

Observations écrites au sujet de l'*Examen 2026 de la Loi sur la protection des renseignements personnels : approches stratégiques*

10 juillet 2026

Introduction

Nous nous réjouissons de l'occasion de nous prononcer sur le document ***Examen 2026 de la Loi sur la protection des renseignements personnels : approches stratégiques*** du Secrétariat du Conseil du Trésor du Canada (le « document »). Nos commentaires sont le fruit du travail d'un ***groupe de travail spécial*** composé d'avocates et d'universitaires spécialisées en droit du travail, de représentantes et représentants syndicaux et de leaders du mouvement syndical. Leurs noms sont fournis à l'annexe A des présentes.

Le groupe réuni des personnes aux horizons professionnels variés qui ont de l'expérience dans la représentation de travailleuses et travailleurs, l'offre de conseils à des équipes de négociation, la recherche en matière de protection de la vie privée et de relations de travail et la lutte pour des milieux de travail justes et équitables. Nous ne portons pas la voix d'une organisation en particulier, mais avons l'objectif commun de nous assurer que le cadre fédéral de protection de la vie privée protège adéquatement les travailleuses et travailleurs face aux pratiques changeantes lorsqu'il est question de technologies et de données.

Nous soutenons la refonte de la *Loi sur la protection des renseignements personnels* (la « *LPRP* ») et sommes ravis que le gouvernement reconnaisse que les avancées technologiques révèlent des lacunes dans le cadre existant. Nous sommes aussi heureux de pouvoir formuler des commentaires sur des thèmes ayant fait l'objet de consultations antérieures du gouvernement et des commissaires à la protection de la vie privée, vu le rythme fulgurant auquel évoluent les technologies, les pratiques en matière de données, les systèmes d'intelligence artificielle et les outils de surveillance au travail¹.

Des pratiques changeantes en matière de données et de vie privée dans les milieux de travail fédéraux

Pour les milieux de travail fédéraux, les réformes proposées arrivent à un moment où les institutions fédérales ont de plus en plus recours à des outils numériques et à des systèmes de prise de décisions automatisée, notamment l'intelligence artificielle (collectivement, les « systèmes numériques »), pour recueillir et analyser des renseignements sur le personnel et prendre des mesures à la lumière de ceux-ci.

La plupart des propositions dans ce document ont trait à l'utilisation de systèmes numériques en lien avec des renseignements personnels. Compte tenu de cette structure, nous estimons qu'il est fondamental que ces systèmes fassent l'objet d'une ***gouvernance continue*** plutôt que d'obligations à exécution unique.

Les avancées dans la surveillance, la gestion algorithmique, l'intelligence artificielle et la prise de décisions automatisée ont grandement accentué le volume et le caractère délicat des renseignements personnels recueillis au sujet du personnel. Ces nouvelles technologies promettant des gains d'efficacité s'accompagnent de risques pour les droits fondamentaux des travailleuses et travailleurs, notamment ceux à la vie privée, à l'équité, à l'égalité (y compris

¹ Commissaires fédéral, provinciaux et territoriaux à la protection de la vie privée et ombuds responsables de la protection de la vie privée (oct. 2023). « La protection de la vie privée des employés sur les lieux de travail modernes ». Québec (Qc). https://www.priv.gc.ca/fr/a-propos-du-commissariat/ce-que-nous-faisons/collaboration-avec-les-provinces-et-les-territoires/resolutions-conjointes-avec-les-provinces-et-territoires/res_231005_02/; Commissariat à la protection de la vie privée du Canada (mars 2008). *L'identification par radiofréquence (IRF) en milieu de travail : Document de consultation sur les recommandations de règles de pratique*. Ottawa (Ont.). Commissariat à la protection de la vie privée du Canada, en ligne : <https://www.priv.gc.ca/fr/a-propos-du-commissariat/ce-que-nous-faisons/consultations/consultations-terminees/rfid/>

l'absence de préjugés, de discrimination et de suppositions), à l'autonomie, à la dignité et à l'équité procédurale. À notre avis, une *LPRP* modernisée devrait répondre à ces nouveaux besoins dans des dispositions claires et exécutoires protégeant le droit à la vie privée dans les milieux de travail d'aujourd'hui.

La jurisprudence récente de la Cour suprême du Canada en lien avec l'article 8 de la *Charte canadienne des droits et libertés* a considérablement élargi la protection constitutionnelle quant à la confidentialité des renseignements, particulièrement dans des environnements numériques. La Cour reconnaît de plus en plus souvent que les atteintes à la vie privée ne proviennent plus seulement de divulgations isolées de renseignements personnels, mais aussi des capacités d'agrégation, d'analyse et d'inférence des systèmes modernes².

De plus, au Canada et ailleurs, de plus en plus d'analyses de politiques et de recherches s'attardent à l'accroissement de la surveillance du personnel depuis la pandémie de COVID-19³. Par exemple, un rapport publié en 2021 a examiné les formes de surveillance apparues avec les nouvelles technologies de télétravail et mis en lumière d'importantes lacunes dans les lois existantes en matière de protection de la vie privée et de droit du travail⁴. Plus récemment, une étude menée auprès d'employeurs au Canada a révélé une forte augmentation du recours aux technologies de surveillance avec l'avènement du télétravail (suivi des heures, de la navigation web et des frappes). Selon les conclusions de l'étude, [TRADUCTION] « si on peut justifier le recours à ces technologies en invoquant un "souci" pour le bien-être des travailleuses et travailleurs, elles peuvent aussi directement servir à les contrôler et à leur imposer des mesures disciplinaires⁵ ».

À notre avis, les réformes proposées devraient comprendre des protections légales contre la surveillance du personnel, la gestion algorithmique, les analyses et la prise de décisions automatisée. Sans ces protections, les changements proposés, particulièrement l'intégration des données à l'échelle de la fonction publique fédérale, risquent de mener à des pratiques incompatibles avec les principes constitutionnels en matière de vie privée et les valeurs fondamentales qui sous-tendent la gouvernance démocratique et les droits individuels et collectifs.

Les propositions arrivent aussi à un moment où les institutions fédérales ont de plus en plus

² Voir : *Conseil scolaire de district de la région de York c. Fédération des enseignantes et des enseignants de l'élémentaire de l'Ontario*, 2024 CSC 22 (CanLII). Citant son arrêt *Cole*, la CSC conclut au paragraphe 140 que « les renseignements que contiennent les appareils connectés à Internet, d'un point de vue normatif, tendent à révéler "nos intérêts particuliers, préférences et propensions", et se situent donc "au cœur même de l'ensemble de renseignements biographiques" protégés par l'art. 8" ».

³ Bernhardt, Annette, Lisa Kresge et Reem Suleiman. *Data and Algorithms at Work: The Case for Worker Technology Rights*. UC Berkeley Labor Center, 3 nov. 2021; Aloisi, A. et De Stefano, V. (2022). Essential jobs, remote work and digital surveillance: Addressing the COVID-19 pandemic panopticon. *International Labour Review*, 161(2), 289-314. DOI: 10.1111/ilr.12219; Moore, Phoebe V et al. *Electronic Monitoring and Surveillance in the Workplace: Literature Review and Policy Recommendations*. Luxembourg, Office des publications de l'Union européenne, 2021.

⁴ Masoodi, M.J., Abdelaal, N., Tran, S., Stevens, Y., Andrey, S. et Bardeesy, K. (septembre 2021). « Workplace Surveillance and Remote Work: Exploring the Impacts and Implications Amidst Covid-19 in Canada. » Extrait de <https://www.cybersecurepolicy.ca/workplace-surveillance>.

⁵ Thompson, Danielle E. et Adam Molnar. « Workplace Surveillance in Canada: A Survey on the Adoption and Use of Worker Monitoring Applications. » *The Canadian Review of Sociology*, vol. 60, n° 4, 2023, pp. 801–19, <https://doi.org/10.1111/cars.12448>.

⁶ Redden, J., Brand, J., Sander, I., Warne, H., (septembre 2022). « Automating Public Services: Learning from Cancelled Systems. » Extrait de <https://carnegieuk.org/wp-content/uploads/2024/10/Automating-Public-Services-Learning-from-Cancelled-Systems-Final-Full-Report-2.pdf>

recours à des systèmes numériques pour recueillir et traiter de l'information sur la clientèle des services publics et prendre des mesures à la lumière de celle-ci. L'utilisation de systèmes de prise de décisions automatisée dans la fonction publique fait miroiter des gains d'efficacité, mais elle augmente aussi les risques pour les droits fondamentaux, dont ceux à l'équité, à l'égalité, à la dignité et à l'équité procédurale. Nombre de ces utilisations ont été contestées, suspendues ou abandonnées, ont fait l'objet d'importants correctifs ou ont été annulées en raison des préjudices réels ou potentiels pour la clientèle des services publics⁶.

La *LPRP* modernisée devrait contrer ces risques à l'aide de dispositions claires et exécutoires protégeant les droits de la clientèle des services publics.

Chaque proposition de réforme abordée dans les présentes l'est selon une structure uniforme. Nous résumons d'abord la proposition, puis énonçons des préoccupations du point de vue de la protection de la vie privée au travail. Nous posons ensuite des questions clés qui, à notre avis, méritent un examen plus approfondi par le gouvernement, et formulons des recommandations précises visant à renforcer le cadre proposé et à mieux protéger les droits des travailleuses et travailleurs en matière de vie privée. Nous offrons ces commentaires dans le but d'améliorer la transparence et la responsabilisation et d'obtenir des protections adéquates sans nuire aux besoins opérationnels légitimes des milieux de travail et du secteur public fédéraux.

Les protections doivent englober la collecte, l'analyse, le traitement, l'utilisation et la communication de renseignements personnels. Elles doivent comprendre des dispositions de nature procédurale, comme nous le décrivons dans les présentes observations. Elles doivent aussi reconnaître et intégrer toutes les protections offertes dans les conventions collectives; elles ne sauraient constituer des exceptions à celles-ci. Les protections prévues dans les conventions collectives qui dépassent les exigences de la *LPRP* doivent être maintenues et respectées. Les deux régimes (législation sur la protection de la vie privée et conventions collectives) doivent renforcer mutuellement leurs protections respectives.

Le droit à la vie privée est un droit fondamental, tout comme celui de ne pas subir de discrimination. Les droits à la libre négociation collective et au déclenchement d'une grève sont tout aussi fondamentaux. Chacun est garanti par la *Charte canadienne des droits et libertés*. Tout examen et toute révision de la *LPRP* concernant les travailleuses et travailleurs et leur emploi doit tenir compte de ces principes et les respecter.

Thème 1 : Facilitation des services intégrés : seulement après l'obtention de conseils et du consentement explicite

Proposition 1 – Communication de données à l'échelle du gouvernement – approche fondée sur l'objectif

On propose de permettre un plus grand partage de données personnelles et leur réutilisation d'une organisation ou d'un programme gouvernemental à l'autre, sans consentement, lorsque cela est jugé nécessaire pour l'intérêt public ou la prestation de programmes. On ne précise pas comment les données personnelles des travailleuses et travailleurs seraient traitées sous ce nouveau régime.

Préoccupations

Le gouvernement canadien n'est pas un simple fournisseur de services. C'est aussi le plus grand employeur au pays. Un régime de partage de données qui pourrait (ou pas, voir les autres préoccupations et recommandations des présentes) être avantageux pour la prestation de services publics soulève des questions particulières lorsque ces mêmes données peuvent avoir une incidence sur l'emploi d'une personne, les mesures disciplinaires prises à son sujet, son congédiement, les mesures d'adaptation ou la cote de sécurité lui étant accordées, son cheminement professionnel ou sa situation financière.

Les propositions 1 et 2 illustrent deux aspects du même problème fondamental. La proposition 1 pose la question : « À qui pouvons-nous communiquer les données? » La proposition 2 demande : « Quelle est la source faisant autorité quant à cette information? » et « Quelles sont les sources permises de données liées à l'emploi? »

Ensemble, elles créent la possibilité d'un dossier accessible à l'échelle du gouvernement qui pourrait contenir de l'information non liée à l'emploi (renseignements financiers et fiscaux personnels, recours aux services gouvernementaux, statut auprès de différents régimes comme l'immigration et l'assurance emploi) et suivre la personne tout au long de sa carrière. Même si ce n'est pas l'intention, le libellé de la loi doit fermer la porte à cette possibilité.

Le gouvernement doit préciser comment il entend traiter les données des fonctionnaires fédéraux selon ce nouveau plan. Une plus grande circulation des renseignements sur les travailleuses et travailleurs au gouvernement pourrait brouiller la ligne entre les données « ordinaires » liées au travail et les « données sensibles » liées à la situation personnelle (sur la santé, le comportement, la biométrie et la sécurité, et le dossier auprès des ressources humaines, y compris les mesures disciplinaires et renvois).

Pour en savoir plus, consultez la page [Fichiers de renseignements personnels ordinaires](#).

Questions

Le nouveau plan proposé pour le partage et la réutilisation des données personnelles visera-t-il aussi celles des fonctionnaires fédéraux? Si oui, quelles limites et quels mécanismes de surveillance seront mis en place pour s'assurer qu'elles soient communiquées de façon responsable aux différentes institutions?

Est-ce que d'autres protections sont prévues pour l'information sensible liée à l'emploi (évaluation du rendement, assiduité, dossiers disciplinaires et demandes de mesure d'adaptation)? Comment les travailleuses et travailleurs pourront-ils faire une contestation ou demander une correction ou une mesure de redressement si leurs renseignements personnels sont réutilisés ou communiqués d'une façon qui est inappropriée ou qui mène à des conséquences défavorables pour leur emploi?

Recommandations

- Reconnaître, à titre de principe fondamental sous-tendant toutes les lois adoptées et les protections mises en place en matière de vie privée, que le consentement de la personne travailleuse ou du syndicat qui la représente ne suffit pas à lui seul pour autoriser la collecte, l'utilisation, la communication ou la réutilisation de données sur le lieu de travail en raison du déséquilibre de pouvoir inhérent à la relation d'emploi. La loi doit prévoir des dispositions adéquates sur les avis (contenu et fin à laquelle l'information est destinée, notamment), le consentement éclairé (y compris la possibilité de le refuser) et le droit de contestation, d'appel et de redressement, le tout pouvant faire l'objet d'une révision humaine et être invoqué par une personne travailleuse et son syndicat (collectivement, des « protections procédurales adéquates »).
- Exclure par défaut les dossiers d'emploi du régime de communication à l'échelle du gouvernement fondé sur l'objectif, sauf pour les cas que la loi autorise expressément.
- Si une loi semble autoriser cette communication, elle doit :
 - être manifestement conforme aux articles 7, 8 et 15 de la *Charte canadienne des droits et libertés*;
 - être manifestement conforme à la *Loi canadienne sur les droits de la personne*;
 - être manifestement conforme aux droits relatifs à la vie privée prévus par les modifications proposées à la *LPRP*;
 - être manifestement conforme à l'équité procédurale;
 - exiger une évaluation exhaustive des facteurs relatifs à la vie privée comprenant expressément une analyse comparative entre les sexes plus et une analyse des répercussions sur l'équité, sous réserve d'un contrôle décrit ci-après, avant la mise en œuvre;
 - être soumise à la surveillance d'un organisme désigné doté d'un mandat clair, de définitions pour les concepts de nécessité et de proportionnalité et de pouvoirs, notamment celui d'interdire la collecte, la communication et l'utilisation de renseignements d'une personne travailleuse lorsque les circonstances le justifient. Voir à ce sujet les recommandations relatives aux propositions 15, 19, 20 et 22;
 - exiger une analyse de la nécessité et de la proportionnalité avant la transmission de tout renseignement sur une personne travailleuse à d'autres institutions – les motifs pourraient faire l'objet d'une publication, d'une révision, d'une supervision et d'une contestation par la personne touchée ou son syndicat, avant toute mise en œuvre. Les motifs doivent faire état d'une prise en compte d'autres solutions moins intrusives et, pour que la communication soit autorisée, une réflexion basée sur des données probantes doit démontrer que l'avantage anticipé l'emporte sur les préjudices potentiels en matière de vie privée, d'équité et d'équité procédurale;
 - créer une catégorie spéciale pour les renseignements sensibles sur les personnes travailleuses (santé, mesures d'adaptation, mesures disciplinaires, renvois, contrôle de sécurité, biométrie, enquêtes, gestion du rendement, finances personnelles, etc.), qui devra soit être complètement exclue soit être visée par des protections plus rigoureuses, et prévoir des dispositions exigeant que la personne travailleuse ou son syndicat soit informé de la collecte, de l'analyse, du traitement, de l'utilisation ou de la communication de tels renseignements et puisse s'y opposer;
 - offrir des droits en matière de transparence aux personnes travailleuses touchées et aux syndicats les représentant, y compris un avis de collecte de données personnelles ou sensibles et de communication entre ministères, et un historique des renseignements recueillis ou communiqués. Les personnes travailleuses et

- leurs syndicats devraient avoir le droit d'être informés de la collecte, de l'analyse, du traitement, de l'utilisation et de la communication de ces renseignements;
- créer des droits de consultation et de correction permettant aux personnes travailleuses ou aux syndicats de s'opposer aux collectes, analyses, traitements, utilisations et communications inexacts ou inappropriés avant que les données soient utilisées, à quelque fin que ce soit, mais particulièrement en présence de conséquences défavorables pour l'emploi;
 - interdire l'utilisation secondaire de données d'emploi pour des raisons disciplinaires ou de ressources humaines non liées, sauf si la loi l'autorise expressément, et même dans ce cas, sous réserve de dispositions permettant aux personnes travailleuses ou à leurs syndicats d'être informés de cette utilisation et de s'y opposer;
 - adopter des mesures de protection correspondantes en droit public à l'égard des risques de nouvelle communication des données au public, que ce soit en l'interdisant complètement ou en mettant en place des restrictions claires sur l'utilisation des données et leur communication au-delà de cette utilisation. Toute utilisation ou réutilisation de données doit être conforme aux articles 7, 8 et 15 de la *Charte canadienne des droits et libertés* et aux autres protections légales pertinentes. Toute réutilisation devrait être soumise aux mêmes protections procédurales rigoureuses que l'utilisation initiale.

Proposition 2 – Sources officielles de données numériques gouvernementales

On propose d'exiger que tous les programmes obtiennent des données personnelles auprès de sources officielles désignées plutôt que de les recueillir de nouveau.

Préoccupations

On ne sait trop comment un cadre de partage de données centralisé ou polycentrique fonctionnera dans les milieux de travail fédéraux. Par exemple, est-ce que ce régime élargi visera les décisions liées à l'emploi (embauche, promotion, imposition de mesures disciplinaires et cessation)? La proposition est vague sur la manière dont le gouvernement traitera les enjeux d'exactitude, de reddition de comptes et de sécurité. Des clarifications sont requises.

Questions

Comment le gouvernement s'assurera-t-il que les renseignements personnels sont exacts, à jour et utilisés uniquement à des fins appropriées et prévues? Quelles mesures seront mises en place pour protéger ce qui pourrait devenir une vaste base de données interconnectées sur les personnes travailleuses et citoyennes recueillies à différents moments et pour différents buts, surtout lorsque les personnes visées n'ont pas consenti à un partage interministériel ou intergouvernemental?

Recommandations

- Reconnaître, à titre de principe fondamental sous-tendant toutes les lois adoptées et les protections mises en place en matière de vie privée, que le consentement de la personne travailleuse ou du syndicat qui la représente ne suffit pas pour autoriser la collecte, l'utilisation, la communication ou la réutilisation de données sur le lieu de travail en raison du déséquilibre de pouvoir inhérent à la relation d'emploi.
- Prévoir des dispositions procédurales adéquates.
- Exclure les décisions (surtout, mais pas exclusivement, celles prises à l'aide d'algorithmes) et les dossiers liés à l'emploi de tout régime obligatoire de partage centralisé de données, sauf si le partage est expressément autorisé par la loi, manifestement nécessaire et proportionné et accompagné de mesures de protection procédurales adéquates. Voir à ce sujet les recommandations relatives à la proposition 1.
- S'assurer que toute « source officielle » de renseignements personnels est soumise à des normes rigoureuses en matière de gouvernance des données, notamment des exigences quant à l'examen régulier des données et à leur caractère exact, à jour et exhaustif. Les personnes travailleuses et leurs syndicats devraient avoir le droit de consulter, de corriger et de contester les renseignements inexacts en temps utile avant qu'ils servent à prendre une décision touchant à leurs droits ou à leur emploi.
- Interdire la réutilisation de renseignements recueillis à une fin précise pour prendre des décisions qui ne sont pas liées à cette fin concernant l'emploi, les mesures disciplinaires, la gestion du rendement ou la sécurité, sauf si la loi l'autorise expressément et que cela est manifestement nécessaire et proportionné.
- Exiger la réalisation d'une évaluation exhaustive des facteurs relatifs à la vie privée avant de constituer ou d'élargir des répertoires centralisés, en portant une attention particulière aux risques liés à l'agrégation, aux usages détournés, à la cybersécurité et aux usages secondaires non autorisés.

- S'assurer que ces répertoires centralisés et leurs fonctions sont soumis à la surveillance d'un organisme désigné doté d'un mandat clair, de définitions pour les concepts de nécessité et de proportionnalité et de pouvoirs, notamment celui d'interdire de tels répertoires ou de restreindre leur portée. Voir à ce sujet les recommandations relatives aux propositions 1, 15, 19, 20 et 22.
- L'accès aux données centralisées du gouvernement doit être encadré par des contrôles stricts fondés sur les rôles, des journaux d'audit complets et une supervision indépendante, pour que les renseignements personnels ne soient consultés que par les personnes qui ont un besoin opérationnel légitime.
- Informer la personne travailleuse et son syndicat lorsque les bases de données centralisées du gouvernement contiennent des renseignements sur la personne travailleuse et lorsque l'ajout d'importantes nouvelles catégories de données partagées est prévu. S'assurer que ces personnes ont accès à des dispositions procédurales adéquates, surtout si des renseignements inexacts ou une communication inappropriée sont susceptibles d'entraîner des conséquences défavorables pour l'emploi. Voir à ce sujet les recommandations relatives à la proposition 1.
- Reconnaître, dans la *LPRP*, que si la réduction de la collecte de renseignements en double est un objectif administratif légitime, l'efficacité n'est pas plus importante que le respect des droits fondamentaux en matière de vie privée, des droits de la personne, notamment ceux garantis par la *Charte*, de l'équité procédurale ou des obligations distinctes du gouvernement en sa qualité de plus grand employeur au Canada.

Proposition 3 – Évaluation des facteurs relatifs à la vie privée obligatoire

On propose de rendre obligatoires les évaluations des facteurs relatifs à la vie privée (EFVP) lorsque des renseignements personnels sont utilisés pour prendre des décisions au sujet de personnes, y compris de fonctionnaires fédéraux. Cela pourrait offrir à ces derniers une meilleure transparence et une responsabilisation accrue, car les ministères et organismes seraient tenus d'évaluer et d'atténuer les risques relatifs à la vie privée avant de mettre en place de nouveaux programmes ou de nouvelles technologies en milieu de travail, ou des processus décisionnels basés sur des données qui touchent l'emploi.

Le groupe de travail spécial appuie cette proposition. Nous souhaitons que les EFVP soient exigées par la loi.

Préoccupations

Les EFVP n'auraient pas à être réalisées de façon périodique ou continue; l'obligation serait déclenchée à la survenance de certains événements. Ce qui est alimenté par l'IA n'est pas immuable. Les systèmes numériques qui utilisent l'IA sont nécessairement dynamiques. Leur fonctionnement peut changer au fil du temps et des mises à jour, de l'entraînement successif, des modifications aux jeux de données, des nouveaux contextes de déploiement ou des modifications aux paramètres du système. L'évolution des systèmes d'IA et de l'apprentissage automatique peut aussi changer leur fonctionnement. Il peut y avoir des changements imprévus, et certains peuvent même passer inaperçus, car l'IA peut graduellement changer la façon dont elle évalue, raisonne et prend des décisions.

Cela s'explique du fait que la structure algorithmique fonctionne à partir de probabilités plutôt que de certitudes. Voilà pourquoi il faudrait évaluer les systèmes d'IA à des intervalles réguliers, et ponctuellement selon les besoins, plutôt qu'une seule fois à l'implantation ou avant une modification. Le fait que les EFVP soient requises seulement lorsque des renseignements personnels sont utilisés pour prendre une décision à propos de quelqu'un est préoccupant. L'EFVP est un outil essentiel qui aide les institutions fédérales à apprécier les risques associés à la collecte, à l'analyse, à l'utilisation, à la communication et à la rétention de données personnelles et favorise le minimalisme des données.

Questions

Les EFVP seront-elles obligatoires pour tous les systèmes numériques et autres technologies en milieu de travail qui recueillent, surveillent, analysent, utilisent ou communiquent des données sur le personnel, y compris les outils de surveillance et de gestion de la productivité et les systèmes de prise de décision utilisant l'IA?

Recommandations

- Faire des EFVP une obligation juridique lorsque des renseignements personnels sont recueillis ou utilisés pour prendre des décisions touchant des personnes. Une EFVP devrait être exigée pour toute utilisation de l'IA impliquant des renseignements personnels, notamment lorsque les données d'une personne sont utilisées aux fins d'entraînement, d'essai, de profilage, de catégorisation ou de classement des risques, ou autrement pour prendre des décisions relatives à l'institution ou au programme, même si la personne n'est pas directement touchée par la décision ou le résultat.
- Reconnaître, dans la *LPRP*, que les systèmes numériques utilisant l'IA ou autrement fondés sur des données sont dynamiques, et non statiques. Pour les systèmes numériques qui recueillent, surveillent, analysent, utilisent ou communiquent

des renseignements personnels ou s'en servent pour faire des recommandations, il ne suffit pas de réaliser une seule EFVP au moment de l'implantation. Il faut :

- exiger des révisions et mises à jour périodiques des EFVP pendant tout le cycle de vie des systèmes utilisant l'IA et des autres technologies à haut risque;
- revoir les EFVP dès qu'un changement important est apporté à un système, aux données qu'il utilise, à l'usage auquel il est destiné ou à ses fonctions décisionnelles, et à des intervalles prescrits même en l'absence de changement important;
- traiter l'EFVP comme une obligation continue de gouvernance, et non comme un exercice de conformité unique.
- Exiger expressément des EFVP pour les technologies en milieu de travail qui recueillent, surveillent ou analysent des renseignements sur le personnel, comme les systèmes de gestion de la productivité et autres technologies de surveillance, les outils de prise de décisions automatisée et les systèmes d'IA qui influent sur les décisions relatives à l'embauche, à la promotion, à l'évaluation du rendement, à la prise de mesures disciplinaires ou d'adaptation ou à la cessation d'emploi.
- Exiger expressément que les EFVP évaluent les risques en matière de vie privée et les répercussions potentielles sur les droits constitutionnels, les droits de la personne, les droits procéduraux, les biais algorithmiques, l'exactitude des données, la transparence et la capacité des travailleuses et travailleurs à comprendre et à contester les décisions prises par des systèmes numériques ou à l'aide de tels systèmes.
- Exiger que les ministères et les organismes, dans la réalisation des EFVP, consultent les personnes travailleuses touchées et leurs syndicats et collaborent avec eux, et ce, avant l'intégration de systèmes numériques et d'autres technologies à haut risque en milieu de travail qui utilisent des renseignements personnels.
- Rendre les EFVP d'importance accessibles au public, sous réserve seulement de limites légitimes liées à la sécurité ou à la confidentialité.

Thème 2 : Amélioration de la responsabilisation et de la transparence

Proposition 5 – Exigences de transparence pour l'utilisation de l'IA et de systèmes décisionnels automatisés

On propose d'exiger que les institutions fédérales informent les personnes lorsque l'IA ou des systèmes décisionnels automatisés sont utilisés pour prendre des décisions qui ont une incidence sur elles et expliquent comment la décision a été prise et quelles données personnelles ont été utilisées. Les personnes touchées pourraient vérifier l'exactitude de leurs renseignements, demander des correctifs au besoin et solliciter une révision humaine si elles croient que le système a fait une erreur ou s'est appuyé sur des données incomplètes ou inexacts. Ces exigences s'appliqueraient seulement lorsque des systèmes décisionnels automatisés (SDA) sont utilisés pour prendre des décisions qui ont un effet direct sur l'accès d'une personne à des services, des avantages ou des droits, ou pour faciliter la prise de telles décisions.

Préoccupations

Le recours à des systèmes numériques, dont les SDA et l'IA, préoccupe beaucoup les fonctionnaires fédéraux. Les SDA et les systèmes d'IA sont souvent opaques; il est difficile pour les travailleuses et travailleurs de comprendre comment les décisions sont prises ou de contester des erreurs.

La transparence ne suffira pas à elle seule à régler le problème. Les dispositions législatives existantes en matière de transparence ne permettent déjà pas aux travailleuses et travailleurs de comprendre quels systèmes numériques sont utilisés et comment ils le sont. En ce qui a trait à cette proposition (et à la proposition 6), en plus d'exigences légales concernant le partage de renseignements, le gouvernement doit prendre des mesures pour promouvoir la participation démocratique en milieu de travail et s'assurer que les travailleuses et travailleurs et leurs syndicats sont consultés et peuvent participer véritablement à l'examen, au développement, à l'introduction et à l'utilisation des systèmes d'IA et des SDA.

Questions

Cette exigence s'appliquera-t-elle à toutes les décisions liées à l'emploi touchant les fonctionnaires fédéraux, y compris l'embauche, la promotion, la prise de mesures disciplinaires et d'adaptation, l'octroi de cotes de sécurité et la cessation d'emploi?

Quelles seront les mesures mises en place pour détecter et prévenir les biais et les effets discriminatoires dans les décisions en milieu de travail prises à l'aide de SDA ou de l'IA? Quels recours et quelles mesures de redressement sont prévus pour les travailleuses et travailleurs? Des mécanismes de contrôle sont-ils offerts aux travailleuses et travailleurs? Si oui, prévoient-ils un plein droit d'appel, pour faire en sorte que les principes d'équité procédurale et de justice naturelle et les droits de la personne, dont ceux prévus par la *Charte*, sont respectés? Les syndicats seront-ils consultés avant l'introduction de SDA ou de systèmes d'IA dans les milieux de travail fédéraux?

Recommandations

- Exiger de la transparence chaque fois qu'un SDA ou l'IA est utilisé pour prendre des décisions ayant une incidence sur des personnes, ou pour influencer grandement sur ces décisions. Le principe directeur devrait être de donner aux travailleuses et travailleurs et à leurs syndicats l'accès en temps utile à des recours efficaces pour contester une décision prise à l'aide de l'IA en raison de son inexactitude, d'un manquement à l'équité procédurale, de son caractère discriminatoire ou du fait qu'elle est basée sur une utilisation inappropriée de renseignements personnels. Il faut toutefois aussi reconnaître que la transparence ne suffit pas à elle seule à assurer l'équité, la responsabilisation et la conformité au droit administratif et aux obligations en matière de droits de la personne.
- Appliquer expressément les exigences légales suivantes à l'utilisation de l'IA ou de systèmes de prise automatisée de décisions liées à l'emploi qui touche les fonctionnaires fédéraux, notamment en matière de recrutement, d'embauche, de promotion, de gestion du rendement, de prise de mesures disciplinaires ou d'adaptation, d'octroi de cote de sécurité, de gestion des effectifs et de cessation d'emploi :
 - Les ministères et autres organismes gouvernementaux devraient consulter les travailleuses et travailleurs touchés et leurs syndicats, et collaborer avec eux, avant d'introduire un SDA ou un système d'IA qui surveille le personnel ou influe sur les décisions liées à l'emploi. Une véritable consultation doit être menée assez tôt pour influencer sur la conception, l'introduction et la gouvernance du système.
 - Lorsque l'IA ou un SDA est utilisé pour prendre des décisions liées à l'emploi, les appuyer ou influencer sur elles, les personnes travailleuses et les syndicats devraient avoir le droit :
 - d'être informés de l'utilisation à venir de l'IA ou du SDA;
 - de recevoir une explication éloquent, exacte et vérifiable de la façon dont le système a contribué à la décision;
 - de savoir quels renseignements personnels ont été utilisés;
 - de corriger les renseignements inexacts ou incomplets avant que la décision finale soit prise;
 - de demander une révision humaine par une personne décideuse ayant le pouvoir de modifier le résultat, et de connaître le nom de cette personne, de son poste et de la portée de son pouvoir de révision;
 - de contester la décision au moyen d'un mécanisme clair et transparent reposant sur les principes de justice naturelle et d'équité, qu'il soit prévu par la loi (pour les personnes travailleuses non représentées) ou par une clause contractuelle obligatoire, sous réserve des dispositions sur les griefs et l'arbitrage (pour les personnes représentées), avec de plein droit d'appel.
- Interdire, dans la loi, aux institutions fédérales de s'appuyer principalement sur des décisions automatisées pour prendre des décisions d'emploi qui ont une incidence importante sur les droits, les moyens de subsistance ou le cheminement professionnel d'une personne travailleuse. Une véritable supervision humaine doit demeurer obligatoire.
- Exiger que les institutions fédérales réalisent régulièrement des essais et audits indépendants sur les systèmes d'IA pour vérifier leur exactitude, leurs biais, leur caractère discriminatoire et leur incidence disproportionnée sur des groupes protégés, fassent part de façon adéquate des résultats au public et mettent en place des mécanismes de révision et de redressement appropriés pour les personnes touchées par les incidences relevées. Les erreurs commises en raison de ces incidences doivent pouvoir être corrigées, surtout pour les personnes touchées.

Proposition 6 – Exigences en matière d’avis

On propose de rendre les avis de confidentialité plus explicites : ils devront être rédigés en langage clair, être faciles à trouver et être publiés dans un registre centralisé pour que les gens comprennent comment leurs données personnelles sont utilisées et communiquées. Un avis serait aussi obligatoire lorsqu’un SDA utilisant l’IA est utilisé pour prendre ou appuyer des décisions ayant une incidence sur des personnes.

Préoccupations

À lui seul, l’avis ne satisfait pas à l’exigence de consentement éclairé. Toute tentative de présenter l’avis seul comme un consentement implicite pourrait affaiblir les protections des fonctionnaires fédéraux en matière de vie privée et être vue comme une forme de consentement forcé, surtout dans les milieux de travail où la participation n’est pas facultative.

Questions

Comment le gouvernement s’assurera-t-il que les avis de confidentialité sont compréhensibles et cohérents d’un ministère ou organisme à l’autre, vu la complexité technique de bien des programmes, outils d’IA et SDA?

Les fonctionnaires fédéraux pourront-ils présenter une véritable contestation ou demander des précisions s’ils croient que l’avis de confidentialité ne reflète pas fidèlement les données qui ont été utilisées et la façon dont elles l’ont été?

Quelles mesures de protection feront en sorte que les exceptions à la remise d’un avis demeurent restreintes, justifiées et soumises à un contrôle indépendant?

Recommandations

- Reconnaître, à titre de principe fondamental sous-tendant toutes les lois adoptées et les protections mises en place en matière de vie privée, que l’avis seul n’est pas une mesure de protection suffisante; il doit être accompagné de dispositions procédurales adéquates.
- Préciser, dans la *LPRP*, que l’avis seul ne remplace pas la norme de consentement éclairé.
- S’assurer que les exceptions à la remise d’un avis demeurent restreintes, justifiées et soumises à un contrôle indépendant.
- La transmission d’un avis aux personnes travailleuses et à leurs syndicats doit avoir lieu *avant* que les données personnelles de la personne soient utilisées dans un système d’IA ou un SDA dans un contexte d’emploi. Un avis préalable devrait aussi être exigé pour l’utilisation d’un système d’IA ou d’un SDA dans la prestation de services publics.
- La *LPRP* devrait établir une protection minimale en matière de vie privée et des exigences minimales en matière d’avis pour les fonctionnaires fédéraux. Les protections prévues dans les conventions collectives en matière d’avis et de consultation qui sont supérieures aux exigences de la *LPRP* doivent être maintenues et respectées.
- Préciser, dans la *LPRP*, quels éléments doivent figurer dans l’avis, y compris les données personnelles recueillies, l’utilisation qui en sera faite, la fin de la collecte, les personnes ou le ministère ou l’organisme responsables des données, l’endroit où les données seront stockées, la fréquence à laquelle les données seront revues, la période pendant laquelle les données seront stockées et à quel moment elles seront détruites.

- Préciser, dans la *LPRP*, quels éléments doivent figurer dans l'avis concernant l'utilisation de l'IA ou d'un SDA, y compris les données personnelles utilisées pour prendre la décision, la nature, le but et la portée des décisions prises à l'aide de ces systèmes, la logique et les principaux paramètres ayant une incidence sur les résultats de l'IA ou du SDA, les types d'extrants produits, la personne, le fournisseur ou l'entité qui a créé le système d'IA ou le SDA et le fait que les travailleuses et travailleurs ont le droit de contester la décision et de corriger les données que le système a utilisées pour la prendre.

Thème 3 : Amélioration des mesures de protection pour l'ensemble du spectre de sensibilité des données

Proposition 7 – Reconnaître un spectre de sensibilité et d'identifiabilité des données

On propose de reconnaître que différents types de renseignements personnels demandent différents niveaux de protection, selon le degré de sensibilité et la facilité avec laquelle ils peuvent être rattachés à une personne. La sensibilité renvoie au degré de préjudice si les données étaient exposées ou mal utilisées.

Préoccupations

La proposition reconnaît que les données sensibles nécessitent des protections plus robustes, mais elle n'établit pas de limite claire pour la collecte, l'analyse, le traitement, l'utilisation ou la communication des renseignements hautement sensibles du personnel. Par ailleurs, elle ne dresse pas une liste exhaustive des données jugées sensibles et omet certains critères comme l'identité de genre, d'autres identités protégées par les droits de la personne et l'adhésion à un syndicat ou à un autre agent négociateur.

Questions

Est-ce que les renseignements propres à une personne travailleuse (dossier de santé, demandes de mesures d'adaptation, données biométriques, dossiers disciplinaires, cote de sécurité, adhésion à un syndicat, information sur l'équité et la diversité) seront explicitement reconnus comme des renseignements personnels sensibles nécessitant une protection renforcée?

Quelles restrictions s'appliqueront à la collecte, à l'analyse, au traitement, à l'utilisation, à la communication et à la rétention de données sensibles sur les personnes travailleuses, et ces dernières seront-elles informées lorsque ces données sont communiquées ou utilisées pour une autre fin que celle prévue lors de la collecte initiale? Comment le gouvernement empêchera-t-il les données dépersonnalisées concernant des personnes travailleuses de permettre à nouveau leur identification, d'être combinées à d'autres jeux de données ou d'être utilisées pour créer des profils servant à l'analyse de la main-d'œuvre, à la gestion du rendement ou à l'imposition de mesures disciplinaires, entre autres fins?

Les syndicats seront-ils consultés avant que les ministères ou les organismes introduisent de nouvelles technologies ou de nouveaux programmes qui recueillent, analysent, traitent, utilisent ou communiquent des renseignements sensibles sur les personnes travailleuses, comme des données biométriques, comportementales ou démographiques?

Quels seront les recours et mesures de responsabilisation en cas d'atteinte aux droits à la vie privée impliquant des renseignements sensibles sur une personne travailleuse, en particulier si cette atteinte a des effets sur son emploi, sa réputation, sa cote de sécurité, ses droits fondamentaux ou sa sécurité?

Recommandations

- Reconnaître, à titre de principe fondamental sous-tendant toutes les lois adoptées et les protections mises en place en matière de vie privée, que les renseignements n'ont pas à être désignés comme étant sensibles pour avoir le potentiel de causer un préjudice. Par

précaution, les renseignements comme l'assiduité, les congés et les demandes de mesures d'adaptation devraient être automatiquement considérés comme étant sensibles. Cela dit, même les renseignements qui ne sont pas catégorisés ainsi peuvent causer un préjudice à une personne, car ils révèlent ou sous-entendent l'existence, la nature ou les particularités de sa situation personnelle. Ainsi, tous les renseignements personnels doivent être considérés et évalués sous l'angle de leur sensibilité. Une omission à cet égard peut mener à un manquement aux protections en matière de vie privée, à la *Loi canadienne sur les droits de la personne* et à la *Charte*.

- Créer, pour les renseignements sensibles sur les personnes travailleuses, une catégorie spéciale visée par les mesures de protection les plus rigoureuses. Des interdictions et des restrictions particulières devraient s'appliquer à la collecte, à l'analyse, au traitement, à l'utilisation, à la communication et à la rétention de tels renseignements.
- Imposer des limites strictes à la collecte, à l'utilisation, à la rétention et à la communication des renseignements sensibles des personnes travailleuses.
- Reconnaître explicitement que les renseignements propres à une personne travailleuse (dossier de santé, demandes de mesures d'adaptation, données biométriques, dossiers disciplinaires, cote de sécurité, adhésion à un syndicat, information sur l'équité et la diversité) sont des données personnelles sensibles nécessitant une protection renforcée.
- Interdire la collecte, l'utilisation et le traitement de données hautement sensibles, comme les données biométriques et celles provenant de technologies de reconnaissance des visages et des émotions.
- Informer les personnes travailleuses et leur syndicat lorsque des données sensibles à leur sujet sont communiquées ou utilisées pour une autre fin que celle prévue lors de la collecte initiale.
- Interdire la communication de données sensibles dépersonnalisées concernant des personnes travailleuses, vu le risque qu'elles permettent à nouveau de les identifier.
- Interdire la combinaison de jeux de données comprenant des données sensibles sur des personnes travailleuses à d'autres jeux de données.
- Interdire la création de profils sur des personnes travailleuses (dépersonnalisés ou non) aux fins d'analyse de la main-d'œuvre, de gestion du rendement ou d'imposition de mesures disciplinaires, en particulier lorsqu'ils contiennent des données sensibles.
- Prévoir des recours et des mesures de responsabilisation en cas d'atteinte à la vie privée impliquant des renseignements sensibles sur une personne travailleuse. Les recours devraient comprendre la correction ou la suppression des renseignements, la cessation de l'utilisation concernée, la suppression des renseignements aux fins d'autres pratiques de l'employeur, des dommages-intérêts et des décisions de la ou du commissaire à la protection de la vie privée pouvant être exécutées par les tribunaux.

Proposition 9 – Obligation légale de protéger les renseignements personnels stockés ou traités à l'extérieur du pays

Cette proposition rendrait obligatoire pour les institutions fédérales la mise en place de mesures de sécurité physiques, techniques et administratives pour protéger les renseignements personnels qu'elles détiennent, notamment lorsqu'ils sont stockés ou traités à l'extérieur du pays ou dans toute autre situation présentant un risque. Ces mesures devraient tenir compte de la nature des renseignements et des risques connexes.

Préoccupations

Cette proposition soulève d'importantes préoccupations pour les fonctionnaires fédéraux si leurs renseignements personnels devaient être stockés, traités ou consultés à l'extérieur du pays, où ils pourraient être assujettis à des lois étrangères, à des demandes d'accès gouvernemental ou à des régimes de protection de la vie privée qui ne correspondent pas aux normes canadiennes. Nous craignons que les renseignements transférés à l'extérieur du pays ne bénéficient pas de la même protection que ceux stockés ici. Si des renseignements personnels sont stockés, traités ou consultés à l'extérieur du pays, les travailleuses et travailleurs concernés pourraient être exposés à des risques d'atteintes à la vie privée à l'étranger (p. ex., profilage, surveillance, discrimination, détention et arrestation, accusations criminelles ou administratives, incarcération, expulsion, représailles ou autre utilisation abusive de leurs renseignements). Les pratiques transfrontalières en matière de données peuvent accroître les risques auxquels sont exposés les travailleuses et travailleurs autochtones, noirs, racisés, ayant un handicap, faisant partie de la communauté 2SLGBTQIA+, les femmes, les personnes proches aidantes, les personnes immigrantes ou ayant de la famille à l'étranger, les demandeurs d'asile, les personnes réfugiées, ainsi que les travailleuses et travailleurs prenant part à des griefs, à des arbitrages, à des plaintes ou à des activités de représentation syndicale.

Questions

Les renseignements personnels des travailleuses et travailleurs devraient-ils être stockés, traités ou consultés à l'extérieur du Canada?

Si la modification proposée prévoit que les renseignements personnels des personnes travailleuses seront traités à l'extérieur du pays, quelles mesures de protection seront mises en place pour garantir que les renseignements personnels des fonctionnaires fédéraux ne sont pas assujettis à une surveillance étrangère, à des obligations de divulgation imposées par des autorités étrangères ou à des normes de protection de la vie privée moins strictes?

Recommandations

- Reconnaître comme principe fondamental que les renseignements personnels des fonctionnaires fédéraux ne devraient être stockés, traités et consultés qu'au Canada, en particulier quand il s'agit de renseignements sensibles.
- Réduire au strict minimum les exceptions à l'interdiction de stocker, de traiter et de consulter à l'étranger les renseignements sur les travailleuses et travailleurs, en exigeant dans chaque cas une justification rigoureuse reposant sur des données probantes et la preuve que c'est nécessaire. Les raisons de commodité et d'efficacité ne constituent pas des justifications suffisantes et ne prouvent pas la nécessité.

- Interdire aux fournisseurs et aux entrepreneurs d'utiliser les renseignements personnels des fonctionnaires fédéraux pour entraîner, mettre à l'essai, améliorer ou développer des systèmes d'IA, des outils d'analyse, des ressources ou d'autres outils, sauf si la loi l'autorise expressément et sous réserve de la réalisation d'EFVP.
- Informer les personnes travailleuses et leurs syndicats lorsque les renseignements sont stockés ou traités à l'extérieur du pays et leur garantir le droit à des dispositions procédurales adéquates dans de telles situations.
- Veiller à ce que des mesures de protection robustes soient mises en place lorsque les renseignements personnels des travailleuses et travailleurs sont stockés ou traités à l'extérieur du pays, afin qu'ils ne soient pas assujettis à une surveillance étrangère, à des obligations de divulgation ou à des normes de protection de la vie privée moins strictes. La prise en compte des répercussions sur les travailleuses et travailleurs issus de groupes d'équité doit constituer un facteur d'analyse explicite lors de la réalisation d'EFVP ou d'autres processus visant à autoriser ou à refuser le stockage et le traitement de renseignements personnels à l'extérieur du pays.
- Garantir clairement aux travailleuses et travailleurs le droit de savoir où leurs renseignements sont stockés, quelles personnes ou institutions y ont accès, quelles lois leur sont applicables où ils sont détenus, de quelle manière ils peuvent être communiqués et à qui, ainsi que les recours dont ils disposent, notamment en cas d'atteinte à leurs droits. Lorsque les renseignements des travailleuses et travailleurs sont transférés, traités, stockés ou consultés à l'extérieur du pays, le risque auquel est exposée chaque personne peut accroître de façon importante, voire devenir extrêmement élevé. Les mesures de protection doivent être proportionnelles aux risques.

Proposition 10 – Ajouter le critère de nécessité au seuil de limitation de la collecte

Cette proposition ajouterait la nécessité comme critère d'évaluation préalable à toute utilisation de renseignements personnels, de sorte que la collecte soit limitée aux données raisonnablement requises pour atteindre un objectif clairement défini, directement lié à un programme opérationnel ou à une activité.

Préoccupations

Bien qu'une norme fondée sur la nécessité puisse offrir une meilleure protection en matière de vie privée, son efficacité pourrait être limitée dans la pratique. Les milieux de travail fédéraux sont déjà soumis à des niveaux importants de surveillance du personnel, d'analyse de la main-d'œuvre et de vastes pratiques de collecte de renseignements. Il y a un risque que les institutions interprètent la notion de « nécessité » de manière trop large, ce qui leur permettrait de continuer à recueillir de grandes quantités de renseignements sur les travailleuses et travailleurs. Sans une surveillance indépendante rigoureuse et des limites clairement établies, les exigences de nécessité risquent de devenir un simple exercice procédural plutôt qu'une véritable garantie contre la collecte excessive de renseignements et la surveillance en milieu de travail.

Questions

Comment la notion de « nécessité » sera-t-elle définie dans le contexte de la collecte de renseignements sur les travailleuses et travailleurs, et quelles mesures empêcheront les ministères et les organismes d'interpréter ce terme de manière si large que la surveillance et le suivi courants en milieu de travail puissent se poursuivre sans véritable encadrement?

Les ministères et organismes devront-ils démontrer qu'ils ont envisagé des solutions moins intrusives sur le plan de la vie privée avant de recueillir des renseignements sur les personnes salariées à des fins d'analyse de la main-d'œuvre, de surveillance, de mesure de la productivité ou d'autres fins liées à la gestion du milieu de travail?

Quels mécanismes indépendants de surveillance ou d'examen seront mis en place afin d'évaluer si la collecte est réellement nécessaire, proportionnée et justifiée?

Quelles limites seront imposées à la collecte de données télémétriques, comportementales, sur la productivité et d'autres données de surveillance des travailleuses et travailleurs pour prévenir une surveillance excessive ou injustifiée en milieu de travail?

Recommandations

- Définir le terme « nécessité » dans son sens le plus strict.
- Exiger une EFVP pour la collecte de renseignements personnels, comme indiqué dans la proposition 3. Ces EFVP devraient faire appliquer le critère de nécessité en obligeant les institutions à expliquer pourquoi les renseignements personnels sont nécessaires à la réalisation de la finalité visée, à évaluer si une méthode moins intrusive pour la vie privée permettrait raisonnablement d'atteindre cette finalité et, le cas échéant, à justifier au moyen d'une analyse fondée sur des éléments probants le rejet d'une telle méthode.

- Établir un mécanisme indépendant de surveillance ou d'analyse comprenant des procédures rigoureuses permettant d'évaluer que la collecte de renseignements sur les travailleuses et travailleurs répond à un besoin réel, demeure proportionnée et repose sur des motifs valables.
- Exiger des ministères et organismes qu'ils démontrent qu'ils ont envisagé des solutions de rechange moins intrusives pour la vie privée avant de recueillir des renseignements sur les personnes salariées à des fins d'analyse de la main-d'œuvre, de surveillance, de mesure de la productivité ou de toute autre activité de gestion du milieu de travail.
- Exiger que les mesures de suivi et de surveillance soient proportionnées, justifiées et le moins intrusives possible.
- Limiter la collecte de données télémétriques, comportementales, données liées à la productivité et d'autres données de surveillance des travailleuses et travailleurs afin de prévenir toute surveillance excessive ou injustifiée en milieu de travail.
- Interdire la collecte de données biométriques au moyen d'outils de reconnaissance des émotions, de reconnaissance faciale ou de tout outil visant à influencer le comportement humain dans le milieu de travail.

Proposition 11 – Nouvelle exigence d'éliminer des données personnelles non nécessaires

On propose d'exiger que les institutions fédérales éliminent les renseignements personnels qui ont été recueillis involontairement ou qui ne sont plus nécessaires pour l'accomplissement de l'objectif initial. On espère ainsi atténuer les risques associés à la rétention excessive de données.

Préoccupations

L'exigence d'éliminer les données non nécessaires pourrait être incompatible avec l'obligation de conserver des dossiers pour des litiges anticipés ou en cours liés au travail (congédiement injustifié ou plainte en droit de la personne, par exemple). L'absence de dossiers dans ces circonstances peut porter atteinte aux droits des travailleuses et travailleurs.

Il faut trouver l'équilibre entre la volonté d'éliminer les données non nécessaires et l'obligation de conserver les dossiers pour des litiges anticipés ou en cours.

Cette exigence pourrait être incompatible avec l'obligation normale de l'employeur de conserver des dossiers d'emploi de base exacts sur son personnel.

Questions

Comment va-t-on définir l'expression « nécessaires pour remplir l'objectif pour lequel on les a recueillies » dans le contexte des données liées au travail, et qui décidera quand il faut les supprimer ou les conserver?

Quels mécanismes de surveillance ou d'audit indépendants seront mis en place pour vérifier que les ministères et les organismes éliminent promptement et avec assiduité les renseignements personnels des travailleuses et travailleurs dont ils n'ont plus besoin?

Recommandations

- S'assurer que la *LPRP* exige la conservation des dossiers lorsque nécessaire pour des litiges en cours liés au travail, notamment les affaires de congédiement injustifié ou de plaintes en droits de la personne.
- Définir l'expression « nécessaires pour remplir l'objectif pour lequel on les a recueillies » dans le contexte des données liées au travail et déterminer, en consultation avec les syndicats, quelles sont les données sur les travailleuses et travailleurs qui doivent être supprimées et lesquelles doivent être conservées.
- Prévoir des mécanismes de surveillance ou d'audit indépendants pour vérifier que les ministères et les organismes éliminent promptement et avec assiduité les renseignements personnels des travailleuses et travailleurs dont ils n'ont plus besoin et conservent ceux qui sont encore nécessaires.

Proposition 12 – Modifier la *LPRP* pour faire de la protection de la vie privée un droit fondamental

Cette proposition vise à mettre à jour la *LPRP* afin de reconnaître, dans le préambule ou l'objet de la *Loi*, la protection de la vie privée comme un droit fondamental, de souligner l'importance de faciliter les services et de promouvoir la réconciliation avec les peuples autochtones.

Préoccupations

Nous sommes d'accord avec le fait de reconnaître le droit à la vie privée comme un droit fondamental. Protéger la vie privée, c'est favoriser la participation démocratique, la liberté et l'épanouissement personnel au sein des institutions sociales. Toutefois, selon la proposition, la reconnaissance de ce droit ne serait mentionnée que dans le préambule. Comme les préambules sont sujets à interprétation et ne sont pas exécutoires, nous craignons que la reconnaissance du droit à la vie privée comme droit fondamental ne se traduise pas par des mesures de protection concrètes pour les fonctionnaires fédéraux.

Cette reconnaissance doit aussi s'inscrire dans une perspective antiraciste et anticoloniale. Par exemple, ce n'est pas tout le monde qui vit la surveillance de la même manière, au travail comme à l'extérieur. En effet, les travailleuses et travailleurs autochtones, noirs, racisés, ayant un handicap, faisant partie de la communauté 2SLGBTQIA+, les femmes, les personnes proches aidantes, les personnes immigrantes ou ayant de la famille à l'étranger, les demandeurs d'asile, les personnes réfugiées, ainsi que les travailleuses et travailleurs prenant part à des griefs, à des arbitrages, à des plaintes ou à des activités de représentation syndicale sont souvent marginalisés et plus surveillés que le reste de la population. Les communautés autochtones et noires sont encore aujourd'hui surveillées de façon disproportionnée.

Questions

Que fera le gouvernement pour s'assurer que de considérer les données personnelles comme un « atout stratégique » n'entraînera pas la collecte accrue ou l'utilisation secondaire des renseignements personnels des fonctionnaires fédéraux à des fins de surveillance ou de gestion du rendement?

Reconnaître le droit à la vie privée comme un droit fondamental dans la *LPRP* donnerait lieu à quelle sorte de protections procédurales concrètes, exécutoires et adéquates, outre les orientations interprétatives qu'on retrouverait dans le préambule et l'objet de la *Loi*? Si la disposition en question ne prévaut pas expressément sur les lois ou les politiques contradictoires, en quoi cela donnerait-il au droit à la vie privée le statut juridique de droit fondamental, en particulier lorsque d'autres exigences légales ou opérationnelles ont préséance?

Recommandations

- Reconnaître dans le texte de la *Loi*, et pas seulement dans le préambule, le droit à la vie privée comme droit fondamental, et l'accompagner de protections procédurales concrètes, exécutoires et adéquates, et non seulement d'une mention dans le préambule ou l'objet, pour éviter de laisser place à l'interprétation.
- Préciser comment ce droit fondamental à la vie privée s'articulera avec les lois et les politiques contradictoires, et veiller à ce que son poids soit suffisant et généralement prépondérant par rapport aux intérêts concurrents et aux autres dispositions législatives.

- Préciser expressément dans la *LPRP* que le fait de considérer les renseignements personnels comme des « atouts stratégiques » ne pourrait servir de motif pour justifier une collecte à grande échelle ou une utilisation secondaire des renseignements personnels des travailleuses et travailleurs à des fins de surveillance, de mesure de la productivité ou de gestion du rendement.

Proposition 13 – Intégrer des principes dans la *LPRP* afin de renforcer les pratiques relatives à la protection de la vie privée et d’harmoniser la loi avec celles du secteur privé et d’autres normes internationales

Cette proposition vise à moderniser la *LPRP* en y intégrant des principes reconnus de protection de la vie privée issus de cadres nationaux et internationaux (Règlement général sur la protection des données [RGPD]), notamment la reddition de compte, le minimalisme des données, la sécurité et la transparence.

Préoccupations

L’arrimage à ces cadres internationaux permettrait d’intégrer au contexte canadien plusieurs concepts clés en matière de protection de la vie privée. Nous sommes favorables à la modernisation de la *LPRP* par l’intégration de principes reconnus en matière de protection de la vie privée, comme la reddition de compte, le minimalisme des données, la sécurité et la transparence, mais la proposition contient également plusieurs termes vagues et non définis. Plus précisément, les notions de « nécessité », de « proportionnalité » et d’« efficacité » peuvent être interprétées de manière à justifier une collecte de données à grande échelle et une surveillance continue au travail. Pour éviter un tel problème, il faudrait définir clairement ces concepts et les accompagner de dispositions procédurales adéquates.

Questions

Comment seront définies les notions de « nécessité », de « proportionnalité » et d’« efficacité » pour assurer leur application uniforme et empêcher les différences d’interprétation entre les organisations? Quelles dispositions procédurales adéquates permettront aux travailleuses et travailleurs de contester efficacement les cas de non-conformité sans se heurter à des obstacles (coûts, complexité, crainte de représailles, etc.)?

Recommandations

- Définir dans la *LPRP* certains concepts, notamment ceux de « nécessité », d’« intrusion minimale », d’« efficacité » et de « proportionnalité », avec des critères assez précis pour garantir une application uniforme et éviter de laisser place à l’interprétation.
- Appliquez ces définitions au seuil renforcé pour la collecte mentionnée à la proposition 10.
- Prévoir dans la *LPRP* des mécanismes d’application et des recours accessibles et efficaces pour les travailleuses et travailleurs et leurs syndicats, dans le but d’éliminer les obstacles liés aux coûts, à la complexité et aux délais et de protéger contre les représailles les personnes qui soulèvent des préoccupations en matière de protection de la vie privée.
- Exiger que ce soient les institutions gouvernementales, et non les travailleuses et travailleurs individuellement, qui doivent justifier la nécessité, l’intrusion minimale, l’efficacité et la proportionnalité de la collecte des renseignements personnels.

Proposition 15 – Harmoniser le régime de demandes en intégrant les demandes de données personnelles dans la *Loi sur l'accès à l'information (LAI)*

Cette proposition vise à retirer le processus de demande de renseignements personnels de la *LPRP* et de l'intégrer à la *LAI*.

Préoccupations

L'intégration du processus de demande de renseignements personnels dans la *LAI* risque d'affaiblir les mesures de protection propres à la *LPRP*, puisque la *LAI* vise principalement l'accès aux documents gouvernementaux, et non la protection des renseignements personnels sensibles. Cela pourrait confondre les travailleuses et travailleurs quant aux règles qui s'appliquent à leurs renseignements personnels et mener à une application inégale des exemptions ou des droits d'accès.

Questions

Comment le processus harmonisé enchâssé dans la *LAI* garantira-t-il une protection des renseignements personnels équivalente à celle actuellement prévue dans la *LPRP*? Sur quels critères s'appuieront les exemptions (notamment en ce qui concerne les dossiers médicaux, les autorisations de sécurité ou d'autres renseignements sensibles sur les travailleuses et travailleurs) afin de garantir des droits d'accès et de correction suffisants? Comment le gouvernement garantira-t-il la cohérence et la clarté de ce régime d'accès combiné pour que les travailleuses et travailleurs comprennent leurs droits et les procédures applicables aux demandes liées aux données personnelles?

Recommandations

- Préciser la différence entre, les demandes d'accès à l'information et les mécanismes permettant de contester l'utilisation de renseignements personnels au moyen de dispositions procédurales concrètes. Pour chaque processus, préciser l'instance chargée de la surveillance. Préciser le régime ou les règles qui s'appliquent à chaque catégorie.
- Veiller à ce que le régime harmonisé préserve expressément les normes de protection de la vie privée prévues dans la version actuelle de la *LPRP* et s'assurer que cette harmonisation ne restreignent pas les droits actuels des travailleuses et travailleurs en matière d'accès, de correction ou de protection.
- Réglementer le recours aux exceptions entourant les renseignements personnels des travailleuses et travailleurs au moyen de critères clairs et strictement définis, de manière à préserver toute la portée des droits d'accès et de correction.
- Établir un ensemble de règles distinctes et clairement identifiables concernant les demandes de renseignements personnels dans le cadre d'un régime combiné, afin que les travailleuses et travailleurs comprennent facilement quelles mesures de protection et quelles procédures s'appliquent à leur cas. Les renseignements inexacts, incomplets ou utilisés à mauvais escient doivent pouvoir être corrigés dans le cadre d'un régime combiné.

Thème 5 : L'accès des peuples autochtones à leurs données et protection de celles-ci

Proposition 17 – Définir les données personnelles autochtones comme étant soumises à des considérations distinctes en matière de gouvernance

Les données personnelles des peuples autochtones qui ne sont pas désignées comme données personnelles autochtones seraient gérées et communiquées conformément au reste de la *LPRP*. Il s'agirait, entre autres, de données qu'une personne a choisi de ne pas consentir à ce qu'elles aient cette désignation, de données précédant l'ajout de la désignation et celles appartenant à un ensemble de données non lié aux programmes clés définis dans la proposition 18.

Préoccupations

Les données personnelles des fonctionnaires autochtones sont parfois considérées comme des « données personnelles autochtones » et parfois traitées comme les autres types de renseignements visés par la *LPRP*, ce qui pourrait engendrer des lacunes dans la gestion des renseignements confidentiels. Nous appuyons la mise en place d'un cadre de gouvernance distinct pour les données autochtones, mais nous craignons que le fait de classer certains renseignements comme des « données personnelles autochtones » alors que le reste des données serait assujéti à la *LPRP* ne fragmente en deux régimes la gouvernance de l'information liée à l'emploi des fonctionnaires fédéraux autochtones, au risque de donner lieu à une application variable des règles et à un niveau de protection inégal.

Questions

Comment le cadre garantirait-il une protection uniforme des renseignements personnels des travailleuses et travailleurs autochtones, alors que certaines parties de leurs données liées à l'emploi sont classées différemment selon qu'elles appartiennent à la catégorie des « données personnelles autochtones » ou qu'elles relèvent de la *LPRP*? Quels mécanismes permettront aux travailleuses et travailleurs autochtones de comprendre, d'examiner ou de contester la manière dont leurs données personnelles liées au travail sont classées et gérées au fil du temps, particulièrement en ce qui concerne les dossiers d'archives ou datant de plusieurs années?

Comment le gouvernement compte-t-il éviter les lacunes ou les disparités dans les normes de protection de la vie privée pour le personnel autochtone, considérant que des types de données similaires sont assujettis à des règles de gouvernance différentes?

Recommandations

- Faire en sorte que le cadre offre aux travailleuses et travailleurs autochtones un mécanisme clair et révoquant de consentement éclairé pour la collecte, l'analyse, le traitement, l'utilisation ou la communication des données d'emploi des travailleuses et travailleurs autochtones.
- Fournir au personnel autochtone les moyens de comprendre, d'examiner et de contester la classification et la gestion de leurs données liées au travail, y compris les dossiers d'archives ou datant de plusieurs années qui sont antérieurs à la désignation, en prévoyant des dispositions procédurales concrètes.

- Exiger du gouvernement qu'il adopte des mesures de protection contre les lacunes ou l'incohérence des normes lorsque des catégories similaires de données d'emploi sont régies par des règles différentes, en veillant à garantir une protection égale à tout le personnel autochtone, peu importe la catégorie du dossier.
- Exiger la consultation sérieuse des travailleuses et travailleurs autochtones et de leurs personnes représentantes pour l'élaboration des règles de classification et de gouvernance qui s'appliquent à leurs données d'emploi, et ce, avant leur mise en vigueur.

Thème 6 : Mise à jour du cadre de conformité – les mécanismes d'application actuels ne sont pas conçus pour gérer l'IA

Proposition 19 – Accorder à la ou au commissaire des pouvoirs contraignants pour l'exécution des plans de mesures correctives et permettre de discontinuer ou de refuser des plaintes à leur discrétion

Cette proposition conférerait à la ou au commissaire à la protection de la vie privée des pouvoirs contraignants et la capacité d'exiger des plans de mesures correctives et leur publication, avec la possibilité de porter l'affaire devant la Cour fédérale. Un pouvoir discrétionnaire limité permettrait aussi de refuser des plaintes ou de mettre fin à l'enquête sur certaines d'entre elles.

Préoccupations

Le pouvoir discrétionnaire de refuser d'enquêter sur des plaintes ou de mettre fin à de telles enquêtes pourrait limiter la capacité des travailleuses et travailleurs à faire examiner rigoureusement leurs cas d'atteinte à la vie privée, en particulier lorsque les plaintes sont jugées de faible priorité ou laissées sans suite, voire considérées comme frivoles ou vexatoires, de sorte que certaines atteintes à la vie privée en milieu de travail ne seraient pas examinées.

Bien que les mesures proposées visant à renforcer la surveillance institutionnelle, à renforcer la confiance du public et à accroître la responsabilisation soient les bienvenues, elles ne précisent pas comment la ou le commissaire déterminera si une plainte est « futile ou vexatoire », et donc susceptible d'être rejetée à sa discrétion. On pourrait améliorer ces propositions en rehaussant la transparence de ce pouvoir discrétionnaire. De plus, les pouvoirs contraignants de la ou du commissaire ne doivent ni porter atteinte aux droits fondamentaux des travailleuses et travailleurs ni les outrepasser.

En clarifiant les modalités d'exercice de ce pouvoir discrétionnaire, on favoriserait la cohérence et la transparence tout en assurant au public que les plaintes pour atteinte à la vie privée feront l'objet d'un traitement équitable et ne seront pas rejetées arbitrairement ni reportées déraisonnablement.

Questions

Quelles mesures seront prises pour veiller à ce que les décisions de refuser une plainte ou de mettre fin à une enquête sur une plainte pour atteinte à la vie privée ne minent pas l'accès des travailleuses et travailleurs à de réels recours?

Recommandations

- Ajouter à la *LPRP* des critères clairs pour déterminer si une plainte est considérée comme « futile ou vexatoire », et prévoir des dispositions définissant le processus d'évaluation et de traitement des plaintes par le Commissariat.
- Veiller à ce que les pouvoirs contraignants de la ou du commissaire ne réduise pas la portée des protections procédurales et de fond supérieures prévues dans les conventions collectives existantes ni ne les remplace, et à ce qu'ils ne portent pas atteinte aux droits de déposer un grief et de recourir à l'arbitrage en cas de différend.

Proposition 20 – Autoriser le commissaire à collaborer avec d'autres organisations et à leur communiquer des renseignements

Cette proposition prévoit la modification de la *LPRP* afin de permettre à la ou au commissaire, dans des conditions définies, de communiquer des renseignements, y compris des données personnelles, à des organismes de réglementation et de surveillance, tels que des organismes de contrôle fédéraux et des organismes de réglementation provinciaux et territoriaux, ainsi qu'à leurs homologues internationaux. Une telle communication serait permise lorsque nécessaire pour faire progresser son mandat dans l'intérêt public.

Préoccupations

Un partage accru des données personnelles entre les organismes de réglementation d'ici et d'ailleurs pourrait accroître le risque que ces renseignements soient utilisés d'une manière à laquelle les travailleuses et travailleurs ne s'attendaient pas ou à laquelle ils n'ont pas consenti. Cela pourrait soulever des questionnements quant à la protection des renseignements personnels une fois qu'ils ont quitté leur contexte d'origine. Nous craignons que cela ne compromette la capacité des personnes travailleuses et de leurs syndicats à collaborer de façon concrète à la gouvernance de ces enjeux.

Toutes les préoccupations et recommandations formulées aux propositions 7 et 9 s'appliquent ici.

Questions

Quelles mesures de protection permettront de garantir que les renseignements personnels des travailleuses et travailleurs ne seront communiqués à d'autres organismes de réglementation que lorsque cela est strictement nécessaire dans le cadre d'une enquête ou d'un mandat précis? Lorsque des données personnelles seront communiquées à des organismes de surveillance nationaux et internationaux, comment en seront informées les personnes à qui elles appartiennent et de quels recours disposeront-elles si elles estiment que cela est inapproprié ou excessif?

Recommandations

- Reconnaître comme principe fondamental que la transmission de données sur les travailleuses et travailleurs à d'autres organismes de réglementation et de surveillance est présumée interdite.
- Préciser clairement dans la *LPRP* les cas possibles de dérogation à ce principe et les organismes de surveillance concernés. Voici les conditions qui devraient être requises pour obtenir une telle dérogation : prouver de façon convaincante que cette dérogation est nécessaire et proportionnée et que les intérêts à défendre sont suffisamment importants pour primer sur les droits individuels et collectifs à la vie privée des travailleuses et travailleurs. La commodité et l'efficacité ne justifient pas l'octroi d'une telle exemption.
- Exiger la réalisation d'EFVP et la mise en place de protections procédurales adéquates en ce qui concerne l'utilisation de ce pouvoir de collaboration et de partage d'information avec d'autres organismes de réglementation et de surveillance.
- Prévoir dans la *LPRP* l'obligation d'obtenir le consentement des travailleuses et travailleurs *chaque fois* que l'on souhaite transmettre leurs renseignements personnels et sensibles à d'autres territoires.
- Prévoir expressément dans la *LPRP* des recours pour les préjudices découlant de la

communication non consentie des renseignements personnels des travailleuses et travailleurs, et ce, en plus de renforcer les pouvoirs et le mandat de la ou du commissaire à la protection de la vie privée.

Proposition 21 – Infractions pour tentatives de réidentification des données, sauf dans des circonstances précises et limitées

Cette proposition prévoit l'établissement d'infractions pour des personnes ou entités qui rétablissent intentionnellement le caractère identificateur des données qui ont été dépersonnalisées, sauf lorsque ce rétablissement est autorisé par la loi ou nécessaire à des fins particulières, comme les enquêtes, la sécurité nationale ou d'autres circonstances strictement définies dans la réglementation. Une réidentification accidentelle ou inévitable survenant lors d'un traitement légitime ne serait pas considérée comme une infraction.

Préoccupations

L'incertitude quant à ce qui constitue ou non une réidentification « nécessaire » pourrait nuire aux travailleuses et travailleurs, particulièrement en contexte d'enquête ou de situation liée à la sécurité, ce qui pourrait avoir comme effet d'élargir le champ d'exception. De plus, les fonctionnaires fédéraux ne sachant pas nécessairement à quel moment et pour quelles raisons leurs données sont réidentifiées, la détection d'une mauvaise utilisation ou la contestation a posteriori est d'autant plus difficile.

Questions

La réidentification « nécessaire à des fins particulières » ou autorisée par la loi sera-t-elle assez clairement définie pour éviter une interprétation trop large dans la pratique? Quels mécanismes de surveillance et d'audit permettront de garantir que la réidentification autorisée (par exemple, dans le cadre d'enquêtes ou pour des raisons de sécurité nationale) ne soit pas utilisée pour justifier le rapprochement systématique ou excessif de données dépersonnalisées sur les travailleuses et travailleurs? Comment les gens seront-ils informés que leurs données dépersonnalisées ont été réidentifiées, et de quels recours disposeront-ils pour contester ou examiner le processus? Quelles mesures seront mises en place pour que les travailleuses et travailleurs qui traitent des données dépersonnalisées dans le cadre de leur travail ne fassent pas l'objet de mesures disciplinaires ou de poursuites en cas de réidentification accidentelle?

Recommandations

- Reconnaître comme principe fondamental que la réidentification de données dépersonnalisées sans autorisation légale constitue une infraction, mais qu'une telle infraction doit également être assujettie à des protections procédurales adéquates.
- Préciser expressément dans la *LPRP* dans quels cas la réidentification est « autorisée par la loi » ou « nécessaire à des fins particulières ».
- Veiller à ce que l'infraction vise la réidentification malveillante de renseignements dépersonnalisés où il y a intention de nuire à autrui ou d'obtenir un avantage illégitime. Une personne qui, dans l'exercice légitime de ses fonctions, réidentifie accidentellement des données dépersonnalisées ne devrait pas en être tenue responsable, à moins que cela ait été fait avec une intention malveillante ou dans le but de nuire ou d'obtenir un avantage illégitime.
- Veiller à la mise en place de mécanismes de surveillance et d'audit visant à empêcher le rapprochement non autorisé de données dépersonnalisées sur les travailleuses et travailleurs avec d'autres données susceptibles de permettre leur réidentification.
- S'assurer que la *LPRP* précise les recours dont dispose le personnel en cas de réidentification de leurs données à des fins illégales ou non autorisées.

Proposition 22 – Élargir les recours judiciaires et préciser l'autorité de la Cour fédérale

Cette proposition prévoit d'élargir l'autorité de la Cour fédérale pour permettre aux personnes et à la ou au commissaire de demander des recours pour une gamme élargie de violation à la vie privée. Elle permettrait également de préciser des options de recours supplémentaires pour le mauvais traitement des données personnelles, garantissant ainsi que les institutions soient tenues responsables en cas de non-conformité.

Préoccupations

Élargir la compétence de la Cour fédérale n'éliminerait pas toutes les barrières. Les fonctionnaires fédéraux auraient encore à faire face à certains obstacles persistants, comme les coûts, la longueur des procédures et la complexité juridique des recours judiciaires. Ce genre d'obstacle peut limiter l'accessibilité à de tels recours.

Questions

Compte tenu des obstacles potentiels liés aux coûts, au temps et à la complexité, quelles mesures seront mises en place pour s'assurer que les travailleuses et travailleurs aient réellement accès aux recours devant la Cour fédérale? Comment définir clairement « atteinte à la vie privée » de façon à ce que les travailleuses et travailleurs comprennent ce qui constitue un motif valable pour exercer un recours et pour favoriser une prise de décision cohérente? Quels délais ou processus accélérés seront proposés par la Cour fédérale pour veiller au règlement rapide des litiges en matière de vie privée?

Recommandations

- Veiller à ce que l'élargissement des recours judiciaires soit cohérent avec les recommandations formulées aux propositions 19, 20 et 21.
- S'assurer que le terme « atteinte à la vie privée » dans la *LRPR* soit clairement défini et accompagné d'une liste non exhaustive d'exemples de violations de la vie privée pour lesquels un recours est possible.
- Faire en sorte que les règles de la Cour fédérale soient suffisamment claires pour assurer l'efficacité des recours pour atteinte à la vie privée.
- Mettre en place à la Cour fédérale un processus accéléré conçu spécialement pour les recours en cas d'atteinte à la vie privée systémique ou à grande échelle.

Annexe A : Liste des membres du groupe spécial

Susan Ursel, associée principale, Ursel Phillips Fellows Hopkinson L.L.P.

Hannah Johnston, professeure adjointe, Université York, École de gestion des ressources humaines

Sarah Ryan, directrice de recherche intérimaire, Syndicat canadien de la fonction publique

Eman Cheema, avocate et conseillère juridique, Syndicat canadien de la fonction publique

Jésaël Lisiecki, agent de recherche, Association canadienne des employés professionnels

Krista M. Devine, avocate générale, Alliance de la Fonction publique du Canada

Graham Cox, représentant national, service de recherche d'Unifor

Rubina Boucher, présidente du Syndicat de l'Emploi et de l'Immigration du Canada