Ministère de la Justice Canada
Department of Justice Canada

MODERNISATION DE LA *LOI SUR LA PROTECTION DES RENSEIGNEMENTS PERSONNELS* : DOCUMENT DE DISCUSSION

3. Vers une plus grande certitude pour la population canadienne et le gouvernement: recadrage de la *Loi sur la protection des renseignements personnels* et définition de concepts importants

Un engagement technique auprès d'experts quant à l'avenir de la *Loi sur la protection des renseignements personnels*, la loi fédérale en matière de protection des renseignements personnels s'appliquant au secteur public.

Nous partageons ce document de discussion avec des intervenants experts pour obtenir leurs points de vue et leurs commentaires sur les considérations techniques et juridiques à prendre en compte dans le cadre de la modernisation de la *Loi sur la protection des renseignements personnels*. Cet engagement technique ciblé aidera le Gouvernement du Canada à peaufiner les propositions de modifications à la *Loi sur la protection des renseignements personnels.*

Canada

Assurer la clarté et l'accessibilité de la législation

Des définitions claires et accessibles prévues par la loi jouent un rôle essentiel pour parvenir à une compréhension prévisible du fonctionnement de la législation. En plus de leur rôle d'orientation pour l'application de la loi, les définitions constituent un important outil de transparence. Grâce à des définitions claires et précises, les personnes peuvent mieux comprendre leurs droits juridiques et les institutions fédérales peuvent mieux comprendre quand la loi s'applique, quelles sont leurs obligations à son égard, et l'appliquer plus facilement. À la lumière des recommandations formulées par le Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique de la Chambre des communes (« le Comité ETHI ») à la suite de son étude sur l'examen de la *Loi sur la protection des renseignements personnels* et des approches modernes adoptées dans d'autres administrations, certains concepts et termes clés de la Loi pourraient être définis ou actualisés.

Certaines définitions de la Loi jouent un rôle fondamental dans la détermination de sa portée, dans la mesure où elle s'applique. Par exemple, si les renseignements ne sont pas des « renseignements personnels », la *Loi sur la protection des renseignements personnels* ne s'applique pas, bien que d'autres lois ou instruments de politique puissent s'appliquer. De même, si « le public a accès » aux renseignements personnels, ils peuvent, s'ils sont recueillis conformément à la Loi, être utilisés et communiqués sans que l'institution n'ait à obtenir de consentement ou à se fier à une autorité compétente en vertu du paragraphe 8 (2) de la Loi. Étant donné que ces concepts juridiques établissent effectivement la ligne de démarcation entre le moment où les obligations juridiques s'appliquent et celui où elles ne s'appliquent pas, il convient d'examiner attentivement s'ils demeurent pertinents à l'ère numérique.

D'autres termes clés ne déterminent pas si la Loi s'applique ou non, mais peuvent bénéficier d'une plus grande clarté étant donné le temps écoulé depuis leur formulation initiale. Ces termes pourraient être modifiés afin d'en améliorer la clarté et d'atténuer les difficultés qui ont surgi lors de l'application pratique. De nouveaux concepts pourraient également être introduits dans la Loi, qu'il pourrait être nécessaire de définir.

En fin de compte, la définition de certains concepts d'une manière qui tient compte de l'évolution des attentes, du droit et des développements ailleurs contribuera à clarifier davantage le régime législatif applicable et à faire de la Loi une source plus accessible de protection des renseignements personnels au Canada.

A. Portée : concepts qui ont une incidence sur l'application de la Loi

L'incidence juridique d'une loi donnée dépend de la portée des dispositions fondamentales qui déterminent si la loi s'applique en premier lieu. Par exemple, la *Loi sur la protection des renseignements personnels* ne s'applique qu'aux « institutions fédérales », un terme défini à l'article 3 pour inclure les institutions fédérales énumérées à l'annexe 1 de la Loi, ou celles ajoutées dans la section des définitions (p. ex. les sociétés d'État). Même dans ce cas, les institutions fédérales peuvent ne pas avoir d'obligations en vertu de la Loi selon le type de renseignements en leur possession – si les renseignements ne sont pas considérés comme des « renseignements personnels », alors la Loi n'impose pas d'obligations.

De nombreux concepts importants de la Loi ont une incidence sur la question de savoir si elle s'applique ou non, ou si certaines dispositions de la Loi s'appliquent. Cependant, bon nombre de ces concepts ont été définis au début des années 1980, alors que le monde était très différent. Avec l'avènement de notre société numérique et une réflexion plus poussée sur la façon de protéger le droit à la vie privée à l'ère moderne, bon nombre de ces concepts pourraient bénéficier d'une mise à jour.

De plus, certains termes qui pourraient préciser quand et comment certaines obligations s'appliquent en vertu de la Loi pourraient être introduits. Par exemple, les techniques de dépersonnalisation, combinées à des procédures de mesure du risque de réidentification, constituent un moyen de réduire considérablement, voire d'éliminer, les risques liés à l'utilisation des renseignements personnels. Le règlement général sur la protection

des données de l'Union européenne (« RGPD »), par exemple, incite les entités visées à utiliser des méthodes de dépersonnalisation, de pseudonymisation et de cryptage pour protéger les données personnelles. Il pourrait être utile d'introduire de tels concepts dans la Loi.

Renseignements personnels

L'article 3 de la *Loi sur la protection des renseignements personnels* définit l'expression « renseignements personnels » comme étant « les renseignements, quels que soient leur forme et leur support, concernant un individu identifiable ». Cette définition inclut aussi une liste non exhaustive d'exemples.

Au cours de l'étude du Comité ETHI sur l'examen de la *Loi sur la protection des renseignements personnels*, de nombreux témoins ont souligné la nécessité de réviser la définition des « renseignements personnels ». Une grande partie des commentaires portaient sur la question de savoir si des renseignements non consignés doivent être inclus dans la définition. Plusieurs témoins ont suggéré de modifier la définition de « renseignements personnels » pour supprimer la référence aux renseignements consignés et le Comité ETHI a finalement recommandé que la définition de « renseignements personnels » à l'article 3 de la Loi soit modifiée pour s'assurer qu'elle est neutre sur le plan technologique et qu'elle comprend les renseignements non consignés. Il peut s'agir, par exemple, de séquences vidéo qui sont surveillées, mais ultimement non enregistrées.

Plusieurs témoins devant le Comité ETHI ont également mentionné certains des défis posés par les métadonnées. En général, les métadonnées sont des informations associées à ou concernant une communication, mais pas le contenu informationnel de la communication elle-même. C'est l'information contextuelle entourant une communication qui peut être utilisée pour identifier, décrire, gérer ou acheminer la communication. Certains témoins étaient d'avis que les métadonnées répondaient à la définition de renseignements personnels. D'autres ont souligné que l'un des défis de la définition des métadonnées dans la Loi était de s'assurer qu'une telle définition soit technologiquement neutre, puisque les métadonnées pourraient avoir une signification différente à l'avenir. Lors de sa comparution devant le Comité ETHI le 7 mai 2019, le commissaire à la protection de la vie privée a exprimé son point de vue selon lequel la Loi devrait énoncer certaines règles de base régissant le moment où les institutions pourraient recueillir et partager les métadonnées, plutôt que de définir une approche prescriptive. Le comité ETHI a finalement recommandé que les métadonnées soient définies dans la Loi, d'une manière technologiquement neutre et en mettant l'accent sur les renseignements qu'elles peuvent révéler sur une personne.

Toutefois, une définition de « métadonnées » distincte de la définition de « renseignements personnels » pourrait laisser entendre, dans l'interprétation législative, que les métadonnées sont autre chose que des renseignements sur une personne identifiable. Et ce ne sont pas toutes les parties des métadonnées qui, à elles seules, peuvent révéler des renseignements sur un individu, même si ces renseignements, lorsqu'ils sont accumulés au fil du temps ou consultés avec d'autres renseignements disponibles, peuvent donner une idée des activités personnelles, des points de vue, des opinions et du mode de vie d'une personne. Le Commissariat à la protection de la vie privée a également déclaré que la notion de métadonnées « est indéniablement vaste ». Dans ce contexte, la définition des métadonnées pourrait poser des difficultés pratiques et, si elle était définie comme autre chose que des « renseignements personnels », elle pourrait ouvrir l'application de la Loi à la collecte, à l'utilisation, à la divulgation, à la conservation et à la gestion de renseignements qui, selon le contexte, ne concernent pas nécessairement un individu identifiable.

D'autres éléments de la définition de « renseignements personnels » méritent également d'être discutés, notamment le concept d'« identifiabilité ». Bien que l'« identifiabilité » soit l'une des conditions essentielles pour déterminer si la Loi s'appliquera ou non, il n'existe aucune définition dans la loi qui clarifie ce qu'elle signifie. D'autres lois sur la protection des données définissent le concept d'identifiabilité. Par exemple, le RGPD de l'Union européenne définit les données personnelles comme suit :

« données à caractère personnel », toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée « personne concernée »); est réputée être une « personne physique identifiable » une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale.

En l'absence d'une définition dans la loi, les tribunaux canadiens ont déterminé qu'une personne sera « identifiable » relativement aux renseignements la concernant 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[1] ». Cette approche de l'« identifiabilité », largement fondée sur les faits, s'est avérée difficile à appliquer dans la pratique et soulève d'autres questions : (i) qui porte la responsabilité de la recherche d'» autres informations disponibles » et quel est le degré d'effort requis?; (ii) quelles sources d'« autres renseignements disponibles » faut-il prendre en considération et comprennent-elles uniquement les sources publiques ou également les sources internes du gouvernement?; (iii) l'identifiabilité par un membre du public, un enquêteur expert ou un seul employé du gouvernement est-elle la norme pertinente?; et (iv) comment les changements dans le temps influent-ils sur l'analyse?

Particulièrement à une époque où le gouvernement cherche proactivement à rendre ses fonds de renseignements beaucoup plus accessibles au public, les institutions fédérales pourraient bénéficier de directives plus claires sur la signification de l'« identifiabilité ».

Q.3(a) : La définition de « renseignements personnels » devrait-elle être fondée sur le concept d'identifiabilité et, dans l'affirmative, ce concept devrait-il être défini?

Q.3(b) : Les métadonnées doivent-elles faire l'objet d'une définition distincte ou les questions de protection de la vie privée liées à ces renseignements peuvent-elles être réglées par une définition à jour des renseignements personnels (y compris en ajoutant un exemple)?

Renseignements personnels dépersonnalisés, anonymisés, pseudonymisés, et chiffrés

Une importante question de définition est de savoir si la *Loi sur la protection des renseignements personnels* devrait reconnaître de nouveaux sous-ensembles de renseignements personnels afin de faciliter l'application d'un ensemble de règles plus souple et sensible au contexte. Par exemple, afin de créer un dépôt ou bassin de renseignements qui traiterait les renseignements identifiables différemment de renseignements non identifiables, il serait important de déterminer les règles respectives applicables à ces différents types de renseignements, et ce, avec une mesure d'efficacité et de certitude. L'approche actuelle d'accepter ou de refuser la divulgation des renseignements personnels ne tient pas compte des règles plus nuancées qui peuvent être organisées en fonction de différents niveaux de risque et favoriser la conformité. La définition de renseignements dépersonnalisés, anonymisés et pseudonymisés pourrait appuyer l'élaboration de nouvelles mesures d'incitation à la conformité, permettre une application plus ciblée et plus nuancée de certaines règles et aider à atténuer certaines des difficultés d'application pratique que pose l'approche actuelle.

D'une manière générale, les informations « anonymisées » ont été irréversiblement dépouillées de leurs identificateurs personnels, tandis que les informations « dépersonnalisées » ont été modifiées de sorte qu'elles ne peuvent plus être attribuées à une personne en particulier sans l'utilisation d'informations supplémentaires. La « pseudonymisation » est une forme spéciale de dépersonnalisation qui implique l'ajout de nouveaux éléments qui substituent des informations identifiables. Le chiffrement consiste à prendre l'information et à la

[1] *Gordon c. Canada (Santé),* 2008 CF 258 aux paras. 33-34.

rendre inintelligible en utilisant une « clé » de chiffrement, sans laquelle l'information ne peut être consultée ou comprise. Dans son étude sur l'examen de la *Loi sur la protection des renseignements personnels*, le Comité ETHI ne s'est pas penché sur le rôle que des renseignements personnels effectivement anonymisés ou pseudonymisés pourraient jouer dans une *Loi sur la protection des renseignements personnels* modernisée. Il n'a pas non plus abordé le rôle que peuvent jouer les informations chiffrées.

Actuellement, d'autres régimes de protection des données prévoient un rôle important pour l'utilisation de renseignements personnels dépersonnalisés et limitent certaines obligations lorsque le chiffrement est utilisé. Par exemple, dans le RGPD, plusieurs dispositions incitent les responsables du traitement à utiliser des méthodes de dépersonnalisation, de pseudonymisation, ou de chiffrement, ce qui peut avoir une incidence sur la manière dont les obligations s'appliquent, voire les dispenser de certaines obligations.

Q.3(c) : Quel rôle les renseignements personnels dépersonnalisés, pseudonymisés, ou chiffrés pourraient-ils jouer dans une Loi sur la protection des renseignements personnels moderne, et comment ces termes devraient-ils être définis?

Renseignements personnels auxquels le public a accès

Le paragraphe 69 (2) de la *Loi sur la protection des renseignements personnels* exempte les renseignements personnels « auxquels le public a accès » des règles régissant l'utilisation et la communication secondaires des renseignements personnels. Si l'information était accessible au public en 1983, elle l'était en quantité limitée et sous une forme qui pouvait rendre généralement inutile l'application des règles d'utilisation et de divulgation (p. ex. les registres publics sur papier).

La révolution numérique et les médias sociaux ont changé tout cela. En raison de la numérisation accrue de l'information pour l'utilisation sur Internet, il est maintenant plus facile de trouver, de recueillir, d'utiliser ou de divulguer des renseignements auxquels le public a accès, surtout en ligne. De plus, il devient de plus en plus difficile de déterminer comment l'information a été rendue publique – des acteurs négligents ou malveillants peuvent rendre les renseignements personnels accessibles au public, à l'insu de la personne concernée. Ainsi, la quantité, la nature, et le type de renseignements personnels auxquels le public avait accès en 1983 étaient fondamentalement différents de ce qu'ils sont aujourd'hui.

Ces développements suggèrent la nécessité de reconsidérer notre recours à l'obscurité pratique en ce qui concerne le traitement juridique des renseignements personnels auxquels le public a accès. L'introduction d'une définition qui cherche à protéger les attentes raisonnables des individus dans leur contexte est une approche possible. Dans la pratique, cela peut signifier qu'il faut tenir compte de la nature de l'information, de sa source et de la façon dont elle a été rendue publique, ainsi que des raisons pour lesquelles elle l'a été. L'intégration de ce genre de considérations dans l'approche factuelle actuelle visant à déterminer quand les renseignements personnels sont accessibles au public pourrait mieux répondre aux attentes raisonnables des Canadiens à l'ère numérique.

La LPRPDE ne définit pas expressément les « renseignements auxquels le public a accès », mais permet la collecte, l'utilisation et la communication de renseignements personnels à l'insu du public et sans son consentement si les renseignements sont « accessibles au public et que cela est précisé par règlement ». Le *Règlement précisant les renseignements auxquels le public a accès* dresse ensuite une liste de certains types et catégories de renseignements qui sont précisés à ces fins. Un autre modèle canadien existant est celui de la définition prévue par la loi de « renseignements auxquels le public a accès » que le projet de loi C-59 propose d'inclure dans la *Loi sur le Centre de la sécurité des télécommunications*. Cette définition exclurait de la définition de renseignements auxquels le public a accès « l'information à l'égard de laquelle un Canadien ou

une personne se trouvant au Canada a une attente raisonnable en matière de protection de la vie privée ».

Q.3(d) : Que pensez-vous être les expectatives du public relatives aux renseignements personnels auxquels le public a accès?

Q.3(e) : Comment pourrait-on définir les « renseignements personnels auxquels le public a accès » en vertu d'une Loi sur la protection des renseignements personnels moderne?

B. Définir d'autres concepts clés

Des définitions claires et accessibles prévues par la loi jouent un rôle essentiel pour parvenir à une compréhension commune et prévisible du fonctionnement de la législation. Outre leur rôle d'orientation de l'application de fond de la loi, les définitions constituent un important outil de transparence. Grâce à des définitions claires et précises, le public peut mieux comprendre ses droits juridiques et les institutions peuvent plus facilement appliquer la loi. Plusieurs termes de la Loi pourraient bénéficier d'une mise à jour, à la lumière des réflexions plus modernes sur les questions de protection de la vie privée et des approches adoptées dans d'autres administrations.

Consentement

À l'heure actuelle, la Loi reconnaît le consentement comme fondement sur lequel une institution fédérale peut utiliser ou communiquer des renseignements personnels à des fins autres que celles pour lesquelles ils ont été recueillis. Toutefois, le consentement n'est pas défini dans la Loi. La notion de consentement est un exemple d'un terme qui a été interprété par les tribunaux dans divers contextes, la common law énonçant un certain nombre d'exigences claires, largement acceptées et rigoureuses qui doivent être respectées pour que le consentement soit considéré comme valide. En règle générale, le consentement valide sera sans ambiguïté, pleinement éclairé et donné librement.

Bien que de nombreuses lois sur la protection des renseignements personnels qui s'appliquent aux entités du secteur public indiquent que le consentement sert de fondement à d'autres utilisations ou communications de renseignements personnels, peu d'entre elles le définissent réellement. Parmi celles qui le font, la portée des définitions varie. Le RGPD, par exemple, définit le consentement comme « toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement ». En revanche, la loi australienne sur la protection de la vie privée définit le consentement comme signifiant « consentement exprès ou consentement implicite » [traduction libre].

Les éléments qui ont été identifiés par la common law peuvent être utiles pour délimiter le sens du consentement. La définition du consentement dans la Loi pourrait aider à atténuer les ambiguïtés entourant le concept du consentement. De plus, le fait de définir le consentement d'une manière conforme aux exigences de la common law canadienne améliorerait la transparence en codifiant dans la loi les exigences juridiques existantes à l'intention des institutions fédérales et des individus qui doivent les comprendre. Cela aiderait les personnes à mieux savoir ce qui est nécessaire pour que leur consentement soit considéré comme valide et aiderait à clarifier pour les institutions ce qui est nécessaire pour obtenir un consentement valide et comment concevoir des initiatives pour tenir compte de ces considérations.

Q.3(f) : Le consentement devrait-il être défini en vertu d'une Loi sur la protection des renseignements personnels moderne et, dans l'affirmative, quels éléments devraient en faire partie?

La question cherchant à savoir le rôle que le consentement devrait jouer dans le secteur public est aussi examinée dans le document de discussion intitulé: Principes de protection des renseignements personnels et modernisation des règles à l'ère numérique.

Fins administratives

La Loi définit les fins administratives comme étant « l'usage de renseignements personnels concernant un individu dans le cadre d'une décision le touchant directement ». En fin de compte, la définition interagit avec les dispositions de la Loi pour créer deux niveaux d'obligations en matière de protection de la vie privée : complète et partielle. Lorsqu'il existe des fins administratives, toutes les exigences de la Loi doivent être pleinement respectées. Lorsqu'il n'y a pas de fins administratives en cause, par exemple, l'utilisation de renseignements personnels à des fins de recherche, de statistique, de vérification et d'évaluation, les institutions ont plus de souplesse en ce qui concerne certaines questions, comme la collecte directe, la conservation et l'exactitude.

D'une manière générale, cette approche est judicieuse du point de vue réglementaire. Elle permet aux institutions de concentrer leurs ressources en matière de conformité là où il y a des conséquences directes pour une personne, dans le but de mieux protéger le public des plus grands risques. Il est important de se demander si un processus décisionnel qui ne touche directement que la personne dont les renseignements personnels sont en cause demeure le meilleur seuil pour imposer une série complète de mesures de protection de la vie privée. Les nouvelles technologies, les nouveaux types de préjudices et les nouvelles façons de prendre des décisions donnent à penser qu'il pourrait y avoir un meilleur moyen de canaliser l'application de la Loi.

Par exemple, lorsque la définition actuelle s'applique à l'utilisation de l'intelligence artificielle dans le secteur public, elle oriente l'enquête sur des aspects techniques qui, en fin de compte, pourraient ne pas convenir aux individus. L'une de ces questions est de savoir si la création d'un système d'intelligence artificielle contenant des renseignements personnels constitue une « fin administrative » ou si c'est seulement l'application du système d'intelligence artificielle dans des cas particuliers qui donne lieu à des « fins administratives ». Dans ce dernier cas, il se peut que l'obligation d'utiliser des renseignements personnels exacts prévue par la Loi ne soit pas suffisamment prise en compte à l'étape de la conception. Bien qu'une interprétation juridique fondée sur l'objet visé puisse suffire à garantir que la création de systèmes d'intelligence artificielle fait l'objet d'une diligence raisonnable, il est peut-être préférable que les considérations juridiques pertinentes soient plus claires à première vue.

La définition actuelle de « fins administratives » vise à déterminer si les individus sont exposés à un risque de préjudice suffisant pour que l'ensemble des protections juridiques s'appliquent. Autrement dit, elle vise à reconnaître certaines obligations en matière de renseignements personnels qui peuvent être assouplies lorsque les personnes ne sont pas touchées de façon importante. Une façon de s'assurer que la *Loi sur la protection des renseignements personnels* suscite les bonnes questions serait d'être plus clair sur ce rôle. Par exemple, la définition de « fins administratives » pourrait être réduite à des principes de base et reformulée en fonction d'un seuil de préjudice (p. ex. certaines exigences de la Loi pourraient être assouplies lorsqu'il n'y a pas ou peu de risque de préjudice pour une personne, en utilisant des critères subjectifs ou objectifs, ou les deux, pour déterminer le préjudice). Sinon, une autre approche plus adaptée à l'ère numérique pourrait être élaborée (par exemple, si une protection technologique était disponible et appliquée pour éliminer le besoin d'une protection juridique particulière, les exigences de conformité pourraient être assouplies ou éliminées).

Une troisième approche consisterait à reconsidérer complètement l'inclusion du concept.

Q.3(g) : Une Loi sur la protection de la vie privée moderne devrait-elle toujours faire la distinction entre les utilisations administratives et non administratives et, dans l'affirmative, comment devrait-on définir une « utilisation administrative »?

Usage compatible

Le concept d'« usage compatible » est un autre exemple d'un concept qui pourrait bénéficier d'une plus grande clarté. En vertu de la *Loi sur la protection des renseignements personnels*, une institution fédérale est autorisée à utiliser et à communiquer des renseignements personnels à de nouvelles fins lorsque ces nouvelles fins sont compatibles avec celles pour lesquelles les renseignements personnels ont été recueillis – en d'autres termes, pour un « usage compatible ». La Cour suprême du Canada a affirmé que le critère permettant de déterminer la validité d'un usage compatible repose sur les attentes raisonnables d'un individu : dans un cas où « il serait raisonnable que l'employé s'attende à ce que les renseignements soient utilisés de la manière proposée » en raison d'un lien suffisamment direct avec les fins pour lesquelles ils ont été recueillis, il s'agit d'un usage compatible[2].

Cette approche fondée sur une définition est respectueuse des attentes raisonnables des individus en contexte, mais elle est également difficile à appliquer dans la pratique. Il peut être difficile de déterminer ce à quoi les personnes pourraient raisonnablement s'attendre dans un contexte donné, et la Loi ne fournit actuellement aucune orientation. Les institutions hésitent généralement à fonder leurs nouveaux programmes et activités sur un fondement juridique aussi incertain. De plus, les mesures actuelles de responsabilisation et de transparence obligent les individus à chercher de l'information sur la fiabilité des institutions à l'égard de ce pouvoir sans fournir d'indices de validité auxquels les individus pourraient comparer les institutions. À l'instar de l'approche des « usages compatibles » dans le cadre du RGPD, ces questions pourraient être réglées par l'introduction d'une définition dans la loi de l'usage compatible. Cette définition pourrait déterminer une série de facteurs à prendre en considération et élaborer une liste non exhaustive de pratiques gouvernementales communes en matière de renseignements personnels qui pourraient servir d'exemples clairs et précis d'usage compatible pour éclairer la prise de décisions.

L'article 6 du RGPD identifie un plusieurs considérations que les entités qui y sont assujetti doivent prendre en ligne de compte afin de déterminer si une pratique relative aux renseignements personnels est "compatible" avec l'objectif pour laquelle les renseignements ont recueillies à l'origine. Ces considérations comprennent le lien entre l'objectif original et le nouvel objectif, le contexte dans lequel les renseignements ont été recueillis – y compris la relation entre l'individu et l'entité réglementée, la nature des renseignements personnels en question, les conséquences pour l'individu si les renseignements sont utilisés à de nouvelles fins, et l'existence de mesures de sécurité appropriées, qui pourraient comprendre le chiffrage ou la pseudonymisation.

[2] *Bernard c. Canada (Procureur général),* [2014] 1 RCS 227, 2014 CSC 13 à l'article 31.

Q.3(h) : Le concept d'« usage compatible » devrait-il être défini dans la Loi sur la protection des renseignements personnels et, dans l'affirmative, quels éléments devraient en faire partie?

Q.3(i) : Est-ce que la démarche fondée sur des critères préconisée par le RGPD relative aux usages compatibles pourrait aider à clarifier l'étendue du concept d'« usage compatible » aux termes de la Loi sur la protection des renseignements personnels? Quels éléments devront être considérés par les institutions fédérales, le cas échéant?