



NATIONAL
POLICE
FEDERATION

FÉDÉRATION
DE LA POLICE
NATIONALETM

Cadre canadien pour les enquêtes numériques

Comprendre les parties 14 et 15 du
projet de loi C-2





Que se passe-t-il s'il n'y a pas de changements?

Les services de police doivent recourir à des solutions de rechange extrêmes en l'absence de cadres d'interception pratiques :

- Outils très coûteux
- Longs délais
- Risques juridiques complexes

Dans de nombreux cas :

- Des accusations sont reportées ou abandonnées.
- Des outils sensibles sont dévoilés devant les tribunaux.
- Des enquêtes n'aboutissent pas, même lorsque les crimes sont réels.

Cette situation n'est ni sécuritaire, ni abordable, ni durable.

Principaux points à retenir

- Le fait d'appuyer les parties 14 et 15 du projet de loi C-2 comme fondement d'un projet de loi sur l'accès légal aux données numériques permettrait de faire ce qui suit :
 - Aider les services de police à exécuter les mandats accordés par les juges.
 - Établir des règles claires pour les fournisseurs de services.
 - Protéger la vie privée grâce à une surveillance rigoureuse effectuée par les tribunaux.
 - Remplacer des solutions de rechange risquées par des pouvoirs clairs conférés par la loi.
- Il faut accepter les réalités documentées par les membres du CPSNR, la GRC et le SCRS.
- La vie privée et la sécurité peuvent coexister.
- Le Canada est le seul pays du Groupe des cinq à ne pas disposer d'un cadre d'accès légal clair pour les communications modernes.
 - Royaume-Uni (*Investigatory Powers Act*)
 - Australie (*Telecommunications and Other Legislation Assistance and Access Act*)
 - États-Unis (*Communications Assistance for Law Enforcement Act*)
 - Nouvelle-Zélande et 11 autres démocraties occidentales (France, Allemagne, Pays-Bas, Suède, etc.)



Le défi

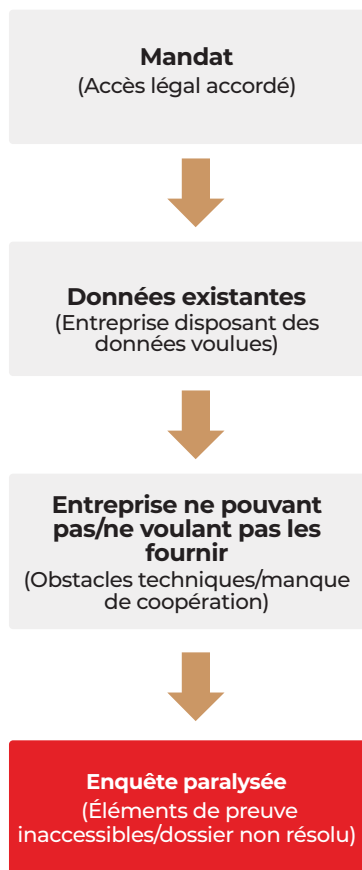
- Les criminels utilisent quotidiennement des téléphones intelligents, des applications et des services en ligne.
- Les lois actuelles ne suivent pas les avancées technologiques rapides.
- L'évolution des plateformes numériques entrave les méthodes d'enquête traditionnelles.
- Pour obtenir des éléments de preuve essentiels, les forces de l'ordre doivent surmonter des obstacles.
- Le phénomène « devenir invisible » menace la sécurité publique.

Avertissement émanant du Parlement : le rapport du CPSNR

Les députés et sénateurs faisant partie du Comité des parlementaires sur la sécurité nationale et le renseignement (CPSNR) ont mené un examen approfondi des défis liés à l'accès légal et ils ont déposé un rapport en septembre 2025.

Le Comité a conclu que :

- les lois du Canada sont figées dans le passé;
- les services de police utilisent de vieux outils pour lutter contre des crimes modernes;
- le fossé entre ce que la loi permet et ce que la technologie rend possible est grandissant;
- les affirmations selon lesquelles les services de police ont « trop de pouvoir de surveillance » sont dépassées.



Ce qui ne va pas

Sécurité nationale

Les services de police obtiennent l'autorisation de surveiller une menace grave. L'application est chiffrée, et l'entreprise n'a aucune obligation d'apporter son aide. Le mandat est inutile.

Exploitation d'enfants

Les comptes sont hébergés à l'étranger. Le traitement des requêtes internationales prend des mois. Les suspects suppriment les éléments de preuve et continuent de commettre des infractions.

Crime organisé

Les services de police doivent s'adresser aux tribunaux simplement pour faire correspondre un numéro de téléphone à un nom. Cette étape ralentit les enquêtes qui évoluent rapidement.



- 

Partie 15 : capacité d'interception

- Elle impose aux fournisseurs qu'ils détiennent les compétences techniques pour intercepter des données.
- Elle s'applique aux télécommunications modernes et aux services numériques.
- Elle permet aux forces de l'ordre d'intercepter des communications avec un mandat.
- Elle veille à ce que les fournisseurs comprennent leurs responsabilités légales.

Comment la vie privée est-elle protégée?

Demandes de renseignements	Renseignements de base seulement. Aucun contenu de messages. Délais prescrits en matière de confidentialité.
Ordonnances de communication	Le juge doit donner son autorisation. Le juge contrôle la portée. Des motifs raisonnables doivent être invoqués.
Recherches numériques	Le juge doit croire que les données contiennent des éléments de preuve criminels.

Voie à suivre

- Établir un équilibre entre la sécurité publique et le droit individuel à la vie privée.
- Favoriser la confiance du public par la transparence et la responsabilisation.
- S'adapter de façon continue à l'évolution du paysage numérique.
- Permettre au Canada de rattraper tous les partenaires du Groupe des cinq et d'autres démocraties occidentales.



FÉDÉRATION
DE LA POLICE
NATIONALE

