NATIONS UNIES
DROITS DE L'HOMME
HAUT-COMMISSARIAT

UNITED NATIONS
HUMAN RIGHTS
OFFICE OF THE HIGH COMMISSIONER

Commentaires du Service consultatif du HCDH sur les droits humains dans le domaine des technologies numériques concernant le projet de loi canadien C-22
(Loi de 2026 sur l'accès légal)
3 novembre 2026

Introduction

Le Haut-Commissariat des Nations Unies aux droits de l'homme (HCDH/ONU Droits de l'homme) est la principale entité des Nations Unies en matière de droits de la personne; il a pour mandat de recenser les violations, de contribuer à l'élaboration des normes internationales et d'évaluer les progrès accomplis dans la protection et la promotion des droits de la personne partout dans le monde.

Ce mandat s'étend aux technologies numériques. Dans le cadre du Pacte numérique mondial des Nations Unies, ONU Droits de l'homme conseille les parties prenantes sur l'harmonisation de la gouvernance et de la réglementation du numérique avec les normes et règles internationales relatives aux droits de la personne.

À la suite de demandes en ce sens, le Service consultatif du HCDH sur les droits humains dans le domaine des technologies numériques formule certains commentaires sur le projet de loi C-22, Loi concernant l'accès légal, actuellement à l'étude au Parlement du Canada. Ces commentaires non exhaustifs, formulés dans un esprit de dialogue constructif, mettent en lumière des questions clés en matière de droits de la personne afin d'aider le Canada à harmoniser ses efforts de réglementation avec le droit international des droits de la personne.

Le HCDH rappelle que l'encadrement des mesures d'enquête criminelle doit respecter les obligations internationales du Canada en matière de droits de la personne, notamment celles découlant du Pacte international relatif aux droits civils et politiques (PIDCP), auquel le Canada a adhéré le 19 mai 1976. Les parties 1 et 2 du projet de loi auraient des répercussions importantes sur les droits de la personne, en particulier sur le droit à la vie privée (article 17 du PIDCP). Comme l'a souligné le Comité des droits de l'homme lors de son examen du Canada[1], les lois sur la surveillance doivent respecter l'article 17 du PIDCP ainsi que les principes de légalité, de proportionnalité, de nécessité et de transparence, et prévoir des garanties efficaces, notamment

[1] Voir CCPR/C/CAN/CO/7, par. 45 et 46 [EN ANGLAIS].

un contrôle judiciaire, une supervision indépendante et des recours adéquats[2]. Le HCDH salue l'accent mis sur la légalité dans le titre du projet de loi. Comme l'ont fait observer le Comité des droits de l'homme et les procédures spéciales des Nations Unies, une immixtion dans la vie privée peut néanmoins être illégale si la loi sur laquelle elle repose n'est pas conforme aux dispositions, aux buts et aux objectifs du Pacte. L'analyse qui suit présente des orientations sur les conditions et les garanties requises pour satisfaire à cette norme.

Structure du projet de loi

Le projet de loi C-22, Loi de 2026 sur l'accès légal, compte trois parties : la partie 1 (Accès aux données et aux renseignements en temps opportun), qui modifie le *Code criminel*, la *Loi sur le Service canadien du renseignement de sécurité* et d'autres lois existantes; la partie 2 (*Loi sur le soutien en matière d'accès autorisé à de l'information*), qui édicte une nouvelle loi; et la partie 3 (Examen parlementaire).

La partie 1 modifie notamment le *Code criminel* et régirait l'accès des forces de l'ordre aux renseignements personnels détenus par les fournisseurs de services de communication ainsi que par les entreprises et services technologiques. La partie 2 édicte la *Loi sur le soutien en matière d'accès autorisé à de l'information*, qui créerait un cadre de lutte contre les activités criminelles dans l'espace numérique en élargissant les pouvoirs de perquisition et de saisie des autorités et en fixant les règles sur ce que les enquêteurs peuvent recueillir auprès des fournisseurs de services électroniques ou exiger d'eux.

Analyse

I. Immixtion légale au regard du Pacte international relatif aux droits civils et politiques

Surveillance et accès de l'État au moyen d'intermédiaires

La partie 2 du projet de loi C-22, la *Loi sur le soutien en matière d'accès autorisé à de l'information*, soulève d'importantes préoccupations quant à la légalité des immixtions dans le droit à la vie privée. Le projet de loi autorise la prise d'arrêtés ministériels imposant des obligations aux fournisseurs principaux ainsi qu'une obligation permanente de prêter assistance à l'évaluation ou à la mise à l'essai de dispositifs, d'équipements ou d'autres moyens d'accès autorisé à

[2] Voir CCPR/C/CAN/CO/7, par. 46 [EN ANGLAIS].

l'information[3]. Il est particulièrement préoccupant que ces exigences puissent être imposées par arrêté ministériel, sous le sceau d'une confidentialité présumée et sans autorisation judiciaire. Bien que les arrêtés ministériels soient soumis à l'examen du commissaire au renseignement[4], le Bureau du commissaire au renseignement a un champ d'action limité et n'offre pas les garanties nécessaires, proportionnées au caractère potentiellement intrusif des mesures proposées. Le projet de loi C-22 interdit également la communication de certains arrêtés gouvernementaux, ce qui soulève des préoccupations en matière de transparence[5]. Une surveillance aussi intrusive devrait être assortie d'une autorisation préalable indépendante, d'une vérification a posteriori et d'une divulgation publique. L'Assemblée générale des Nations Unies et le Rapporteur spécial sur la promotion et la protection du droit à la liberté d'opinion et d'expression ont insisté sur l'importance, dans les lois sur la surveillance, de l'absence d'arbitraire, d'une supervision indépendante et de voies de recours[6]. Le Comité des droits de l'homme a fait observer qu'une immixtion peut être considérée comme arbitraire même si elle est prévue par la loi[7], et que le « caractère raisonnable » signifie que toute immixtion dans la vie privée doit être à la fois nécessaire et proportionnée à l'objectif recherché dans les circonstances particulières à chaque cas[8]. Or, le projet de loi permet au ministre de refuser la communication pour des motifs « raisonnables », sans limites définies (qui préciseraient en quoi ces mesures sont nécessaires et proportionnées) ni obligation de publier les motifs du refus[9]. Comme l'a souligné le Comité des droits de l'homme, un pouvoir discrétionnaire excessif de l'exécutif n'a pas les qualités nécessaires d'une loi, le secret aggravant le risque d'arbitraire[10]. Faute de garanties, ces dispositions ne satisfont pas aux exigences d'absence d'arbitraire du droit international.

De plus, le paragraphe 5(2) confère au gouvernement le pouvoir d'obliger les fournisseurs à créer des voies permettant à une personne autorisée d'accéder à de l'information. L'article 20 permet au gouvernement de désigner toute personne pour entrer dans une propriété privée et accéder

[3] Voir le projet de loi C-22, partie 2, art. 7 et par. 5(2) et 13(1).

[4] Voir A/HRC/39/29, par. 39, sur le contrôle judiciaire : « Les organes de contrôle ne peuvent dépendre des autorités chargées de la surveillance et doivent être dotés d'une expérience, de compétences et de ressources appropriées et adéquates. L'autorisation et le contrôle devraient être séparés sur le plan institutionnel. […] Les processus de contrôle doivent également être transparents et soumis à un examen public approprié, et les décisions des organes de contrôle doivent pouvoir faire l'objet d'un appel ou d'un examen indépendant. »

[5] Voir le projet de loi C-22, partie 2, al. 14c) et par. 6(1) et 7(1).

[6] Voir A/RES/77/211 et A/HRC/34/61, par. 36.

[7] Voir A/HRC/27/37, par. 21.

[8] *Ibid.*

[9] Voir le projet de loi C-22, partie 2, par. 15(1) et art. 14.

[10] Voir A/HRC/27/37, par. 29.

à des données informatiques sans mandat. L'effet conjugué de ces deux articles et de vastes obligations de conservation des données crée des situations où le gouvernement pourrait, dans les faits, contourner le fournisseur de services pour accéder directement à l'information. En vertu des Principes directeurs des Nations Unies relatifs aux entreprises et aux droits de l'homme, les fournisseurs de services électroniques conservent une responsabilité propre de respecter les droits de la personne, y compris lorsqu'ils répondent aux demandes d'accès à l'information des gouvernements[11]. Cette responsabilité justifie l'examen attentif et, s'il y a lieu, la contestation des demandes qui auraient des incidences négatives sur les droits de la personne. Les dispositions permettant aux pouvoirs publics de contourner les fournisseurs pourraient empêcher ceux-ci d'évaluer ces demandes et de prendre les mesures appropriées pour prévenir ou atténuer ces incidences.

II. Perquisitions et saisies

Comme il est indiqué plus haut, le projet de loi édicterait la Loi sur le soutien en matière d'accès autorisé à de l'information, qui élargit les pouvoirs de perquisition et de saisie pour lutter contre la criminalité numérique et définit ce que les enquêteurs peuvent recueillir auprès des fournisseurs de services électroniques ou exiger d'eux.

Les saisies doivent respecter les principes de légalité, de nécessité et de proportionnalité prévus par le droit international des droits de la personne. Les termes généraux employés dans le projet de loi, comme « urgence de la situation » et « difficilement réalisable[12] », risquent de permettre des saisies sans contrôle judiciaire, tandis que l'autorisation de saisir « les renseignements relatifs à l'abonné » ne comporte pas de limites claires quant à la portée, à la justification et à la durée. Compte tenu de la facilité d'accès aux mandats d'urgence en droit pénal fédéral canadien, y compris les télémandats décernés en quelques heures, le HCDH recommande vivement de prévoir des garanties assurant la légitimité et la proportionnalité des perquisitions et des saisies et empêchant la conservation indéfinie et arbitraire de données ou de biens. Laisser ces décisions aux forces de l'ordre au moment de la saisie risque d'entraîner des immixtions illégales et arbitraires dans le droit au respect de la correspondance et dans la liberté d'expression, garantis respectivement par les articles 17 et 19 du PIDCP.

[11] Principe 23 b), lu conjointement avec le principe 11, invite les entreprises à rechercher des moyens d'honorer les droits de l'homme internationalement reconnus lorsqu'elles sont confrontées à des exigences nationales contradictoires.
[12] Projet de loi C-22, partie 1, art. 487.11.

Au regard de l'article 17 du PIDCP, le Comité des droits de l'homme a jugé illégales des saisies de biens et des collectes de données lorsqu'elles étaient disproportionnées par rapport à la menace alléguée et qu'il était impossible de déterminer précisément quelles données avaient été recueillies. L'accès légal aux données suppose des motifs identifiables et non arbitraires ainsi que des recours utiles en matière de perquisition et de saisie. Le HCDH souhaite attirer l'attention sur l'imprécision de certains termes du *Code criminel* canadien, comme « bâtiment » et « lieu[13] », dont les tribunaux canadiens ont déjà souligné le manque de précision[14].

Cela reflète l'exigence de l'article 17 du PIDCP selon laquelle le droit interne doit préciser en détail les circonstances dans lesquelles des mandats de perquisition peuvent être décernés[15]. Il en va de même pour le terme « ordinateur [16]», puisqu'un ordinateur peut contenir une quantité considérable de données personnelles sans lien avec une personne soupçonnée. Une autorisation préalable visant la perquisition précise est donc nécessaire au respect du principe de proportionnalité. Le HCDH recommande que les modifications imposent une plus grande précision à l'égard des lieux et des ordinateurs, et que le paragraphe 487(2.5) soit modifié en conséquence.

Le paragraphe 20(3) autorise les personnes désignées en vertu du paragraphe 20(1) à examiner toute chose se trouvant dans le lieu, à reproduire des documents et des données électroniques, à emporter des documents et à utiliser des ordinateurs et des appareils de reproduction, tandis que le paragraphe 20(5) oblige quiconque se trouve dans le lieu à prêter assistance. Ces pouvoirs ne sont soumis à aucun contrôle judiciaire ni à aucune supervision indépendante, ce qui crée un risque important d'immixtion arbitraire et disproportionnée dans le droit à la vie privée garanti par l'article 17 du PIDCP.

Mandats

L'alinéa 487(2.4)a) risque de conférer un pouvoir discrétionnaire trop large en permettant de décerner des mandats autorisant l'examen de données informatiques sur la base de la croyance qu'une infraction « sera commise ». Il devrait énoncer des motifs précis liés à un comportement et à une intention concrets, plutôt qu'à un danger futur hypothétique, et prévoir une évaluation

[13] Voir le projet de loi C-22, partie 1, par. 487(2.1).
[14] Voir *R. c. Vu*, 2013 CSC 60.
[15] Voir le projet de loi C-22, partie 1, par. 487(1).
[16] Voir le projet de loi C-22, partie 1, par. 487(2.4).

judiciaire au cas par cas afin de prévenir les immixtions arbitraires dans la vie privée[17]. En droit des droits de la personne, les mandats doivent être autorisés au cas par cas par une autorité désignée par la loi et viser un but légitime[18]. L'information obtenue dans le cadre du mandat devrait se limiter à ce qui est nécessaire à l'enquête et ne doit pas constituer du harcèlement[19]. Selon les principes de nécessité et de proportionnalité, les autorisations doivent être limitées dans le temps, renouvelées uniquement sur la base d'une nouvelle justification, et le mandat doit prendre fin lorsqu'il n'est plus nécessaire[20]. Le HCDH craint que le paragraphe 487(2.8) ne satisfasse pas à ce critère. Les personnes visées devraient être informées de la surveillance dès que cette notification ne risque plus d'en compromettre l'objectif, afin de pouvoir exercer des recours. Toute restriction ou tout report doit être strictement limité[21].

III. Conservation généralisée des métadonnées et droit à la vie privée

La collecte de données constitue une immixtion dans le droit à la vie privée[22]. Le droit à la vie privée protège à la fois le contenu des communications et les métadonnées, lesquelles, une fois agrégées et analysées, peuvent donner des indications sur « la conduite d'un individu, ses relations sociales, ses préférences privées et son identité qui vont bien au-delà de ce que l'on obtient en accédant au contenu d'une communication privée[23] ». La collecte et l'utilisation des données supposent « des règles claires et détaillées régissant la portée et l'application des mesures, ainsi que des garanties minimales concernant, entre autres, la durée, le stockage, l'utilisation, l'accès des tiers, les procédures de préservation de l'intégrité et de la confidentialité des données et les procédures de destruction de celles-ci, offrant ainsi des garanties suffisantes contre les risques d'abus et d'arbitraire[24] ». Le HCDH recommande d'ajouter au paragraphe 487(2.8) des garanties pour que les prolongations de mandat satisfassent aux exigences de nécessité du droit international des droits de la personne. Les types de données demeurent mal définis dans l'ensemble du projet de loi, notamment les « données de

[17] Voir CCPR/C/GC/16.
[18] Voir CCPR/C/GC/16, par. 8.
[19] *Ibid*.
[20] Voir A/HRC/27/37, par. 28 et A/HRC/39/29.
[21] Voir A/HRC/27/37, par. 47 et A/HRC/23/40, par. 82.
[22] Voir A/HRC/27/37, par. 20.
[23] Voir A/HRC/27/37, par. 19.
[24] *Podchasov c. Russie*, requête nº 33696/19, arrêt, Cour européenne des droits de l'homme, 13 février 2024 [TRADUCTION].

transmission », qui renvoient de façon générale à un moyen de télécommunication « qui est inconnu au moment où le mandat est délivré ».

La conservation obligatoire et généralisée des métadonnées par les entreprises de télécommunications et les fournisseurs de services électroniques constitue une immixtion dans la vie privée, limite les communications anonymes, présente des risques d'abus et de communication à des tiers[25], et excède ce qui est nécessaire et proportionné. Le paragraphe 5(2) permet une telle conservation sans que les données soient susceptibles de donner lieu à des poursuites criminelles ou nécessaires pour contrer des menaces à la sécurité nationale[26]. Cela soulève de graves préoccupations au sujet d'un régime de surveillance qui permettrait de conserver des données de transmission et de localisation sans préciser l'infraction faisant l'objet de l'enquête, sans établir la nécessité de la mesure pour une enquête criminelle ou une menace précise à la sécurité nationale et sans démontrer la proportionnalité de la surveillance. L'absence d'autorisation judiciaire, d'examen indépendant et de notification accroît en outre le risque que des ordres de conservation secrets échappent à toute contestation efficace.

IV. Mesures de protection techniques essentielles

Le projet de loi C-22 risque de compromettre le chiffrement de bout en bout et de porter atteinte de manière disproportionnée au droit à la vie privée. Le projet de loi prévoit de vastes obligations de faciliter l'accès, ainsi que la possibilité de prendre ultérieurement des règlements[27] pour imposer d'autres capacités techniques de surveillance. Le HCDH se réjouit que le paragraphe 5(5) soustraie les fournisseurs principaux aux exigences qui les obligeraient à introduire une « vulnérabilité systémique », ce qui semble viser à protéger le chiffrement de bout en bout. En pratique, toutefois, il est très difficile, voire impossible, de respecter les obligations prévues aux paragraphes 2(4), 5(2) et 7(1) sans introduire de telles vulnérabilités. Le HCDH insiste constamment sur le caractère essentiel d'un chiffrement robuste pour la vie privée, la sécurité en ligne et la protection des droits, et propose l'ajout d'une disposition explicite : « *rien dans la présente loi ne doit être interprété comme obligeant les fournisseurs de services à briser des mesures de protection techniques essentielles, comme le chiffrement de bout en bout* ».

[25] Voir A/HRC/39/29, par. 18.
[26] Voir le projet de loi C-22, partie 2, par. 5(2).
[27] Voir le projet de loi C-22, partie 2, par. 5(2).

Le HCDH a fait observer que « la plupart des restrictions au chiffrement ont des effets disproportionnés sur le droit à la vie privée et les droits connexes, qui touchent souvent non seulement les personnes visées, mais aussi l'ensemble de la population[28] ». Le Comité s'est aussi dit préoccupé par le fait que le projet de loi C-8, qui modifie la *Loi sur les télécommunications*, permettrait au gouvernement d'accéder à des données sensibles sans autorisation judiciaire préalable ni garanties essentielles concernant les données obtenues, et pourrait contraindre les entreprises à briser des mesures de protection techniques essentielles comme le chiffrement[29].

V. Échange transfrontalier de données

Le projet de loi C-22 élargit les conditions d'échange transfrontalier de données, notamment en matière d'entraide juridique (article 29, paragraphe 22.07(3), article 487.0142). Il semble abaisser le seuil d'accès des forces de l'ordre aux renseignements relatifs à l'abonné, en passant de la norme des motifs raisonnables de croire à celle des motifs raisonnables de soupçonner, la seule condition étant « qu'il existe des motifs raisonnables de soupçonner » que les renseignements « seront utiles » à l'enquête, une norme de pertinence peu exigeante et facile à satisfaire[30]. L'accès et l'échange constituent des immixtions dans la vie privée; ces seuils risquent donc d'en affaiblir la protection dans le cadre des demandes transfrontalières. Le droit international des droits de la personne impose un contrôle judiciaire indépendant et préalable de la nécessité et de la proportionnalité afin de prévenir les immixtions arbitraires. L'absence de cette garantie et l'absence apparente d'obligations de minimisation des données accroissent, dans la pratique, le risque d'immixtions arbitraires et illégales.

Le HCDH reconnaît que l'échange transfrontalier de données répond souvent à un besoin légitime dans les enquêtes criminelles. L'expérience mondiale montre néanmoins qu'il est fréquemment utilisé en dehors de telles enquêtes, pour des infractions qui ne devraient pas être criminalisées en vertu du droit international ou à des fins de répression transnationale[31]. Un cadre juridique doit donc définir clairement quand et comment l'échange peut avoir lieu et réduire au minimum les risques d'abus. Compte tenu de l'essor de la répression transnationale fondée sur les données, la loi devrait imposer le principe de la double incrimination et le rejet des demandes lorsqu'il existe des motifs raisonnables de croire que l'échange entraînera de

[28] Voir A/HRC/51/17.
[29] Voir CCPR/C/CAN/CO/7, par. 45 [EN ANGLAIS].
[30] Voir le projet de loi C-22, par. 487.0142(2).
[31] Voir A/HRC/56/53.

graves violations des droits de la personne. Sans ces garanties, le cadre juridique canadien risque de favoriser la persécution de personnes, notamment de défenseurs des droits de la personne et de journalistes, dans d'autres États.

Les préoccupations concernant les dispositions qui autorisent ou obligent les fournisseurs de services canadiens à communiquer des données de transmission, des renseignements relatifs à l'abonné ou d'autres renseignements personnels à des États étrangers sont d'autant plus vives qu'il n'existe aucun accès à des recours pour les violations des droits de la personne qui pourraient en résulter. Le HCDH recommande vivement de revoir les dispositions du projet de loi relatives à l'échange transfrontalier de données afin d'établir des conditions supplémentaires garantissant le respect du droit international des droits de la personne.

FIN