[00:00:01 Le logo de l’EFPC apparaît à l’écran.]

[00:00:03 Tom Dufour apparaît dans un vidéoclavardage.]

Tom Dufour, Statistique Canada : Bonjour et bienvenue à nouveau à la Conférence sur les données de 2022 intitulée Valoriser les données et leur interprétation pour servir la population canadienne. Bonjour et bienvenue à nouveau à la Conférence sur les données de 2022, Valoriser les données et leur interprétation pour servir la population canadienne. Nous espérons que vous avez apprécié les séances simultanées de cet après-midi.

Je tiens à vous rappeler que vous pouvez nous envoyer vos questions dans le cadre de cette webdiffusion. Dans le coin supérieur droit de votre écran, cliquez sur le bouton Participer, puis saisissez vos questions. Nous en sommes à notre dernière allocution principale. J’ai le grand plaisir d’inviter mon collègue, Éric Rancourt, directeur général de la Direction des méthodes statistiques modernes et de la science des données de Statistique Canada, à présenter notre prochaine invitée, Chantal Bernier. Cette dernière discutera des cadres de protection de la vie privée et des données pour le bien public. À toi Éric.

[00:01:02 Deux autres panélistes se joignent à la conversation.]

Éric Rancourt, Statistique Canada : Merci beaucoup, Tom. Nana, bonjour. Bonjour. Bon après-midi et bienvenue au discours-programme d’aujourd’hui. Je m’appelle Éric Rancourt et serai votre modérateur. Je tiens à vous rappeler que vous avez accès à des services d’interprétation simultanée dans le cadre de cette discussion. Vous pouvez également accéder CART service de sous-titrage et à un service d’interprétation en langue des signes sur la plateforme de webdiffusion. Alors, commençons la séance.

L’événement porte sur les cadres de protection de la vie privée et sur l’utilisation des données dans l’intérêt public, mais qu’est-ce que cela signifie? J’ai survolé les séances sur les données qui ont eu lieu hier et aujourd’hui. Les conférenciers ont abordé explicitement ces sujets ou y ont fait référence dans bon nombre des séances. Car il s’agit de deux aspects importants des travaux que nous devons effectuer à l’aide des données. Il faut cerner les intérêts personnels. Les intérêts mutuels et collectifs. Il faut favoriser l’utilisation des données dans l’intérêt des Canadiens et du Canada. Ce qu’on veut, c’est trouver un point optimal entre ces aspects. Il existe un lien clair avec les aspects juridiques, mais aussi de façon plus globale avec les cadres, les principes et les approches. Alors, pour discuter de ces enjeux, j’ai le très grand plaisir d’accueillir Chantal Bernier. Bonjour, Chantal.

Chantal Bernier, Dentons : Bonjour.

Éric Rancourt : Chantal est une experte en système légal et tout le fondement qui vient appuyer, ce qu'on peut faire avec les données, comment se cadrent la protection de la vie privée, comment se cadrent les accès, et on va discuter de cela dans la prochaine heure. Chantal Bernier dirige le groupe canadien Vie privée et cybersécurité et est membre du groupe Affaires et politiques gouvernementales de Dentons. Ayant agi à titre de commissaire adjointe et intérimaire à la protection de la vie privée du Canada, Chantal a dirigé des enquêtes nationales et internationales sur la protection de la vie privée dans les secteurs public et privé ainsi que de vérifications de la protection de la vie privée, des examens des évaluations des facteurs relatifs à la vie privée, des analyses technologiques et des activités d'élaboration de politiques et de recherche. Chantal fournit des conseils stratégiques à ses clients et met en valeur, dans le service, son expérience de haute fonctionnaire au sein du gouvernement du Canada. Elle siège actuellement au Conseil consultatif sur l'éthique et la modernisation de l'accès aux microdonnées de Statistique Canada. Elle siège aussi au comité directeur du Collectif canadien de normalisation en matière de gouvernance des données du Conseil canadien des normes. Alors, bienvenue encore, Chantal.

Chantal Bernier : Merci.

Éric Rancourt : Donc, pour la présente séance, je poserai quelques questions à Chantal, puis lui soumettrai les questions du public. Commençons donc par une présentation de l'enjeu global. Nous avons tous pu remarquer que les participants aux groupes de discussion sur les données s'intéressent beaucoup à la protection de la confidentialité. Parallèlement, les données constituent un atout sans pareil pour produire un bien public et faire progresser le Canada. Comment pouvons-nous donc concilier ces deux réalités?

Chantal Bernier : Eh bien, Éric, premièrement, je tiens à vous dire que je suis très heureuse de me retrouver à vos côtés après avoir passé 27 ans au sein du secteur public et du gouvernement du Canada. Même si j'ai recommencé à travailler au sein du secteur privé, je n'oublierai jamais la grande famille de la fonction publique. C'est une grande joie de me trouver avec vous aujourd'hui. Vous avez bien résumé la tension, Éric. Vous avez abordé le sujet de l'incroyable potentiel des données, puis du droit fondamental à la confidentialité. Pourquoi cela crée-t-il une tension? D'où celle-ci vient-elle? En fait, elle découle des éléments que nous devions auparavant concilier. Avant, nous disposions de données plutôt statiques. Par exemple, chaque année, je dois dire à l'Agence du revenu du Canada quels sont mes revenus, puis celle-ci utilise ces chiffres pour déterminer le montant de mes impôts. Il s'agit d'une situation statique. Or, en ce moment, nous nous retrouvons dans un important contexte de données dynamiques.

Cela signifie que nous pouvons transformer les données que je fournis en données encore plus personnelles. C'est le profilage, les algorithmes. Vous avez souvent dû entendre cette phrase : « Les données sont le nouveau pétrole. » Jim Balsillie dit plutôt « Les données sont le nouveau plutonium ». J'aime bien cette image, car elle décrit la nature explosive des données et le fait qu'elles ne sont pas statiques. « Je vous donne ces données, et vous devez faire telle chose avec celles-

ci. » C’est plus dynamique, car avec les données que je vous donne, vous pouvez découvrir beaucoup d’autres choses sur moi. Comment pouvons-nous concilier cette réalité avec le droit fondamental à la vie privée? Comment pouvons-nous concilier le droit fondamental à la vie privée avec le fait que nous disposons d’un trésor, oui, un trésor, qui permet d’orienter les politiques publiques d’une manière hautement efficace et efficiente? Je vais déclarer d’emblée, et j’en parlerai plus en détail plus tard, que les restrictions qui vous concernent devraient être revues. Elles sont trop restrictives pour favoriser une véritable optimisation des données. Nous ne pouvons pas protéger la vie privée et optimiser la valeur des données en même temps. Nous ne disposons pas actuellement du cadre législatif qui permet de le faire, mais nous pouvons faire appel aux instruments dont nous disposons.

Le premier pilier d’orientation est la Charte. La Charte permet d’utiliser des données personnelles de façon raisonnable, dans la mesure où cette utilisation peut être justifiée dans le cadre d’une société démocratique La *Loi sur la protection des renseignements personnels* autorise la collecte de données personnelles et l’utilisation de données personnelles, dans la mesure où ces activités sont directement liées aux activités de programme de l’entité qui les collecte. Il y a également des directives du Conseil du Trésor concernant les évaluations des facteurs relatifs à la vie privée. Ces directives constituent un véritable schéma pour aider à déterminer les types de données personnelles dont nous avons besoin. De combien de données avons-nous besoin? Pourquoi en avons-nous besoin? Cela officialise notre analyse sous forme de structure très concrète qui documente, essentiellement, l’application de l’article 1 de la Charte et des articles 3, 4 et 5 relatifs à l’utilisation cohérente de la *Loi sur la protection des renseignements personnels*.

Je vous dirais donc de commencer par démontrer qu’il est nécessaire d’utiliser des données, dans la mesure où cette nécessité demeure valide, naturellement. Ensuite, pourvu que la collecte et l’utilisation des données soient proportionnelles à cette nécessité et soient efficaces et qu’il n’existe aucune autre solution de rechange moins intrusive, vous disposez de solides raisons constitutionnelles d’utiliser des données personnelles. Si vous ne disposez pas de ce fondement, vous ne pourrez pas démontrer que votre utilisation de données est nécessaire. Par exemple, la réalisation d’une étude longitudinale sur une question précise pourrait être très avantageuse pour le Canada. Si la nécessité ne peut pas être démontrée, vous devez obtenir le consentement des personnes concernées. Il faut ensuite obtenir le consentement valide des gens. Si aucune des solutions n’est possible ou pratique, il faut anonymiser les données, directement à la source, ce qui signifie qu’il faut recueillir les données sans recueillir d’éléments d’identification, de façon à ce que les données demeurent anonymes de façon irréversible. Les données ne doivent jamais permettre d’identifier une personne. Ce sont là les principaux éléments de base. Nous en parlerons plus en détail plus tard, mais ce sont les composantes de base qui permettent d’équilibrer la recherche de valeurs et de données ainsi que la protection de la confidentialité.

Éric Rancourt : Merci. Vous insistez sur la grande importance de la nécessité. J’aimerais poursuivre sur ce sujet, car je crois qu’en tant qu’entreprise d’État en

général, nous y accordons également une grande importance, tout comme le fait l'équipe de Statistique Canada. Mais, en général, les organisations ont de la difficulté à bien expliquer ce concept, surtout en ce qui concerne les besoins des Canadiens, comparativement aux besoins du ministère ou de la partie prenante. Pouvez-vous nous en dire plus sur l'importance d'aborder les besoins des Canadiens plutôt que les besoins d'un programme ou les besoins d'un employé? Pouvez-vous nous dire quelques mots à ce sujet?

Chantal Bernier : Eh bien, vous venez d'aborder un domaine pour lequel la loi devrait être revue, car en ce moment, la *Loi sur la protection des renseignements personnels* permet l'utilisation de données personnelles de façon très cloisonnée. Selon la loi, « un établissement peut recueillir et utiliser des renseignements personnels dans le cadre de ses programmes et de ses activités ». Elle n'aborde pas le bien collectif. Je proposerais assurément cette modification dans le cadre de la réforme de la *Loi sur la protection des renseignements personnels*. Ce que vous pouvez faire maintenant, c'est lier l'utilisation des données pour votre programme et la façon dont votre programme s'inscrit dans le bien collectif. Naturellement, la notion de bien collectif est également un peu vague, mais lorsque je travaillais pour le Commissariat à la protection de la vie privée du Canada, j'ai été témoin d'utilisations très audacieuses de données personnelles. Voici un exemple concret d'une situation où cela était légitime.

L'histoire se déroule à l'époque où les détecteurs corporels, qui sont très intrusifs, ont fait leur entrée au Canada. Le procédé n'est pas le même que celui qui consiste à utiliser un grand nombre de données personnelles pour dégager des tendances, mais c'était tout de même très intrusif. Qu'est-ce que l'ACSTA a fait? Elle a d'abord fait appel au CPVP dès le départ. Elle a expliqué la nécessité de faire appel à cette technologie en disant « nous disposons de sources de renseignements qui confirment que les explosifs non métalliques constituent actuellement le risque le plus important pour la sécurité aérienne. Nous devons donc régler ce problème. » Nous avons effectué des tests de fouille sommaire auprès de nos employés. Nous avons constaté que comme ils étaient prudes, les agents de l'ACSTA ne fouillaient pas partout et étaient réticents à fouiller certaines personnes. Les tests ont donc démontré que beaucoup d'explosifs non métalliques n'étaient pas interceptés et que les détecteurs corporels constituaient la seule solution. Ils sont parvenus à anonymiser le processus en faisant appel à une tierce personne pour voir l'image. Donc, la personne qui voyait le passager entrer dans le capteur et la personne qui voyait l'image était deux personnes différentes.

L'image était également brouillée. En fait, l'image n'était qu'une silhouette montrant que vous aviez oublié d'enlever la monnaie qui se trouvait dans votre proche. C'était donc entièrement anonyme. L'utilité de cette solution a rapidement été démontrée, car deux mois après l'annonce de la mise en œuvre des capteurs corporels, le terroriste qui cachait des explosifs dans ses sous-vêtements a été arrêté. Ça prouvait donc la pertinence de faire appel à ce dispositif.

Et c'est comme ça qu'ils ont géré l'opinion publique. Le recours à cette technologie était très bien documenté. Je ne dis pas par là qu'il n'y a eu aucun scandale. Mais les responsables avaient de bons arguments. Cette situation a retenu l'attention médiatique pendant trois jours. Je me souviens, j'ai fait environ 21 entrevues en trois jours, car tous les détails semblaient contrevenir à la loi. Ce sont les instruments dont vous disposez maintenant. Vous disposez d'objectifs valables dans le cadre des activités de votre programme pour tirer parti des données personnelles, et vous devez tenir compte des répercussions sur la vie privée qui justifient la raison pour laquelle vous tirez parti des données. Et il y a le Commissariat à la protection de la vie privée qui n'approuvera pas l'évaluation des facteurs relatifs à la vie privée. Mais si vous suivez ses recommandations, vous pourriez vous retrouver dans une situation qui vous permettra de tirer parti des données de la façon que vous le souhaitez en gagnant la confiance du public. Ce sont les instruments dont vous disposez maintenant.

Éric Rancourt : Merci infiniment. J'espère que vous tirez tous de précieux enseignements de cette discussion, car il s'agit en quelque sorte d'une recette pour s'y retrouver dans le processus. Vous venez de parler de confiance, et j'aimerais revenir à ce que vous avez dit plus tôt, lorsque vous avez comparé les données au pétrole et au plutonium. Je crois que les membres de la société commencent à comprendre que les données sont importantes. Et parfois, lorsque nous demandons des données aux Canadiens, ils pourraient dire « Vous avez déjà ces données. Je les ai transmises à tel autre ministère. » Mais, d'un autre côté, il faut bien protéger le plutonium, car il ne peut pas être volé. Nous entendons aux nouvelles des histoires d'atteinte à la sécurité des données qui pourraient miner la confiance du public. Comment pouvons-nous sensibiliser les membres du public pour qu'ils comprennent qu'une atteinte à la sécurité des données n'entache pas l'importance du partage de données entre les différents organes du gouvernement. Il ne s'agit alors pas d'une atteinte à la sécurité des données, mais d'un partage de données.

Chantal Bernier : Tout à fait. Comme nous le savons tous, une atteinte à la sécurité des données est un accès non autorisé à des données personnelles. Le partage de données consiste à partager des données à l'aide d'un processus de gouvernance et de protocoles d'autorisation. Et c'est ce qui fait toute la différence. Comme je l'ai dit il y a quelques instants, j'ai été témoin de méthodes de partage de données audacieuses. Laissez-moi maintenant aborder l'approche des quatre filtres. Donc, l'approche des quatre filtres est utilisée dans le domaine de la prévention du crime. Il s'agit d'un protocole dans le cadre duquel les tables d'intervention multidisciplinaires s'échangent des données. Concrètement, la police, les établissements scolaires, l'hôpital et les services sociaux, par exemple, et parfois les services de logement, unissent leurs efforts pour aider les familles à risque. Nous parlons de prévention du crime.

Le premier filtre consiste à présenter un cas non identifié aux autres intervenants. On indique, par exemple, que cette famille est aux prises avec plusieurs problèmes. Le groupe décidera ensuite s'il faut appliquer le deuxième filtre, c.-à-d. s'il faut réunir les acteurs qui pourraient faire une différence. Si on décide d'appliquer le deuxième filtre, de plus amples renseignements sont fournis. Et si on passe au

troisième filtre, des renseignements permettant d'identifier les personnes sont partagés. Et le quatrième filtre consiste à effectuer un véritable travail de collaboration afin d'obtenir des résultats intégrés. Il s'agit d'un processus très rigoureux... Comme vous le disiez, le plutonium doit être maîtrisé. Le cadre de gouvernance qui permet le partage de renseignements personnels est très strict. Et la protection de ce processus découle du protocole que doivent respecter tous les intervenants et dans le cadre duquel ils s'entendent sur la façon de partager et de protéger ces renseignements. C'est un autre exemple.

Éric Rancourt : D'accord. Merci beaucoup. Je me demande comment on pourrait éduquer le public ou l'aider à bien comprendre ces principes-là, puis ces étapes-là. Je pense qu'entre producteurs, acteurs, utilisateurs de données, on se convainc assez bien les uns les autres, on améliore nos processus et nos protocoles et notre gouvernance. Mais comment on… D'après votre expérience, comment on peut aider le public à mieux comprendre?

Chantal Bernier : La transparence. La transparence, et je vais vous donner encore des exemples concrets. Je vais vous parler de MetroLinks. Donc MetroLinks, il y a quelques années, enfin, bon, peut-être 20 ans, a installé des caméras de surveillance dans son système de transport en commun à Toronto. Et évidemment, ça n'a pas fait l'unanimité. Mais ils avaient l'aval, à l'époque, de la commissaire de l'information à vie privée de l'Ontario. Comme quoi il y avait nécessité, proportionnalité, mais MetroLinks ajoutait quelque chose à cela. Chaque année, MetroLinks publie un rapport de transparence dans lequel il est indiqué combien de demandes de la police ils ont reçues pour avoir des renseignements personnels, parce que c'est avec – il y a les caméras de surveillance, mais également les cartes à puces – voilà, pour utiliser les transports, qui donnent également des itinéraires. Alors, combien de demandes ils ont reçues de la police pour ces renseignements personnels, combien ils en ont accepté, combien ils en ont refusé, et les motifs connexes. Alors, c'était pour retrouver une personne disparue. C'était pour retrouver un objet volé. Il y avait toutes les raisons. Alors, au fil des années, année après année, ça a bâti une confiance.

Pour ce qui est du gouvernement fédéral, moi je trouve que l'idée de publier les évaluations des facteurs relatifs à la vie privée, EFVP en français ou « PIAs » en anglais, c'est extrêmement utile. Je sais très bien qu'il y a des évaluations, les EFVP, qui contiennent des renseignements protégés. Bon, d'accord, on les retire, mais le fait de publier les EFVP sur votre site Web, ça, je pense que ça peut aider énormément. Aussi, faire une annonce. Ne pas prendre les Canadiens par surprise. Je regarde ce que vos collègues de l'Agence de la santé publique vivent en ce moment. Je ne veux pas d'information pour dire si leur projet d'aller chercher les données cellulaires était légitime ou pas. Tout ce que je sais, c'est qu'il n'y avait pas eu de préparation du public.

C'est probablement tout à fait légitime, ce que l'Agence fait, et c'est connu partout dans le monde, le fait de retracer les données cellulaires, c'est pertinents pour maîtriser une pandémie. Mais je pense qu'il faut être très sensible, justement, à la

susceptibilité des Canadiens face à la protection de leur vie privée, et donc aller au-devant. Et même si, tu le disais très bien tout à l'heure, nous, on est très convaincus parce que, bon, on a nos programmes, on sait que c'est bien d'aller chercher des données personnelles parce que notre programme est bon, mais plus que ça, on peut également savoir qu'on ne va pas chercher des données personnelles. Par exemple, dans le cas de l'Agence de la santé publique, il disent, « mais non, on ne va pas chercher les données personnelles », c'est dissocié de l'identifiant. Mais, le fait est que les Canadiens sont très susceptibles. Donc il faut aller même au-delà, est-ce que ça pourrait avoir l'air d'être une utilisation de données personnelles? Alors, vraiment comprendre le caractère névralgique de la question et donc être, comme on dit, proactif. Et disséminer l'information pour préparer les Canadiens à accepter ces projets de valorisation des données personnelles.

Éric Rancourt : Merci, ça me fait penser que les Canadiens sont en droit de s'attendre à avoir la possibilité de pouvoir commenter ou de pouvoir s'objecter. Ça ne veut pas dire qu'ils vont s'objecter, en fait, peut-être qu'ils ne vont jamais s'objecter à certaines choses qui nous semblent évidentes, mais c'est le fait d'avoir la possibilité de le faire. Puis ça me fait penser à un lien avec le consentement, le consentement dans le contexte public et privé, il y a des enjeux différents. Donc peut-être, si tu veux parler de ce qu'est le consentement, puis en quoi ça entre en jeu ou pas, dans le contexte des données pour le bien public.

Chantal Bernier : Voilà, alors, l'assise juridique de l'utilisation des données personnelles dans le secteur public, c'est la nécessité. Il s'agit fondamentalement de l'assise juridique. Un gouvernement collecte des données personnelles parce qu'il en a besoin, et c'est établi. Maintenant, il y a des utilisations des données personnelles, comme je le disais tout à l'heure. Par exemple, une étude longitudinale sur le rapport au marché du travail dans un certain groupe démographique, etc., où la notion de nécessité est peut-être un peu forcée. Alors, à ce moment-là, il faut aller chercher le consentement. Et donc le consentement doit être express, il doit être éclairé. Et il faut également communiquer aux individus leurs droits liés à leurs données personnelles. Alors, on va prendre l'exemple d'une étude longitudinale fondée sur le consentement. On offre à un groupe démographique de faire partie d'une étude, on va les suivre sur plusieurs années. Il faut absolument que ce soit identifié parce qu'on a besoin de retracer les données pour avoir, à la fin, une conclusion qui soit fiable. Et ils doivent savoir exactement dans quoi ils s'engagent. Ils doivent savoir également qu'ils ont le droit à l'accès à leurs données personnelles, que s'ils veulent faire une demande d'accès « mais qu'est-ce que vous avez sur moi? », etc. « Ça fait cinq ans que je fais partie de cette étude longitudinale, qu'est ce que vous avez sur moi? Qu'est-ce que… », etc. Ils y ont accès.

Il faut aussi leur dire qu'ils ont un droit de se plaindre, d'abord au ministère, à l'institution en question, mais ensuite aussi au commissariat. Donc on a vraiment deux situations tout à fait distinctes. Pour le secteur privé, c'est-à-dire là où la nécessité comble l'assise juridique, pas besoin de consentement. L'Agence canadienne du revenu, il ne me demande pas mon consentement. Et d'ailleurs bon, toi qui es à

Statistique Canada, tu te rappelles le débat d'il y a quelques années. Tu n'as pas besoin de consentement de répondre à un recensement ou non, parce qu'on n'a pas un recensement fiable, s'il n'est pas obligatoire, n'est-ce pas? Nécessité. Là où il y a le consentement, alors là, il doit être libre, éclairé et manifeste. Et aussi, il faut pouvoir le retirer. Mais là, ça c'est un petit peu compliqué parce que, pour une étude longitudinale, par définition, on veut des données sur le long terme.

Alors, si une personne… je ne sais pas, après une participation de cinq ans à l'étude qui est sur répartie sur 10 ans, décide de retirer son consentement, eh bien… Est-ce que ça peut s'appliquer, est-ce qu'on peut détruire les données qu'on a déjà sur cette personne? Alors ça, il faut évaluer, mais il faut que la personne le sache à l'avance, et il faut tout de même que la personne ait le droit de retirer son consentement ou, en tout cas, pour l'avenir. Pour les donner à percevoir. Et la troisième porte d'ouverture, on a nécessité, on a consentement, la troisième porte d'ouverture, c'est l'anonymisation. Mais là, il faut que ce soit dans un contexte où vous n'avez pas besoin de garder les identifiants.

Éric Rancourt : Merci. Puisqu'il est question d'anonymisation, je crois que le moment est venu d'aborder les pratiques de sécurité, car ces deux sujets sont étroitement liés. Donc, nous avons besoin d'intégrer des pratiques de sécurité aux systèmes de sécurité des TI pour protéger les données. J'aimerais que vous nous en disiez plus à ce sujet et que vous nous donniez les principales caractéristiques des pratiques exemplaires en place. Pourriez-vous également nous donner des exemples d'organisations qui œuvrent dans le domaine des données au Canada et qui ont un excellent bilan en la matière?

Chantal Bernier : Eh bien, vous venez de me rappeler une histoire, Éric. Un jour... C'était lorsque je travaillais pour le Commissariat à la protection de la vie privée du Canada. Un sous-ministre m'a appelée pour me dire qu'il aimerait concevoir un programme de protection des renseignements personnels. Il m'a demandé s'il y avait un ministère qui constituait la norme de référence en la matière. J'ai recommandé RHDCC, qui fait un excellent travail. Et un mois plus tard, RHDCC a dévoilé qu'il avait perdu un disque dur contenant les renseignements financiers de 500, peut-être de 3000 personnes. Comment ce fabuleux système a-t-il pu dérailler? À cette époque, j'ai demandé aux membres de mon personnel de mener une enquête afin de produire un rapport qui constituerait un document de référence pour tout le monde. Car RHDCC faisait un excellent travail. C'est relativement à un aspect de la gestion des actifs que RHDCC qui a fait défaut. Aucun employé n'avait été désigné comme responsable du disque dur.

Il n'y avait aucun registre qui indiquait « Chantal avait le disque dur en sa possession et était celle qui était censée le protéger. » Mais, autrement, RHDCC accomplissait un travail extrêmement impressionnant. Maintenant, passons aux organisations qui, selon moi, font un excellent travail en général. Qu'ont-elles en commun? Pourquoi, selon moi, RHDCC sort-elle du lot? Et quelle est mon opinion sur les nombreuses autres organisations? Certains de mes clients sont des organisations privées qui me confient qu'elles aimeraient mettre à niveau leurs systèmes. Et je me dis

alors qu'elles ont vraiment besoin de moi, car ce sont de très bons systèmes. Donc, qu'ont-elles en commun? D'abord, elles disposent toutes d'une structure très claire en matière de conformité à la *Loi sur la protection des renseignements personnels*. Il y a une personne à l'interne qui s'occupe uniquement de ce volet. Celle-ci occupe souvent le poste de chef de la protection des renseignements personnels. Cette personne dispose des ressources adéquates et occupe un poste suffisamment élevé au sein de l'organisation pour disposer de l'autorité nécessaire pour garantir la conformité.

Deuxièmement, ces organisations ont l'appui de la haute direction. Donc, dans votre cas, il s'agit du sous-ministre, du statisticien en chef, peu importe la structure de votre organisation. La haute direction doit donner son appui. Cette personne au sommet doit comprendre que la protection des données est devenue un risque institutionnel central. Vous devez faire de même. Ce qui signifie que cette personne doit être régulièrement informée. « Où en sommes-nous? » me demande le responsable de la confidentialité. Où en sommes-nous? Avez-vous vérifié? Le responsable de la confidentialité doit entretenir des liens étroits avec le dirigeant principal de la technologie ou le dirigeant principal de l'information, mais il ne peut s'agir de la même personne. Parce que le dirigeant principal de la technologie est la personne qui met en œuvre les politiques et les pratiques que le responsable de la confidentialité déploiera. Et le responsable de la confidentialité est la personne qui veille à ce qu'on les respecte. Donc, le DPT ne peut pas vérifier la conformité de son propre travail. Nous avons besoin de deux personnes, mais qui entretiennent une relation étroite. Ajoutons à cela les employés de ces personnes, qui doivent être pleinement mobilisés.

Les employés se rendent compte qu'ils constituent à la fois la première ligne de défense et la plus grande vulnérabilité. On entend souvent parler d'employés malhonnêtes aux nouvelles, par exemple. D'erreurs commises par des employés. Donc, les employés sont pleinement mobilisés, et on les forme de façon continue. Par exemple, tous les ans ou tous les six mois, des cours de formation sont offerts en fonction du niveau de sensibilité des données à protéger. Le personnel dispose d'un mois pour les suivre. Ces cours sont offerts en ligne. Les employés n'ont qu'à cliquer, à suivre les cours et à réussir ces derniers. Ils doivent répondre à des questions pour obtenir la note de passage. Si leur note n'est pas suffisamment élevée, ou s'ils ne se soumettent pas au test, ils perdent l'accès aux réseaux de l'organisation.

Pour terminer, il est important de disposer d'un plan d'intervention en cas d'atteinte. Ce dernier doit non seulement être impeccable et comporter des étapes très claires, mais doit aussi être présenté à tous les membres de l'organisation. Je me souviens d'un exemple où une personne responsable d'une entreprise m'a téléphoné un dimanche parce que, le matin même, une de leurs comptables s'était rendue au bureau pour travailler et avait remarqué quelque chose d'anormal. Et parce que le plan d'intervention en cas d'atteinte avait été si bien diffusé, elle savait exactement quoi faire et a pu prendre des mesures en moins de 30 minutes. Ils ont pris les choses en main et ont rebâti ce qui avait été atteint, ce qui a permis d'atténuer considérablement les

dégâts. Autrement dit, Éric, la meilleure façon de procéder, c'est de disposer d'un cadre de gouvernance exemplaire en matière de conformité aux mesures de protection de la vie privée distribué dans toute l'organisation et qui rallie véritablement les employés.

Éric Rancourt : Merci. Cela ressemble beaucoup à ce qu'a dit Catherine Luelo, la DPI du Canada, à savoir qu'il faut disposer d'une gouvernance suffisamment rigoureuse pour que nous, c.-à-d. tous les intervenants de l'organisation, nous remettions en question et nous préparions vraiment à faire face – non seulement faire face aux conséquences, mais réfléchir à l'avance à ce que nous faisons. Et ceci est lié aux questions que je vais maintenant vous poser. J'aimerais vous dire que nous partageons la tribune avec les gens. Alors, comment voyez-vous l'équilibre entre la vie privée et l'innovation? Comment peut-on utiliser la vie privée pour promouvoir l'innovation au lieu de l'entraver?

Chantal Bernier : C'est l'un de mes sujets préférés. Donc, pour moi, la vie privée n'est jamais un obstacle à quoi que ce soit, c'est une modalité. Elle ne peut donc pas freiner l'innovation. Elle fixe les modalités d'innovation. L'innovation peut se produire avec nos données personnelles, mais un grand potentiel d'innovation repose entièrement sur l'utilisation des données personnelles. Alors, qu'ont fait les grands innovateurs? Et je vous renvoie à l'Institut Alan Turing. Vous pouvez aller en ligne et regarder ce que l'Institut fait en matière de gouvernance concernant l'échange de renseignements, qui s'applique également ici. Et elle a adopté une forme que j'aime beaucoup, appelée « fiducie de données ».

Cela signifie donc que les organisations qui extrairont des données, qui partageront des données personnelles, qui adopteront un protocole ou qui créeront une entité, la fiducie de données sera le gardien de l'accès et du partage de renseignements. En fait, ce que vous faites à Statistique Canada se rapproche beaucoup de cela. Vous gérez l'accès des chercheurs aux fonds de données dont vous disposez. Et ce processus s'appuie sur un accès légitime, des fins légitimes, un accès très limité, et vous avez des pistes de vérification, vous les vérifiez; ces personnes peuvent seulement faire ce que vous leur autorisez à faire sur votre système ou avec les données, etc. Donc, ma réponse est que la protection de la vie privée détermine la manière dont nous innovons, mais elle n'empêche pas l'innovation. Et qu'il existe de plus en plus de modèles de gouvernance qui nous permettent de concilier la vie privée et l'innovation.

Éric Rancourt : Merci. Questions intéressantes. Par ailleurs, l'identification numérique unique peut-elle jouer un rôle dans l'amélioration de la vie privée, comme ce que fait l'Estonie depuis le début des années 2000?

Chantal Bernier : Tout à fait. Et bien sûr, l'Estonie est le modèle à suivre. Il est intéressant de savoir que l'identification numérique semble pousser les défenseurs de la vie privée dans deux directions opposées. Il y a ceux qui crient au meurtre parce qu'ils disent : « Oh mon Dieu, le gouvernement suit les citoyens ». Et puis il y a les autres qui disent, « Eh bien, non. Parce que cela permet à l'individu d'accéder à ses

données sous une identification qui, en réalité, est presque comme un code. Il s'agit donc d'une forme de protection de la vie privée. » L'Estonie est certainement considérée comme un modèle en raison de sa structure de gouvernance; elle dispose d'une plateforme X-Road et d'une structure de gouvernance qui permettent à diverses institutions d'utiliser l'identification du citoyen et d'y accéder. En bref, je crois que l'identification numérique a un énorme potentiel et qu'elle devrait être envisagée comme un moyen d'améliorer la transmission des données. Elle pourrait même améliorer la protection de la vie privée ou le partage des données entre les ministères, sans compromettre le droit à la vie privée.

Éric Rancourt : Merci. Voyons voir. Pour revenir sur le sujet des quatre filtres, s'agit-il d'un secteur où nous envisageons d'utiliser l'IA pour simplifier et améliorer le partage des données personnelles dans le domaine de l'application de la loi?

Chantal Bernier : D'après la façon dont les quatre filtres sont appliqués, ceux-ci n'ont jamais, à ma connaissance, été utilisés pour l'IA. C'est vraiment du travail communautaire. On cherche surtout à rassembler les acteurs communautaires autour de... La prévention de la criminalité est vraiment une approche à divers volets. On ne devient pas un criminel en raison d'un seul facteur. En ce qui concerne l'IA, les règlements sont en cours d'élaboration, comme vous le savez. La nouvelle loi québécoise sur les renseignements personnels pour le secteur privé contient désormais des dispositions sur l'utilisation de systèmes de décision automatique. Au gouvernement du Canada, vous avez les lignes directrices sur la transparence de l'IA. Donc, à ma connaissance, l'approche des quatre filtres n'a jamais été appliquée à l'IA, mais on s'affaire à concevoir d'autres mesures de protection de la vie privée liées à l'IA. Et la transparence fait partie de ces mesures, la transparence des algorithmes, parce qu'elle permet l'exercice du droit d'accès à des renseignements particuliers. Si vous avez l'intention d'utiliser mes données personnelles par le biais de l'IA et que je vous demande comment vous avez procédé, vous devez être en mesure de l'indiquer. C'est pourquoi les algorithmes doivent être transparents. Voilà donc un exemple d'intégration de la vie privée à l'IA.

Éric Rancourt : Oui. Merci. La question suivante, je pense, vise à obtenir des précisions ou des explications sur ce que vous avez dit au sujet du consentement. Selon ma compréhension et en vertu des conseils que nous recevons de Justice Canada, le fait de demander un consentement n'atténue pas le risque de violation de la Loi sur la protection des renseignements personnels lorsqu'il n'existe pas de fondement juridique. Êtes-vous d'accord avec cette interprétation?

Chantal Bernier : Tout à fait. Absolument. Ils mettent de l'avant la multiplicité des facteurs. Vous ne pouvez donc pas décider de demander le consentement pour obtenir des renseignements personnels sur quelque chose qui n'a rien à voir avec vos programmes et vos activités. Je suis donc tout à fait d'accord. Ils disent « ah oui », le consentement ne vous autorise pas à faire ce que vous voulez. Le consentement signifie simplement que si vous ne pouvez pas atteindre le seuil nécessaire pour quelque chose de facultatif, vous devez respecter le cadre de la Loi sur la protection

des renseignements personnels. En ce qui concerne la vie privée et les données recueillies directement auprès des personnes, vous disposerez alors d'une base plus solide pour ce que vous faites. Mais oui, ils ont tout à fait raison. Cela doit se faire dans le cadre de la Loi sur la protection des renseignements personnels.

Éric Rancourt : Merci. Ma prochaine question porte sur l'ouverture. Alors, dans quelle mesure serait-il réaliste de mettre en œuvre un cadre à conception ouverte pour la protection de la vie privée et le partage des données au sein du gouvernement du Canada?

Chantal Bernier : Eh bien, regardez ce que la Saskatchewan a fait. Il y a donc de plus en plus d'initiatives qui voient le jour et qui concernent le partage des données. L'idée de l'ouverture me préoccupe un peu. Je suis tout à fait en faveur d'un plus grand partage des données afin d'en tirer profit et d'obtenir de meilleurs résultats pour les Canadiens. Mais comme vous l'avez dit il y a un instant, les données doivent tout de même être gérées par un système très clair qui indique pour quelle raison vous les partagez, avec qui vous les partagez, combien vous en partagez, comment elles sont protégées, etc. Donc, selon moi, l'ouverture soulèverait certainement un problème de surveillance. Je vais vous donner un exemple concret. J'étais directrice des opérations pour l'appareil gouvernemental au Bureau du Conseil privé au moment où nous avons établi le CANAFE. Et la grande question était de savoir où placer le CANAFE. « Doit-on le placer sous la responsabilité du ministre de la Sécurité publique, qui était auparavant le solliciteur général? »

Et la réponse était « Non, on ne peut pas faire ça. » Parce que le ministre qui dirige le SCRS et la GRC se retrouverait en conflit d'intérêts lorsqu'il souhaiterait accéder aux données du CANAFE. Nous devons nous assurer que l'accès aux données du CANAFE, qui contient l'ensemble des données financières des Canadiens, est protégé. Ainsi, cet accès n'est pas ouvert, mais plutôt réglementé, ce qui explique pourquoi le CANAFE s'est retrouvé sous la tutelle du ministre des Finances. Je dirais donc que, même si je crois que nous devrions trouver des façons de partager les données, l'idée d'ouverture soulève un problème d'utilisation et de surveillance qui manque de cohérence. C'est peut-être une question de sémantique, mais c'est ainsi que je réagis au mot « ouvert ».

Éric Rancourt : Merci. L'idée des données ouvertes, ça me fait penser à un espace où les données sont vraiment très ouvertes, ce sont les médias sociaux, Twitter, Foursquare, etc. Les gens partagent l'information à des niveaux qu'on n'aurait peut-être jamais pensé… qu'ils oseraient le faire. Mais donc la société, les gens, peuvent-ils s'attendre à ce que les données soient utilisées pour l'intérêt général? On parle… C'est ouvert, mais ce n'est pas complètement ouvert. Puis la compréhension des gens n'est peut-être pas aussi mature, ou n'a pas maturé à la même vitesse que la prolifération des systèmes. Donc qu'est ce que tu en penses, de ça?

Chantal Bernier : Tout à fait. D'ailleurs, il y a un rapport d'enquête, précisément là-dessus, du commissariat à la protection de la vie privée du Canada, que j'avais

publiée à l'époque, c'était une enquête que j'ai dirigée. Il y en a un deuxième qui est sorti. Encore là sur les réseaux sociaux dernièrement, avec Daniel Therrien. Et le commissariat à la protection de la vie privée a très bien établi que les réseaux sociaux ne peuvent pas être considérés comme, essentiellement, un abandon du droit à la vie privée. Ce n'est pas parce qu'une personne a affiché des données personnelles sur les réseaux sociaux qu'une institution gouvernementale a le droit de les recueillir. D'abord, la *Loi sur la protection des renseignements personnels* indique que les institutions doivent recueillir les renseignements directement de la personne concernée. Bon, déjà, il y aurait contravention envers cette disposition.

Ensuite, il y a le fait qu'il y a une bifurcation, si on peut dire, dans l'utilisation. Une personne affiche ses données personnelles sur Internet… dans un certain but, avec certainement l'attente raisonnable que le gouvernement n'utilisera pas ces données à d'autres fins, des fins qui sont non annoncées, qui sont… Il y a une rupture, vraiment, dans les attentes en matière de vie privée, une notion juridique qui empêche cette utilisation. Donc si vous regardez la position du Commissariat à la protection de la vie privée du Canada, là-dessus, vous verrez bien que c'est très clair. Les données affichées sur les réseaux sociaux ne peuvent être considérées comme n'étant plus personnelles et comme étant disponibles au gouvernement pour quelque fin que ce soit.

Éric Rancourt : Merci. On a parlé tantôt un peu des personnes, des responsabilités. J'aimerais qu'on aille sur le côté des employés, puis les compétences et les comportements qui sont attendus parce qu'il y a des données de plus en plus. On le sait, c'est bien établi, il y a de plus en plus de gens qui vont être des manipulateurs et des estimateurs, des gens qui font de la modélisation, qui font des prévisions, tout ça. Mais ce n'est pas tout le temps des gens qui sont à l'affût des enjeux de vie privée et d'éthique des données. Donc, selon toi, quelles sont les compétences, puis les types de capacités qu'on devrait rechercher ou essayer de mettre en place dans la fonction publique, auprès des employés en général?

Chantal Bernier : Oui, alors une chose qu'on voit à travers toutes les organisations publiques ou privées où il y a une bonne protection des données personnelles, c'est qu'il y a une culture de protection des données personnelles. Et que cette culture est partagée. Parce qu'une chose que je vois beaucoup dans ma pratique, c'est exactement, comme tu viens de le dire… un groupe, par exemple d'ingénieurs, qui voit un potentiel extraordinaire dans les données personnelles. Mais ne sont pas tout à fait conscients, disons, des répercussions sur la vie privée. C'est normal, ils ont leur expertise, ils ont leurs objectifs.

Ou alors dans le privé, c'est les gens de marketing, qui voient une occasion en or de miner des données personnelles et ils sont vraiment imbus de cet objectif, c'est normal, ce sont des gens de marketing. Alors, comme on ne peut pas transformer tout le monde, ce qui est important, c'est de réunir tout le monde autour d'un cadre de responsabilisation, de la protection des données. Et là-dessus, je vais donner un exemple, encore une fois, un exemple concret. Google Street View. Alors, vous vous

rappellerez peut-être qu'en 2011, il a été découvert que Google, par son programme Street View, où une petite voiture se promène et filme toutes les rues pour ensuite de ça nous donner les résultats sur Street View, avait également capté des communications entières, des messages entiers, sur le système sans fil. Ils avaient capté ça.

Alors, c'est le commissaire à la vie privée de Hambourg, en Allemagne, qui l'a découvert, et il a alerté tous les autres commissaires. On a fait nos recherches, on a découvert qu'effectivement, il y avait des données des Canadiens également là-dessus, alors on a fait une enquête. Ce qui est ressorti de toutes ces enquêtes, le Federal Trade Commission aussi a fait une enquête… C'est qu'il y avait un problème de gouvernance, c'est-à-dire que Google donne 20 % de temps libre à ses ingénieurs pour, justement, innover. Créer, c'est génial. Un ingénieur avait développé un code qui, croyait-on, permettait de déterminer où étaient les *hot spots*, les routeurs, une cartographie des routeurs. Eh bien, quelle idée géniale, il insère ça dans Street View, alors que personne n'a vérifié qu'effectivement, ça ne faisait que ça. Mais ça ne faisait pas que ça, ça captait les conversations, les échanges au complet. C'était donc un problème de gouvernance. Cet ingénieur, il a bien fait son travail et tout ça, mais il n'était pas relié à un système organisationnel de conformité à la protection de la vie privée. Donc pour moi, c'est ça la solution. On ne peut pas changer les gens, on ne peut pas changer notre expertise, mais on peut se rassembler autour d'un objectif commun qui est la protection des renseignements personnels.

Éric Rancourt : Merci infiniment. Nous arrivons à la fin de notre discussion. Elle m'a semblé ne durer que quelques minutes. C'est toujours un plaisir de discuter avec vous. J'aimerais résumer brièvement certaines des choses que j'ai retenues et que vous avez dites. Les principes de protection de la vie privée sont ancrés dans la Charte, et il existe plusieurs lois connexes, comme la Loi sur la protection des renseignements personnels. Mais comme vous l'avez dit, on doit se tenir à jour. La nécessité constitue un point central des activités de protection de la vie privée secteur gouvernemental. Il est essentiel de bien définir et expliquer ce point.

C'était un bon conseil. Je ne passerai pas en revue tous les points, mais à deux ou trois reprises, vous avez énuméré ce qui peut être fait point par point. Et je suis sûr que cela sera très utile pour beaucoup de gens. Vous avez également insisté sur le fait qu'il s'agit d'une question de gestion des risques, qui se fait du haut vers le bas. Et comme vous l'avez dit il y a un instant, il s'agit aussi d'une question de culture. Il faut que ce soit une culture commune au sein de l'organisation. Et parfois, certaines personnes ont tendance à voir la vie privée comme un obstacle, mais c'est une modalité. Et comme vous l'avez dit, la question n'est pas de savoir si, mais comment. Ainsi, l'innovation peut être améliorée. Donc, peut-être en 30 secondes, pourriez-vous nommer les points principaux que nous devrions retenir de ce qui a été dit au cours de la dernière heure?

Chantal Bernier : Eh bien, je pense que vous avez déjà tout très bien résumé. En tant que fonctionnaires, vous êtes assujettis à la Charte, qui interdit l'utilisation des

renseignements personnels, à moins que celle-ci ne soit raisonnablement justifiée au sein d'une société libre et démocratique. Et cela comprend la réalisation de vos objectifs à l'aide de renseignements personnels. Je pense donc que si vous fondez votre travail sur ce paradigme, vous serez en position de force pour valoriser les données personnelles.

Éric Rancourt : D'accord. Merci infiniment, Chantal. Ce fut un plaisir. Voilà qui conclut la séance. J'aimerais remercier Chantal et l'auditoire. Thank you, merci, miigwetch.

[00:55:52 Le vidéoclavardage s'estompe et laisse place au logo de l'EFPC et à l'adresse « canada.ca/ecole-school ».]

[00:55:59 Le logo du gouvernement du Canada apparaît, puis l'écran devient noir.]