en 2018, remplacera la Directive de l'UE. En vertu de ce règlement, le consentement devra être une manifestation de volonté libre, spécifique et informée. Les entreprises n'auront pas à obtenir le consentement si elles peuvent prouver que le traitement est « nécessaire à la réalisation de l'intérêt légitime poursuivi par [une partie privée] à condition que ne prévalent pas l'intérêt ou les droits et libertés fondamentales de la personne concernée[18]. Le RGPD imposera aussi des restrictions en ce qui a trait à la capacité des enfants à consentir au traitement de données sans l'autorisation parentale.

La Directive de l'UE autorise un consentement implicite dans certaines circonstances, mais le RGPD exigera un consentement explicite sous forme de déclaration ou d'acte non équivoque. Il pourra s'agir, par exemple, de cocher une case sur un site Web ou de choisir un paramètre technique. Le RGPD précise explicitement que [traduction] « le silence ou l'inactivité ne devraient pas constituer un consentement ». Si une personne concernée a retiré son consentement, elle aura le droit d'obtenir que ses données personnelles soient effacées et ne soient plus traitées.

2) États-Unis

Aux États-Unis, la vie privée est protégée par une mosaïque de lois au niveau des États et au niveau fédéral. Dans de nombreux cas, il s'agit de lois sectorielles reflétant l'approche fondée sur le préjudice qui caractérise la réglementation américaine dans le domaine de la protection de la vie privée. Les principes relatifs aux pratiques équitables de traitement de l'information (Fair Information Practice Principles), entre autres la notion d'avis et de choix, servent de base aux mesures de protection de la vie privée. La Federal Trade Commission (FTC) a fait activement la promotion de la protection des renseignements personnels des consommateurs en exerçant son pouvoir de s'attaquer aux « pratiques déloyales et trompeuses », que lui confère la *Federal Trade Commission Act*[19]. Dans les conclusions qu'elle formule sous le régime de la *Federal Trade Commission Act,* la FTC peut prendre en compte les concepts d'avis et de choix dans le contexte des politiques régissant la protection de la vie privée et des conditions de service, car les entreprises ont l'obligation d'informer les individus de leurs pratiques de protection des renseignements personnels et de leur offrir le choix d'y consentir ou non.

La FTC réglemente aussi la protection de la vie privée des enfants sous le régime de la *Children's Online Privacy Protection Act* (COPPA)[20]. Cette loi oblige les exploitants de sites Web, les autres services en ligne et les applications mobiles qui recueillent les renseignements personnels d'enfants de moins de 13 ans à obtenir un consentement parental vérifiable. Malgré les dispositions de la COPPA, le consentement n'est pas exigé dans tous les cas pour recueillir ou utiliser des renseignements personnels d'individus aux États-Unis. Toutefois, les lois sectorielles et les codes de conduite contraignants exigent souvent que l'utilisateur ait le choix de donner un consentement par défaut [21]. Un consentement positif est exigé dans le cas des données sensibles, comme les renseignements médicaux ou financiers.

En 2012, la FTC a publié un rapport préconisant une [traduction] « législation de base d'application générale sur la protection de la vie privée qui conférerait au respect de la vie privée un statut de droit fondamental[22] ». La même année, la Maison-Blanche a publié un plan directeur en matière de protection de la vie privée (*Privacy Blueprint*) pour répondre à ce qui était qualifié d'absence d'« engagement soutenu de tous les intervenants à s'attaquer aux problèmes de protection des renseignements personnels des consommateurs découlant des progrès technologiques et des nouveaux modèles d'affaires[23] ». Le plan directeur propose une déclaration des droits des consommateurs en matière de protection de la vie privée qui repose sur des grands principes, entre autres l'exercice du contrôle par les individus, la transparence et la prise en compte du contexte.

La prise en compte du contexte constitue un principe clé de ce projet de déclaration. Selon ce principe, [traduction] « les consommateurs sont en droit de s'attendre à ce que les entreprises recueillent, utilisent et communiquent leurs renseignements personnels de manière conforme au contexte dans lequel ils les fournissent[24] ». D'après le plan directeur en matière de protection de la vie privée, ce principe découle de principes relatifs aux pratiques équitables de traitement de l'information largement reconnus, soit la « spécification des finalités » et la « limitation de l'utilisation » et il prévoit les éléments suivants :

- À moins d'indications contraires prévues par la loi, les entreprises devraient limiter l'utilisation et la communication des renseignements personnels à des fins compatibles avec la relation qu'elles entretiennent avec les consommateurs et le contexte dans lequel ces derniers ont fourni cette information au départ.
- Si les entreprises ont l'intention d'utiliser ou de communiquer des renseignements personnels à d'autres fins, elles devraient faire preuve d'une transparence accrue et offrir un choix aux consommateurs en leur indiquant ces autres fins de façon évidente et de manière à ce qu'ils puissent facilement se manifester au moment de la collecte des données.

En février 2015, le président Obama a rendu public le *Consumer Privacy Bill of Rights Act*[25]. En vertu de ce projet de loi, les organisations seraient tenues d'offrir aux individus un moyen raisonnable d'exercer un contrôle sur le traitement de leurs renseignements personnels, et ce moyen devrait être proportionnel aux risques d'atteinte à la vie privée. Les individus ont le droit de retirer leur consentement sous réserve d'exceptions particulières, par exemple la prévention de la fraude. Si une organisation traite des renseignements personnels d'une manière qui n'est pas raisonnable compte tenu du contexte, elle doit analyser les risques d'atteinte à la sécurité des renseignements et prendre des mesures raisonnables pour atténuer tous les risques qui ressortent de cette démarche. Elle pourrait, par exemple, faire preuve d'une transparence accrue ou renforcer le contrôle exercé par les individus. Ce projet de loi a été critiqué par certains défenseurs de la vie privée[26] qui jugent frileuses les dispositions relatives à l'application de la loi. Au moment de la rédaction du présent rapport, aucun nouveau développement n'avait été observé.

30, rue Victoria, 1er étage, Gatineau (Québec) K1A 1H3 • Sans frais : 1-800-282-1376 • Télécopieur : (819) 994-5424 • ATS : (819) 994-6591
www.priv.gc.ca • Suivez-nous sur Twitter : @priveeprivacy

Difficulté à obtenir un consentement valable

1) Nouvelles technologies et nouveaux modèles d'affaires

Le modèle de protection des renseignements personnels fondé sur le consentement a été élaboré à une époque où l'échange de renseignements dans le cadre des transactions se faisait à des moments clairement définis. Qu'il s'agisse d'une transaction bancaire ou d'une réclamation à une compagnie d'assurance, les transactions étaient souvent binaires et visaient généralement des fins distinctes ou limitées. Elles étaient la plupart du temps routinières, prévisibles et transparentes. De façon générale, les gens connaissaient l'identité des organisations avec lesquelles ils faisaient affaire, quels étaient les renseignements recueillis et comment ils seraient utilisés. Aujourd'hui, avec l'infonuagique, les mégadonnées et l'Internet des objets, l'environnement est radicalement différent. En outre, les transferts traditionnels de données d'un point à un autre sont remplacés par des flux de données qui transitent par des systèmes répartis, si bien que les individus ont de la difficulté à savoir quelles organisations traitent leurs données et à quelles fins.

Le législateur a pris de nombreuses précautions pour assurer la neutralité technologique des principes qui sous-tendent les lois sur la protection des renseignements personnels s'appliquant au secteur privé au Canada. Néanmoins, en raison de la complexité de l'écosystème d'information d'aujourd'hui, il est difficile d'obtenir et de donner un consentement valable. Comme le montrent les travaux du Commissariat à la protection de la vie privée du Canada sur l'analyse prédictive[27] et sur l'Internet des objets[28], les nouvelles technologies et les nouveaux modèles d'affaires ont créé un environnement dynamique en évolution rapide, où une foule d'acteurs souvent invisibles recueillent, communiquent et utilisent des quantités sans précédent de renseignements personnels à de multiples fins qui existent déjà ou qui n'ont pas encore été définies. Le consentement ponctuel binaire est de plus en plus contesté, car il reflète une décision prise à un moment donné dans des circonstances particulières et il est associé au contexte initial où s'inscrivait la décision. Or, nombre de modèles d'affaires et de technologies ne fonctionnent plus de cette façon aujourd'hui.

a) Mégadonnées

Grâce à des avancées technologiques considérables, les organisations ont la capacité de recueillir, de stocker et d'analyser des quantités d'information sans précédent. Ces avancées sont à l'origine des « mégadonnées », c'est-à-dire des ensembles de données si énormes, si peu structurés et si instables que les méthodes traditionnelles d'analyse des données ne conviennent plus. On utilise des algorithmes complexes pour trouver des corrélations dans ces ensembles de données afin de résoudre des problèmes et de générer de la valeur et des avantages pour les organisations, les individus et la société. Les gens et les organismes de réglementation ont de la difficulté à comprendre bon nombre de ces algorithmes, que les organisations considèrent comme leur propriété exclusive [29].

L'analyse des mégadonnées a ouvert la voie à de nombreux progrès dans tous les domaines de l'économie, y compris la recherche scientifique, la gestion des ressources et la fabrication. Les avantages qui en découlent pour la société sont substantiels. En l'absence de cette analyse, le traitement individualisé des maladies, l'optimisation de la circulation et l'enseignement personnalisé seraient probablement impossibles. Néanmoins, l'analyse des mégadonnées ne donne pas toujours des résultats positifs. Il peut y avoir des utilisations douteuses sur le plan éthique, par exemple une discrimination dans l'établissement des prix fondée sur des

attributs associés aux consommateurs[30] ou des publicités fondées sur un profilage racial[31]. Dans un rapport résumant les discussions qui ont eu lieu dans le cadre de son atelier public intitulé *Big Data: A Tool for Inclusion or Exclusion*, la FTC explique les préoccupations exprimées par les participants. Selon eux, malgré les nombreuses améliorations que l'analyse des mégadonnées pourrait engendrer pour la société, [traduction] « les inexactitudes et les préjugés éventuels pourraient avoir des effets préjudiciables sur les populations à faible revenu et défavorisées[32] ».

L'analyse des mégadonnées est attrayante pour les entreprises, parce qu'elle permet de créer de la valeur à partir d'information qui en soi vaudrait beaucoup moins. Puisque les coûts de stockage des données ont diminué et que la puissance des algorithmes a augmenté, les organisations ne sont guère motivées à détruire l'information. Au contraire, nombre d'entre elles la conservent au cas où elle se révélerait utile dans l'avenir. En fait, les avancées technologiques ouvrent la voie à des utilisations inédites des données qui défient l'imagination et il devient de plus en plus difficile de prévoir les utilisations que l'on en fera ultérieurement. On ne peut exclure le risque que les renseignements personnels fassent l'objet de nouvelles utilisations auxquelles les personnes concernées n'ont pas consenti ou auxquelles, selon toute probabilité, elles n'auraient pas consenti au moment de la collecte.

Il y a aussi la question de la distinction entre les renseignements personnels et non personnels, car la réglementation sur la protection de la vie privée ne s'applique généralement pas aux renseignements non personnels, si bien qu'aucun consentement n'est exigé en pareil cas. Les algorithmes de mégadonnées visent à établir des corrélations entre des éléments d'information. Or, si chacun des éléments d'information disparates ne constitue pas forcément un renseignement personnel en soi, le traitement consistant à amasser, à combiner et à analyser les éléments pourrait bien permettre d'obtenir des renseignements concernant un individu identifiable. En analysant les mégadonnées, on peut reconstituer l'identité des personnes auxquelles se rapportent des renseignements dépersonnalisés[33]. Il est difficile, voire impossible, de savoir à l'avance quand on pourra réidentifier une personne grâce à un algorithme ou quels éléments d'information permettront de le faire[34]. Dans le passé, lorsqu'il s'agissait de déterminer si des renseignements concernaient un individu identifiable et, par conséquent, s'ils constituaient des renseignements personnels, il était possible de répondre par oui ou non. Toutefois, certains ont récemment proposé une approche plus nuancée et davantage axée sur le risque [35]. On peut donc se demander quel est le point de bascule à partir duquel les renseignements deviennent personnels et obligent l'organisation à obtenir le consentement des individus ou s'il devrait effectivement y avoir un point de bascule.

L'analyse des mégadonnées permet aussi parfois d'obtenir par inférence des renseignements nouveaux et potentiellement *sensibles* concernant des individus à partir d'éléments d'information disparates qui, pris isolément, pourraient être des renseignements non personnels ou, s'il s'agit de renseignements personnels, pourraient être non sensibles. En vertu de la LPRPDE, un consentement explicite est exigé pour utiliser des renseignements sensibles. Or, dans un environnement de mégadonnées, ce type de consentement n'a peut-être pas été obtenu au moment de la collecte. Certains estiment[36] que l'obligation de recontacter les individus pour obtenir un consentement modifié pourrait décourager les organisations d'utiliser l'information à des fins nouvelles en raison du coût associé à l'obtention d'un nouveau consentement, ce qui freine la dynamique de l'innovation. Pourtant, la LPRPDE exige expressément un nouveau consentement.

En 2014, lors de leur conférence internationale annuelle, les commissaires à la protection des données et de la vie privée ont adopté une résolution sur les mégadonnées[37] qui réaffirme les principes relatifs à l'équité dans le traitement de l'information, y compris le consentement. Tout en reconnaissant les avantages des mégadonnées pour la société dans des domaines comme la médecine et la protection de l'environnement, les commissaires signalent que [traduction] « certains peuvent aussi penser que les mégadonnées vont à l'encontre des principes clés relatifs à la protection de la vie privée, en particulier ceux de limitation des

finalités et de limitation des données au minimum nécessaire[38] ». En parallèle, les commissaires soulignent l'importance de maintenir les mécanismes de protection de la vie privée comme mesures de sécurité contre les préjudices découlant du profilage à grande échelle, par exemple les conséquences discriminatoires et les atteintes au droit à l'égalité de traitement. Ils encouragent les organisations qui analysent des mégadonnées à prendre diverses mesures, notamment à faire preuve de transparence concernant leurs pratiques, à obtenir le consentement des individus et à protéger la vie privée en protégeant les renseignements personnels dès la conception et, s'il y a lieu, en les anonymisant.

Selon le rapport de recherche du Commissariat à la protection de la vie privée portant sur l'analyse prédictive, « d'un côté, les données massives et une analyse prédictive intelligente pourraient contribuer à faire avancer la recherche, à stimuler l'innovation et à générer de nouvelles approches en vue d'une meilleure compréhension du monde et de la prise de décisions importantes et socialement bénéfiques dans des domaines comme la santé publique, le développement et les prévisions économiques. D'un autre côté, une analyse poussée entraîne une augmentation de la collecte, du partage et du couplage des données et peut également s'avérer incroyablement invasive, intrusive et discriminatoire, en plus de constituer un autre pilier d'une société de surveillance[39] ».

b) Internet des objets

La prédominance croissante de l'infrastructure de l'Internet des objets présente des défis uniques en leur genre pour les cadres de protection de la vie privée qui reposent sur le consentement. L'expression « Internet des objets » désigne un environnement d'objets physiques qui recueillent des données au moyen de capteurs et qui les transmettent sur des réseaux de télécommunications. Cette technologie existe depuis des dizaines d'années, mais on l'utilisait généralement sans que le public en ait conscience, par exemple dans le secteur de la fabrication pour vérifier l'état de l'équipement et faire le suivi des pièces. Récemment, des appareils de l'Internet des objets sont devenus d'usage courant et des produits de consommation, ce qui a plusieurs répercussions sur la vie privée et suscite l'intérêt des organismes de réglementation en matière de protection de la vie privée. Par exemple, le Groupe de travail « Article 29 » sur la protection des données a pris position sur l'Internet des objets[40]. Cet organisme de la Commission européenne a conclu que la quantité, la qualité et la sensibilité des données recueillies par les appareils de l'Internet des objets sont telles que l'on doit considérer et traiter ces données comme des données à caractère personnel.

Comme en fait état le document de recherche sur l'Internet des objets publié par le Commissariat à la protection de la vie privée du Canada[41], la collecte d'information par l'Internet des objets découle de la volonté de comprendre les activités, les déplacements et les préférences des individus et de faire des déductions à leur sujet. Le Commissariat a montré par ailleurs qu'il est possible de glaner des renseignements très utiles sur une personne à partir de données comme l'adresse IP[42], les métadonnées[43] et les données de suivi sur le Web[44].

L'Internet des objets procure des avantages aux individus et à la société grâce à l'automatisation et à la surveillance accrues de tous les aspects de l'environnement, ce qui peut conduire à une meilleure gestion des ressources, à des gains d'efficience et à une utilisation plus pratique. Au nombre des applications de l'Internet des objets, mentionnons les automobiles connectées, les appareils de suivi de la santé et de la condition physique ainsi que la domotique. L'Internet des objets peut servir à réduire les coûts énergétiques dans une habitation en mettant en marche les appareils électriques pendant les périodes où les tarifs sont le moins élevés ou à gérer la circulation en surveillant le nombre de véhicules au moyen de capteurs intégrés dans la chaussée. Pour les organisations, sa valeur réside non pas dans les revenus tirés de la vente des appareils, mais dans les données gérées et traitées grâce aux algorithmes de mégadonnées.

L'information recueillie par les capteurs intégrés à des objets interconnectés dans l'environnement de l'Internet des objets peut générer des quantités phénoménales de données que l'on peut combiner ou analyser et à partir desquelles on peut agir. La plupart de ces données peuvent être sensibles ou le devenir si on les combine avec d'autres données de différentes sources. Par exemple, en combinant les données générées par une personne qui porte sur elle un téléphone intelligent, qui utilise un appareil de suivi de la condition physique et qui vit dans une maison dotée d'un compteur intelligent, on peut établir un profil indiquant le lieu où elle se trouve, les personnes avec lesquelles elle est en relation, ses goûts et intérêts, sa fréquence cardiaque et l'activité qu'elle est susceptible de pratiquer à tout moment.

La collecte de données dans l'environnement de l'Internet des objets est souvent imperceptible pour les personnes concernées. Il n'y a entre les consommateurs et les organisations aucune interface où la communication de données pourrait se faire de façon visible et transparente. En réalité, la collecte et la communication se font d'appareil à appareil, sans aucune intervention humaine, dans le cadre d'activités courantes.

Dans ce contexte, il est difficile de déterminer comment diffuser l'information utile concernant les risques d'atteinte à la vie privée pour aider l'utilisateur à décider en toute connaissance de cause de donner ou non son consentement. Dans la Déclaration de Maurice sur l'Internet des objets[45], les commissaires à la protection des données et de la vie privée du monde entier ont souligné que la transparence constitue une préoccupation clé. Ils y ont affirmé que le consentement obtenu sur la base des politiques actuelles de protection de la vie privée, souvent longues et complexes, a peu de chances d'être éclairé. Selon une recherche[46] portant sur les véhicules connectés financée par le Commissariat à la protection de la vie privée du Canada, l'information concernant la protection de la vie privée fournie aux consommateurs est tellement insuffisante qu'il leur est impossible de donner un consentement valable. Avec les accessoires intelligents à porter sur soi, qui ont fait l'objet d'un document de recherche du Commissariat[47], il est encore plus difficile de communiquer aux utilisateurs au moment opportun la bonne information sur leur droit à la vie privée, sous une forme intelligible et accessible.

Dans un rapport à l'intention de son personnel[48] portant sur l'Internet des objets, la Federal Trade Commission (FTC) a mentionné que la collecte généralisée de données et la possibilité d'utilisations inattendues des données constituent deux des risques les plus graves d'atteinte à la vie privée associés à l'Internet des objets. Elle a insisté sur l'importance d'aviser les individus des pratiques des entreprises en matière de gestion des données et recommandé que les organisations informent les consommateurs de la façon dont leurs renseignements seront utilisés, en particulier lorsqu'il s'agit de données sensibles ou que leur utilisation va au-delà des attentes raisonnables des consommateurs.

2) Comportement humain

En vertu de la LPRPDE en matière d'information et de consentement, il incombe aux individus de se renseigner eux-mêmes sur les pratiques d'une organisation en matière de gestion des renseignements personnels et de comprendre la nature, les fins et les conséquences de leur consentement à la collecte, à l'utilisation et à la communication de leurs renseignements par l'organisation. Cette exigence, qui peut sembler simple en théorie, pourrait comporter dans la pratique son lot de risques et d'obstacles en raison non seulement de la complexité de l'écosystème numérique, mais aussi des paradoxes du comportement humain et des réalités pratiques selon lesquelles la personne concernée dispose de peu de temps et n'a pas assez d'énergie pour s'intéresser comme il se doit aux politiques de confidentialité.

Même avant que les technologies de l'information et les modèles d'affaires aient évolué pour prendre leur forme actuelle, le modèle de consentement était critiqué par certains, qui le disaient trop théorique. Dans leur

30, rue Victoria, 1er étage, Gatineau (Québec) K1A 1H3 • Sans frais : 1-800-282-1376 • Télécopieur : (819) 994-5424 • ATS : (819) 994-6591
www.priv.gc.ca • Suivez-nous sur Twitter : @priveeprivacy

article intitulé « Soft Surveillance, Hard Consent » publié en 2009, le professeur Ian Kerr et ses collègues soutenaient que [traduction] « pour permettre aux individus d'exercer un véritable contrôle sur leurs renseignements personnels, les lois sur la protection des renseignements personnels doivent prévoir un modèle de consentement qui reflète fidèlement le comportement des gens[49] ».

Il est prouvé que le comportement humain nuit à l'efficacité du modèle de consentement. De nombreuses études montrent que des personnes affirmant se préoccuper de la protection de la vie privée peuvent tout de même communiquer d'énormes quantités de renseignements personnels en ligne. Par exemple, selon une étude[50] menée en 2015 à la demande de TRUSTe, alors que 54 % des parents se disent préoccupés par la vie privée de leurs enfants, 66 % affichent en ligne des photos de leur progéniture. Dans le cadre d'un sondage[51] effectué en 2015 par l'Institut AIMIA , 70 % des répondants qui prennent des mesures défensives pour protéger leurs renseignements sont également ouverts à l'idée de les communiquer.

Les spécialistes de la psychologie du comportement commencent à trouver un sens à ce comportement en apparence contradictoire et mentionnent plusieurs facteurs qui influent sur la capacité à prendre des décisions concernant la protection de la vie privée. Le professeur Alessandro Acquisti et ses collègues avancent l'idée[52] que trois éléments clés influencent le comportement des individus en ce qui a trait à la protection de leurs renseignements personnels :

- L'incertitude entourant la nature des compromis à faire au chapitre du droit à la vie privée – Les gens n'ont pas une idée claire et exacte de ce qui arrive à leurs renseignements personnels lorsque les organisations les ont recueillis, d'où leur incertitude concernant la quantité d'information à communiquer.
- La variation en fonction du contexte – La sensibilité d'une personne à l'égard de la protection de la vie privée varie en fonction de la situation et d'éléments tels que l'environnement physique qui l'entoure, la conception du site Web et la quantité d'information affichée par d'autres sur le site Web.
- La malléabilité des préférences en matière de protection de la vie privée – Les gens se laissent facilement influencer pour ce qui est du type et de la quantité de renseignements qu'ils communiquent. Par exemple, les paramètres de confidentialité par défaut sont souvent interprétés comme des recommandations, si bien que les comportements varient en fonction des paramètres à ce chapitre.

De l'avis d'autres chercheurs[53], il est très difficile d'évaluer les risques d'atteinte à la vie privée en comparaison des avantages concrets découlant de la communication de renseignements personnels en ligne. Les gens ne sont pas toujours conscients des conséquences de la communication, d'autant plus que les bribes d'information, une fois regroupées, finissent par tracer au fil du temps un portrait plus complet. En outre, ils se laissent facilement distraire par l'illusion du respect de la vie privée. Une recherche[54] montre que le simple fait d'afficher une politique de confidentialité renforce chez les utilisateurs l'idée que le site protège leurs renseignements personnels.

L'attitude générale de l'individu à l'égard du monde qui l'entoure joue aussi un rôle dans la communication de renseignements personnels. Une enquête[55] réalisée par l'École de communication Annenberg de l'Université de Pennsylvanie a exploré l'idée que les gens affichent en ligne de l'information les concernant en échange de certains avantages. D'après les chercheurs, [traduction] « plus de la moitié des gens ne veulent pas perdre le contrôle qu'ils exercent sur les renseignements qui les concernent, mais ils estiment que cette perte de contrôle s'est déjà concrétisée ». Convaincus qu'ils n'ont pas le choix, ils se résignent et font des compromis.

La section qui suit présente des solutions possibles pour s'attaquer aux défis que pose le modèle de consentement sur le plan technique et humain.

Solutions possibles

Nous avons vu les défis que présente l'écosystème d'information numérique au chapitre du consentement pour les individus et les organisations. Nous avons aussi vu que les particuliers font face à des distorsions cognitives et à des contraintes pratiques au moment de prendre des décisions concernant la protection de la vie privée et qu'ils ont la responsabilité de comprendre un environnement très complexe. On peut difficilement s'attendre à ce que des gens laissés à eux-mêmes démystifient des relations d'affaires complexes et des algorithmes compliqués afin de faire un choix éclairé lorsqu'il s'agit de consentir à la collecte, à l'utilisation et à la communication de leurs renseignements personnels. Le fardeau de comprendre des pratiques compliquées et d'y consentir ne devrait pas reposer uniquement sur les épaules des individus : il faut mettre en place des mécanismes de soutien appropriés pour faciliter le processus de consentement.

Pour leur part, les organisations se heurtent à des difficultés concrètes lorsqu'elles essaient d'expliquer leurs pratiques de gestion des renseignements personnels, en particulier dans l'environnement mobile et compte tenu de l'évolution rapide des services en ligne et de la vive concurrence qui règne dans ce secteur. Les organisations doivent innover rapidement pour soutenir la concurrence dans l'économie mondiale et elles bénéficieraient de mécanismes les aidant à se conformer de façon plus efficiente aux exigences en matière de consentement.

Le consentement ne devrait être un fardeau ni pour les particuliers ni pour les organisations et il ne devrait pas faire obstacle à l'innovation ni priver les individus, les organisations et la société des avantages découlant du progrès technologique. Mais quelle est la meilleure façon de s'y prendre pour préserver cet important contrôle dans le paysage actuel et trouver un juste équilibre entre le droit des individus à la vie privée et la nécessité pour les organisations de gérer les renseignements personnels à des fins commerciales raisonnables en vue de réaliser l'objet et les objectifs mêmes de la LPRPDE? Quels outils seraient efficaces et qui est le mieux placé pour les mettre en œuvre? Le présent rapport constitue la première mesure prise par le Commissariat à la protection de la vie privée du Canada pour déterminer les mécanismes qui pourraient aider à renforcer la validité du consentement tout en favorisant l'innovation dans une économie numérique. Le rôle et les responsabilités des acteurs clés demeurent un facteur essentiel dans l'élaboration de ces mécanismes.

Divers intervenants ont proposé un éventail de solutions pour résoudre certains défis en matière de protection de la vie privée découlant des nouvelles technologies et des nouveaux modèles d'affaires, c'est-à-dire :

- améliorer le processus de consentement éclairé en expliquant aux personnes de façon plus simple et plus utile les pratiques de gestion de l'information et en leur offrant des moyens plus conviviaux pour exprimer leurs préférences concernant la protection de la vie privée;
- trouver des solutions de remplacement qui permettraient d'introduire certaines utilisations restreintes autorisées sans le consentement de l'intéressé ou certaines « zones interdites » correspondant à des utilisations formellement interdites;
- renforcer les mécanismes de reddition de comptes afin que les organisations montrent qu'elles se conforment aux obligations que leur impose actuellement la loi, y compris les garanties par des tiers auxquelles s'en remettent les utilisateurs au moment de donner leur consentement;

30, rue Victoria, 1er étage, Gatineau (Québec) K1A 1H3 • Sans frais : 1-800-282-1376 • Télécopieur : (819) 994-5424 • ATS : (819) 994-6591
www.priv.gc.ca • Suivez-nous sur Twitter : @priveeprivacy

- adopter de nouveaux mécanismes de reddition de comptes qui élargissent les notions d'équité et d'éthique dans l'évaluation d'utilisations prévues des renseignements personnels des individus; ces mécanismes s'ajouteraient à l'obtention du consentement, tel qu'il est traditionnellement défini ou qui, dans certains cas, le remplaceraient;
- renforcer la surveillance réglementaire pour s'assurer que les solutions proposées permettent de protéger efficacement la vie privée.

Certaines de ces solutions soulignent de nouveau l'importance des principes existants relatifs aux pratiques équitables de traitement de l'information. Elles obligent les organisations, les chercheurs et les technologues à faire preuve d'une plus grande créativité dans la façon dont ils présentent l'information aux gens et utilisent la technologie pour intégrer des mesures de protection de la vie privée en vue de renforcer la validité du consentement. D'autres proposent des solutions de remplacement pour les cas où il ne serait pas réaliste d'obtenir le consentement de l'intéressé. Avec les solutions axées sur la gouvernance, il incombe aux organisations d'évaluer et d'atténuer les risques et de se prononcer sur le caractère raisonnable de diverses utilisations des renseignements personnels.

Chacune de ces solutions comporte des avantages et des inconvénients. Si le consentement peut s'avérer un excellent outil pour remédier au déséquilibre des pouvoirs entre les organisations et les particuliers dans l'économie du savoir, certaines solutions donnent-elles assez ou trop de contrôle aux individus? Certaines d'entre elles donnent-elles trop de pouvoirs aux organisations pour lesquelles la valeur commerciale des renseignements personnels présente un intérêt particulier? Dans l'affirmative, comment peut-on atténuer le risque?

La discussion portant sur les solutions s'articule autour d'une question clé : Comment répartir entre les organisations, les personnes, les organismes de réglementation et les législateurs la responsabilité d'assurer la protection de la vie privée? Idéalement, les organisations devraient mettre en place des solutions pratiques offrant un choix véritable aux personnes, après quoi les personnes commenceraient à faire valoir de façon réfléchie leurs préférences en matière de protection de la vie privée. Mais dans les cas où le consentement n'est ni réaliste ni valable, quelles solutions de remplacement raisonnables devrait-on autoriser? Quels mécanismes pourraient aider les organismes de réglementation à maintenir un juste équilibre entre le droit à la vie privée des individus et la nécessité pour les organisations d'utiliser les renseignements personnels et à s'assurer que l'on respecte un niveau minimal de protection de la vie privée?

Nous présentons ci-après différentes options. Il ne s'agit pas d'une liste exhaustive, mais nous décrivons à tout le moins les types d'approches envisagées. Il serait étonnant qu'une de ces options soit à elle seule la solution miracle. Toutefois, la bonne combinaison de solutions pourrait aider les gens à exercer un meilleur contrôle sur leurs renseignements personnels dans la sphère numérique. Les questions figurant à la fin de chaque section et à la fin du présent document visent à stimuler la discussion sur les solutions privilégiées aux problèmes qui, selon nous, posent des difficultés au chapitre du consentement.

1) Amélioration du consentement

Certes, il est possible de renforcer le modèle de protection de la vie privée actuel axé sur le consentement en mettant en place des mécanismes destinés à améliorer la capacité pratique des personnes à donner un consentement valable. Une transparence accrue dans les politiques de confidentialité et les avis concernant la protection de la vie privée, des moyens plus simples pour les personnes de gérer leurs préférences en la matière et une amélioration des approches techniques et des approches de gouvernance pourraient tous

permettre que le modèle de consentement continue à fonctionner comme prévu. Certains mécanismes visant à améliorer le consentement sont présentés ci-après.

a) Transparence accrue dans les politiques de confidentialité et les avis concernant la protection de la vie privée

Dans le monde numérique, la circulation des renseignements personnels entre les particuliers et les organisations s'est multipliée et diversifiée. Toutefois, le véhicule pour communiquer l'information sur les pratiques de protection de la vie privée – c'est-à-dire la politique de confidentialité – n'a pas évolué au même rythme que l'écosystème.

Lorsque les organisations utilisent un seul document pour décrire des pratiques de protection de la vie privée complexes afin de limiter leur responsabilité juridique et de respecter les lois sur la protection des renseignements personnels d'un grand nombre de pays, il ne faut pas s'étonner si le résultat n'est pas toujours particulièrement utile. Les politiques de confidentialité ont fait l'objet de nombreuses critiques en raison du jargon juridique qui y est utilisé et des efforts requis pour les lire. D'après des recherches largement citées[56] menées en 2008, les internautes auraient besoin de 244 heures par an pour lire, voire comprendre, les politiques de confidentialité des sites qu'ils ont visités. Le nombre d'heures serait vraisemblablement encore plus élevé aujourd'hui.

Selon la professeure Helen Nissenbaum[57], le « paradoxe de la transparence » constitue la principale limite des politiques de confidentialité. D'une part, si les responsables de l'élaboration de ces politiques essaient de décrire de façon exhaustive les pratiques des organisations, ils obtiendront un document long et complexe illisible et inintelligible pour l'utilisateur moyen. D'autre part, une politique de confidentialité brève et simple ne saurait refléter la complexité de la circulation de l'information de manière suffisamment détaillée pour permettre un consentement éclairé.

Diverses solutions pratiques ont été proposées pour alléger le fardeau des personnes qui doivent se renseigner sur des pratiques complexes de gestion de l'information. Les organismes de réglementation dans le domaine de la protection de vie privée, entre autres le Commissariat à la protection de la vie privée du Canada[58], font valoir que les organisations devraient non seulement se doter d'une politique de confidentialité claire et détaillée, mais aussi s'efforcer de communiquer l'information concernant la protection de la vie privée à des étapes clés de l'expérience des utilisateurs pour les aider à comprendre la circulation complexe de l'information.

Ces dernières années, on s'est tourné vers les politiques de confidentialité à plusieurs niveaux dans le cadre des efforts visant à faire en sorte que les politiques de confidentialité soient assez détaillées et faciles à lire. Il y a lieu d'explorer également des options créatives pour adapter le consentement à l'évolution de la situation et des préférences et alléger le plus possible le fardeau associé à la prise de décisions. Par exemple, les organisations pourraient améliorer leur politique de confidentialité au moyen de cartes de données, d'outils infographiques dynamiques et interactifs ou de courtes vidéos. Les icônes peuvent aussi être utiles comme outil complémentaire afin que les individus comprennent d'un seul coup d'œil comment leurs renseignements personnels sont utilisés. Les « icônes de protection de la vie privée[59] » illustrent une approche axée sur les symboles utilisée pour présenter les caractéristiques des politiques de confidentialité, par exemple en ce qui a trait à la conservation des données, à leur utilisation par des tiers et à l'accessibilité pour les organismes d'application de la loi.

Les organisations doivent tenir les consommateurs informés. Il s'agit non seulement d'une exigence réglementaire, mais aussi d'une pratique qui contribue au succès global des organisations. Dans un rapport publié en 2015[60], le Conseil des consommateurs du Canada souligne que les modalités complexes, y compris

30, rue Victoria, 1er étage, Gatineau (Québec) K1A 1H3 • Sans frais : 1-800-282-1376 • Télécopieur : (819) 994-5424 • ATS : (819) 994-6591
www.priv.gc.ca • Suivez-nous sur Twitter : @priveeprivacy

les politiques de confidentialité, peuvent miner la confiance des consommateurs envers les entreprises. Il y recommande des pratiques exemplaires à l'intention des organisations, leur conseillant par exemple d'afficher les points saillants de leur politique de confidentialité, de mettre en évidence les modifications par rapport à la version antérieure et de définir les principales notions.

b) Gestion des préférences concernant la protection de la vie privée pour l'ensemble des services

D'après le rapport de la Maison-Blanche intitulé *Big Data and Privacy: A Technological Perspective*[61], une organisation aurait la responsabilité d'utiliser les renseignements personnels en respectant les préférences de l'utilisateur. Elle pourrait à cette fin se faire aider par un intermédiaire accepté mutuellement. Les personnes adhéreraient à un ensemble standard de préférences en matière de protection de la vie privée offerts par des tiers. Le site Web des tiers approuverait ensuite les applications et les services en fonction du profil de l'utilisateur.

On trouve une suggestion du même ordre dans le rapport du Forum économique mondial 2013 intitulé *Unlocking the Value of Personal Data: From Collection to Usage* [62]. Le Forum propose de marquer toutes les données recueillies au moyen de métadonnées indiquant les préférences de l'intéressé concernant la façon dont les données peuvent être utilisées. Une fonction de vérification serait intégrée pour déterminer si une utilisation réelle est conforme aux préférences préalablement codées. Le marquage des données au moyen des préférences ou des règles (pratique parfois appelée « création de données intelligentes ») a fait l'objet de certains travaux techniques. Le langage XACML (eXtensible Access Control Markup Language) constitue une norme pour la création de conditions et d'obligations aux fins du contrôle de l'accès aux données. On a élargi la portée de ce langage afin de créer des mécanismes applicables aux politiques de confidentialité « problématiques » concernant des renseignements personnels stockés dans des paquets ou des enveloppes dont on se sert pour contrôler la diffusion et l'utilisation de ces renseignements[63].

Ces deux approches pourraient simplifier le processus de consentement, car elles éliminent la nécessité de comprendre parfaitement toutes les pratiques de protection de la vie privée d'une organisation et de décider de donner ou non son consentement chaque fois que l'on veut utiliser un nouveau service numérique. Elles aideraient également à prendre en compte le consentement lorsque l'analyse de mégadonnées conduit à de nouvelles utilisations après l'obtention du consentement initial à la collecte de données.

c) Mesures de sécurité propres à une technologie donnée

Les politiques et avis transparents et les mécanismes visant à faciliter la gestion des préférences ne sont pas les seules solutions possibles. On propose aussi des mesures pour satisfaire aux exigences en matière de consentement valable lorsque les renseignements personnels sont traités au moyen de technologies particulières. Par exemple, les caractéristiques uniques de l'environnement de l'Internet des objets créent les conditions idéales pour ce type d'approche.

En Europe, le Groupe de travail « Article 29 » sur la protection des données préconise[64] l'intégration de mécanismes de conformité dans les appareils et les services de l'Internet des objets pour compenser la « mauvaise adaptation » des mécanismes de consentement traditionnels. Ce groupe de travail affirme que les appareils et les services de l'Internet des objets doivent comporter des fonctions permettant aux utilisateurs de retirer leur consentement en tout temps, et ce, sans subir de pénalité financière ni être privés de l'accès aux fonctions de l'appareil.

Dans son rapport sur l'Internet des objets[65], la Federal Trade Commission présente à son personnel plusieurs solutions prometteuses qui sont mises en œuvre pour améliorer l'efficacité des messages sur la protection de la vie privée dans l'environnement de l'Internet des objets, par exemple :

- ajout de codes sur l'appareil, comme les codes QR, afin de permettre aux consommateurs d'avoir accès à une information détaillée;
- choix en matière de protection de la vie privée au moment de la configuration de l'appareil afin que le consommateur puisse tirer parti des assistants de configuration pour obtenir des explications et sélectionner les paramètres de confidentialité;
- portails de gestion ou tableaux de bord renfermant les paramètres de confidentialité que les consommateurs peuvent configurer et modifier par la suite;
- communications hors bande permettant aux gens de recevoir de l'information sur la protection de la vie privée au moyen d'un autre appareil, par exemple par courriel.

L'Online Trust Alliance[66] (OTA) a élaboré l'*Internet of Things Trust Framework*[67] à l'intention des fabricants, des concepteurs et des détaillants d'appareils connectés pour la maison et d'accessoires intelligents à porter sur soi pour le suivi de la santé et de la condition physique. Ce cadre préconise des pratiques exemplaires, par exemple :

- communiquer, avant l'achat de l'appareil, la politique concernant la collecte de données et préciser l'incidence sur les principales fonctions de l'appareil si les clients choisissent de ne pas communiquer leurs données;
- indiquer si l'utilisateur peut supprimer ou anonymiser tous ses renseignements personnels à la fin de la durée de vie de l'appareil ou lorsqu'il cesse de s'en servir.

d) Protection des renseignements personnels en tant que paramètre par défaut (protection de la vie privée dès la conception)

La protection de la vie privée dès la conception[68] vise à s'assurer que l'on prend en compte cet aspect tout au long de l'élaboration et de la mise en œuvre d'initiatives qui donnent lieu au traitement de renseignements personnels. Elle oblige les entreprises à intégrer la protection de la vie privée à l'étape de la création de leurs produits et systèmes pour s'assurer que les mécanismes de protection, y compris le consentement valable, seront bien ancrés. Autrement dit, la protection de la vie privée est intégrée par défaut comme élément inhérent au programme ou au système.

Le concept à la base de la protection de la vie privée dès la conception est global, en ce sens qu'il intègre des mesures techniques et des principes de gouvernance. La protection de la vie privée doit faire partie intégrante non seulement de la technologie, mais aussi des priorités organisationnelles, des objectifs du projet et de la planification globale des activités. Cette approche proactive en matière de protection de la vie privée inspire confiance en donnant aux individus l'assurance que leurs renseignements personnels ne seront pas utilisés à des fins inattendues et sans leur consentement. Elle permet aussi aux organisations d'améliorer leur reddition de comptes et de s'acquitter de leurs obligations en matière de protection de la vie privée.

La protection de la vie privée dès la conception est reconnue dans le monde entier. En 2010, lors de leur conférence internationale annuelle, les commissaires à la protection des données et de la vie privée ont adopté une résolution sur la protection de la vie privée dès la conception[69] en faisant valoir qu'il s'agit d'un élément essentiel de la protection de la vie privée. Ils ont aussi exhorté les organismes de réglementation dans

le domaine à promouvoir l'adoption des principes de protection de la vie privée dès la conception dans la formulation des politiques de confidentialité et dans la législation sur la protection des renseignements personnels. Les commissaires ont donné leur aval à ces principes dans plusieurs résolutions adoptées par la suite, y compris celle de 2014 sur les mégadonnées[70].

Aux États-Unis, dans son rapport intitulé *Protecting Consumer Privacy in an Era of Rapid Change*[71] publié en 2012, la FTC a proposé à l'intention des organisations et des décideurs un cadre dans lequel la protection de la vie privée dès la conception constitue une valeur fondamentale. En 2015, l'Agence européenne chargée de la sécurité des réseaux et de l'information a publié un inventaire[72] des approches, des stratégies et des mécanismes techniques de protection de la vie privée dès la conception pour promouvoir des façons de mettre en pratique les principes énoncés dans la législation sur la protection des renseignements personnels.

Par ailleurs, au sein de l'Union européenne, le nouveau *Règlement général sur la protection des données* (RGPD) imposera aux organisations l'obligation d'intégrer les principes de protection de la vie privée dès la conception au développement de procédés opérationnels pour les produits et services. Dans le modèle européen, la gouvernance se superpose au cadre technique de protection de la vie privée dès la conception. Par exemple, en raison de l'obligation d'obtenir un consentement explicite et de pouvoir faire la preuve que le consentement a été donné, il revient aux organisations de concevoir et de mettre en œuvre un mécanisme de consentement qui remplit ces critères.

Questions pour alimenter la réflexion

1) Quelles mesures pourrait-on adopter pour renforcer le consentement? Comment devrait-on promouvoir l'élaboration ou la mise en œuvre de ces mesures?

2) Quelles mesures devrait-on mettre en place pour inciter les organisations à accroître la transparence et à mettre en œuvre des mécanismes axés sur les préférences concernant la protection de la vie privée pour renforcer la capacité des gens à donner leur consentement?

3) Comment devrait-on traiter la protection de la vie privée dès la conception dans le contexte des lois canadiennes sur la protection des renseignements personnels? Devrait-on se contenter de promouvoir ce principe comme étant souhaitable dans un régime axé sur la responsabilisation? Devrait-on plutôt en faire une exigence prévue par la loi comme ce sera bientôt le cas en Europe?

2) Solutions de remplacement du consentement

La quête de solutions aux difficultés inhérentes au modèle de consentement dans le monde numérique pourrait nous amener au constat que le consentement n'est tout simplement pas réaliste dans certaines situations. Dans la présente section, nous envisageons des solutions de remplacement pour protéger la vie privée qui pourraient s'ajouter au consentement dans ces cas. En évaluant le mérite de ces solutions, nous devrions déterminer les changements à mettre en œuvre pour assurer leur efficacité. Certaines approches, comme la désidentification, pourraient s'insérer dans le cadre législatif actuel. D'autres, comme l'ajout de motifs supplémentaires pour traiter en toute légitimité des renseignements personnels sans le consentement de l'intéressé, pourraient introduire un changement par rapport à la norme actuelle et exigeraient des modifications législatives.

a) Désidentification

Plusieurs termes connexes sont utilisés pour désigner le spectre allant des données entièrement anonymisées à celles dévoilant pleinement l'identité. Selon la définition retenue par le Commissariat à l'information du Royaume-Uni, on entend par « données anonymisées » les données présentées sous une forme qui ne permet pas d'identifier les individus et dont la combinaison avec d'autres données ne devrait pas permettre de les identifier[73]. Sur ce spectre, les données pseudonymisées se situent quelque part entre les données anonymisées et celles dévoilant pleinement l'identité, car elles présentent à un degré variable un risque de réidentification. D'après l'Organisation internationale de normalisation (ISO), la pseudonymisation « est un processus par lequel les données perdent leur caractère nominatif. Elle diffère de l'anonymisation car les données restent liées à la même personne dans tous les dossiers et systèmes informatiques sans que l'identité ne soit révélée[74] ». On peut dire que les données pseudonymisées constituent un sous-ensemble des données désidentifiées, c'est-à-dire des données à partir desquelles [traduction] « l'association entre un ensemble de données d'identification et la personne concernée » a été supprimée[75].

Les lois sur la protection de la vie privée et des renseignements personnels considèrent les données anonymisées comme des renseignements non personnels qui ne sont pas visé par des mesures de protection de la vie privée. Quant au RGPD de l'Union européenne, il exclut expressément de son application les données anonymisées. Ce règlement reconnaît que la pseudonymisation des données à caractère personnel peut atténuer les risques d'atteinte à la vie privée des individus et constituer une mesure de sécurité propre à aider les responsables du traitement à s'acquitter de leurs obligations en matière de protection de la vie privée. Dans la version actuelle du RGPD[76], la pseudonymisation est définie comme étant « le traitement des données à caractère personnel de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires pour autant que, ces infomrations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractèrepersonnel ne sont pas attribuées à une personne physique identifiée ou identifiable ».

L'évaluation du risque de réidentification constitue un aspect clé de la désidentification. Si les données désidentifiées présentent généralement un risque de réidentification, le degré de protection de la vie privée accordé aux données désidentifiées devrait-il être proportionnel au niveau de risque de réidentification? Autrement dit, devrait-on intensifier la protection à mesure que le risque de réidentification augmente?

Les dispositions de la LPRPDE s'appliquent aux renseignements personnels, c'est-à-dire à « tout renseignement concernant un individu identifiable ». Le Commissariat à la protection de la vie privée du Canada interprète de façon très large la notion de renseignement personnel. Par exemple, d'après la *Position de principe sur la publicité comportementale en ligne,* il considère généralement comme des renseignements

30, rue Victoria, 1er étage, Gatineau (Québec) K1A 1H3 • Sans frais : 1-800-282-1376 • Télécopieur : (819) 994-5424 • ATS : (819) 994-6591
www.priv.gc.ca • Suivez-nous sur Twitter : @priveeprivacy

personnels les renseignements recueillis aux fins de ce type de publicité. Au Canada, les tribunaux ont statué que « les renseignements seront des renseignements concernant un individu identifiable lorsqu'il y a de fortes possibilités que l'individu puisse être identifié par l'utilisation de ces renseignements, seuls ou en combinaison avec des renseignements d'autres sources[77] ». On peut en déduire que les données pseudonymisées pourraient être des renseignements personnels au sens de la LPRPDE et visées par toutes les dispositions de cette loi.

L'utilité de la désidentification pour protéger la vie privée dans l'environnement actuel des grands ensembles de données, des services personnalisés et du suivi continu fait actuellement débat. D'après le professeur Paul Ohm[78] et d'autres observateurs, les renseignements ne peuvent jamais être parfaitement désidentifiés pour la simple raison qu'il y a trop de renseignements secondaires accessibles pouvant permettre d'identifier l'individu lorsqu'on les combine avec les renseignements désidentifiés. Par exemple, dans l'étude notoire portant sur la réidentification des données de Netflix, les chercheurs ont pu identifier différents utilisateurs de Netflix figurant dans un sous-ensemble supposément « anonymisé » simplement grâce à la cote que les utilisateurs avaient attribuée à six films[79] et le moment où ils les avaient évalués.

Certains spécialistes mettent en garde contre la nature ponctuelle de nombreuses techniques de désidentification et laissent entendre qu'il suffit de posséder des compétences de base en programmation et en statistique pour réidentifier de nombreux ensembles de données publiés[80]. Ils soutiennent également que le risque de réidentification des ensembles de données désidentifiées va en augmentant à mesure que les techniques de réidentification gagnent en efficacité et que l'on a accès à des ensembles de données supplémentaires pour les apparier.

D'autres, comme le Groupe de travail « Article 29 » sur la protection des données, estiment que la désidentification constitue une stratégie utile pour atténuer les risques d'atteinte à la vie privée. Ils reconnaissent toutefois qu'il est difficile de créer un ensemble de données parfaitement désidentifiées qui demeure assez pertinent pour permettre aux organisations de réaliser les fins visées. D'après ce groupe de travail, les techniques de désidentification peuvent servir à protéger la vie privée, mais uniquement si elles sont élaborées de façon rigoureuse et que l'on surveille et atténue en permanence les risques de réidentification[81]. Par exemple, l'article 38 du RGPD prévoit des codes de conduite sur le recours à la pseudonymisation pour protéger le traitement des données à caractère personnel.

D'après Khaled El Emam, la désidentification peut s'avérer un précieux outil pour renforcer la protection de la vie privée, parce que le fait de suivre des procédures de désidentification établies réduit considérablement le risque de réidentification. Il a démontré[82] que la désidentification est particulièrement utile dans la recherche en santé, car elle permet d'utiliser des renseignements personnels très sensibles dans l'intérêt du public, par exemple pour faire progresser la recherche en santé et améliorer la qualité des soins. Dans ce contexte, l'obtention du consentement ne serait peut-être pas réaliste. M. El Emam préconise une approche fondée sur le risque selon laquelle on évalue le risque de réidentification et on optimise la désidentification pour s'assurer que le risque demeure sous un seuil acceptable.

Robert Gellman[83] propose de protéger la vie privée en contrôlant la réidentification des données désidentifiées grâce à des moyens contractuels. Selon la proposition de ce spécialiste de la protection de la vie privée, les parties qui échangent des renseignements désidentifiés devraient conclure un contrat sur une base volontaire en vertu duquel elles s'engageraient officiellement à ne pas réidentifier les données et à offrir des mécanismes de recours si les mesures de protection de la vie privée ne sont pas maintenues. Si l'on part de l'hypothèse que les méthodes techniques de désidentification atténuent le risque de réidentification, sans toutefois l'éliminer, la solution contractuelle offre une protection supplémentaire en responsabilisant ceux qui s'engagent à ne pas réidentifier les renseignements.

Le Future of Privacy Forum (FPF) préconise la désidentification pour assurer la protection de la vie privée tout en préservant la valeur commerciale et scientifique de grands ensembles de données. Il travaille à l'établissement d'un cadre visant à appliquer les mesures de protection de la vie privée aux données désidentifiées en fonction de la nature des données, du risque de réidentification et de la présence de mesures de sécurité administratives ou de protection juridique supplémentaires – par exemple une politique de protection des données ou des modalités contractuelles limitant les façons dont les tiers peuvent utiliser les données[84].

Questions pour alimenter la réflexion

1) Quels sont les critères d'évaluation et de classement des risques de réidentification?

2) Le consentement devrait-il être exigé pour la collecte, l'utilisation et la communication de données désidentifiées? Dans l'affirmative, dans quelles conditions?

3) Existe-t-il une approche pragmatique axée sur le risque qui pourrait faire varier le niveau de l'exigence en matière de consentement en fonction du risque de réidentification des données?

4) Quel rôle les filets de sécurité contractuels devraient-ils jouer? Y a-t-il d'autres moyens de protéger les données désidentifiées?

b) « Zones interdites »

Une « zone interdite » renvoie à des mesures interdisant la collecte, l'utilisation ou la communication de renseignements personnels dans certaines circonstances. Cette interdiction peut être fondée sur divers critères, par exemple la sensibilité du type de renseignements, la nature de l'utilisation ou de la communication proposée ou encore les vulnérabilités associées au groupe auquel se rapportent les renseignements traités. Une « zone interdite » véritable revient à interdire complètement le traitement. Il existe toutefois une variante de cette idée, une « zone de prudence », où des exigences supplémentaires portant sur le fond ou sur la procédure sont imposées dans certains cas avant la collecte, l'utilisation ou la communication.

30, rue Victoria, 1er étage, Gatineau (Québec) K1A 1H3 • Sans frais : 1-800-282-1376 • Télécopieur : (819) 994-5424 • ATS : (819) 994-6591
www.priv.gc.ca • Suivez-nous sur Twitter : @priveeprivacy

i) « Zones interdites » véritables

Le paragraphe 5(3) de la LPRPDE, qui impose une limite globale s'appliquant à tout traitement, qu'il y ait consentement ou non, constitue une forme d'interdiction de traitement inapproprié. En limitant « à des fins qu'une personne raisonnable estimerait acceptables dans les circonstances » la collecte, l'utilisation et la communication de renseignements personnels par une organisation, ce paragraphe interdit tout traitement qui pourrait être jugé inapproprié dans un contexte donné.

Une organisation ne peut recueillir, utiliser ni communiquer des renseignements personnels si cette activité n'est pas conforme à la norme de pertinence, que l'intéressé ait donné son consentement ou non. Pour appliquer cette disposition, il faut établir une comparaison entre l'utilisation ou la communication proposée et les circonstances qui les entourent. La nature contextuelle du paragraphe 5(3) laisse place à une certaine souplesse pour ce qui est de faire obstacle au traitement inapproprié de données. Par exemple, dans sa *Position de principe sur la publicité comportementale en ligne*[85], le Commissariat à la protection de la vie privée du Canada a imposé deux restrictions ou « zones interdites » en tant que pratiques exemplaires, à savoir : les organisations ne peuvent utiliser aucune méthode de suivi qu'un individu ne peut contrôler, par exemple l'empreinte de l'appareil; et elles devraient éviter de suivre des enfants et de faire du suivi sur des sites Web ciblant des enfants. La première restriction répondait à la nécessité de s'assurer que les utilisateurs étaient en mesure d'exercer un contrôle sur les technologies utilisées pour les suivre en ligne; la seconde, à la difficulté d'obtenir auprès des enfants un consentement éclairé à l'égard de ce type de pratiques. Le Commissariat a récemment constaté qu'un site Web qui republiait les décisions judiciaires sans supprimer les renseignements personnels et en permettant leur indexation par les moteurs de recherche contrevenait au paragraphe 5(3) de la LPRPDE. Dans ce dossier, il a conclu que l'objectif principal visé par l'organisation était d'inciter des personnes à payer pour faire supprimer leurs renseignements personnels du site Web. Or, il s'agit dans ce cas d'une fin que le Commissariat a jugé « inappropriée ».

On peut également établir des « zones interdites » par rapport à certains types de données, soit de façon générale ou relativement à des utilisations particulières de cette information. Par exemple, c'est ce que vise à faire le projet de loi S-201 en interdisant que la communication des résultats de tests génétiques constitue une condition requise pour fournir des biens et services ou conclure un contrat. Il est intéressant de se demander si, même en l'absence de la législation proposée, le principe 4.3.3 et le paragraphe 5(3) de la LPRPDE permettraient de limiter la collecte et l'utilisation des résultats de tests génétiques dans des circonstances similaires. Toutefois, comme ces dispositions de la LPRPDE sont de nature générale et laissent place à l'interprétation, l'adoption de zones d'interdiction précises et claires serait-elle souhaitable?

ii) « Zones de prudence »

La législation sur la protection de la vie privée prévoit parfois des mesures de protection procédurales renforcées à l'égard de certains types de renseignements et de traitement ou de groupes particulièrement vulnérables.

L'approche de la LPRPDE en ce qui a trait à la forme de consentement appropriée en est un bon exemple. En vertu de cette loi, la forme de consentement demandée par une organisation peut varier en fonction des circonstances et du type de renseignements. La sensibilité des renseignements et les attentes raisonnables de l'intéressé dans les circonstances sont deux facteurs pertinents dans cette évaluation. S'il s'agit de renseignements sensibles, un consentement exprès sera généralement exigé (par exemple dans le cas de renseignements médicaux ou financiers).

Le RGPD mise sur un renforcement des procédure de protection pour certains types de renseignements et de traitement particuliers. Dans le cas des types de renseignements sensibles (notamment ceux se rapportant à la race ou à l'origine ethnique, à la religion ou aux croyances), le traitement est interdit de façon générale, sous réserve de nombreuses exceptions, notamment si l'intéressé consent expressément au traitement de ses renseignements personnels. Le RGPD impose une interdiction similaire en ce qui a trait à la prise de décisions automatisée concernant des individus : une personne a le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage, si la décision pourrait avoir sur elle une incidence juridique ou similaire directe. Là encore, cette interdiction est imposée sous réserve de toute une gamme d'exceptions, dont le consentement exprès de l'intéressé.

Le *Consumer Privacy Bill of Rights Act* proposé aux États-Unis prévoit un système à plusieurs niveaux pour le traitement des renseignements personnels selon le principe de « prise en compte du contexte ». En vertu de ce projet de loi, si une organisation traite des renseignements personnels d'une manière qui n'est pas raisonnable compte tenu du contexte dans lequel ils ont été recueillis à l'origine, elle doit analyser les risques d'atteinte à la vie privée et prendre des mesures raisonnables pour atténuer ces risques le cas échéant. Elle doit notamment assurer « une transparence accrue et un contrôle renforcé par l'individu » à l'égard du traitement. Lorsque les organisations utilisent ou communiquent des données par des moyens prenant en compte le contexte, elles ont davantage tendance à déduire que l'intéressé a consenti au traitement. En revanche, si 'une utilisation ou une communication envisagée ne prend pas en compte le contexte, une transparence accrue et des mesures visant à faciliter le choix individuel s'imposeraient. Selon ce modèle, aucune restriction de fond n'est imposée à l'égard des fins auxquelles l'information peut être recueillie, utilisée ou communiquée. Le système à plusieurs niveaux a une incidence uniquement sur le degré de diligence raisonnable exigé concernant les procédures de l'organisation.

Les concepts inhérents au principe de « prise en compte du contexte » présentent certaines similitudes avec l'idée des « usages compatibles » évoquée dans la *Loi sur la protection des renseignements personnels* du Canada. Selon cette loi, un usage ou une communication compatible avec les fins auxquelles les renseignements ont été recueillis à l'origine ne requiert pas forcément le consentement de l'intéressé. La façon dont est défini le « contexte » initial ou l'« usage » initial constitue un élément clé pour l'emploi d'un concept ou de l'autre, car c'est ce qui déterminera l'éventail des utilisations qui peuvent être considérées comme conformes aux principes de prise en compte du contexte ou d'usages compatibles.

D'après le rapport de la Maison-Blanche intitulé *Big Data: Seizing Opportunities, Preserving Values*[86], si la réglementation était axée sur les *utilisations* raisonnables des données, on pourrait accorder plus d'attention à l'équilibre entre les avantages que présentent les utilisations des mégadonnées pour la société, d'une part, t les préjudices sur le plan de la vie privée d'un individu, d'autre part. Pour mettre en pratique cette théorie, on pourrait, par exemple, élaborer une taxonomie du traitement des données établissant une distinction entre les fins autorisées sans consentement, celles autorisées uniquement avec un consentement exprès et celles interdites en *toutes* circonstances. Cette approche semble combiner les procédures de protection à plusieurs niveaux pour différentes formes de traitement et une interdiction absolue de certaines utilisations ou communications.

30, rue Victoria, 1er étage, Gatineau (Québec) K1A 1H3 • Sans frais : 1-800-282-1376 • Télécopieur : (819) 994-5424 • ATS : (819) 994-6591
www.priv.gc.ca • Suivez-nous sur Twitter : @priveeprivacy

Questions pour alimenter la réflexion

1) Si le paragraphe 5(3) pouvait offrir la possibilité d'imposer de véritables interdictions, en quoi devraient-elles consister?

2) Le paragraphe 5(3) est-il suffisant ou avons-nous besoin d'autres règles concernant les « zones d'interdiction » pour la collecte, l'utilisation et la communication, comme celles portant sur les pratiques qui pourraient être discriminatoires ou les cas où il s'agit d'enfants?

3) En vertu de la LPRPDE, le contexte et la sensibilité aident à déterminer si l'on peut s'appuyer sur un consentement exprès ou implicite. Devrait-on adopter d'autres règles s'appliquant à certains types de renseignements ou d'utilisations?

c) Intérêts commerciaux légitimes

En vertu de la LPRPDE, un consentement valable est exigé pour recueillir et traiter des renseignements personnels, sous réserve d'exceptions limitées tenant compte du fait que certaines situations ne se prêtent pas au consentement individuel. L'idée selon laquelle l'obtention du consentement n'est pas toujours réaliste est reprise dans le nouveau cadre de l'Union européenne, qui prévoit plusieurs motifs légitimes pour le traitement des données tout en exigeant un consentement lorsqu'il s'agit de renseignements sensibles.

Les cas d'exception prévus par la LPRPDE pour lesquels il n'est pas nécessaire d'obtenir un consentement correspondent à plusieurs motifs donnant lieu à un traitement licite des données énoncés dans le nouveau cadre de l'Union européenne. Par exemple, l'Union européenne permet de traiter des renseignements lorsque c'est nécessaire pour respecter une obligation légale imposée au responsable du traitement, tandis que la LPRPDE autorise la collecte, l'utilisation ou la communication des renseignements personnels sans consentement si la loi l'exige.

Cependant, au sein de l'Union européenne, les intérêts légitimes constituent un motif valable pour traiter des renseignements sans le consentement de l'intéressé. Plus précisément, le traitement des données est licite s'il est nécessaire à la poursuite des « intérêts légitimes » du responsable du traitement ou d'un tiers, sauf si les droits fondamentaux de la personne concernée priment sur ces intérêts, en particulier s'il s'agit d'un enfant. Autrement dit, le traitement sans consentement est licite, mais il faut soupeser les intérêts de l'organisation et ceux de l'individu. Cette mise en balance peut s'avérer un processus complexe qui prend en compte des facteurs tels que la nature des données, l'intérêt public et les attentes raisonnables de la personne concernée[87].

Compte tenu des défis associés au modèle de consentement dans l'environnement numérique, en particulier en ce qui concerne les mégadonnées et l'Internet des objets, y aurait-il lieu de revoir l'importance accordée par la LPRPDE au consentement dans les cas où l'on pourrait avoir recours à d'autres mécanismes pour atteindre un juste équilibre entre les besoins commerciaux de l'organisation et le droit de l'individu à la vie privée? On pourrait élargir l'éventail de motifs valables pour le traitement des données sans consentement prévus par la LPRPDE afin d'y ajouter les intérêts commerciaux légitimes, sous réserve de la mise en balance

des intérêts. La création de nouvelles exceptions sous le régime de la LPRPDE, qu'il faudrait définir, pourrait être une autre possibilité. Si l'on envisage cette avenue, d'autres cadres, par exemple la *Loi de 2004 sur la protection des renseignements personnels sur la santé* de l'Ontario, pourraient aider à déterminer les conditions à respecter avant de traiter des renseignements personnels sans le consentement de l'intéressé. Ces conditions préalables s'inscrivent dans le contexte de la recherche sur la santé et de l'intérêt public, mais elles peuvent tout de même offrir une piste à suivre.

Questions pour alimenter la réflexion

1) En l'absence de consentement, quels motifs de traitement licite pourraient justifier l'autorisation de la collecte, de l'utilisation et de la communication de renseignements personnels?

2) Comment peut-on s'assurer que les organisations évaluent de façon équitable et éthique les motifs de traitement licite dans le but d'atteindre un juste équilibre?

3) Quel serait le rôle des organismes de réglementation dans l'évaluation des motifs de traitement licite?

3) Gouvernance

Dans la présente section, nous présentons des solutions possibles reposant sur la reddition de comptes pour assurer de solides mesures de protection de la vie privée. Certaines solutions proposées renforcent le consentement, d'autres le remplacent et d'autres encore peuvent s'inscrire dans un cadre d'autoréglementation.

En vertu du principe de responsabilité énoncé dans la LPRPDE, les organisations doivent élaborer et mettre en œuvre des politiques et des pratiques qui respectent les principes relatifs aux pratiques équitables de traitement de l'information, y compris l'obligation d'obtenir un consentement valable. Prises dans leur ensemble, ces politiques et ces pratiques constituent un programme de gestion de la protection de la vie privée. Les lignes directrices[88] publiées par le Commissariat à la protection de la vie privée du Canada en collaboration avec les commissariats de la Colombie-Britannique et de l'Alberta présentent les éléments essentiels de ce programme.

Un programme de gestion de la protection de la vie privée à l'interne constitue un bon point de départ pour une organisation. Toutefois, il faut adopter une approche plus transparente et tangible pour donner aux Canadiens l'assurance que les organisations s'en tiennent aux pratiques responsables qu'elles affirment avoir ou qu'elles sont tenues d'avoir en matière de gestion des renseignements personnels. L'obligation de faire preuve de responsabilité gagne du terrain dans d'autres pays, notamment au sein de l'Union européenne, où le RGPD exigera que les organisations démontrent qu'elles se

30, rue Victoria, 1er étage, Gatineau (Québec) K1A 1H3 • Sans frais : 1-800-282-1376 • Télécopieur : (819) 994-5424 • ATS : (819) 994-6591
www.priv.gc.ca • Suivez-nous sur Twitter : @priveeprivacy

conforment à la loi. On trouvera ci-après quelques exemples d'applications pratiques d'approches fondées sur la reddition de comptes qui peuvent aider à mettre sur un pied d'égalité les organisations et les particuliers lorsqu'il s'agit de demander ou de fournir un consentement valable à l'égard de pratiques commerciales complexes.

a) Codes de pratiques

Les codes de pratiques sont des outils d'usage courant qui donnent une orientation concrète concernant les pratiques exemplaires de l'industrie pour toute une gamme d'activités, y compris la conformité à la réglementation. Dans le domaine de la protection de la vie privée, ils peuvent aider à promouvoir la transparence et l'ouverture quant à la façon dont les organisations s'y prennent pour respecter les obligations en la matière. Partout dans le monde, plusieurs autorités de protection des données et organisations du secteur privé ont participé à l'élaboration de codes de pratiques qui cadrent avec les exigences des principes ou des lois sur la protection des données. Selon la législation en vigueur, il peut s'agir de pratiques exemplaires élaborées par l'industrie sur une base volontaire ou par les autorités de protection des données pour servir d'outil d'application.

Par exemple, au Royaume-Uni, le commissaire à l'information peut encourager ou amorcer lui-même l'élaboration de codes de pratiques après avoir consulté l'industrie et le public. En Australie, les agences d'évaluation du crédit peuvent élaborer des codes de pratiques que le commissaire homologuera par la suite. Le commissaire peut faire enquête en cas d'infraction à un code de pratiques homologué.

Aux États-Unis, le *Consumer Privacy Bill of Rights Act* proposé par la Maison-Blanche fait valoir l'idée d'adopter de codes de conduite contraignants pour des marchés ou des contextes commerciaux particuliers. Les consommateurs auraient ainsi accès à des mesures de protection de la vie privée uniformes grâce à la normalisation des pratiques dans le domaine au sein des secteurs.

Au Canada, en vertu de l'alinéa 24(*c*) de la LPRPDE, le Commissariat à la protection de la vie privée encourage les organisations à élaborer des instruments, par exemple des politiques et des codes de pratiques, en accord avec les exigences de cette loi. Toutefois, nous n'avons pas encore exploré pleinement cette disposition. Lorsqu'il s'agit du consentement, certains pourraient faire valoir que les codes de pratiques dans des secteurs particuliers pourraient apporter une prévisibilité et une uniformité supplémentaires pour aider les entreprises à comprendre leurs obligations concernant le consentement valable ainsi que les limites appropriées touchant le traitement des données. Mais on peut aussi soutenir que ces codes indiqueraient plus clairement aux individus que leurs renseignements personnels sont traités de manière transparente et équitable conformément à leurs attentes.

Questions pour alimenter la réflexion

1) Des codes de pratiques sectoriels pourraient-ils renforcer efficacement le consentement ou la protection de la vie privée?

2) Comment ces codes de pratiques devraient-ils être appliqués?

3) Qui devrait participer à l'élaboration des codes de pratiques sectoriels? Qui devrait être chargé de surveiller la conformité à ces codes?

b) Marques de confiance garantissant la protection de la vie privée

À l'instar des codes de pratiques, les sceaux garantissant la protection de la vie privée pourraient s'avérer utiles pour aider les organisations à assurer la conformité aux lois sur la protection des renseignements personnels et à faire la preuve de leur détermination à protéger la vie privée. Comme pour les codes de pratiques, les organismes de réglementation de la protection de la vie privée ou les organisations elles-mêmes peuvent se charger des activités s'y rattachant, selon le pays.

En France, la Commission nationale de l'informatique et des libertés (CNIL) exploite un programme de sceaux de garantie pour les entreprises qui se conforment à sa norme en ce qui a trait à la responsabilité en matière de protection de la vie privée dans la pratique. Au Royaume-Uni, le Commissariat à l'information a récemment mis en place un programme de sceaux garantissant la protection de la vie privée[89]. Il accréditera des tiers pour mettre le programme en œuvre et en assurer la gestion au quotidien.

TRUSTe est l'un des programmes de sceaux garantissant la protection de la vie privée les mieux connus. Ce programme américain en vigueur depuis 1997 certifie principalement des sites Web. En Europe, EuroPriSe offre une certification à des fabricants et à des fournisseurs de produits et de services de TI. Le Sceau européen de protection de la vie privée certifie que [traduction] « le traitement des données issues des interactions d'un serveur Web et du navigateur d'un utilisateur est conforme aux lois européennes sur la protection des données[90] ».

Le Système de règles transfrontalières de protection de la vie privée de la Coopération économique Asie-Pacifique (APEC) est un autre exemple d'un mécanisme dans le cadre duquel des agents tiers sont chargés de certifier la conformité aux normes de protection de la vie privée. Ce système prévoit le recours à des agents chargés de la reddition de comptes pour s'assurer que les entreprises participantes se conforment aux normes de sécurité et de protection de la vie privée imposées en vertu du cadre de protection de la vie privée de l'APEC[91].

Pour qu'un programme de sceaux de garantie fonctionne de façon efficace au Canada, il faudrait mettre en place un mécanisme objectif pour évaluer la conformité aux exigences des lois sur la protection des renseignements personnels ainsi qu'une fonction de vérification indépendante pour assurer le maintien de la conformité du programme aux normes. Si l'on envisageait d'introduire des sceaux de garantie dans un cadre de réglementation, il faudrait évaluer la pertinence de modifier de la LPRPDE, y compris en ce qui a trait au rôle du Commissariat à la protection de la vie privée.

Questions pour alimenter la réflexion

1) Dans quelles circonstances les marques de confiance constituent-elles un outil adaptable et fiable pour protéger la vie privée des consommateurs dans l'environnement numérique en pleine évolution?

2) Comment un programme de sceaux de garantie fonctionnerait-il en parallèle avec la LPRPDE?

30, rue Victoria, 1er étage, Gatineau (Québec) K1A 1H3 • Sans frais : 1-800-282-1376 • Télécopieur : (819) 994-5424 • ATS : (819) 994-6591
www.priv.gc.ca • Suivez-nous sur Twitter : @priveeprivacy

c) Évaluations éthiques

Dans le contexte des mégadonnées et de données similaires, plusieurs initiatives en cours visent à s'ajouter au modèle de consentement ou à le remplacer. Ces initiatives intègrent les notions d'équité et d'éthique dans le cadre de la réflexion en vue de trouver un juste équilibre entre la nécessité pour l'organisation de traiter des renseignements à des fins commerciales légitimes et le droit des individus à la vie privée. En fin de compte, dans ces initiatives, le fardeau repose sur les organisations qui doivent se prononcer sur les avantages et les risques associés au traitement des données pour l'organisation, l'individu et la société en général.

i) Centre for Information Policy Leadership

Pour protéger la vie privée à l'ère des mégadonnées, le Centre for Information Policy Leadership (CIPL) élabore actuellement une approche qui met l'accent sur le renforcement de la reddition de comptes, l'amélioration de la gestion du risque et une nouvelle interprétation des principes et concepts de base de la protection de la vie privée. Dans une série de livres blancs[92], cet organisme américain indique que les organisations devraient renforcer la reddition de comptes pour intervenir dans les contextes où [traduction] « le consentement exprès et le contrôle granulaire exercé par les individus à l'égard d'activités particulières de traitement de données ne sont pas possibles ». Le modèle de reddition de comptes renforcé intégrerait davantage de transparence et une gestion du risque plus poussée ainsi que la mise en pratique d'un traitement équitable et d'une éthique des données. Le but est de disposer d'un cadre pour protéger la vie privée [traduction] « en exigeant un consentement éclairé lorsque c'est possible et approprié et par d'autres mécanismes lorsque c'est nécessaire et pertinent [93] ».

Pour ce qui est d'améliorer la gestion du risque, le CIPL préconise l'élaboration et l'intégration d'un cadre des atteintes à la vie privée et d'autres préjudices et d'un cadre pour analyser les avantages découlant du traitement des données ainsi que la reconnaissance de la gestion du risque en tant que pilier des concepts et outils de protection des données. En particulier, d'après le CIPL, une meilleure gestion du risque renforcera l'efficacité des outils de traitement des intérêts légitimes, de traitement équitable et de transparence et remettra au premier plan le contexte et l'utilisation des données[94].

ii) Future of Privacy Forum

Les travaux du Future of Privacy Forum (FPF) portant sur le remplacement du modèle de consentement par un modèle axé sur l'utilisation nous donnent un exemple d'un modèle de reddition de comptes de prochaine génération qui propose de remplacer le consentement lorsque la situation s'y prête. Le livre blanc sur les mégadonnées[95] publié en 2014 par le FPF offre un cadre pour aider les organisations à évaluer les mérites des projets qui font appel à des mégadonnées en prenant en compte les intérêts des organisations et ceux des particuliers et en permettant aux organisations de soupeser les avantages des mégadonnées par rapport aux risques d'atteinte à la vie privée.

iii) Information Accountability Foundation

L'Information Accountability Foundation (IAF) travaille sur des approches en matière de protection des données à l'ère des mégadonnées. Elle mène une série de projets interreliés qui visent à élaborer des solutions à des questions telles que l'évaluation de l'équité des utilisations novatrices des données ainsi que la détection et l'atténuation des risques pour les individus. Le cadre éthique intégré[96] de cet organisme offre une démarche afin de déterminer dans une perspective éthique si un projet d'analyse de mégadonnées est approprié. On s'appuiera à cette fin sur les valeurs de base en matière de protection des données pour prendre en compte les droits fondamentaux.

Le projet de gouvernance holistique de l'IAF vise à améliorer l'efficacité globale de la protection des données grâce à une meilleure harmonisation des responsabilités des participants dans la circulation de l'information. Par exemple, les gens seraient appelés à donner leur consentement uniquement lorsque celui-ci prend tout son sens, mais non dans le cas contraire, par exemple lorsqu'une nouvelle utilisation est compatible avec les fins précisées à l'origine. Les organisations élargiraient la portée de l'évaluation du risque, de la transparence et de la reddition de comptes afin que les organismes de réglementation soient mieux informés des pratiques commerciales[97]. D'après l'IAF, le projet de gouvernance holistique reconnaît que la collecte et l'utilisation des données devraient s'inscrire dans une structure de gouvernance efficace.

Au Canada, l'IAF travaille à un projet de gouvernance ayant une double finalité : appliquer des mécanismes de protection de la vie privée lorsque l'obtention du consentement n'est pas réaliste et explorer des façons de créer efficacement un mécanisme qui fonctionnerait de manière similaire aux intérêts légitimes pour utiliser les données dans les situations où leur utilisation va au-delà des attentes d'une personne raisonnable[98].

Les travaux du CIPL, du FPF et de l'IAF soulèvent une question : Qui déterminera si les utilisations des données sont éthiques, équitables ou appropriées et, dans un contexte canadien, si ces solutions obligeront à modifier le cadre législatif? En ce qui a trait au premier volet de la question, on pourrait regarder ce qui se fait dans le milieu de la recherche scientifique, qui a été le premier à créer des comités d'éthique indépendants pour examiner les projets de recherche proposés sous l'angle de leurs répercussions sur le plan éthique. Ces comités soupèsent les avantages éventuels de la recherche par rapport aux risques pour les participants. Des universitaires et des entreprises ont récemment commencé à se demander si l'on n'aurait pas besoin d'un mécanisme équivalent pour guider les organisations commerciales qui veulent exploiter des mégadonnées afin d'étudier le comportement des consommateurs. Le concept de comités d'éthique assurant la protection des consommateurs a été proposé. Ces comités joueraient un rôle consultatif auprès des entreprises pour les aider à évaluer les répercussions globales de l'utilisation des renseignements personnels, en particulier dans un environnement de mégadonnées.

Pour certains observateurs, on devra dès lors déterminer s'il est pertinent que les organisations, même avec les avis de comités d'éthique, soient autorisées à décider comment utiliser les renseignements personnels d'individus, en particulier si ces comités ne sont pas vraiment indépendants ou n'ont pas de droit de veto véritable. Ces observateurs voudront savoir comment on peut protéger les droits des individus et par quels autres mécanismes on peut atteindre le juste équilibre exigé en vertu de la LPRPDE. Il est important de comprendre plus clairement ce qu'il pourrait advenir du rôle du consentement selon ces propositions et comment elles cadrent avec les dispositions existantes de la LPRPDE.

Les partisans de cette solution expliquent leurs propositions en les présentant comme un mécanisme qui s'ajoute au consentement, le remplace ou permet d'atteindre un équilibre entre la nécessité pour l'organisation de traiter des renseignements personnels à des fins légitimes et le droit des individus à la vie privée. Chacune de ces propositions aurait des répercussions différentes sur le plan de la LPRPDE, selon la façon dont elle serait mise en pratique.

30, rue Victoria, 1er étage, Gatineau (Québec) K1A 1H3 • Sans frais : 1-800-282-1376 • Télécopieur : (819) 994-5424 • ATS : (819) 994-6591
www.priv.gc.ca • Suivez-nous sur Twitter : @priveeprivacy

Questions pour alimenter la réflexion

1) Dans quelle mesure les mesures proposées par le CIPL, le FPF et l'IAF sont-elles utiles et réalistes pour évaluer sur le plan éthique les utilisations des données?

2) Dans quelle mesure peut-on s'attendre à ce que les entreprises s'auto-réglementent d'une manière qui protège la vie privée des individus en cette nouvelle ère numérique?

3) Comment devrait-on créer et financer ces comités d'éthique et en déterminer la composition? De qui devraient-ils relever et quel devrait être leur pouvoir décisionnel?

4) Modèles d'application

Les solutions fondées sur la reddition de comptes mentionnées dans le présent rapport s'en remettent aux organisations pour l'élaboration et la mise en œuvre de mesures qui permettent de respecter leurs obligations en matière de protection de la vie privée, notamment l'obtention d'un consentement valable. Or, l'objet de la LPRPDE consiste à assurer un juste équilibre entre le droit des individus à la vie privée et la nécessité légitime pour les organisations de recueillir, d'utiliser et de communiquer des renseignements personnels. Les propositions de cadre éthique analysées ci-dessus comportent des avantages, mais le processus reste au sein de l'organisation et les intérêts de cette dernière demeurent prépondérants. Des organismes de surveillance indépendants sont nécessaires pour assurer le maintien de cet équilibre de manière à protéger les intérêts des individus au chapitre de la protection de leur vie privée. Ce type de surveillance indépendante peut s'avérer encore plus incontournable lorsque l'obtention du consentement n'est pas réaliste et que les organisations jouent un rôle accru lorsqu'il s'agit de déterminer les utilisations des renseignements personnels qui peuvent être autorisées.

Pour que le Commissariat soit un organisme de surveillance vraiment efficace et apte à protéger le droit des individus à la vie privée, quels doivent être ses pouvoirs et ses fonctions en plus d'être habilité à intervenir en toute indépendance? Il pourrait être utile d'envisager une activité d'application de la loi proactive (dans le cadre du modèle réglementaire en place ou avec l'aide d'un tiers), qui s'ajouterait à l'application fondée sur les plaintes à laquelle on a généralement recours selon le modèle actuel. Par exemple, si l'on envisage d'autoriser certains types d'utilisation ou de communication par des mécanismes autres que le consentement (p. ex. en s'appuyant sur un intérêt commercial légitime, en s'en remettant à la « prise en compte du contexte » ou en utilisant un outil technique comme la désidentification) ou de les juger illicites en raison de l'instauration d'une « zone interdite », ces solutions de remplacement du consentement pourraient obliger les organisations à faire la preuve de leur conformité. Elles pourraient aussi justifier des mesures d'application ou des interventions moins musclées de la part de l'organisme de réglementation à une étape en amont dans le processus par rapport à celles actuellement en vigueur (p. ex. des vérifications de la conformité ou des contrôles ponctuels). Cela dit, la mise en œuvre d'un modèle de conformité proactif ne devrait pas imposer

aux organisations un fardeau réglementaire et, si les règles sont respectées, elle pourrait amener les organisations à éviter les coûts élevés qui découleraient du lancement d'un programme non conforme ou de la tenue d'une enquête officielle. Il faudrait également s'abstenir d'imposer aux organisations un fardeau supplémentaire au chapitre des ressources.

Pour améliorer les choses de façon appréciable, les mécanismes de transparence analysés dans le présent rapport doivent être mis en œuvre à grande échelle. Comme les pratiques des organisations en matière de protection de la vie privée demeurent difficiles à comprendre pour les individus, quels sont les éléments qui inciteraient les organisations à investir dans la transparence? Les conséquences de la non-conformité à la LPRPDE devraient-elles être plus sévères que la capacité de « montrer du doigt » les organisations fautives? Les sanctions pécuniaires constituent un moyen de s'assurer que les organisations fassent preuve d'une responsabilité accrue lorsqu'il s'agit d'informer les individus de ce qu'elles ont l'intention de faire de leurs renseignements personnels. Dans certains pays de l'Union européenne, les lois sur la protection des données permettent d'imposer des amendes. D'ailleurs, le nouveau RGPD de l'Union européenne prévoit aussi ce mécanisme.

À l'heure actuelle, le commissaire à la protection de la vie privée du Canada doit se contenter de formuler des recommandations non contraignantes. Il n'a pas le pouvoir de rendre des ordonnances. À cet égard, sa situation est différente de celle de ses homologues des provinces dotées de lois essentiellement similaires à la loi fédérale ou des organismes de réglementation de l'Union européenne et des États-Unis, lesquels sont habilités à rendre des ordonnances. Dans un rapport[99] publié en 2010, les professeurs Houle et Sossin ont examiné en profondeur la question du renforcement des pouvoirs du commissaire à la protection de la vie privée sous le régime de la LPRPDE. Ces spécialistes ont constaté que les commissaires provinciaux investis de ce pouvoir l'utilisent avec parcimonie, préférant s'en remettre à la médiation, à la conciliation et à d'autres mécanismes informels pour régler les plaintes. Néanmoins, ils estiment que le pouvoir de rendre des ordonnances constitue un bon incitatif qui peut amener les parties à en arriver à un règlement raisonnable. D'après les professeurs Houle et Sossin, « en se fiant à l'expérience des organismes de réglementation provinciaux du Canada ainsi qu'à l'expérience américaine et européenne, la capacité d'imposer une amende et autres possibilités de rendre des ordonnances peuvent entraîner une conformité supplémentaire et constituer un important élément dissuasif malgré un emploi peu fréquent. »

Question pour alimenter la réflexion

1) Quels pouvoirs supplémentaires, le cas échéant, devrait-on conférer au Commissariat à la protection de la vie privée du Canada en matière de surveillance de la conformité et d'application de règles nouvelles ou renforcées régissant le consentement?

Conclusion

Il est fort difficile de déterminer et de mettre en œuvre des mécanismes à l'appui du modèle de consentement dans le contexte des mégadonnées, de l'Internet des objets et des défis futurs sur le front de la protection de la vie privée. Il faut pour ce faire adopter une approche qui est systémique et qui fait appel à toute une batterie de solutions stratégiques, techniques, réglementaires et législatives.

En nous attaquant à la question du consentement, nous voulons trouver des solutions qui allégeront le fardeau des individus pour ce qui est de comprendre des processus opérationnels complexes, et qui mettront à leur disposition un moyen plus efficace pour faire valoir leurs préférences dans le domaine. Le consentement

30, rue Victoria, 1er étage, Gatineau (Québec) K1A 1H3 • Sans frais : 1-800-282-1376 • Télécopieur : (819) 994-5424 • ATS : (819) 994-6591
www.priv.gc.ca • Suivez-nous sur Twitter : @priveeprivacy

demeure un moyen important pour aider les individus à exercer un contrôle sur leurs renseignements personnels et, de façon plus générale, pour conserver leur dignité et leur autonomie. Toutefois, il nous faut aussi reconnaître que, en raison de l'environnement technologique actuel et futur, il est de plus en plus difficile de demander et de donner un consentement éclairé. Dans ce contexte, la solution consiste-t-elle uniquement à offrir aux individus une information et des mécanismes améliorés leur permettant de faire des choix éclairés ou devons-nous trouver d'autres façons de protéger leurs intérêts?

Les organisations se heurtent aussi à des défis pour ce qui est d'obtenir auprès des individus le consentement valable exigé. Dans leur quête d'innovation, les organisations bénéficieraient d'une plus grande clarté quant aux fins acceptables du traitement des renseignements personnels en l'absence d'un consentement exprès et de mécanismes internes qui les aideraient à trouver le juste équilibre entre les avantages pour l'organisation et les risques d'atteinte à la vie privée des individus. Avec ce type de mécanismes, la difficulté consiste à s'assurer que l'on évalue en toute indépendance les risques d'atteinte à la vie privée et que l'on protège les intérêts des individus.

En recherchant des solutions, nous devons veiller à ce qu'un juste équilibre soit atteint. Il faut examiner périodiquement le rôle et les responsabilités de l'organisme de réglementation ainsi que le cadre global de protection de la vie privée pour s'assurer qu'ils sont en phase avec le nouvel environnement. Faut-il modifier la législation afin de renforcer les efforts déployés par l'organisme de réglementation pour demander des comptes aux organisations et représenter adéquatement les individus? Quel devrait être le rôle des codes de pratiques sectoriels, des marques de confiance et des certificateurs tiers dans un régime de conformité efficace?

Questions aux fins de consultation

Nous invitons les intervenants à participer à la discussion en exprimant leur opinion sur la viabilité du modèle de consentement et à proposer des solutions pour améliorer le contrôle exercé par les individus sur leurs renseignements personnels dans l'environnement commercial. Nous aimerions connaître leur opinion sur tous les sujets se rapportant au consentement, mais nous nous intéressons tout particulièrement à leurs réponses aux questions posés plus tôt ainsi qu'aux questions suivantes :

1) Parmi les solutions proposées dans le présent rapport, lesquelles présentent selon vous le plus d'avantages? Veuillez expliquer pourquoi.

2) Avez-vous d'autres solutions à proposer pour relever les défis associés au consentement? Veuillez expliquer.

3) Quels rôle, responsabilités et pouvoirs devrait-on attribuer aux parties chargées de promouvoir l'élaboration et l'adoption de solutions pour mettre en place le système le plus efficace possible?

4) Le cas échéant, quelles modifications devrait-on apporter à la législation?

[1] *Loi sur la protection des renseignements personnels et les documents électroniques* (L.C. 2000, ch. 5), http://laws-lois.justice.gc.ca/fra/lois/P-8.6/index.html.

[2] Fred H. Cate, Peter Cullen et Victor Mayer-Schönberger. *Data Protection Principles for the 21st Century: Revising the 1980 OECD Guidelines,* mars 2014, http://www.repository.law.indiana.edu/facbooks/23/. Voir aussi Éloïse Gratton, *Understanding Personal Information: Managing Privacy Risks*, LexisNexis, 2013, qui préconise une approche axée sur le *risque de préjudice,* ce qui réduirait le fardeau de l'obligation de signaler les atteintes (et, parallèlement, l'obligation de consentement).

[3] Center for Information Policy Leadership. *The Role of Enhanced Accountability in Creating a Sustainable Data-driven Economy and Information Society,* document de discussion, 21 octobre 2015.

[4] Ann Cavoukian, Alexander Dix et Khaled El Emam. *The Unintended Consequences of Privacy Paternalism*, 5 mars 2014, https://www.privacybydesign.ca/index.php/paternalistic-approach-privacy-will-deliver-unintended-consequences/. M^me^ Cavoukian, ancienne commissaire à l'information et à la protection de la vie privée de l'Ontario, est actuellement directrice générale du Privacy and Big Data Institute à l'Université Ryerson.

[5] Alan F. Westin. *Privacy and Freedom*, New York, Atheneum, 1967, p. 33.

[6] Ministère des Communications et ministère de la Justice. *L'ordinateur et la vie privée*, 1972. p. 14.

[7] *R. c. Dyment*, [1988] 2 RCS 417, par. 17, https://scc-csc.lexum.com/scc-csc/scc-csc/fr/item/375/index.do.

[8] Stephanie Perrin, Heather H. Black, David H. Flaherty et T. Murray Rankin. *The Personal Information Protection and Electronic Documents Act*: *An annotated guide*, Irwin Law, 2001, p. 23.

[9] *Information and Privacy Commissioner of Alberta c. Travailleurs et travailleuses unis de l'alimentation et du commerce, section locale 401,* [2013] RCS 62, par. 22, https://scc-csc.lexum.com/scc-csc/scc-csc/fr/item/13334/index.do.

[10] Article 3 de la LPRPDE.

[11] Article 6.1 de la LPRPDE.

[12] Lisa M. Austin. « Is Consent the Foundation of Fair Information Practices? Canada's Experience under PIPEDA », University of Toronto Legal Studies Series, rapport de recherche n^o^ 11-05, novembre 2005, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=864364

[13] Philippa Lawson et Mary O'Donoghue. « Approaches to consent in Canadian data protection Law », dans *Lessons from the identity trail,* 2009, http://www.idtrail.org/files/ID%20Trail%20Book/9780195372472_kerr_02.pdf.

[14] La sensibilité des renseignements varie en fonction de leur nature et du contexte dans lequel ils sont recueillis, utilisés ou communiqués.

[15] Commissariat à la protection de la vie privée du Canada. *Bulletin d'interprétation : Forme de consentement,* https://www.priv.gc.ca/leg_c/interpretations_07_consent_f.asp.

[16] Groupe de travail « Article 29 » sur la protection des données. *Avis 15/2011 sur la définition du consentement,* 13 juillet 2011, http://www.cnpd.public.lu/fr/publications/groupe-art29/wp187_fr.pdf.

[17] Article 6 de la directive 95/46/CE du Parlement européen et du Conseil.

[18] *Règlement général sur la protection des données.* Voir article 6 et points 38, 56 et 57 du préambule.

[19] US Code, Title 15, Subchapter 1, Federal Trade Commission, texte intégral en ligne, https://www.law.cornell.edu/uscode/text/15/chapter-2/subchapter-I.

[20] US Code, Title 15, Chapter 91, Children's Online Privacy Protection, texte intégral en ligne, https://www.law.cornell.edu/uscode/text/15/chapter-91.

[21] 37^e^ Conférence internationale des commissaires à la protection des données et de la vie privée. *Privacy Bridges: EU and US privacy experts in search of transatlantic privacy solutions*, Amsterdam, 2015, https://privacybridges.mit.edu/sites/default/files/documents/PrivacyBridges-FINAL.pdf.

[22] Federal Trade Commission. *Protecting consumer privacy in an era of rapid change: Recommendations for Businesses and Policymakers*, mars 2012, https://www.ftc.gov/reports/protecting-consumer-privacy-era-rapid-change-recommendations-businesses-policymakers.

30, rue Victoria, 1er étage, Gatineau (Québec) K1A 1H3 • Sans frais : 1-800-282-1376 • Télécopieur : (819) 994-5424 • ATS : (819) 994-6591
www.priv.gc.ca • Suivez-nous sur Twitter : @priveeprivacy

[23] The White House. *Consumer Data Privacy In a Networked World: A Framework for protecting privacy and promoting innovation in the global digital economy*, février 2012, https://www.whitehouse.gov/sites/default/files/privacy-final.pdf.
[24] *Ibid.,* p. 1.
[25] *Administration Discussion Draft: Consumer Privacy Bill of Rights Act of 2015, t*exte intégral en ligne, https://www.whitehouse.gov/sites/default/files/omb/legislative/letters/cpbr-act-of-2015-discussion-draft.pdf.
[26] Voir, par exemple, l'article affiché en ligne par le Centre for Democracy and Technology, « Analysis of the Consumer Privacy Bill of Rights Act », 2 mars 2015, https://cdt.org/insight/analysis-of-the-consumer-privacy-bill-of-rights-act/.
[27] Commissariat à la protection de la vie privée du Canada. *L'ère de l'analyse prédictive : des tendances aux prédictions,* août 2012, https://www.priv.gc.ca/information/research-recherche/2012/pa_201208_f.pdf.
[28] Commissariat à la protection de la vie privée du Canada. *L'Internet des objets : Introduction aux enjeux relatifs à la protection de la vie privée dans le commerce de détail et à la maison,* février 2016, https://www.priv.gc.ca/information/research-recherche/2016/iot_201602_f.asp
[29] Danielle Keats Citron et Frank Pasquale. « The Scored Society: Due Process for Automated Predictions », University of Maryland Francis King Carey School of Law, Legal Studies Research Paper n° 2014-8, *Washington Law Review*, vol. 89, no 1, 2014.
[30] The White House. *Big Data: Seizing Opportunities, Preserving Values*, mai 2014, https://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf.
[31] Latanya Sweeney. *Discrimination in Online Ad Delivery*, Université Harvard, 28 janvier 2013, http://arxiv.org/ftp/arxiv/papers/1301/1301.6822.pdf.
[32] Federal Trade Commission. *Big Data: A toll for Inclusion or Exclusion?*, janvier 2016, https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf.
[33] Paul Ohm. « Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization », *UCLA Law Review*, vol. 57, 2010, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1450006.
[34]Kate Crawford et Jason Schultz. *Using Procedural Due Process to Redress Big Data's Privacy Harms*, New York University School of Law, octobre 2013.
[35] Voir Ira Rubinstein et Woodrow Hartzog, « Anonymisation and Risk » (17 août 2015), *Washington Law Review*, vol. 91, n° 2, 2016; Éloïse Gratton, « If Personal Information is Privacy's Gatekeeper, then Risk of Harm is the Key: A proposed method for determining what counts as personal information », *Albany Law Journal of Science & Technology*, vol. 24, n° 1, 2013; Paul Schwartz et Daniel Solove, « The PII Problem: Privacy and a New Concept of Personally Identifiable Information », *N.Y.U. Law Review,* vol. 86, 2011, p. 1814.
[36] Fred H. Cate et Viktor Mayer-Schönberger. *Notice and Consent in a World of Big Data: Microsoft Global Summit Summary Report and Outcomes*, novembre 2012, http://www.microsoft.com/en-ca/download/confirmation.aspx?id=35596.
[37] 36e Conférence internationale des commissaires à la protection des données et de la vie privée. *Résolution sur les mégadonnées,* octobre 2014, https://icdppc.org/wp-content/uploads/2015/02/Resolution-on-Big-Data-French.pdf.
[38] *Ibid*.
[39] Commissariat à la protection de la vie privée du Canada. *L'ère de l'analyse prédictive : des tendances aux prédictions*, août 2012, https://www.priv.gc.ca/information/research-recherche/2012/pa_201208_f.pdf.
[40] Groupe de travail « Article 29 » sur la protection des données. *Opinion 8/2014 on the Recent Developments on the Internet of Things*, 16 septembre 2014, http://www.privacyconference2014.org/media/16602/Resolution-Big-Data.pdf.
[41] Commissariat à la protection de la vie privée du Canada. *L'Internet des objets : Introduction aux enjeux relatifs à la protection de la vie privée dans le commerce de détail et à la maison,*février 2016, https://www.priv.gc.ca/information/research-recherche/2016/iot_201602_f.asp
[42] Commissariat à la protection de la vie privée du Canada. *Ce qu'une adresse IP peut révéler à votre sujet,* mai 2013, https://www.priv.gc.ca/information/research-recherche/2013/ip_201305_f.asp.

[43] Commissariat à la protection de la vie privée du Canada. *Métadonnées et vie privée : Un aperçu technique et juridique,* https://www.priv.gc.ca/information/research-recherche/2014/md_201410_f.asp.

[44] Commissariat à la protection de la vie privée du Canada. *Position de principe sur la publicité comportementale en ligne,* https://www.priv.gc.ca/information/guide/2012/bg_ba_1206_f.asp.

[45] 36e Conférence internationale des commissaires à la protection des données et de la vie privée. *Mauritius Declaration on the Internet of Things*, 14 octobre 2014, http://privacyconference2014.org/media/16596/Mauritius-Declaration.pdf.

[46] BC Freedom of Information and Privacy Association. *The Connected Car: Who is in the driver's seat?,* 2015, https://fipa.bc.ca/connected-car-download/.

[47] Commissariat à la protection de la vie privée du Canada. *Les accessoires intelligents : Défis et possibilités pour la protection de la vie privée,* janvier 2014, https://www.priv.gc.ca/information/research-recherche/2014/wc_201401_f.pdf.

[48] Federal Trade Commission. *Internet of Things: Privacy & Security in a Connected World*, rapport à l'intention du personnel, janvier 2015, https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.

[49] Ian Kerr, Jennifer Barrigar, Jacquelyn Burkell et Katie Black. « Soft Surveillance, Hard Consent », dans *Lessons from the Identity Trail,* Oxford University Press, 2009, p. 21, http://idtrail.org/files/ID%20Trail%20Book/9780195372472_Kerr_01.pdf.

[50] PR Newswire. « According to a Study, Parents of Pre-Teens Don't Always Protect Their Children's Privacy Online », 1er avril 2015, http://news.sys-con.com/node/3319012.

[51]Columbia Business School Center on Global Brand Leadership. « What is the future of data sharing? », 2015, http://www8.gsb.columbia.edu/globalbrands/research/future-of-data-sharing.

[52] Alessandro Acquisti, Laura Brandimarte et George Loewenstein. « Privacy and human behavior in the age of information », *Science,* vol. 347, no 6221, 30 janvier 2015, p. 509-514. http://www.sciencemag.org/content/347/6221/509.abstract.

[53] Leslie John. « We say we want privacy online, but our actions say otherwise », *Harvard Business Review*, https://hbr.org/2015/10/we-say-we-want-privacy-online-but-our-actions-say-otherwise.

[54] Chris Jay Hoofnagle et Jennifer M. Urban. « Alan Westin's Privacy Homo Economicus », *The Wake Forest Law Review*, vol. 49, no 261, 19 mai 2014, p. 261-317, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2434800.

[55] Joseph Turow, Michael Hennessy et Nora Draper. «The Tradeoff Falacy: How Marketers Are Misrepresenting American Consumers And Opening Them up to Exploitation», Annenberg School for Communication, University of Pennsylvania, juin 2015, https://www.asc.upenn.edu/sites/default/files/TradeoffFallacy_1.pdf.

[56] Aleecia M. McDonald et Lorrie Faith Cranor. « The Cost of Reading Privacy Policies ». *I/O Journal of Law and Policy for the Information Society,* 2008, Privacy Year in Review Issue, http://aleecia.com/authors-drafts/readingPolicyCost-AV.pdf.

[57] Helen Nissenbaum. « A contextual approach to privacy online », *Dædalus, the Journal of the American Academy of Arts & Sciences,* 140 (4), automne 2011. http://www.amacad.org/publications/daedalus/11_fall_nissenbaum.pdf

[58] Commissariat à la protection de la vie privée du Canada. *Lignes directrices en matière de consentement en ligne,* https://www.priv.gc.ca/information/guide/2014/gl_oc_201405_f.asp. Voir aussi *Une occasion à saisir : Développer des applis mobiles dans le respect du droit à la vie privée,* https://www.priv.gc.ca/information/pub/gd_app_201210_f.asp.

[59] Maria Popova. « Mozilla's Privacy Icons: A Visual Language for Data Rights », BigThink.com, http://bigthink.com/design-for-good/mozillas-privacy-icons-a-visual-language-for-data-rights

[60] Conseil des consommateurs du Canada. « Canadian Businesses and Consumers Both Face Risk from Poorly Understood Terms and Conditions Statements», octobre 2015 http://www.consumerscouncil.com/improving-online-agreements-release.

[61] The White House. *Big Data and Privacy: A Technological Perspective*, mai 2014, https://www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf.

[62] Forum économique mondial. *Unlocking the Value of Personal Data: From Collection to Usage*, http://www3.weforum.org/docs/WEF_IT_UnlockingValuePersonalData_CollectionUsage_Report_2013.pdf.

[63] Siani Pearson et Marco Casassa Mont. « Sticky Policies: An Approach for Managing Privacy across Multiple Parties », *Computer*, vol. 44, n° 9, septembre 2011, p. 60-68.
[64] Groupe de travail « Article 29 » sur la protection des données. *Opinion 8/2014 on the Recent Developments on the Internet of Things*, 16 septembre 2014, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp223_en.pdf.
[65] Federal Trade Commission. *Internet of Things: Privacy & Security in a Connected World*¸ rapport à l'intention du personnel, janvier 2015, https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf.
[66] L'Online Trust Alliance est un groupe industriel sans lucratif qui compte parmi ses membres Microsoft, Symantec, ADT et TRUSTe.
[67] Online Trust Alliance. *OTA releases new Internet of Things Trust Network to Address Global Consumer Concerns*, 28 octobre 2015, https://otalliance.org/news-events/press-releases/ota-releases-new-internet-things-trust-framework-address-global-consumer.
[68] Pour en savoir plus, consultez https://www.privacybydesign.ca/.
[69] 32e Conférence internationale des commissaires à la protection des données et de la vie privée. *Resolution on Privacy by Design*, octobre 2010, https://icdppc.org/wp-content/uploads/2015/02/32-Conference-Israel-resolution-on-Privacy-by-Design.pdf.
[70] 36e Conférence internationale des commissaires à la protection des données et de la vie privée. *Résolution sur les mégadonnées,* octobre 2014, https://icdppc.org/wp-content/uploads/2015/02/Resolution-on-Big-Data-French.pdf.
[71] Federal Trade Commission. *Protecting Consumer Privacy in an Era of Rapid Change*, 2012, https://www.ftc.gov/reports/protecting-consumer-privacy-era-rapid-change-recommendations-businesses-policymakers.
[72] Agence européenne chargée de la sécurité des réseaux et de l'information. *Privacy and Data protection by Design,* 12 janvier 2015, https://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/privacy-and-data-protection-by-design.
[73] Information Commissioner's Office du Royaume-Uni. *Anonymization: managing data protection risk code of practice*, https://ico.org.uk/media/for-organisations/documents/1061/anonymisation-code.pdf.
[74] Organisation internationale de normalisation. *« Pseudonymisation – nouvelle spécification ISO pour mieux protéger la confidentialité dans l'informatique de santé,* 10 mars 2009, http://www.iso.org/iso/fr/home/news_index/news_archive/news.htm?refid=Ref1209.
[75] Organisation internationale de normalisation. *Informatique de santé – Pseudonymisation,* ISO/TS 25237:2008(F), Genève (Suisse), 2008, http://www.iso.org/iso/fr/home/store/catalogue_tc/catalogue_detail.htm?csnumber=42807.
[76] Version à jour au moment de la rédaction du présent rapport.
[77] *Gordon c. Canada (Santé),* 2008 CF 258 (CanLII), http://www.canlii.org/fr/ca/cfpi/doc/2008/2008cf258/2008cf258.html
[78] Paul Ohm. « Broken Promises of Privacy: Responding to the surprising failure of anonymization ». *UCLA Law Review*, vol. 57, 2009, p. 1701, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1450006.
[79] Arvind Narayanan et Vitaly Shmatikiv. « Robust de-anonymization of large sparse datasets », dans *Proceedings of the 2008 IEEEE Symposium on Security and Privacy*, 2008, p. 111-125, https://www.cs.utexas.edu/~shmat/shmat_oak08netflix.pdf.
[80] Arvind Narayanan, Joanna Huey et Edward Felten. *A Precautionary Approach to Big Data Privacy*, 19 mars 2015, http://randomwalker.info/publications/precautionary.pdf.
[81] Groupe de travail « Article 29 » sur la protection des données. *Avis 05/2014 sur les Techniques d'anonymisation*, 10 avril 2014, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp216_fr.pdf.

[82] Ann Cavoukian et Khaled El Emam. *Dispelling the Myths Surrounding De-identification: Anonymization Remains a Strong Tool for Protecting Privacy,* Bureau du commissaire à l'information et à la protection de la vie privée de l'Ontario, juin 2011, https://www.ipc.on.ca/images/Resources/anonymization.pdf.

[83] Robert Gellman. « The Deidentification Dilemma: A Legislative and Contractual proposal », *Fordham Intellectual Property, Media and Entertainment Law Journal*, vol. 21, n° 1, 2011, http://ir.lawnet.fordham.edu/iplj/vol21/iss1/2/.

[84] Pour en savoir plus, consultez *About De-Identification*, Future of Privacy Forum en ligne, https://fpf.org/issues/deid/.

[85] Commissariat à la protection de la vie privée du Canada. *Position de principe sur la publicité comportementale en ligne,* https://www.priv.gc.ca/information/guide/2012/bg_ba_1206_f.asp.

[86] The White House. *Big Data: Seizing Opportunities, Protecting Values*, mai 2014, https://www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf.

[87] Groupe de travail « Article 29 » sur la protection des données. *Avis 06/2014 sur la notion d'intérêt légitime poursuivi par le responsable du traitement des données au sens de l'article 7 de la directive 95/46/CE*, 9 avril 2014, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp217_fr.pdf.

[88] Commissariat à la protection de la vie privée du Canada. *Un programme de gestion de la protection de la vie privée,* https://www.priv.gc.ca/information/guide/2012/gl_acc_201204_f.asp.

[89]UK Information Commissioner's Office Blog. «What you need to know about ICO Privacy Seals», le 28 janvier 2015, https://iconewsblog.wordpress.com/2015/01/28/what-you-need-to-know-about-ico-privacy-seals/.

[90] EuroPriSe European Privacy Seal, https://www.european-privacy-seal.eu/EPS-en/About-EuroPriSe.

[91] Coopération économique Asie-Pacifique. *APEC Privacy Framework*, http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx.

[92] Au moment de la rédaction du présent rapport, l'ébauche des livres blancs intitulés *The Role of Enhanced Accountability in Creating a Sustainable Data-Driven Economy and Information Society* et *The Role of Risk Management* avait été affichée sur le site Web du CIPL, https://www.informationpolicycentre.com/.

[93] Centre for Information Policy Leadership. *The Role of Enhanced Accountability in Creating a Sustainable Data-driven Economy and Information Society*, document de discussion, 21 octobre 2015, https://www.informationpolicycentre.com/files/Uploads/Documents/Centre/World_of_Big_Data_Accountability_and_Digital_Responsibility_Sustainable_Data-Driven_Economy_and_Information_Society.pdf.

[94] Centre for Information Policy Leadership. *The Role of Risk Management*, document de discussion, 16 février 2016, https://www.informationpolicycentre.com/files/Uploads/Documents/Centre/Protecting_Privacy_in_World_of_Big_Data_Role_of_Risk_Management.pdf.

[95] Jules Polonetsky, Omer Tene et Joseph Jerome. *Benefit Risk Analysis for Big Data Projects*, septembre 2014, https://fpf.org/wp-content/uploads/FPF_DataBenefitAnalysis_FINAL.pdf.

[96] Information Accountability Foundation. *Unified Ethical Framework for Big Data Analysis: IAF Big Data Ethics Initiative, Part A*, mars 2015, http://informationaccountability.org/wp-content/uploads/IAF-Unified-Ethical-Frame.pdf.

[97] Information Accountablity Foundation. *Holistic Governance and Policy project: Introduction to the HGP Framework*, 29 octobre 2015, http://informationaccountability.org/wp-content/uploads/HGP-Overview.pdf.

[98] Martin Abrams. « Information Impact Assessments Key to Protection with Innovation », *IAF Blog*, 21 janvier 2016, http://informationaccountability.org/category/canada/.

[99] France Houle et Lorne Sossin. *Les pouvoirs et fonctions de l'ombudsman dans la* Loi sur la protection des renseignements personnels et les documents électroniques *: Une étude d'effectivité*, août 2010, https://www.priv.gc.ca/information/research-recherche/2010/pipeda_h_s_f.asp.

30, rue Victoria, 1er étage, Gatineau (Québec) K1A 1H3 • Sans frais : 1-800-282-1376 • Télécopieur : (819) 994-5424 • ATS : (819) 994-6591
www.priv.gc.ca • Suivez-nous sur Twitter : @priveeprivacy