CANADIAN MUSLIM PUBLIC AFFAIRS COUNCIL

Projet de loi C-22 : Mémoire du CMPAC présenté au Comité permanent de la sécurité publique et nationale

---

Introduction

Le Canadian Muslim Public Affairs Council (CMPAC) est une organisation non partisane qui se consacre à la promotion des libertés civiles, de la participation démocratique et de la protection des droits de la personne au Canada. Par son travail de plaidoyer et de politique publique, le CMPAC s'est constamment engagé sur les questions relatives à la discrimination, à la responsabilité gouvernementale et à l'impact des politiques publiques sur les communautés marginalisées.

Les initiatives législatives visant à élargir les pouvoirs de surveillance et de collecte de renseignements de l'État ont à maintes reprises soulevé des inquiétudes quant à la protection des droits et libertés fondamentaux. Bien que la protection de la sécurité publique soit un objectif légitime et important, de telles mesures doivent demeurer conformes à la Charte canadienne des droits et libertés et aux obligations plus larges du Canada en matière de droits de la personne.

Le projet de loi C-22 élargirait l'accès de l'État aux renseignements personnels tout en affaiblissant des garanties importantes conçues pour protéger les droits et libertés fondamentaux. La législation soulève des préoccupations majeures concernant le droit à la vie privée, la liberté d'expression, la liberté d'association, la liberté de religion et le droit à l'égalité, en particulier compte tenu de l'impact documenté que les mesures de surveillance et de sécurité ont eu sur différentes communautés et groupes racialisés.

Pour ces raisons, le CMPAC invite instamment le Parlement à examiner attentivement la nécessité, la proportionnalité et les conséquences potentielles des pouvoirs proposés dans le projet de loi C-22.

Position sur le projet de loi C-22

Le CMPAC craint que, s'il est adopté, le projet de loi C-22 n'élargisse considérablement les pouvoirs de surveillance de l'État tout en abaissant des garanties importantes régissant l'accès aux renseignements personnels. Ces changements soulèvent de graves préoccupations concernant le droit à la vie privée, la liberté d'expression, la liberté d'association, la liberté de religion et le droit à l'égalité protégés par la Charte canadienne des droits et libertés.

De telles préoccupations ne peuvent être séparées du vécu des communautés qui ont historiquement[1] été touchées de manière disproportionnée par les cadres canadiens de sécurité nationale et d'application de la loi. Les communautés musulmanes du Canada subissent depuis longtemps les conséquences de la collecte de renseignements, du partage d'informations et des enquêtes de sécurité dont il a été démontré par la suite qu'elles reposaient sur des présomptions erronées, des renseignements non fiables ou un profilage discriminatoire. Par conséquent, les propositions qui élargissent les autorités de surveillance sans preuve suffisante de leur nécessité exigent un examen particulièrement attentif.

[1] Reem Bahdi, ""All Arabs Are Liars": Arab and Muslim Stereotypes in Canadian Human Rights Law" (2019) 31:1 J L & Soc Pol'y 92.

Sur la base de ces préoccupations, le CMPAC demande aux députés de rejeter le projet de loi C-22 et de voter contre son adoption. Si la législation devait suivre son cours au Parlement, des amendements substantiels devraient être apportés pour renforcer les garanties, accroître la surveillance et atténuer les impacts discriminatoires sur les communautés racialisées et les minorités religieuses.

Partie 1 : Accès opportun aux données et aux renseignements

a. Abaissement des normes aux « motifs raisonnables de soupçonner

En vertu du projet de loi C-22, les forces de l'ordre seraient autorisées à obtenir des renseignements relatifs aux abonnés sur la base d'un seuil de preuve inférieur, soit des « motifs raisonnables de soupçonner » plutôt que des « motifs raisonnables de croire ». Bien que les renseignements relatifs aux abonnés soient souvent présentés comme de simples détails d'identification, les renseignements visés par la législation s'étendent aux noms d'utilisateur, aux pseudonymes, aux données sur les appareils et aux identifiants en ligne.

L'abaissement de ce seuil de preuve normalise un accès plus large de l'État aux renseignements personnels tout en offrant des garanties insuffisantes contre des enquêtes discriminatoires ou excessives. Lorsque les pouvoirs de surveillance sont exercés sur la base de simples soupçons, le risque est accru que des préjugés individuels ou institutionnels influencent la prise de décision au cours de l'enquête. Pour les Canadiens musulmans, arabes et palestiniens qui font fréquemment l'objet de signalements injustifiés en raison de conventions d'appellation[2], de dons de bienfaisance[3] ou de liens avec l'étranger,[4] cette norme augmente le risque d'un ciblage injuste par les forces de l'ordre. Le seuil requis pour obtenir des renseignements relatifs aux abonnés doit demeurer les « motifs raisonnables de croire ».

b. Dissuasion du plaidoyer et atteinte aux droits garantis par la Charte

L'élargissement des pouvoirs d'accès légal décourage directement l'engagement civique, entraînant de graves effets dissuasifs sur les libertés civiles protégées par la Charte, notamment la protection contre les fouilles, perquisitions et saisies abusives[5], la liberté d'expression[6], la liberté de réunion pacifique[7], la liberté d'association[8] et la liberté de religion[9].

---

[2] Richard Marcuse, ed, Racial Profiling: A Special BCCLA Report on Racial Profiling in Canada (Vancouver: BC Civil Liberties Association, 2010).

[3] "Project Profile: Under Layered Suspicion", online: University of Toronto Digital Humanities Networkhttps://dhn.utoronto.ca/project/under-layered-suspicion/.

[4] Uzma Jamil, "Can Muslims Fly? The No Fly List as a Tool of the “War on Terror”" (2017) 4:1 Islamophobia Studies J 72 [Jamil].

[5] *Charte canadienne des droits et libertés*, art 8, partie I de la Loi constitutionnelle de 1982, constituant l'annexe B de la Loi de 1982 sur le Canada (R-U), 1982, c 11.

[6] *Ibid*, art 2b).

[7] *Ibid,* art 2c).

[8] *Ibid,* art 2 d).

[9] *Ibid,* art 2 a).

De nombreuses études[10] ont documenté que les individus qui pensent pouvoir faire l'objet d'une surveillance sont plus susceptibles d'autocensurer leurs propos, de limiter leur participation aux activités de la société civile et d'éviter de s'engager sur des questions politiques controversées.

Pour les groupes de plaidoyer musulmans, arabes et palestiniens, la sensibilisation à la politique étrangère et aux droits de la personne fait fréquemment l'objet de vérifications minutieuses et de déformations.L'affaiblissement de la protection de la vie privée envoie le signal qu'un engagement démocratique actif comporte un risque personnel et numérique. Ce risque est renforcé par un environnement de sécurité nationale post-11 septembre[11] marqué par une surveillance de longue date des mosquées[12], des organismes de bienfaisance[13], des associations étudiantes[14] et des leaders communautaires[15].

L'élargissement de l'accès de l'État aux renseignements personnels transforme ces inquiétudes en éléments dissuasifs actifs, érodant les garanties fondamentales de la Charte et sapant la confiance entre les communautés touchées et les institutions publiques.

c. Élargissement des pouvoirs d'urgence sans mandat (Article 14)

L'article 14[16] du projet de loi C-22 propose de modifier l'article 487.11 du Code criminel afin d'élargir les pouvoirs qui peuvent être exercés lorsque « en raison de circonstances urgentes, l'obtention d'un mandat ne serait pas réalisable ». Actuellement, dans une situation d'urgence, un agent peut, sans mandat, exercer un pouvoir général de perquisition en vertu de l'article 487 ou installer un enregistreur de données de localisation sur des biens en vertu de l'article 492.1. S'ils sont adoptés, en plus de ces pouvoirs, les agents de police pourraient, sans mandat :

- Installer un enregistreur de données de localisation sur une personne, un pouvoir prévu à l'article 492.1(2), qui exige généralement un mandat fondé sur des motifs raisonnables de croire;
- Installer un enregistreur de données de transmission, un pouvoir prévu à l'article 492.2(1);
- Obtenir la communication de données de transmission, un pouvoir prévu à l'article 487.016;
- Obtenir la communication de données de localisation, un pouvoir prévu à l'article 487.017;
- Obtenir la communication de renseignements relatifs aux abonnés en vertu de l'article 487.0142.

---

[10] Karen Gullo, "Surveillance Chills Speech—As New Studies Show—And Free Association Suffers", (19 May 2016), online: *Electronic Frontier Foundation* https://www.eff.org/deeplinks/2016/05/when-surveillance-chills-speech-new-studies-show-our-rights-free-association.
[11]Tabasum Akseer, *Understanding the Impact of Surveillance and Security Measures on Muslim Men in Canada*, Martello Papers No 42 (Kingston: Centre for International and Defence Policy, Queen's University, 2018), online: https://www.queensu.ca/cidp/sites/cidpwww/files/uploaded_files/Martello42EN.pdf.
[12] Baljit Nagra & Paula Maurutto, "Anti-Muslim Surveillance: Canadian Muslims' Experiences with CSIS" (2023) 9:3 Soc Race & Ethnicity 311.
[13] "Report: Humanitarianism and the Exclusion of Muslim Charities from the Financial Sector", (30 April 2026), online: *Institute of Islamic Studies, University of Toronto* https://islamicstudies.artsci.utoronto.ca/report-humanitarianism-and-the-exclusion-of-muslim-charities-from-the-financial-sector/.
[14] Paula Maurutto & Baljit Nagra, "Racializing Surveillance: The Impact of the Security Certificate Regime on Young Canadian Muslims" (2022) 13:1 Islamophobia Studies J 73.
[15] *Ibid.* à la pp 11.
[16] Ligue des droits et libertés, *Bill C-22: An Act Respecting Lawful Access — Establishing a Surveillance Architecture in Canada* (mémoire présenté au Comité sénatorial permanent de la sécurité nationale, de la défense et des affaires des anciens combattants, 29 octobre 2026), en ligne : liguedesdroits.ca [Ligue des droits et libertés].

Le pouvoir d'installer un enregistreur de données de localisation sur une personne, plutôt que sur un objet,permet le suivi en temps réel des déplacements physiques d'un individu. Ce pouvoir serait exercé sans aucune autorisation judiciaire préalable, sur la seule base de l'évaluation subjective d'un agent estimant que l'urgence le justifie, et sans que la personne concernée n'en soit jamais informée.

Laisser la détermination d'une « situation d'urgence » à la discrétion de la police pose des risques aigus pour les membres des communautés musulmanes, arabes et palestiniennes qui assistent à des manifestations publiques, à des rassemblements politiques ou à des lieux de culte, les exposant à un suivi arbitraire sans contrôle judiciaire. Plus précisément, la suppression de l'autorisation judiciaire préalable permet aux préjugés institutionnels préexistants au sein des forces de l'ordre de recadrer des rassemblements religieux légitimes, la mobilisation communautaire ou la défense des droits de la personne palestiniens en menaces urgentes pour la sécurité, ce qui entraîne un suivi de localisation incontrôlé et le profilage de communautés racialisées et religieuses entières sous le couvert de circonstances urgentes.

d. Autorisation relative aux « renseignements accessibles au public »

Le projet de loi C-22 permet aux forces de l'ordre d'obtenir des « renseignements accessibles au public » et d'agir sur la base de ceux-ci sans exiger d'ordonnance de communication ni de mandat, tout en omettant de fournir une définition juridique de ce qui constitue de tels renseignements.

Accorder aux organismes d'application de la loi une autorité illimitée pour recueillir et utiliser des informations simplement parce qu'elles sont accessibles en ligne comporte de graves risques. Les données personnelles publiées sur des plateformes publiques ou sur les réseaux sociaux ne donnent pas aux autorités publiques carte blanche pour collecter, regrouper ou surveiller ces données sans consentement ou sans contrôle judiciaire, comme l'ont rappelé les normes de protection de la vie privée dans l'affaire Clearview AI[17]. Les organisateurs des droits des Palestiniens, les groupes de la société civile arabe et les groupes de jeunes musulmans s'appuient fortement sur les plateformes numériques publiques pour leur sensibilisation communautaire. Sans limites légales strictes, la surveillance sans restriction des réseaux sociaux sera instrumentalisée pour cartographier la dissidence politique légitime et les activités de plaidoyer sous le couvert de la collecte de renseignements de sources ouvertes.

e. Facilitation de la répression transnationale et du partage international de données

La répression transnationale[18] est une menace permanente au Canada[19], où des acteurs étatiques étrangers intiment, surveillent et harcèlent les communautés de la diaspora pour faire taire les critiques et

---

[17] Office of the Privacy Commissioner of Canada, *Joint investigation of Clearview AI, Inc. by the Office of the Privacy Commissioner of Canada, the Commission d'accès à l'information du Québec, the Information and Privacy Commissioner for British Columbia, and the Information Privacy Commissioner of Alberta*, PIPEDA Findings #2021-001 (2 February 2021), online: https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2021/pipeda-2021-001/.

[18] Phil Gurski & Marie Lamensch, *Transnational Repression in Canada: A Threat to Democracy and Public Safety*(Montreal: Montreal Institute for Global Security, 2026), online: https://migsinstitute.org/wp-content/uploads/2026/02/Transnational-repression-in-Canada_MIGS.pdf.

[19] Noura Al-Jizawi et al, *Psychological and Emotional War: Digital Transnational Repression in Canada*, Citizen Lab Research Report No 151 (Toronto: Citizen Lab, University of Toronto, 2022), online: https://utoronto.scholaris.ca/server/api/core/bitstreams/84d7937d-3383-48e7-9b0d-51ba9a70b4ef/content.

saper la participation démocratique. Plutôt que de protéger les populations vulnérables, le projet de loi C-22 contient des dispositions qui faciliteront activement les abus transfrontaliers par des gouvernements étrangers.

L'article 29 du projet de loi C-22 modifie la Loi sur l'entraide juridique en matière criminelle (LEJMC) pour permettre aux autorités canadiennes d'exécuter des ordonnances étrangères et de partager des données relatives aux abonnés et des données de transmission détenues au Canada avec des gouvernements étrangers, sur la base du faible seuil de preuve des « motifs raisonnables de soupçonner ». De plus, le projet d'article 487.0181 permet aux autorités canadiennes de demander et de traiter des données provenant d'entités de télécommunication étrangères en vertu de ce même seuil réduit.

Ce cadre de partage d'informations transfrontalier établit un canal dangereux pour l'ingérence étrangère.Les communautés musulmanes, arabes et palestiniennes du Canada entretiennent fréquemment des liens actifs avec des membres de leur famille vivant sous des régimes autoritaires ou des occupations militaires étrangères. En vertu du projet de loi C-22, des États étrangers pourraient exploiter ces dispositions de partage de données pour demander des renseignements sur des militants, des journalistes ou des dissidents canadiens sous prétexte d'enquêter sur des infractions étrangères. La transmission de données privées d'utilisateurs ou d'identifiants en ligne à des entités étrangères expose les résidents canadiens et leurs proches à l'étranger à des menaces, à du harcèlement, à des arrestations arbitraires et à des atteintes physiques, ce qui revient à instrumentaliser l'infrastructure étatique canadienne pour appuyer la répression étrangère.

Partie 2 : Loi visant à soutenir l'accès autorisé à l'information (LSAAI)

a. La LSAAI crée un cadre propice à une surveillance discriminatoire

La création proposée de la Loi visant à soutenir l'accès autorisé à l'information (LSAAI) constitue la préoccupation majeure du projet de loi C-22.

Tant par le biais de règlements publics que d'arrêtés ministériels secrets, la LSAAI permettrait au gouvernement d'exiger des fournisseurs de services électroniques (FSE) qu'ils conçoivent, maintiennent et modifient des systèmes qui facilitent l'accès à l'information pour les forces de l'ordre et les organismes de renseignement. Bien que ces pouvoirs soient présentés comme des outils permettant de lutter contre les activités criminelles graves, la législation ne tient pas compte de manière adéquate de la façon dont l'élargissement des infrastructures de surveillance peut toucher de manière disproportionnée les communautés qui ont historiquement fait l'objet d'une surveillance accrue.

Le CMPAC est également préoccupé par la définition exceptionnellement large de « fournisseur de services électroniques » contenue dans la législation. La portée de cette définition semble en mesure d'aller bien au-delà des entreprises de télécommunications pour englober un large éventail d'organisations sur lesquelles les Canadiens comptent pour leurs communications, leurs services financiers, leurs déplacements, leur éducation, leurs services de santé et leur engagement communautaire. L'étendue de cette définition élargit considérablement la portée potentielle des autorités de surveillance et soulève d'importantes questions quant à la nécessité, à la proportionnalité et à l'étendue des renseignements qui pourraient devenir accessibles à l'État.

Le cadre de sécurité nationale du Canada doit être compris à la lumière de son impact sur les communautés touchées. Les Musulmans ont supporté une part disproportionnée du fardeau des mesures de sécurité et des pratiques de surveillance. Cet historique souligne l'importance de s'assurer que tout élargissement des pouvoirs de l'État s'accompagne de garanties solides et d'un contrôle significatif.

Bien que le projet de loi C-22 soit technologiquement différent des législations précédentes sur la sécurité nationale, il soulève des inquiétudes similaires. Un accès élargi aux informations relatives aux communications, aux métadonnées et aux données du réseau offre aux autorités la possibilité d'identifier, de cartographier et de surveiller des communautés entières au lieu de se concentrer sur des individus à l'égard desquels il existe des preuves crédibles d'actes préjudiciables.

Le CMPAC craint en outre que les pouvoirs autorisant la modification de systèmes techniques ne créent des vulnérabilités en matière de cybersécurité qui compromettraient la sécurité des communications et des renseignements personnels des Canadiens. Tout cadre facilitant l'accès du gouvernement aux informations numériques doit veiller à ne pas affaiblir la protection du chiffrement, à ne pas créer de nouvelles vulnérabilités techniques ou à ne pas augmenter le risque d'accès non autorisé par des acteurs malveillants,des gouvernements étrangers ou des cybercriminels. Les mesures introduites au nom de la sécurité publique ne doivent pas se faire au détriment de la sécurité et de l'intégrité des communications numériques.

Le gouvernement n'a pas démontré pourquoi les pouvoirs d'enquête existants sont insuffisants, et il n'a pas non plus évalué si ces nouveaux pouvoirs risquent de toucher de manière disproportionnée les communautés racialisées et les minorités religieuses. Pour ces raisons, le CMPAC recommande que le Parlement exige une évaluation complète d'impact sur la Charte et sur l'égalité avant la mise en œuvre de tout pouvoir autorisé en vertu de la LSAAI.

Une telle évaluation devrait examiner:

- Les impacts potentiels sur la liberté de religion, la liberté d'expression et la liberté d'association;
- Les effets discriminatoires potentiels sur les communautés racialisées, autochtones, immigrantes,réfugiées et les minorités religieuses;
- L'existence d'alternatives moins intrusives;
- Le caractère nécessaire et proportionné des pouvoirs proposés par rapport aux objectifs énoncés.

Sans une telle évaluation, le Parlement ne peut évaluer de manière adéquate si la législation est conforme aux obligations constitutionnelles et aux engagements du Canada en matière de droits de la personne.

b. Retrait du marché

Les mandats d'accès technique prévus par la LSAAI menacent d'isoler le Canada de l'écosystème mondial des communications sécurisées. Le fournisseur de messagerie chiffrée Signal[20] a publiquement déclaré qu'il préférerait se retirer complètement du Canada plutôt que d'être contraint de compromettre les promesses de confidentialité qu'il a faites à ses utilisateurs. Des chercheurs techniques ont souligné

[20] Martin Shelton, "Signal could leave Canada over metadata bill", (20 May 2026), online: *Freedom of the Press Foundation* https://freedom.press/digisec/blog/signal-could-leave-canada-over-metadata-bill/.

que le projet de loi C-22 pourrait forcer les créateurs d'applications à collecter des métadonnées d'utilisateurs intrusives,notamment la cartographie des conversations et les détails de localisation. Si des plateformes comme Signal se retirent du marché canadien, les citoyens canadiens, les défenseurs des droits de la personne et les groupes de plaidoyer se verraient privés de boucliers de sécurité numérique essentiels.

Perdre l'accès à ces outils sécurisés laisse les communautés vulnérables musulmanes, arabes et palestiniennes directement exposées aux cybermenaces, à l'interception par des États hostiles et à la surveillance illégale. Ce retrait du marché toucherait de manière disproportionnée ces communautés en éliminant les canaux confidentiels sur lesquels elles comptent pour s'organiser, défendre les droits de la personne et communiquer avec leurs familles vivant sous des régimes étrangers, sans crainte de représailles étatiques ou de harcèlement ciblé.

Recommandations

Compte tenu des préoccupations exposées ci-dessus, le CMPAC recommande au Parlement:

1. Rejeter le projet de loi C-22 dans sa version actuelle.
2. Retirer la partie 2 (Loi facilitant l'accès autorisé à l'information) dans son intégralité, en attendant la tenue de consultations approfondies et la réalisation d'un examen indépendant.

Si le Parlement décide de maintenir la partie 2, le CMPAC recommande :

1. Réaliser une évaluation d'impact sur la Charte et l'égalité avant toute mise en œuvre.
2. Abroger entièrement les dispositions relatives à la conservation obligatoire des métadonnées ou, à tout le moins, les convertir en un régime d'ordonnance judiciaire de communication remplaçant le critère du « soupçon raisonnable » par celui des « motifs raisonnables de croire ».
3. Renforcer la surveillance des arrêtés ministériels secrets en remplaçant l'approbation quasi judiciaire du Commissaire au renseignement par une exigence d'autorisation judiciaire préalable délivrée par un juge d'une cour supérieure.
4. Élargir le pouvoir d'examen de l'Office de surveillance des activités en matière de renseignement et de sécurité (OSSNR) ainsi que son accès à l'information concernant l'application de la LFAAI.
5. Établir des exigences obligatoires en matière de transparence et de rapports publics.
6. Créer un organisme consultatif permanent comprenant des représentants des communautés touchées et des organisations de la société civile.
7. Imposer un examen parlementaire périodique du régime.
8. Veiller à ce que l'ensemble des pouvoirs exercés en vertu de la LFAAI respectent les obligations nationales et internationales du Canada en matière de droits de la personne, notamment les protections relatives à la vie privée, à l'égalité, à la liberté de religion, à la liberté d'expression et à la liberté d'association.
9. Interdire les transferts transfrontaliers de données en vertu de la LEMA ou du projet d'article 487.0181 sans une autorisation judiciaire préalable convainquant le tribunal que la communication ne facilitera pas la répression transnationale, les violations des droits de la personne ou le harcèlement ciblé de résidents canadiens et de leurs familles à l'étranger.
10. Ajouter une garantie législative explicite précisant qu'aucun règlement, arrêté ou directive ne peut contraindre les fournisseurs de services à affaiblir le chiffrement de bout en bout, à imposer des canaux d'accès secrets (« backdoors »), à mettre en œuvre le balayage du côté client ou à compromettre la sécurité numérique.

Conclusion

Le projet de loi C-22 propose un élargissement important des pouvoirs de surveillance de l'État tout en affaiblissant des garanties essentielles régissant l'accès aux renseignements personnels. Bien que présenté comme une réponse à l'évolution des défis technologiques, le gouvernement n'a pas démontré que les autorités existantes sont insuffisantes ou que les pouvoirs contenus dans cette législation sont nécessaires et proportionnés.

Les préoccupations soulevées dépassent le seul droit à la vie privée. L'accès élargi de l'État aux renseignements personnels, aux capacités de suivi et aux infrastructures de communication menace directement la liberté d'expression, la liberté d'association, la liberté de religion et le droit à l'égalité en vertu de la Charte. Ces impacts retombent de manière disproportionnée sur les communautés qui ont historiquement fait l'objet d'une surveillance accrue dans le cadre de la sécurité nationale du Canada,notamment les communautés musulmanes, arabes et palestiniennes.

Compromettre les protocoles de chiffrement, permettre le suivi sans mandat, faciliter le partage international de données et pousser des plateformes sécurisées comme Signal à quitter le Canada affaiblit la sécurité numérique nationale et expose les citoyens à l'ingérence étrangère et à la répression transnationale.

Le CMPAC soutient les efforts légitimes visant à protéger la sécurité publique. Cependant, de tels efforts doivent demeurer conformes aux valeurs constitutionnelles du Canada et à ses obligations internationales en matière de droits de la personne. Pour ces raisons, le CMPAC demande instamment aux députés de rejeter le projet de loi C-22. Si la législation devait être adoptée, des amendements importants seraient nécessaires pour renforcer les garanties, accroître la responsabilité et veiller à ce que l'élargissement des autorités de surveillance ne se fasse pas au détriment des droits et libertés fondamentaux.