Accès légal

Le présent document vise à aider le lecteur à comprendre divers scénarios dans lesquels les dispositions relatives à l'accès légal contenues dans le projet de loi C-2 aideront la police dans le cadre d'enquêtes criminelles graves.

Préparé par :

Association canadienne des chefs de police

Le 9 septembre 2025

PROJET DE LOI C-2 (*LOI VISANT UNE SÉCURITÉ RIGOUREUSE À LA FRONTIÈRE*) - PARTIES 14 ET 15 : ACCÈS LÉGAL

Le projet de loi C-2 contient plusieurs modifications au *Code criminel* qui clarifieront les pouvoirs de la police et augmenteront les délais d'intervention dans le cadre des enquêtes criminelles.

1. **Clarification de la divulgation volontaire des renseignements sur les abonnés**

   Le projet de loi C-2 comble l'ambiguïté découlant de la décision *R. c. Bykovets 2024* de la Cour suprême en codifiant les renseignements sur les abonnés que la police peut obtenir sans mandat, lorsqu'ils sont fournis volontairement. Cette modification rétablit la clarté pour les enquêteurs chargés des affaires d'exploitation d'enfants sur Internet (EEI) qui demandent des renseignements de base sur les abonnés (RBA) aux fournisseurs de services ou à leurs partenaires internationaux. Elle élimine les incertitudes causées par *l'affaire Bykovets,* garantissant ainsi qu'il n'y ait aucun retard dans l'identification des suspects liés à des images d'exploitation d'enfants.

   Exemple hypothétique

   Un père canadien remarque que sa fille de 12 ans discute en ligne avec une personne qui prétend être un adolescent. Il soupçonne qu'il s'agit en réalité d'un adulte. Le père vérifie les registres de clavardage et voit des messages explicites et une image partagée qui semble être du matériel pédopornographique. Il contacte la police locale et fournit des captures d'écran, le nom d'utilisateur et l'adresse IP du suspect, qui sont tous visibles dans l'outil de discussion « peer-to-peer ». Aujourd'hui, à cause de l'*affaire Bykovets*, les agents peuvent hésiter à agir en fonction de l'adresse IP fournie volontairement par le père, ne sachant pas si cela enfreint la loi sur la protection de la vie privée. Ils peuvent retarder leur intervention pendant qu'ils obtiennent une ordonnance de communication, risquant ainsi de prolonger les méfaits. Avec le projet de loi C-2, la police serait en mesure d'agir immédiatement en fonction des informations fournies volontairement et de localiser le fournisseur de service du suspect, ce qui réduirait le temps de réponse. De plus, la police n'aurait plus à craindre d'engager sa responsabilité civile pour avoir utilisé les données ou enfreint la loi sur la protection de la vie privée dans ce type de circonstances.

2. Introduction d'un nouveau régime de demande d'informations fondé sur un soupçon raisonnable

Le projet de loi C-2 crée un nouvel outil permettant aux enquêteurs d'émettre des demandes visant, entre autres, à savoir si la personne fournit ou a fourni des services à un abonné, possède ou contrôle des informations, y compris des données de transmission, relatives à cet abonné, etc. Cela simplifie les délais d'enquête et aide à réduire le champ des informations recherchées par les services de police, qui peuvent ensuite être obtenues par voie judiciaire.

Exemple (Alberta)

Dans une affaire de harcèlement criminel/traque, la victime a découvert un dispositif de repérage fixé à son véhicule. Le dispositif utilisait une carte SIM mondiale qui se connectait aux réseaux de télécommunications canadiens pour transmettre des données à son propriétaire. Les enquêteurs ont émis des ordres de préservation à l'intention des principaux fournisseurs de services canadiens (FSC), leur demandant de conserver toutes les données associées au numéro IMSI du dispositif de repérage. Toutefois, les ordres de préservation n'exigent que la conservation des données pendant 21 jours et n'obligent pas les entreprises à confirmer qu'elles sont en possession des données pertinentes. Dans ce cas, seuls deux des quatre FSC ont confirmé qu'ils ne disposaient d'aucune donnée, laissant les enquêteurs dans l'incertitude quant aux dossiers des autres entreprises, ce qui rendait difficile d'établir les motifs justifiant de nouvelles ordonnances. Les ordres de préservation n'exigent pas des FSC qu'ils confirment l'existence des données. Les enquêteurs ont du mal à atteindre le seuil de conviction qu'un fournisseur détient ou contrôle des données, ce qui ralentit les enquêtes et crée de l'incertitude. Le projet de loi C-2 introduit la demande d'information, qui obligerait les FSC à confirmer si leur réseau a transmis les données du dispositif de repérage. Cette confirmation permettrait aux enquêteurs de demander des ordonnances de communication afin d'obtenir les informations de routage et de localisation liées à l'appareil, ce qui permettrait de gagner du temps dans l'enquête et d'assurer la sécurité de la victime.

Exemple (provinces de l'Atlantique)

Dans le dossier d'une personne disparue qui s'est transformé en dossier d'homicide/entrave à la justice, les enquêteurs avaient un suspect qui changeait régulièrement de numéro de téléphone et de fournisseur de services de télécommunications. Les enquêteurs ont dû recourir à plusieurs mandats d'enregistrement des données de transmission sur les téléphones de ses associés afin d'identifier son nouveau numéro de téléphone. Dans le contexte de cette enquête, la nouvelle demande d'information prévue dans le projet de loi C-2 aurait considérablement accéléré l'identification des nouveaux numéros de téléphone du suspect et réduit le nombre de mandats d'enregistrement des données de transmission nécessaires, ce qui aurait finalement accru l'efficacité et la rapidité de l'enquête.

Exemple (Québec)

Les enquêteurs ont mené une enquête de plusieurs années sur des activités frauduleuses en ligne impliquant le trafic d'informations personnelles et l'abus de confiance. Cette enquête a été compliquée par le fait que tout se passait en ligne et que la véritable identité des suspects n'était pas connue. Les enquêteurs ont envoyé plusieurs demandes à un FSC spécifique afin de confirmer que les informations qu'ils souhaitaient obtenir au moyen d'une ordonnance de communication étaient disponibles et sous son contrôle. Cependant, pour la plupart de leurs demandes, le fournisseur de services a refusé d'effectuer les vérifications demandées afin de confirmer l'existence des données et/ou des enregistrements. Les ordres de préservation n'obligent pas les FSC à confirmer l'existence des données. À l'heure actuelle, les enquêteurs doivent obtenir une ordonnance de communication pour obtenir des informations dont ils ne sont même pas certains de l'existence (obtenir des autorisations judiciaires pour constater 30 jours plus tard qu'aucun enregistrement n'existait chez ce FSC). Cela entraîne des retards inutiles, des autorisations judiciaires et des revers dans une enquête, ce qui allonge les délais d'enquête au détriment des victimes et des citoyens. Le projet de loi C-2 introduit l'outil de demande d'informations pour permettre aux enquêteurs d'exiger des informations des FSC qui détiennent ou contrôlent ces informations.

3. Modification du seuil pour les renseignements sur les abonnés

Les exigences actuelles en matière d'autorisation judiciaire pour obtenir les renseignements sur les abonnés sont des motifs raisonnables de croire (MRC) qu'une infraction a été commise et que le document ou les données fourniront des preuves de l'infraction. Le projet de loi C-2 crée une nouvelle ordonnance de communication spécifique aux renseignements sur les abonnés, fondée sur des motifs raisonnables de soupçonner.

Exemple hypothétique

Une enquête sur une personne disparue dont la victime potentielle était impliquée dans des vols antérieurs de voitures. Le réseau de vol de voitures serait un motif potentiel de la disparition de la victime et l'on soupçonne que la personne disparue a été tuée ou blessée. Les relevés téléphoniques du téléphone portable de la victime indiquent que plusieurs numéros inconnus ont contacté la personne disparue dans les jours qui ont précédé sa dernière apparition connue. Connaître les renseignements sur les abonnés associés à ces numéros aiderait la police à interroger ces personnes au sujet du meurtre présumé ou du réseau présumé de vol de voitures, qui pourrait avoir motivé le crime. À l'heure actuelle, dans la plupart des cas, au début d'enquêtes comme celle-ci, il n'existe que des motifs raisonnables

de soupçonner qu'une infraction a été commise. Une demande pourrait être rejetée uniquement en raison de ces circonstances. Les informations qui facilitent l'enquête (telles que les noms des contacts associés aux numéros de la victime ou du suspect) constituent une piste utile pour la police. Ces informations fournissent un point de départ pour interroger des personnes, éliminer celles qui ne présentent manifestement aucun intérêt et/ou établir un profil d'utilisation pour un utilisateur de téléphone. Il n'est pas nécessaire que le déclarant puisse démontrer que des preuves seront obtenues par rapport aux motifs raisonnables de soupçonner que cela faciliterait l'enquête sur l'infraction.

Exemple hypothétique

Une enseignante canadienne signale qu'une de ses élèves, âgée de 13 ans, lui a confié avoir reçu à plusieurs reprises des messages Instagram de la part d'une personne lui demandant des photos à caractère sexuel. L'enseignante fournit à la police une capture d'écran montrant le nom d'utilisateur et une indication générale de la date à laquelle les messages ont commencé. À l'heure actuelle, la police a besoin de motifs raisonnables de croire qu'un crime a été commis pour obtenir une ordonnance générale de communication, ce qui représente un seuil élevé au début de l'enquête. Avec des preuves limitées, elle pourrait se heurter à un obstacle juridique et être incapable d'agir rapidement. Grâce à la nouvelle ordonnance de communication d'informations sur les abonnés prévue par le projet de loi C-2, qui repose sur des soupçons raisonnables, les agents peuvent demander plus tôt dans l'enquête au conseiller juridique canadien d'Instagram de leur fournir les informations de base sur l'abonné liées au nom d'utilisateur. Ils reçoivent l'adresse IP, l'adresse électronique associée et le nom, et peuvent ainsi faire avancer l'enquête plus rapidement.

4. Délai de réponse aux ordonnances de communication

En vertu du *Code criminel* actuel, une personne, une institution financière ou une entité peut demander par écrit la révocation ou la modification d'une ordonnance de communication dans un délai de 30 jours. Le projet de loi C-2 modifie ce délai de 30 jours pour le ramener à 5 jours. Cela permet d'accéder beaucoup plus rapidement aux preuves essentielles. Certaines juridictions au Canada ont payé pour demander des ordonnances de communication accélérées afin de hâter le processus. À titre d'exemple, au 6 août 2025, le Service de police régionale de York a versé 500 $ à diverses entreprises de télécommunications à 35 reprises afin d'accélérer l'obtention de relevés téléphoniques. Ce processus a entraîné un coût total de 17 500 $. Ces demandes étaient appuyées par des mandats approuvés par les tribunaux et associées à des infractions minimales. L'accès rapide à ces relevés de télécommunications est une nécessité pour les enquêtes policières.

Exemple (Ontario)

Dans une affaire d'homicide, les auteurs ont attiré la victime à l'extérieur grâce à des appels provenant d'une personne se faisant passer pour un « ami ». Après une brève rencontre, la victime a été abattue et mortellement blessée. L'enquête s'est largement appuyée sur des ordonnances de communication et des preuves vidéo. Les enquêteurs ont obtenu les relevés téléphoniques de la victime, qui ont permis d'identifier le numéro du suspect. D'autres ordonnances de communication ont révélé l'identité des appelants concernés, ce qui a permis de mener rapidement une enquête vidéo. Les images de vidéosurveillance ont permis de relier les suspects à un véhicule, à des réunions dans un hôtel et, finalement, au crime. Les FSC ont rendu certains résultats des ordonnances de communication en moins de 48 heures, ce qui était essentiel pour obtenir des preuves vidéo urgentes avant qu'elles ne soient effacées. L'affaire a abouti à des condamnations pour meurtre au premier degré. Cependant, dans d'autres affaires semblables, les FSC ont pris les 30 jours autorisés, ce qui aurait entraîné la perte de preuves cruciales.

Exemple (Ontario)

En novembre 2024, une intrusion armée a eu lieu dans une maison, et la seule victime, une femme, a été confrontée à deux suspects, dont l'un était armé d'une arme à feu. Les suspects ont exigé que la victime désactive l'alarme qui s'était déclenchée, ce qu'elle a fait. L'époux de la victime a tenté de la contacter après avoir reçu une alerte sur son téléphone indiquant que l'alarme s'était déclenchée. Ne parvenant pas à la joindre, il a demandé à un voisin d'aller vérifier la résidence. Alors que le voisin entrait dans le hall d'entrée de la résidence, il a été abattu par l'un des suspects. La victime était en compagnie de son enfant de 6 ans au moment de la fusillade. Cette résidence avait également été la cible d'une effraction en octobre 2024, au cours de laquelle le véhicule suspect avait frappé les voitures de police qui étaient intervenues. Deux suspects ont pris la fuite à pied, dont l'un a été appréhendé. Deux armes à feu chargées ont été retrouvées lors de cet incident. Plusieurs pistes ont été identifiées pour chaque incident, mais les enquêteurs ont dû attendre 30 jours pour obtenir les résultats, ce qui a considérablement retardé l'enquête.

Exemple (Ontario)

Entre les mois d'août et septembre 2024, une victime de sexe féminin a rencontré un homme inconnu sur un site de rencontres en ligne. La relation amoureuse s'est transformée en une opportunité d'investissement. Les représentants du service à la clientèle du suspect se sont rendus à trois reprises au domicile de la victime pour collecter un total de 170 000 $ en espèces. La fraude totale s'élevait à plus de 2 millions de dollars. Bien que l'incident ne soit pas de nature violente, l'accès immédiat aux résultats permettant d'identifier les suspects aurait été utile pour éviter que cette victime ne subisse d'autres méfaits et/ou pour identifier d'autres victimes.

Exemple (Ontario)

En juin 2025, des suspects masqués et armés de marteaux se sont présentés dans une bijouterie d'un grand centre commercial et ont tenté d'y pénétrer. N'ayant pas réussi à entrer, ils se sont enfuis vers un véhicule qui les attendait. Un incident semblable s'est produit en juillet 2025, au cours duquel toutes les vitrines de la bijouterie ont été brisées. Les enquêteurs ont demandé des ordonnances de communication dans les deux cas et attendent toujours les résultats.

Exemple (juridiction non précisée)

Dans une affaire d'homicide, une victime a été abattue par une connaissance au bord d'une route. Les enquêteurs avaient besoin de toute urgence des relevés téléphoniques pour confirmer les contacts et localiser le suspect, qui était soupçonné d'avoir en sa possession le téléphone de la victime et une arme à feu. Le suspect a ensuite été signalé comme brandissant l'arme, qui n'avait pas été retrouvée. Les enquêteurs avaient obtenu l'autorisation judiciaire d'utiliser un traceur téléphonique, mais aucune donnée n'a pu être obtenue, ce qui a empêché la localisation. Une réponse rapide concernant les relevés d'appels et les données des antennes-relais était nécessaire pour identifier les témoins potentiels, confirmer les communications et récupérer l'arme qui posait un risque continu pour la sécurité de la communauté. Les retards ont menacé, à la fois, la sécurité publique et la conservation des preuves essentielles. Les retards dans les ordonnances de communication ont limité la capacité des enquêteurs à identifier rapidement les suspects, les témoins et l'emplacement d'une arme à feu qui serait toujours en circulation.

5. Accès amélioré aux preuves numériques transfrontalières

Le projet de loi C-2 crée un mécanisme d'ordonnance de communication étrangère pour les informations sur les abonnés et les données de transmission détenues par des entités étrangères, aidant ainsi les enquêteurs à obtenir des preuves essentielles auprès de plateformes basées aux États-Unis (p. ex., Facebook, Dropbox, Snapchat). La plupart des affaires de matériel pédopornographique en ligne impliquent des entreprises technologiques étrangères. Auparavant, les enquêteurs canadiens étaient confrontés à des retards liés à la navigation dans les traités d'entraide juridique (TEJs) ou à la coopération volontaire. Grâce à cette disposition alignée sur le deuxième protocole additionnel à la Convention de Budapest, les unités chargées de la lutte contre l'exploitation des enfants sur Internet (EEI) peuvent désormais faciliter la divulgation des données avec moins de friction, accélérant ainsi la collecte de preuves et la protection des enfants victimes.

Exemple hypothétique

Le Centre national contre l'exploitation d'enfants (Canada) reçoit un signalement du National Center for Missing & Exploited Children (centre de signalement américain) concernant une adresse IP canadienne qui télécharge du matériel pédopornographique sur Dropbox. La police locale identifie l'adresse IP et saisit les appareils du suspect, mais les preuves les plus importantes, notamment les images réelles d'abus sexuels sur des enfants, sont entreposées dans le compte Dropbox du suspect, hébergé aux États-Unis. À l'heure actuelle, la police doit demander l'aide par l'entremise du TEJ, ce qui peut prendre des mois. Au moment où l'accès est accordé, les preuves peuvent avoir été supprimées ou effacées, ce qui peut affaiblir les poursuites. En vertu du projet de loi C-2, les agents peuvent émettre une ordonnance de communication étrangère directement à l'équipe juridique de Dropbox, ce qui accélère l'accès aux preuves et réduit les délais et la dépendance à l'égard des TEJs.

Exemple (Québec)

Dans les affaires de livraison contrôlée, où des cargaisons de contrebande sont décelées, les policiers s'appuient sur des ordonnances de communication pour identifier les destinataires et les suspects. Cependant, les retards dans l'examen judiciaire et les réponses des entreprises permettent souvent aux suspects d'abandonner les cargaisons avant que la police ne puisse agir. Les fournisseurs de services de communication imposent également des frais élevés pour l'accès accéléré aux données, ce qui nécessite l'approbation de la direction pour débloquer les fonds, ce qui retarde davantage la procédure. Les tribunaux sont souvent engorgés par les demandes, les juges étant incapables de les traiter rapidement. À Montréal, les enquêteurs

doivent composer chaque semaine avec des délais simplement pour rencontrer les juges. De plus, certains juges refusent les ordonnances de communication impliquant des fournisseurs de services étrangers, et les entreprises américaines rejettent fréquemment les demandes canadiennes.

Ces retards entraînent des blocages dans les enquêtes, en particulier lorsque des victimes sont impliquées. Le projet de loi C-2 réduit les délais des ordonnances de communication de 30 à 5 jours, clarifie le pouvoir des autorités canadiennes de demander des données à des entités étrangères et simplifie les procédures judiciaires afin de réduire les engorgements et les coûts dans les affaires urgentes de contrebande.

6. Suivi d'objets semblables

Le projet de loi C-2 permet à un juge ou à un magistrat d'autoriser les enquêteurs à obtenir des données de suivi relatives à l'emplacement d'un objet ou d'un objet semblable.

Exemple (juridiction non précisée)

Dans le cadre d'enquêtes sur le crime organisé, les suspects changent régulièrement de véhicule pour échapper à la surveillance. Dans un cas, les enquêteurs ont reçu l'autorisation judiciaire de suivre le véhicule de la cible, mais ont découvert le jour de l'installation que le suspect avait changé de voiture. Le déclarant a dû réécrire la demande d'information pour le deuxième véhicule, rédiger et soumettre un nouveau mandat pour le deuxième véhicule, perdant ainsi du précieux temps. De même, les suspects utilisent souvent des véhicules de location, qu'ils changent fréquemment, afin de contrecarrer les efforts de la police. Chaque fois qu'un suspect change de véhicule ou d'appareil, la police est obligée de demander de nouvelles autorisations de suivi, ce qui crée des lacunes dans l'enquête. Les mandats de suivi actuels ne s'appliquent qu'à des véhicules ou des appareils spécifiques, ce qui oblige à présenter des demandes répétées lorsque les suspects changent de véhicule ou d'appareil. Le projet de loi C-2 permet d'obtenir une autorisation préalable pour suivre des objets « semblables » (tels que des véhicules) dans le cadre d'une enquête.

7. Codification de la divulgation des informations relatives aux abonnés liées aux données de transmission

À l'heure actuelle, l'article 492.2(1) du *Code criminel* permet à un juge ou à un magistrat d'autoriser les enquêteurs à obtenir des données de transmission au moyen d'un mandat d'enregistrement des données de transmission (MEDT). Les informations sur les abonnés (nom et adresse) sont alors généralement obtenues au moyen d'une ordonnance d'assistance, décrite à l'article 487.02 du *Code criminel,* qui accompagne le mandat MEDT. Dans la province de Québec, il est parfois impossible d'obtenir des informations sur les abonnés par l'entremise d'une ordonnance d'assistance, car certains juges refusent de les autoriser. Le projet de loi C-2 clarifie et normalise la façon dont les informations sur les abonnés liées aux données de transmission doivent être obtenues au Canada.

***Exemple (Québec)* – Enquête sur un homicide**

Le juge a refusé l'ordonnance d'assistance visant à obtenir les informations sur l'abonné (nom et adresse) en déclarant que « l'assistance nécessaire à l'exécution du mandat demandé pour l'enregistreur de données de transmission [...] est déterminée en fonction de l'objet du mandat principal, et non pour obtenir des informations supplémentaires qui ne sont pas des données de transmission mais qui peuvent aider à interpréter les données collectées. Si le législateur avait voulu autoriser cela, il aurait pu le dire en termes clairs (...) ».

***Exemple (Québec)* – Agression sexuelle**

Le juge a rejeté l'ensemble du mandat d'enregistrement des données de transmission en déclarant que « les noms et coordonnées ne constituent pas des données de transmission ».

***Exemple (Québec)* – (Infraction non précisée)**

Le juge a refusé l'ordonnance d'assistance visant à obtenir les informations de l'abonné et a déclaré : « Les informations sur l'abonné ne sont pas couvertes par l'article 487.02 du Code criminel. L'article 487.02 du Code criminel n'a pas pour but d'étendre les actes autorisés par l'article 492.2 du Code criminel, qui est autorisé sur la base d'un soupçon. Il y a une atteinte raisonnable à la vie privée en ce qui concerne le nom de l'abonné (en référence à la décision *Spencer*). Je ne suis pas lié par la décision 2019 NLCA 6. »

CONTRIBUTIONS DE :

Association canadienne des chefs de police - Comité sur la criminalité électronique

Association canadienne des chefs de police - Comité des modifications législatives

Police provinciale de l'Ontario

Service de police régional de Peel

Gendarmerie royale du Canada

Sûreté du Québec

Service de police de Toronto

Service de police de Vancouver

Service de police régional de York

Ministère du Procureur général, Ontario