# Évaluation de l'Initiative sur les pouvoirs d'enquête au 21e siècle

## Rapport final

Mars 2020

Direction d'évaluation
Secteur d'audit interne et d'évaluation

Department of Justice Canada | Ministère de la Justice Canada

Canada

# REMERCIEMENTS

La dirigeante principale d'audit et d'évaluation aimerait remercier l'équipe d'évaluation et les autres personnes qui ont contribué à cet engagement, et particulièrement les employés du ministère de la Justice du Canada, du Service des poursuites pénales du Canada, de la Gendarmerie royale du Canada et des Affaires mondiales Canada, qui ont fourni des connaissances et des commentaires dans le cadre de cette évaluation.

# ACRONYMES

| | |
|---|---|
| AMC | Affaires mondiales Canada |
| Charte | *Charte canadienne des droits et libertés* |
| Convention de Budapest | *Convention sur la cybercriminalité du Conseil de l'Europe* |
| EC3 | Centre européen de lutte contre la cybercriminalité (Europol) |
| EDT | Enregistreur de données de transmission |
| EJ | Entraide juridique |
| FSI | Fournisseur de services Internet |
| FST | Fournisseurs de services de télécommunication |
| GC | Gouvernement du Canada |
| GEI | Groupe d'entraide internationale (Justice) |
| GIO | Gestion de l'information opérationnelle (GRC) |
| GICT | Groupes intégrés de la criminalité technologique |
| GRC | Gendarmerie royale du Canada |
| IAL | Initiative sur l'accès légal |
| IAM | Identificateur d'appareil mobile |
| ICANN | Société pour l'attribution des noms de domaine et des numéros sur Internet |
| IDT | Direction du crime international et du terrorisme (AGC) |
| IOCTA | Évaluation de la menace que représente la criminalité organisée sur Internet |
| JLA | Direction du droit criminel, de la sécurité et de la diplomatie, Direction générale des affaires juridiques (AMC) |
| Justice | Ministère de la Justice du Canada |
| LEJMC | *Loi sur l'entraide juridique en matière criminelle* |
| LPCCC | *Loi sur la protection des Canadiens contre la cybercriminalité* |
| NAC | Nom et adresse du client |
| OEA | Organisation des États américains |
| PE21S | Pouvoirs d'enquêtes au 21e siècle |
| PSC | Prestataire de services de communication |
| RBA | Renseignements de base sur les abonnés |
| SPDP | Section de la politique en matière de droit pénal (Justice) |
| SPPC | Service des poursuites pénales du Canada |

| | |
|---|---|
| T-CY | Comité de la Convention sur la cybercriminalité (Conseil de l’Europe) |
| TEJ | Traité d’entraide juridique |
| UE | Union européenne |
| USJ | Unité des services juridiques |

# TABLE DES MATIÈRES


**SOMMAIRE ..... iii**

**1. INTRODUCTION ..... 1**

1.1 Objet de l'évaluation ..... 1

1.2 Portée de l'évaluation ..... 1

**2. PROFIL DU PROGRAMME ..... 1**

**3. MÉTHODOLOGIE DE L'ÉVALUATION ..... 4**

3.1 Examen des documents ..... 4

3.2 Examen de l'information sur le rendement ..... 5

3.3 Examen documentaire ..... 5

3.4 Examen des tendances en matière de cybercriminalité et de criminalité assistée par ordinateur ..... 5

3.5 Entrevues avec des informateurs-clés ..... 5

3.6 Limitations ..... 6

**4. CONSTATATIONS ..... 7**

4.1 Pertinence ..... 7

4.1.1 Besoin continu de l'Initiative sur les pouvoirs d'enquête au 21e siècle ..... 7

4.1.2 Harmonisation avec les priorités gouvernementales ..... 10

4.2 Rendement ..... 13

4.2.1 Sensibilisation aux pouvoirs d'enquête et connaissance de ceux-ci ..... 13

4.2.2 Gestion des questions et cohérence de la mise en œuvre et de l'interprétation des pouvoirs d'enquête ..... 14

4.2.3 Amélioration de la capacité opérationnelle pour lutter contre la cybercriminalité et la criminalité assistée par ordinateur ..... 20

4.2.4 Amélioration de la coopération internationale pour l'obtention de preuves numériques ..... 22

4.2.5 Effets non prévus ..... 26

4.3 Conception ..... 27

4.3.1 Gestion horizontale de l'Initiative sur les pouvoirs d'enquête au 21e siècle ..... 27

**5. CONCLUSIONS ET RECOMMANDATIONS ..... 27**

5.1 Conclusion ..... 27

5.1.1 Pertinence ..... 27

5.1.2 Rendement ..... 28

5.1.3 Conception ..... 28

5.2 Recommandations ..... 28

**ANNEXE A: PROFIL DU PROGRAMME ..... 30**

## Liste des tableaux

Tableau 1 : Budget 2015-2016 à 2019-2020 de l'Initiative sur les pouvoirs d'enquête au 21e siècle..4

Tableau 2 : Aperçu de la dotation en équivalents temps plein ……..……4

Tableau 3 : Nombre de demandes d'entraide juridique entrantes et sortantes relativement à des preuves numériques……...24

## Figure

Figure A1 : Modèle logique de l'Initiative sur les pouvoirs d'enquête au 21e siècle ……32

# SOMMAIRE

## Introduction

Le présent rapport présente les résultats d'une évaluation de l'*Initiative sur les pouvoirs d'enquête au 21e siècle* (PE21S), une initiative horizontale dirigée par le ministère de la Justice du Canada (Justice) en collaboration avec le Service des poursuites pénales du Canada (SPPC), la Gendarmerie royale du Canada (GRC) et Affaires mondiales Canada (AMC).

L'Initiative PE21S a favorisé la mise en œuvre de nouveaux pouvoirs juridiques découlant de l'ancien projet de loi C-13, la *Loi sur la protection des Canadiens contre la cybercriminalité* (LPCCC), qui est entrée en vigueur le 10 mars 2015.

## Description du programme

Il y a longtemps que l'on admet la nécessité de nouveaux pouvoirs d'enquête pour protéger les Canadiens et enquêter sur la criminalité facilitée par les technologies informatiques et des communications, et pour lutter contre la criminalité qui a une dimension transnationale.

Depuis l'an 2000, les efforts déployés par le gouvernement du Canada (GC) dans le cadre de l'Initiative sur l'accès légal (IAL) sont axés sur l'évaluation de la nécessité d'adopter des lois nouvelles et modifiées. L'Initiative PE21S découle des parties de l'IAL relatives aux modifications apportées au *Code criminel*, qui sont entrées en vigueur avec l'adoption de la LPCCC. Cette loi a introduit des pouvoirs d'enquête spécialisés en vertu d'une autorisation judiciaire pour l'obtention de preuves numériques. Elle a modifié le *Code criminel*, la *Loi sur l'entraide juridique en matière criminelle*, la *Loi sur la preuve au Canada* et la *Loi sur la concurrence* qui ont :

- étoffé le régime des ordonnances de communication afin de fournir des outils plus précis pour répondre à la technologie contemporaine et aux exigences d'enquête connexes, tout en équilibrant de façon appropriée la vie privée et les droits de la personne;
- introduit un nouveau régime pour conserver rapidement les données volatiles en recourant à des ordres et des ordonnances de préservation;
- appuyé la collecte de preuves numériques dans les enquêtes criminelles, notamment pour aider les autorités étrangères chargées des enquêtes et des poursuites;
- permis au Canada de ratifier le 8 juillet 2015 la Convention sur la cybercriminalité du Conseil de l'Europe (la Convention de Budapest). La Convention est le seul instrument juridique multilatéral de lutte contre la criminalité informatique.

L'Initiative PE21S a été soutenue par un financement de 60,74 millions de dollars sur cinq ans (de 2015-2016 à 2019-2020) et des fonds permanents de 12,25 millions de dollars par année.

Justice, le SPPC, la GRC et AMC sont conjointement responsables de la gestion de la mise en œuvre de l'Initiative PE21S, alors que chacun exerce ses activités particulières dans les systèmes de justice pénale et de politique internationale. Les principaux groupes cibles de l'Initiative PE21S sont les services de police et les poursuivants. L'objectif consiste à les pourvoir de moyens plus efficaces d'enquêter sur la cybercriminalité et la criminalité assistée par ordinateur et d'intenter des poursuites, tout en respectant la vie privée et les libertés des Canadiens.

Cinq activités principales ont été mises en œuvre par l'Initiative :

- **Analyse juridique, élaboration et coordination de politiques sur les questions nationales et internationales –** Comprend les conseils juridiques et stratégiques, le soutien au contentieux et les services de poursuite nécessaires pour gérer la mise en œuvre des dispositions législatives relatives aux pouvoirs d'enquête dans la LPCCC, et pour respecter les obligations internationales du Canada découlant de la ratification de la Convention de Budapest.

- **Sensibilisation et formation** – Comprend l'élaboration de documents de sensibilisation et de formation pour veiller à ce que les réformes législatives prévues par la LPCCC soient mises en œuvre de façon uniforme. Les principaux groupes visés par la formation ont été les services de police et les poursuivants. On a également déployé des efforts pour sensibiliser les partenaires internationaux du Canada aux dispositions de la LPCCC.

- **Recherche technique et outils à l'appui des enquêtes criminelles** – Comprend l'élaboration de nouveaux outils, techniques et solutions pour l'interception justifiée et en temps réel des données de transmission et l'analyse des données saisies, notamment les demandes internationales liées à la Convention de Budapest.

- **Administration d'un système de conservation des données** – Nécessite l'élaboration d'une fonction de triage réservée pour l'administration d'un nouveau système de conservation des données, conformément aux dispositions légales de la LPCCC et pour répondre aux demandes d'aide internationales.

- **Coopération internationale** – Vise à faire progresser la coopération internationale en matière de cybercriminalité et à veiller à ce que les intérêts du Canada en matière de cybercriminalité et d'autres types de criminalité assistée par ordinateur soient pris en compte dans la politique étrangère globale du Canada.

## Constatations

Les principales constatations de l'évaluation horizontale de l'Initiative PE21S concernant les questions d'évaluation sont résumées ci-dessous.

### Pertinence

L'objectif global de l'Initiative PE21S, à savoir fournir les moyens de mettre en œuvre les pouvoirs d'enquête ajoutés au *Code criminel* par la LPCCC et satisfaire les obligations internationales du Canada découlant de la ratification de la Convention de Budapest, demeure pertinent alors que la cybercriminalité et la criminalité assistée par ordinateur sont en croissance rapide tant au Canada qu'à l'international, et que les criminels exploitent de plus en plus les technologies en évolution.

La LPCCC a apporté des réformes législatives nécessaires pour permettre aux pouvoirs d'enquête spécialisés d'obtenir, en vertu d'autorisations judiciaires, des éléments de preuve numériques, non seulement pour la criminalité technologique, comme le piratage ou les activités du crime organisé, mais aussi pour faire face aux infractions quotidiennes, lorsque des criminels envoient un courriel, utilisent leur téléphone cellulaire ou publient des images sur des réseaux sociaux. Ces réformes ont donné lieu à un régime d'ordonnances de communication permettant aux juges de savoir précisément quels types de données sont demandées et d'établir un équilibre adéquat entre les droits relatifs à la vie privée et les droits de la personne. En outre, la LPCCC a introduit un nouveau régime qui permet de préserver rapidement les données volatiles grâce aux ordres et aux ordonnances de préservation.

Les éléments probants de l'évaluation indiquent qu'il existe un besoin continu pour les activités clés financées par l'Initiative PE21S, notamment :

- **Analyse juridique, élaboration de politiques et coordination sur les questions nationales et internationales –** Bien qu'il n'y ait eu que très peu de litiges en ce qui concerne les pouvoirs d'enquête de l'Initiative PE21S jusqu'à maintenant et aucune contestation couronnée de succès en vertu de la *Charte canadienne des droits et libertés* (Charte), Justice doit maintenir sa capacité de défense à l'égard des contestations futures et de modification du *Code criminel* au besoin. AMC doit également continuer de coordonner l'approche du Canada en matière de politique étrangère sur la cybercriminalité sur la scène internationale, qui devient de plus en plus complexe et politisée.

- **Sensibilisation et formation –** La phase de « sensibilisation » de l'Initiative PE21S est terminée, car les poursuivants et les responsables de l'application de la loi connaissent maintenant très bien les pouvoirs d'enquête liés à l'Initiative PE21S. Les activités de sensibilisation devront continuer d'aider les intervenants à appliquer les dispositions du *Code criminel*, principalement de façon réactive ou selon les besoins. La formation continue des poursuivants et des responsables de l'application de la loi sur les modifications au *Code criminel* a été intégrée aux programmes de formation offerts par des organisations comme le Collège canadien de police et l'École des poursuivants du SPPC.

- **Administration du système de conservation des données –** L'Initiative PE21S a permis à la GRC d'élaborer et de mettre en œuvre un système de conservation des données pour traiter un grand nombre de demandes de conservation des données provenant des organismes d'application de la loi étrangers. Cette activité doit se poursuivre, car le Canada continuera de recevoir des demandes de conservation de la part d'organismes étrangers d'application de la loi et doit donc maintenir sa capacité de gestion de telles demandes. La GRC a mis sur pied un Groupe national de coordination contre la cybercriminalité qui sera un point de contact unique.

- **Recherche technique et outils à l'appui des enquêtes criminelles –** Les Services des enquêtes techniques de la GRC ont mis au point des outils pour accéder à des preuves numériques provenant d'un appareil ou d'un support de stockage numérique saisies comme éléments de preuve (données inactives), les obtenir et les traiter, ainsi que des outils déployés dans une situation de communication en direct (données actives). Comme la cybercriminalité est de plus en plus complexe sur le plan technologique, il sera essentiel que la GRC et d'autres organismes fédéraux mettent au point des outils supplémentaires pour appuyer les enquêtes criminelles.

De plus, la Convention de Budapest est le principal instrument international sur la cybercriminalité. Elle vise à aider les États signataires à harmoniser leurs lois nationales, à améliorer leurs techniques d'enquête, et à accroître leur coopération. La ratification de la Convention a permis au Canada de collaborer avec d'autres États signataires dans le cadre d'enquêtes sur la cybercriminalité et a autorisé l'accès à des éléments de preuves numériques que l'on peut trouver dans un autre pays. On considère que le Canada joue un rôle important à l'échelle internationale en appuyant la Convention.

Bien que les éléments probants tirés de cette évaluation indiquent que la LPCCC répond à un besoin important de modernisation des pouvoirs d'enquête prévus dans le *Code criminel*, les lois canadiennes doivent continuellement évoluer afin que les organismes d'application de la loi et les poursuivants disposent des outils nécessaires pour lutter contre la cybercriminalité et d'autres types de criminalité assistée par ordinateur. La police et les poursuivants ont souligné en particulier les défis associés à l'accès aux renseignements de base sur les abonnés et aux données chiffrées.

## Rendement

Voici les constatations de l'évaluation concernant le rendement de l'Initiative PE21S dans l'atteinte de ses principaux résultats attendus :

- **Sensibilisation aux pouvoirs d'enquête liés à l'Initiative PE21S et leur connaissance** – Les groupes cibles de l'Initiative PE21S, notamment les organismes d'application de la loi, les poursuivants et les fournisseurs de services de télécommunications connaissent maintenant très bien les modifications législatives apportées au *Code criminel* et à d'autres lois. Les représentants de l'Initiative PE21S ont consacré des efforts considérables à la sensibilisation par rapport aux éléments clés de la LPCCC et à leur connaissance.

- **Gestion des questions et cohérence de la mise en œuvre et de l'interprétation des pouvoirs d'enquête** – Relativement peu de questions juridiques et opérationnelles ont été soulevées en ce qui a trait aux nouveaux pouvoirs d'enquête. On s'attendait à ce que les nouveaux pouvoirs d'enquête entraînent de nombreuses contestations fondées sur la Charte, mais cela ne s'est pas encore avéré. Les ressources fournies aux partenaires fédéraux par l'Initiative PE21S ont aidé ceux-ci à gérer la mise en œuvre des pouvoirs d'enquête de diverses façons, allant de l'appui aux poursuites fondées sur ces pouvoirs à la prestation de conseils juridiques et stratégiques aux intervenants internes. La principale question juridique soulevée par les informateurs clés a trait au fait que les nouvelles dispositions visant les mandats pour enregistreurs de données de transmission ne donnent pas accès aux renseignements de base sur les abonnés. Les pouvoirs d'enquête ont été largement mis en œuvre partout au Canada.

- **Amélioration de la capacité de lutter contre la cybercriminalité et la criminalité assistée par ordinateur** – L'Initiative PE21S a contribué à améliorer la capacité opérationnelle du Canada de lutter contre la cybercriminalité et d'autres types de criminalité assistée par ordinateur, tant au pays qu'à l'étranger. Les responsables de l'Initiative PE21S ont collaboré étroitement les uns avec les autres et avec les intervenants externes pour soutenir la mise en œuvre des pouvoirs d'enquête liés à l'Initiative PE21S. La GRC a mis en place une fonction de triage réservée au traitement et au suivi des demandes de conservation des données reçues des organismes d'application de la loi étrangers. Elle a également mis au point de nouveaux outils pour accéder à des éléments de preuve numériques provenant d'appareils saisis, les obtenir et les traiter, ainsi que des outils utilisés dans une situation d'interception réelle.

- **Amélioration de la coopération internationale pour l'obtention de preuves numériques** – L'Initiative PE21S a aidé le Canada à accroître son niveau de coopération à l'échelle internationale pour l'obtention de preuves numériques afin de lutter contre la cybercriminalité et la criminalité assistée par ordinateur. Les intervenants internationaux considèrent que le Canada respecte les exigences de la Convention sur la cybercriminalité et d'autres accords d'entraide juridique (EJ) applicables. À l'échelle internationale, le Canada est perçu comme jouant un rôle important dans le soutien à l'égard de la Convention, en raison de son effort considérable consacré à la rédaction du Deuxième Protocole additionnel, toujours en cours de négociation au sein du Conseil de l'Europe. Le Groupe d'entraide internationale (Justice) a amélioré la vitesse à laquelle les demandes d'EJ visant à obtenir des éléments de preuve numériques reçues des organismes étrangers d'application de la loi et des poursuivants sont traitées et exécutées. L'Initiative a également contribué à améliorer la coordination et l'uniformité de l'approche de la politique étrangère du Canada en matière de cybercriminalité et de criminalité assistée par ordinateur.

## Conception

L'Initiative PE21S a été bien coordonnée. Le plan d'activités de l'Initiative PE21S a été préparé de façon minutieuse et l'Initiative a évolué comme prévu.

## Recommandations

Aucune recommandation n'est incluse puisque l'Initiative PE21S a été mise en œuvre comme prévu et qu'aucun obstacle n'a été relevé pour l'atteinte des résultats attendus.

# 1. INTRODUCTION

## 1.1 Objet de l'évaluation

Le présent rapport présente les résultats d'une évaluation de l'*Initiative sur les pouvoirs d'enquête au 21e siècle* (PE21S), une initiative horizontale dirigée par le ministère de la Justice du Canada (Justice) en collaboration avec le Service des poursuites pénales du Canada (SPPC), la Gendarmerie royale du Canada (GRC) et Affaires mondiales Canada (AMC). L'évaluation a été menée en accord avec la *Politique sur les résultats* (2016) du Conseil du Trésor. L'évaluation a été entreprise par la Direction de l'évaluation du ministère de la Justice entre septembre 2018 et septembre 2019, conformément au *Plan d'évaluation ministériel 2018-2019*.

## 1.2 Portée de l'évaluation

L'évaluation a examiné la pertinence, le rendement et la conception de l'Initiative et a porté sur une période suivant l'adoption du projet de loi C-13, *Loi sur la protection des Canadiens contre la cybercriminalité* (LPCCC), soit du 10 mars 2015 au 31 mars 2019. La première année, 2015-2016, a été traitée comme référence, alors que les partenaires fédéraux (responsables de l'Initiative PE21S) ont commencé à embaucher du personnel et à mettre en œuvre les diverses activités financées. C'est aussi l'année où le Canada a ratifié la *Convention sur la cybercriminalité du Conseil de l'Europe* (Convention de Budapest) le 8 juillet 2015.

# 2. PROFIL DU PROGRAMME

L'évolution des technologies informatiques et des communications a changé la façon dont les Canadiens communiquent et vivent leur vie. Ils peuvent utiliser une multitude d'appareils de communication et une grande variété d'outils comme le courriel, la messagerie instantanée et diverses applications de médias sociaux. Bien que cette évolution procure d'énormes avantages à la société canadienne, les criminels utilisent les mêmes technologies à des fins illicites. Les communications numériques constituent maintenant un outil fondamental pour pratiquement toutes les activités criminelles, et l'information numérique est parfois plus importante que les preuves physiques ou les renseignements dans les enquêtes et les poursuites criminelles[1].

On reconnaît depuis longtemps que la police au Canada doit être en mesure de travailler aussi efficacement dans le monde numérique que dans le monde physique. Elle doit également avoir la capacité de collaborer avec leurs partenaires internationaux qui recherchent des preuves numériques auprès du Canada pour appuyer leurs enquêtes et leurs poursuites criminelles. Les lois régissant la collecte de renseignements et de preuves devaient être mises à jour pour tenir compte des progrès de la technologie numérique qui ont commencé à la fin du vingtième siècle.

L'Initiative sur l'accès légal (IAL) du gouvernement du Canada (GC) fournit un cadre pour l'élaboration de solutions techniques et d'options législatives. L'accès légal est une technique importante et bien établie utilisée par la police pour prévenir les infractions graves et mener des enquêtes à leur sujet. Il s'agit de l'interception de communications ainsi que de la perquisition et de la saisie de renseignements effectuées en vertu de pouvoirs légaux. Depuis 2000, les efforts déployés par le GC dans le cadre de la LAI se concentrent sur l'évaluation de la nécessité de nouvelles lois et de lois modifiées. L'approche du gouvernement en matière d'accès légal reconnaît la nécessité de mesures efficaces qui établissent un équilibre entre les droits, la protection des renseignements personnels, la

[1] Gouvernement du Canada, *Notre sécurité, nos droits : Livre vert sur la sécurité nationale de 2016*, Document de contexte, p. 54, tiré de https://www.securitepublique.gc.ca/cnt/rsrcs/pblctns/ntnl-scrt-grn-ppr-2016-bckgrndr/ntnl-scrt-grn-ppr-2016-bckgrndr-fr.pdf

sécurité et le bien-être économique de tous les Canadiens. Pour s'acquitter de leur mandat en matière de sécurité publique, les organismes d'application de la loi et de sécurité nationale doivent maintenir leurs capacités en matière d'accès légal d'une manière qui respecte toujours la Charte. Dans le discours du Trône de 2001[2], le gouvernement s'est engagé à fournir des outils modernes de lutte contre la cybercriminalité et à mettre à jour le cadre juridique existant afin d'aider les organismes d'application de la loi et de sécurité nationale à relever les défis posés par les communications et les technologies de l'information avancées[3].

L'Initiative PE21S découle des parties de l'IAL relatives aux modifications apportées au *Code criminel*, qui sont entrées en vigueur en mars 2015 avec l'adoption de la LPCCC. Cette loi a introduit des pouvoirs d'enquête spécialisés en vertu d'une autorisation judiciaire pour l'obtention d'éléments de preuve numériques. Elle a modifié le *Code criminel*, la *Loi sur l'entraide juridique en matière criminelle,* la *Loi sur la preuve au Canada* et la *Loi sur la concurrence* pour ainsi :

- étoffer ou améliorer le régime canadien des mandats de perquisition et des ordonnances de communication[4] afin de fournir des outils plus précis pour répondre aux exigences de la technologie contemporaine et des enquêtes connexes, tout en établissant un équilibre approprié entre la protection de la vie privée et les droits de la personne;
- introduire un nouveau régime pour conserver rapidement les données volatiles, en utilisant des ordres et des ordonnances de conservation[5];
- appuyer la collecte d'éléments de preuve numériques dans les enquêtes criminelles;
- permettre au Canada de ratifier la Convention de Budapest, ce qui, comme il a été mentionné précédemment, a eu lieu le 8 juillet 2015. La Convention est le seul instrument juridique international de lutte contre la criminalité informatique.

***Principales définitions***

*Un **mandat de perquisition** donne aux organismes d'application de la loi l'autorisation judiciaire de perquisitionner et de saisir des renseignements.*

*Une **ordonnance de communication** est une autorisation judiciaire qui oblige le gardien de l'information (le fournisseur de services Internet, par exemple) à fournir l'information à un organisme d'application de la loi.*

*Un **ordre ou une ordonnance de conservation** ordonne à une personne, comme un fournisseur de services Internet, de conserver les données informatiques qui sont en sa possession ou sous son contrôle.*

L'objectif principal de l'Initiative PE21S consiste à fournir les moyens de mettre en œuvre les modifications apportées au *Code criminel* et aux autres lois par la LPCCC et de respecter les obligations internationales du Canada, notamment celles qui découlent de la ratification de la Convention de Budapest. La LPCCC a également introduit des sanctions pour les fournisseurs de services de télécommunications (FST) qui ne respectent pas les demandes et les ordonnances de communication. L'objectif global de l'Initiative est de veiller à ce que le GC respecte ses engagements en matière de protection des Canadiens contre la cybercriminalité et de fournir un cadre juridique

---

[2] Gouvernement du Canada, Discours du Trône ouvrant la première session de la trente-septième législature du Canada, 2001, tiré de https://lop.parl.ca/sites/ParlInfo/default/fr_CA/Parlement/procedure/discoursTrone/discours371
[3] Ministère de la Justice du Canada, *Accès légal – Document de consultation*, 2002, tiré de https://www.justice.gc.ca/fra/cons/al-la/index.html
[4] Pour plus de renseignements, se référer à : Bibliothèque du Parlement, *Résumé législatif du projet de loi C-13 : Loi modifiant le Code criminel, la Loi sur la preuve au Canada, la Loi sur la concurrence et la Loi sur l'entraide juridique en matière criminelle*, publication n°41-2-C13-E, tiré de https://lop.parl.ca/staticfiles/PublicWebsite/Home/ResearchPublications/LegislativeSummaries/PDF/41-2/c13-f.pdf
[5] *Ibid*

solide relativement à tous les crimes qui comportent des preuves numériques – d'une manière compatible avec la Charte.

Justice, le SPPC, la GRC et AMC sont conjointement responsables de la gestion de sa mise en œuvre, alors que chacun exerce ses activités particulières dans les systèmes de justice pénale et de politique internationale. Le modèle logique de l'Initiative, qui illustre la relation entre les activités prévues et les résultats attendus, se trouve à l'annexe A. L'Initiative comprend cinq activités principales, soit :

- **Analyse juridique, élaboration et coordination de politiques sur les questions nationales et internationales –** Comprend les conseils juridiques et stratégiques, le soutien au contentieux et les services de poursuite nécessaires pour gérer la mise en œuvre des dispositions législatives relatives aux pouvoirs d'enquête dans la LPCCC et respecter les obligations internationales du Canada découlant de la ratification de la Convention de Budapest.

- **Sensibilisation et formation** – Comprend l'élaboration de documents de sensibilisation et de formation pour veiller à ce que les réformes législatives prévues par la LPCCC soient mises en œuvre de façon uniforme. Les principaux groupes visés par la formation ont été les services de police et les poursuivants. On a également déployé des efforts pour sensibiliser les partenaires internationaux du Canada aux dispositions de la LPCCC.

- **Recherche technique et outils à l'appui des enquêtes criminelles** – Comprend l'élaboration de nouveaux outils, techniques et solutions pour l'interception justifiée et en temps réel des données de transmission et l'analyse des données saisies, notamment les demandes internationales liées à la Convention de Budapest.

- **Administration d'un système de conservation des données** – Nécessite l'élaboration d'une fonction de triage réservée pour l'administration d'un nouveau système de conservation des données, conformément aux dispositions légales de la LPCCC, et pour répondre aux demandes d'aide internationales.

- **Coopération internationale** – Vise à faire progresser la coopération internationale en matière de cybercriminalité et à veiller à ce que les intérêts du Canada en matière de cybercriminalité et d'autres types de criminalité assistée par ordinateur soient pris en compte dans la politique étrangère globale du Canada.

Les principaux groupes cibles de l'Initiative PE21S sont les services de police et les poursuivants. L'objectif consiste à leur donner des moyens plus efficaces d'enquêter sur la cybercriminalité et la criminalité assistée par ordinateur et d'intenter des poursuites, tout en respectant la vie privée et les libertés des personnes au Canada. Une description des rôles et des responsabilités de chaque partenaire, ainsi que des renseignements supplémentaires concernant l'Initiative PE21S, figurent à l'annexe A.

L'Initiative PE21S a reçu un financement de 60,74 millions de dollars sur cinq ans (2015-2016 à 2019-2020) et des fonds permanents de 12,25 millions de dollars par année. Le tableau 1 présente un aperçu par ministère du financement, qui comprend les transferts du crédit 1 pour les dépenses de fonctionnement et une affectation pour les locaux (13 %). Compte tenu de la nature du travail, le cours normal des fonctions de la plupart des titulaires comprend le travail sur la cybercriminalité et la criminalité assistée par ordinateur ainsi que d'autres dossiers connexes, comme l'accès légal et la cybersécurité. Par conséquent, les données sur les dépenses ne sont pas disponibles parce que les ressources ne font pas toujours l'objet d'un suivi distinct. Selon les renseignements fournis par les représentants de l'Initiative PE21S, la majorité des postes équivalents temps plein prévus ont été dotés. De plus, comme il est indiqué dans les constatations, toutes les activités prévues ont été mises en œuvre.

**Tableau 1 : Budget 2015-2016 à 2019-2020 de l'Initiative PE21S (en $)**

| Ministère | 2015-2016 | 2016-2017 | 2017-2018 | 2018-2019 | 2019-2020 | Total |
|---|---|---|---|---|---|---|
| Justice | 2 194 268 | 2 138 598 | 2 168 598 | 2 118 598 | 2 118 598 | 10 738 660 |
| SPPC | 4 426 717 | 4 121 778 | 4 127 237 | 3 998 804 | 3 998 804 | 20 673 340 |
| GRC | 4 793 580 | 4 775 210 | 5 542 300 | 5 485 650 | 5 485 650 | 26 082 390 |
| AMC | 650 000 | 650 000 | 650 000 | 650 000 | 650 000 | 3 250 000 |
| **Total** | **12 064 565** | **11 685 586** | **12 488 135** | **12 253 052** | **12 253 052** | **60 744 390** |

Source : Documents de la planification de programme

Le nombre d'équivalents temps plein (ETP) alloués à chaque ministère, par année, est présenté ci-dessous dans le tableau 2.

**Tableau 2 : Aperçu de la dotation en équivalents temps plein allouée**

| Ministère | 2015-2016 | 2016-2017 | 2017-2018 | 2018-2019 | 2019-2020 | Continu |
|---|---|---|---|---|---|---|
| Justice | 9,5 | 9,5 | 9,5 | 9,5 | 9,5 | 9,5 |
| SPPC | 22,0 | 21,5 | 21,5 | 20,8 | 20,8 | 20,8 |
| GRC | 12,0 | 18,0 | 23,0 | 23,0 | 23,0 | 23,0 |
| AMC | 2,0 | 2,0 | 2,0 | 2,0 | 2,0 | 2,0 |
| **Total** | **45,5** | **51,0** | **56,0** | **55,3** | **55,3** | **55,3** |

Source : Documents de la planification de programme

# 3. MÉTHODOLOGIE DE L'ÉVALUATION

Un groupe de travail interministériel sur l'évaluation a été mis sur pied pour appuyer l'évaluation en fournissant des commentaires, des conseils et des suggestions concernant la conception et la réalisation de l'évaluation. Le groupe de travail a été mis sur pied au début de l'évaluation et comportait des représentants de l'Initiative PE21S et des unités d'évaluation de chacun des ministères partenaires fédéraux.

La méthodologie de cette évaluation comprenait plusieurs sources de données et utilisait les méthodes de collecte de données suivantes :

## 3.1 Examen des documents

Parmi les principaux documents internes examinés se trouvent les suivants :

- Stratégie de mesure du rendement de l'Initiative PE21S (avril 2016).
- Feuillets d'information, présentations PowerPoint et documents d'information sur les modifications législatives au projet de loi C-13, préparés par la Section de la politique en matière de droit pénal (SPDP) et le Groupe d'entraide internationale (GEI), Justice.
- Documents liés aux consultations sur la sécurité nationale de 2017 et à la Stratégie nationale de cybersécurité de 2018.

## 3.2 Examen de l'information sur le rendement

Dans le cadre de la stratégie de mesure du rendement de l'Initiative, les responsables de l'Initiative PE21S ont compilé des données sur le rendement associées à chacun des résultats attendus. Au moment de l'évaluation, l'information était disponible pour trois ans : 2015-2016 à 2017-2018 inclusivement. Ces données ont été examinées pour les besoins de l'évaluation.

## 3.3 Examen documentaire

Un examen documentaire ciblé a été entrepris sur des articles et des rapports qui fournissent de l'information sur des sujets tels que les tendances de la cybercriminalité et les défis de l'application de la loi; l'évaluation annuelle de la menace que représente la criminalité organisée sur Internet (IOCTA) d'Europol; et les rapports d'évaluation du Conseil de l'Europe concernant la mise en œuvre de la Convention de Budapest par les États signataires. En outre, une recherche en ligne visant à déterminer les affaires judiciaires se rapportant aux pouvoirs d'enquête de l'Initiative PE21S entre mars 2015 et mars 2019 a été effectuée et la jurisprudence pertinente a été examinée.

## 3.4 Examen des tendances en matière de cybercriminalité et de criminalité assistée par ordinateur

Cette analyse était axée sur la collecte et l'analyse de données sur l'incidence, l'enquête et la résolution de deux catégories générales de criminalité impliquant des services informatiques :

- **La criminalité cyberdépendante :** les infractions qui ne peuvent être commises qu'à l'aide d'ordinateurs, de réseaux informatiques ou d'Internet, et qui ciblent les ordinateurs et les systèmes informatiques de particuliers et d'organisations (aussi appelés les infractions liées à la « technologie en tant que cible »).

- **La criminalité cybernétique :** les infractions « traditionnelles » qui sont facilitées ou dont la portée et les effets sont amplifiés par l'utilisation d'ordinateurs et d'Internet (aussi appelées infractions liées à la « technologie en tant qu'instrument »).

Les documents examinés pour cette analyse des tendances avaient trait au signalement de la cybercriminalité aux services de police au Canada, à des sondages Eurobaromètre en Europe qui comprenaient des questions sur les incidents de cybersécurité vécus par les membres du public, et à des enquêtes auprès d'organisations commerciales au Canada et d'entreprises et d'organismes de bienfaisance d'Angleterre et du Pays de Galles, concernant les approches en matière de cybersécurité et les incidents cybernétiques.

-

## 3.5 Entrevues avec des informateurs clés

Au total, 36 entrevues ont été menées auprès d'informateurs clés, à savoir des principaux intervenants internes et externes, réparties comme suit :

- Représentants de l'Initiative PE21S (administration centrale et régions) de Justice, du SPPC, de la GRC et d'AMC (24 entrevues).

- Autres ministères gouvernementaux ayant des liens avec les activités de l'Initiative PE21S (Sécurité publique Canada et Innovation, Sciences et Développement économique Canada). (2 entrevues).

- Intervenants nationaux (application de la loi et poursuites), notamment des représentants d'organismes d'application de la loi et de services provinciaux des poursuites (services de police municipaux et provinciaux, poursuivants généraux provinciaux) (3 entrevues).

- Intervenants nationaux (autres), constitués des principaux FST (4 entrevues).

- Intervenants internationaux, constitués de responsables de la justice d'autres pays (États-Unis) et de représentants d'entités internationales (Europol, Conseil de l'Europe) où des représentants de l'Initiative PE21S ont participé à des groupes de travail ou mené des consultations sur des questions liées à la cybercriminalité (3 entrevues).

Lors de la présentation des résultats des entrevues, on a utilisé l'échelle suivante :

- Peu : pas plus de 10 % à 15 %

- Un faible nombre : de 15 % à environ 40 %

- Un grand nombre : plus de 40 % à environ 60 %

- La plupart : plus de 60 % à environ 80 %

- Presque tous : plus de 80 %.

## 3.6 Limitations

L'évaluation a fait face à quelques limitations ou défis méthodologiques, tel qu'indiqué plus bas par sources de données.

***Examen des tendances en matière de cybercriminalité et de criminalité assistée par ordinateur***
Nombre d'enquêtes et d'estimations publiées quant à l'ampleur de la cybercriminalité et de ses répercussions sont réputées peu fiables, incomplètes ou incohérentes. En conséquence, ces faiblesses dans les données limitent la base des données probantes visant à éclairer l'élaboration de politiques sur la cybercriminalité, les stratégies d'intervention et l'affectation des ressources, sans parler de l'évaluation des mesures prises. Voici les principales faiblesses et difficultés relevées dans la documentation examinée :

- Sous-déclaration d'incidents de cybercriminalité à la police et à d'autres autorités par des particuliers et des organisations.

- Repérage et différenciation limités des incidents cyberdépendants ou favorisés par la cybernétique dans les systèmes de signalement de la criminalité.

- Méthodologies d'enquête mal conçues pour estimer les taux de victimisation et les répercussions. L'étalon-or pour mesurer l'incidence de la cybercriminalité est l'échantillonnage probabiliste aléatoire au moyen d'un échantillon suffisamment vaste et stratifié pour obtenir une représentation fiable, afin de permettre la préparation d'estimations fiables des taux globaux d'incidents et de répercussions cybernétiques.

- D'autres enquêtes sur la cybercriminalité, en particulier celles publiées par les fournisseurs de services de cybersécurité et/ou de systèmes de surveillance, manquent souvent de transparence et d'uniformité, mais jouent un rôle important dans la détermination et la caractérisation des nouvelles cybermenaces émergentes.

La nature dynamique de la cybercriminalité, dans laquelle les mécanismes utilisés pour la commission de cybercrimes évoluent continuellement, signifie que les réponses des autorités et la mesure de l'incidence et des effets sont toujours en mode « rattrapage ».

***Examen de l'information sur le rendement***. Les responsables de l'initiative PE21S ont été en mesure de fournir de l'information sur le rendement pour les trois années de mise en œuvre. Toutefois, il a été difficile d'évaluer l'efficacité des activités de sensibilisation et de formation entreprises dans le cadre de l'Initiative, car les évaluations postérieures à la formation n'avaient pas été mises en œuvre au moment des événements. Pour remédier à cette situation, l'évaluation a mené des entrevues avec des informateurs clés pour recueillir ces données. Même si bon nombre des informateurs clés ne se souvenaient pas des activités de formation spécifiques auxquelles ils avaient participé, la plupart connaissaient très bien les éléments clés de la LPCCC.

***Entrevues avec des informateurs clés***. Une limitation comprenait la possibilité d'introduire un biais en raison de l'approche d'échantillonnage pour les entrevues avec les informateurs clés, ainsi que la participation volontaire dans cette méthode de collecte de données. Une réponse auto-déclarée est biaisée lorsque les individus font rapport sur leurs propres activités et peuvent désirer se montrer sous leur meilleur jour. Lorsque les participants répondent aux questions avec l'intention de modifier les résultats, on a affaire à une réponse stratégique biaisée. Pour remédier à cette situation, des mesures ont été prises lors de l'évaluation pour assurer que la liste des informateurs clés soit équilibrée afin qu'elle contienne un groupe de répondants bien renseignés et une variété de points de vue internes et externes.

**Stratégie d'atténuation**. Afin d'atténuer ces limitations, l'évaluation a utilisé de multiples sources de données et de triangulation pour confirmer les résultats.

# 4. CONSTATATIONS

## 4.1 Pertinence

### 4.1.1 Besoin continu de l'Initiative PE21S

L'objectif global de la LPCCC, soit de veiller à ce que les menaces liées à la cybercriminalité et à la criminalité assistée par ordinateur soient cernées et que des mesures soient prises à leur égard, demeure pertinent, car la cybercriminalité croît rapidement au Canada et à l'échelle internationale. L'Initiative fournit les moyens de mettre en œuvre les réformes législatives qui ont créé des pouvoirs d'enquête spécialisés en vertu d'une autorisation judiciaire pour la conservation et l'obtention d'éléments de preuve numériques. La ratification de la Convention de Budapest permet au Canada de collaborer avec d'autres États signataires aux activités d'enquête sur la cybercriminalité.

Comme il est indiqué à la section 2, l'objectif principal de l'Initiative PE21S est de fournir les moyens de mettre en œuvre les modifications apportées au *Code criminel* et aux autres lois par la LPCCC, et de respecter les obligations internationales du Canada découlant de la ratification de la Convention de Budapest. Il s'agit de veiller à ce que le GC respecte ses engagements en matière de protection des Canadiens contre la cybercriminalité et de fourniture d'un cadre juridique solide à l'égard de tous les crimes comportant des éléments de preuve numériques, d'une manière conforme à la Charte.

La cybercriminalité est un problème de plus en plus préoccupant au Canada et dans le monde[6]. Les données annuelles compilées par Statistique Canada pour la période de quatre ans allant de 2014 à 2017 montrent que le nombre total d'incidents de cybercriminalité signalés est passé de 15 184 en 2014 à 27 829 en 2017, soit un taux de croissance annuel composé de 22,4 %[7]. Près de la moitié de tous les incidents signalés chaque année (de 47 % à 48 %) étaient attribuables à la cyberfraude, suivis de la production, de la distribution ou de la possession de pornographie juvénile (de 13 % à 17 %), des communications indécentes/harcelantes et la distribution non consensuelle d'images intimes (une nouvelle infraction ajoutée au *Code criminel* par la LPCCC) (de 5 à 10 %), de la profération de menaces (de 6 à 7 %), et de harcèlement criminel (de 4 à 6 %)[8].

Aujourd'hui, beaucoup de crimes sont commis par des criminels qui utilisent des téléphones cellulaires ou des ordinateurs pour envoyer des messages sur l'Internet grâce aux capacités de télécommunications. Contrairement aux preuves médicolégales trouvées sur une scène de crime, les preuves numériques peuvent être disséminées dans de nombreux appareils à différents endroits, relevant parfois d'autorités différentes. En outre, les données électroniques peuvent avoir différents degrés de permanence. Elles peuvent être très volatiles et passagères et ne durer que pendant une fraction de seconde, mais elles peuvent aussi être sauvegardées dans des mémoires à long terme. La LPCCC a apporté des réformes législatives nécessaires assujetties à des autorisations judiciaires pour concevoir des pouvoirs d'enquête spécialisés afin d'obtenir des preuves numériques, non seulement pour la criminalité technologique, par exemple le piratage ou le crime organisé, mais aussi pour faire face aux infractions quotidiennes, lorsque des criminels envoient un courriel, utilisent leur téléphone cellulaire, ou publient une image sur un site de médias sociaux. Les réformes ont mené à la création d'un régime d'ordonnances de communication permettant à un juge de savoir précisément quels types de données sont recherchées et d'établir un équilibre adéquat entre les droits relatifs à la vie privée et les droits de la personne. En outre, la LPCCC a introduit un nouveau régime qui permet de préserver rapidement les données volatiles grâce aux ordres et aux ordonnances de conservation[9].

Il est également nécessaire de maintenir l'Initiative PE21S afin de respecter les obligations internationales du Canada découlant de la ratification de la Convention de Budapest. Le Canada a signé la *Convention sur la cybercriminalité du Conseil de l'Europe* (Convention de Budapest) en novembre 2001 et l'a ratifiée le 8 juillet 2015. Elle n'a pas été ratifiée plus tôt parce que le gouvernement avait besoin de temps pour mettre en place la législation nationale visant à s'assurer que les lois canadiennes sont conformes à la convention, ce qui a été accompli par la LPCCC (l'ancien projet de loi C-13). La Convention de Budapest est le principal instrument international sur la cybercriminalité. Elle vise à aider les États signataires à harmoniser leurs lois nationales, à améliorer leurs techniques d'enquête, et à accroître la coopération internationale. La ratification de la Convention permet au Canada de collaborer avec d'autres États signataires en matière d'enquête sur la cybercriminalité et permet l'accès à des éléments de preuve numériques qui peuvent être trouvés

---

[6] Pour de plus amples renseignements sur les tendances, se référer à : U.S. Federal Bureau of Investigation: Annual Reports of the Internet Crime Complaint Centre (IC3) [ANGLAIS SEULEMENT] tiré de https://www.ic3.gov/media/annualreports.aspx, ou McGuire, M. et Dowling S., *Cyber Crime: A Review of the Evidence: Summary of Key Findings and Implications*, Home Office Research Report 75, U.K. Home Office [ANGLAIS SEULEMENT], octobre 2013, p 5. (https://www.gov.uk/government/publications/cyber-crime-a-review-of-the-evidence)

[7] Statistique Canada. Tableau 35-10-0001-01 : Cybercriminalité signalée par la police, selon l'infraction reliée à la cybercriminaltié, Canada (certains services de police), décembre 2018.
Tiré de https://www150.statcan.gc.ca/t1/tbl1/fr/tv.action?pid=3510000101&request_locale=fr

[8] Centre canadien de la statistique juridique : Programme des services policiers, *Programme de déclaration uniforme de la criminalité par incident : manuel de déclaration*, mars 2006, p. 52. Tiré de : https://www23.statcan.gc.ca/imdb/p2SV_f.pl?Function=getSurvInstrumentList&Id=1244230 et Statistiques sur les crimes signalés par la police au Canada", *Juristat*, Centre canadien de la statistique juridique, 2015, 2016 et 2017, catalogue n° 85-002-X, ISSN 1209-6393. Tiré de https://www150.statcan.gc.ca/n1/pub/85-002-x/2018001/article/54974-fra.htm

[9] Ministère de la Justice du Canada, Modernisation du Code criminel : Document d'information, 2013, tiré de https://www.canada.ca/fr/nouvelles/archive/2013/11/modernisation-code-criminel.html

dans un autre pays. Le nombre de signataires de la Convention a augmenté au fil des ans et s'élève actuellement à 64[10]. Comme nous l'indiquons plus loin dans la section 4.2.4, le Canada est vu comme un acteur important du soutien de la Convention à l'échelle internationale.

Les éléments probants de l'évaluation indiquent qu'il existe un besoin continu pour les activités clés financées par l'Initiative PE21S, qui sont résumées ci-après :

- **Analyse juridique, élaboration de politiques et coordination sur les questions nationales et internationales –** Bien qu'il y n'y ait eu très peu de litiges en ce qui concerne les pouvoirs d'enquête de l'Initiative PE21S jusqu'à maintenant et aucune contestation couronnée de succès en vertu de la Charte, Justice doit maintenir sa capacité de défense à l'égard des contestations futures et de modification du *Code criminel* au besoin. AMC doit également continuer de coordonner l'approche du Canada en matière de politique étrangère sur la cybercriminalité sur la scène internationale, qui devient de plus en plus complexe et politisée.

- **Sensibilisation et formation –** La phase de « sensibilisation » de l'Initiative PE21S est terminée, car les poursuivants et les responsables de l'application de la loi connaissent maintenant très bien les pouvoirs d'enquête liés à l'initiative PE21S. Des activités de sensibilisation continueront d'être nécessaires pour aider les intervenants à appliquer les dispositions du *Code criminel*, principalement de façon réactive ou selon les besoins. La formation continue des poursuivants et des responsables de l'application de la loi sur les modifications au *Code criminel* a été intégrée aux programmes de formation offerts par des organisations telles le Collège canadien de police et l'École des poursuivants du SPPC. De plus, la formation de partenaires étrangers des milieux de la police et des poursuites judiciaires est en cours[11].

- **Administration du système de conservation des données –** L'Initiative PE21S a permis à la GRC d'élaborer et de mettre en œuvre un système de conservation des données pour traiter un grand nombre de demandes de conservation des données provenant d'organismes d'application de la loi étrangers. Comme le Canada peut raisonnablement s'attendre à continuer de recevoir des demandes de conservation de la part de corps policiers étrangers, il doit maintenir sa capacité de gérer de telles demandes. La GRC a mis sur pied un Groupe national de coordination contre la cybercriminalité à titre de point de contact exclusif.

- **Recherche technique et outils à l'appui des enquêtes criminelles –** Les Services des enquêtes techniques de la GRC ont mis au point des outils pour accéder à des preuves numériques provenant d'un appareil ou d'un support de stockage numérique saisies comme éléments de preuve (données inactives), les obtenir et les traiter, ainsi que des outils déployés dans une situation de communication en direct (données actives). Comme la cybercriminalité est de plus en plus complexe sur le plan technologique, il sera essentiel que la GRC et d'autres organismes fédéraux mettent au point des outils supplémentaires pour appuyer les enquêtes criminelles.

- **Coopération internationale en matière criminelle –** La *Loi sur l'entraide juridique en matière criminelle* (LEJMC) donne au Canada le pouvoir légal d'obtenir des ordonnances judiciaires pour le compte d'États signataires d'accords d'entraide juridique (EJ) avec le Canada. Les demandes d'EJ sont coordonnées par le GEI de Justice, qui agit pour le compte du ministre de la Justice en tant qu'autorité centrale canadienne pour les demandes d'EJ entrantes et sortantes. Le nombre de demandes d'éléments de preuve numérique présentées en vertu de

[10] Conseil d'Europe, *État des signatures et ratifications du traité 185 : Convention sur la cybercriminalité*, 2019, tiré de https://www.coe.int/fr/web/conventions/full-list/-/conventions/treaty/185/signatures
[11] Information annuelle sur le rendement de l'Initiative PE21S 2015-2016 à 2017-18.

demandes d'EJ augmente (passant de 81 en 2015-2016 à 448 en 2017-2018). En plus de permettre au Canada de mieux soutenir ses partenaires d'EJ bilatéraux et multilatéraux en leur accordant des pouvoirs supplémentaires de collecte d'éléments de preuve, les représentants de l'Initiative PE21S ont signalé que les ressources fournies par l'Initiative ont également permis au Canada de jouer un rôle important et croissant dans le soutien de la Convention de Budapest et la promotion de celle-ci auprès des pays non signataires de traités. Par exemple, un effort considérable est consacré à la rédaction du Deuxième Protocole additionnel à la Convention sur la cybercriminalité, qui vise à fournir à la police et aux poursuivants des États signataires des outils supplémentaires pour obtenir un accès plus rapide aux éléments de preuve numériques afin de faciliter les enquêtes et les poursuites relatives aux activités criminelles. Le Canada joue également un rôle important dans la promotion de la Convention auprès des pays non signataires de traités. Le renforcement de la pertinence de la Convention de Budapest présente d'importants avantages sur le plan de la politique étrangère pour le Canada. Par exemple, l'un des objectifs de la Convention est d'avoir des cadres et des approches juridiques semblables dans les États signataires. Ce faisant, elle jette les bases des mesures de protection et des outils, en plus de fournir une tribune pour discuter des enjeux et élaborer des accords de coopération, tous destinés à faciliter la capacité des organismes d'application de la loi de réagir aux aspects internationaux ou transfrontaliers de la cybercriminalité.

### 4.1.2 Harmonisation avec les priorités gouvernementales

L'Initiative PE21S reflète l'engagement pris par le GC en 2013 de présenter un projet de loi qui donnerait à la police et aux poursuivants de nouveaux pouvoirs d'enquête pour obtenir des éléments de preuve numériques. Depuis, on continue de mettre l'accent sur la cybercriminalité et, de façon plus générale, sur la cybersécurité. Bien que la LPCCC ait modernisé les pouvoirs d'enquête prévus dans le *Code criminel*, la technologie évolue à un rythme rapide et pose des défis aux organismes d'application de la loi dans la conduite d'enquêtes liées à des crimes graves.

Dans le *discours du Trône* d'octobre 2013, le GC a annoncé qu'une nouvelle loi serait présentée pour donner aux policiers et aux poursuivants de nouveaux outils pour lutter efficacement contre la cyberintimidation, ainsi que de nouveaux pouvoirs d'enquête pour traiter les éléments de preuve numériques et provenant d'Internet associés aux ordinateurs, aux tablettes et aux téléphones cellulaires[12]. Depuis, la cybercriminalité a continué de susciter beaucoup d'intérêt, tout comme la cybersécurité à l'ère numérique en général; il faut trouver un équilibre entre les avantages de l'économie numérique et la sécurité publique[13].

La plupart des informateurs clés ont convenu que la législation subséquente, à savoir la LPCCC, répondait à un besoin important de modernisation des outils législatifs pour lutter contre la cybercriminalité et la criminalité assistée par ordinateur, et est par conséquent harmonisée sur les priorités du gouvernement à cet égard. Les modifications législatives ont été rédigées dans le but d'être neutres sur le plan technologique, à savoir que l'intention est que les organismes d'application de la loi continuent de recourir aux pouvoirs d'enquête pour l'obtention d'éléments de preuve numériques à mesure que les ordinateurs et les technologies de communication évoluent. Par exemple, le mandat d'enregistrement des numéros de téléphone a été introduit dans le *Code criminel* (paragraphe 492.2) en 1993. Il permettait à la police d'installer et de surveiller un enregistreur de

[12] Parlement du Canada, *Discours du Trône ouvrant la deuxième session quarante unième législature du Canada*, 2013, tiré de https://lop.parl.ca/sites/ParlInfo/default/fr_CA/Parlement/procedure/discoursTrone/discours412
[13] Parlement du Canada, *Budget 2018*, tiré de https://www.budget.gc.ca/2018/docs/plan/toc-tdm-fr.html; Sécurité publique Canada, *Stratégie nationale de cybersécurité* 2018, tiré de https://www.securitepublique.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg/index-fr.aspx

numéros, qui fournissait de l'information permettant d'identifier ou d'enregistrer un numéro de téléphone ou l'emplacement d'un téléphone duquel un appel provient ou a été reçu ou devait l'être[14]. Il ne visait toutefois pas les transmissions entre appareils sur Internet (parfois appelées « données liées au trafic »). La modification de cette disposition par l'entremise de la LPCCC a permis la modernisation du paragraphe, qui couvre maintenant un plus large éventail de communications; en plus des appels téléphoniques, les données relatives à l'acheminement des courriels et des messages textes sont incluses par exemple, tout en y excluant explicitement le contenu.

Les représentants de Justice ont souligné que l'un des principes directeurs de la conception des nouveaux pouvoirs d'enquête consistait à « allier protection de la vie privée et précision ». Comme nous le verrons plus loin dans le présent chapitre, il y a eu très peu de litiges concernant ces pouvoirs jusqu'à maintenant. Le fait qu'il n'y ait pas encore eu de contestation couronnée de succès en vertu de l'article 8 de la Charte indique que les pouvoirs d'enquête ont été bien conçus pour assurer la protection des droits à la vie privée. Par exemple, les dispositions relatives aux mandats pour un dispositif de localisation (paragraphe 492.1) établissent la distinction entre la localisation d'une « chose » (notamment un véhicule) qui nécessite l'application du critère du « soupçon raisonnable »[15] et la localisation d'une personne physique (habituellement en localisant un téléphone cellulaire transporté par une personne), qui nécessite l'application du critère plus élevé du « motif raisonnable de penser »[16]. Les représentants de Justice ont souligné que le Canada se distingue des autres pays en ce sens que les pouvoirs d'enquête comprennent plusieurs ordonnances de communication, ce qui a été fait intentionnellement afin que chaque ordonnance vise un problème différent.

**Lacunes perçues dans la législation**

La plupart des informateurs clés ont estimé que les modifications législatives apportées au *Code criminel* par la LPCCC constituaient une étape importante dans la lutte contre la cybercriminalité et la criminalité assistée par ordinateur. Cependant, bon nombre d'entre eux ont relevé ce qu'ils perçoivent comme des lacunes dans la loi actuelle.

La principale question concerne les défis que doit relever la police pour obtenir l'accès aux renseignements de base sur les abonnés[17] (RBA) détenus par les FST. De nombreux informateurs clés ont soulevé la décision rendue en juin 2014 par la Cour suprême dans l'arrêt *R. c Spencer*, qui a conclu que les RBA liés à une activité informatique particulière ne devraient pas être obtenus sans autorisation, comme un mandat, en vertu d'une loi qui n'a rien d'abusif, sauf lorsqu'il existe des circonstances contraignantes. Dans cette affaire où il était question de pornographie juvénile, la Cour a statué que la police avait violé l'attente raisonnable du suspect en matière de respect de la vie privée en ligne lorsque les enquêteurs ont demandé les RBA liés à l'adresse IP utilisée sans obtenir d'abord

---

[14] Anne Turner, « Wiretapping Smart Phones with Rotary-Dial Phones' Law: How Canada's Wiretap Law is in Desperate Need of Updating, » [ANGLAIS SEULEMENT] 2017 CanLIIDocs384, p. 277 tiré de https://commentary.canlii.org/w/canlii/2017CanLIIDocs384.pdf

[15] Le droit pénal canadien établit une distinction entre le critère du « soupçon raisonnable » et celui du « motif raisonnable de penser », nécessaires pour que les policiers puissent arrêter légalement des personnes, effectuer certaines formes de perquisition et obtenir des mandats. Chacune des modifications apportées au *Code criminel* par la LPCCC est liée à l'un de ces deux critères. Pour de plus amples renseignements, se référer à la Bibliothèque du Parlement, *Résumé législatif du projet de loi C-13 : Loi modifiant le Code criminel, la Loi sur la preuve au Canada, la Loi sur la concurrence et la Loi sur l'entraide juridique en matière criminelle,* publication n° 41-2-C13-F, révisé le 28 août 2014, tiré de https://lop.parl.ca/staticfiles/PublicWebsite/Home/ResearchPublications/LegislativeSummaries/PDF/41-2/c13-f.pdf

[16] *Ibid*

[17] Les renseignements de base sur l'abonné comprennent les renseignements d'identification de base qui correspondent à l'abonnement d'un client à un service de télécommunications, notamment le nom, l'adresse domiciliaire, le numéro de téléphone, l'adresse électronique ou l'adresse IP. Pour de plus amples renseignements, se référer au *Livre vert sur la sécurité nationale de 2016, document de contexte*, p. 57, tiré de https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-scrt-grn-ppr-2016-bckgrndr/ntnl-scrt-grn-ppr-2016-bckgrndr-fr.pdf

une ordonnance du tribunal à cet effet. La Cour a conclu qu'il y avait une attente raisonnable en matière de respect de la vie privée en vertu de la Charte en ce qui concerne les RBA qui permettait de faire un lien entre l'identité d'une personne et les activités de la personne menées en ligne révélatrices de renseignements personnels. La demande de divulgation des renseignements par le FST faite par la police constituait donc une perquisition touchant un droit garanti par la Constitution, perquisition qui, en l'absence d'une autorisation précise (comme un mandat), n'était pas autorisée par la loi et violait donc la Charte[18]. Avant cette décision, la police demandait directement et de façon routinière aux FST de divulguer des RBA. En l'absence d'une loi particulière conçue pour avoir accès aux RBA, la pratique actuelle de la police consiste à demander une ordonnance du tribunal, souvent à l'aide d'une requête générale en ordonnance de communication pouvant être utilisée pour obtenir n'importe quel type de renseignements, lorsqu'elle veut obtenir les RBA d'un utilisateur autrement que dans des circonstances contraignantes. Les principaux intervenants représentant la police ont déclaré que l'obtention d'une ordonnance d'un tribunal prend du temps et nécessite des formalités administratives supplémentaires. De plus, au début d'une enquête, la police ne dispose pas toujours des motifs suffisants pour obtenir une ordonnance du tribunal (l'autorisation à laquelle on recourt le plus souvent est une ordonnance générale de communication en vertu du paragraphe 487.014 du *Code criminel*).

La recension des écrits a révélé que cette situation est contraire à ce qui a cours dans de nombreux pays étrangers, où les lois permettent expressément aux organismes d'application de la loi et de sécurité nationale d'obtenir des RBA[19]. Dans de nombreux cas, cela peut se dérouler sans autorisation judiciaire préalable (désignée souvent en tant qu'accès administratif). Ces pays étrangers comprennent les États-Unis, l'Australie, l'Allemagne, la Suède, l'Irlande, le Danemark, l'Espagne, la Finlande, les Pays-Bas et la Norvège

Deuxième problème cerné par les informateurs clés : l'absence d'une disposition précise dans la loi pour régler les problèmes découlant de l'absence d'une capacité d'interception, ainsi que les défis liés au chiffrement. On a proposé d'ajouter au *Code criminel* une disposition exigeant que les FST fournissent leur aide pour l'accès à l'information chiffrée. Certains informateurs clés suggèrent qu'il serait utile d'avoir un mécanisme juridique permettant l'accès « par moyen détourné » ou de déchiffrer des données. Les criminels expérimentés ont tendance à utiliser des technologies de communication qui chiffrent les données (dont des applications de messagerie), ce qui pose des défis aux organismes d'application de la loi et aux poursuivants dans leur capacité d'avoir accès à cette information. Un procureur fédéral a fait remarquer que le nombre d'écoutes électroniques autorisées a diminué de façon spectaculaire au cours des dernières années en raison du chiffrement, ce qui a forcé la police à recourir à d'autres moyens de découvrir de l'information, à savoir l'utilisation d'agents d'infiltration et d'informateurs. De nombreux autres pays imposent une obligation juridique générale aux prestataires de services de communication (PSC), les obligeant à prévoir des capacités d'interception dans leurs réseaux[20].

Ces questions – l'accès aux RBA, la capacité d'interception et les défis posés par le chiffrement – ont été étudiées en profondeur par le GC au cours des dernières années. En 2016, le GC a publié un

---

[18] CBC Investigates, « RCMP boss Bob Paulson says force needs warrantless access to ISP user data », 16 novembre 2016 [ANGLAIS SEULEMENT], tiré de https://www.cbc.ca/news/investigates/police-power-privacy-paulson-1.3851955

[19] Gouvernement du Canada, *Notre sécurité, nos droits : Livre vert sur la sécurité nationale de 2016, Document de contexte*, 2016, tiré de https://www.securitepublique.gc.ca/cnt/rsrcs/pblctns/ntnl-scrt-grn-ppr-2016-bckgrndr/ntnl-scrt-grn-ppr-2016-bckgrndr-fr.pdf

[20] *Ibid* p. 58.

Livre vert sur la sécurité nationale[21] et a mené une consultation sur la sécurité nationale pour aider à éclairer les changements futurs apportés aux outils de sécurité nationale.

Le Livre vert a proposé l'idée de créer un pouvoir spécifique pour permettre à la police l'accès aux RBA. Toutefois, les consultations subséquentes sur la sécurité nationale ont révélé que la plupart des répondants en ligne, ainsi que de nombreux experts et organismes, étaient réticents à accepter de nouveaux pouvoirs et outils pour améliorer les capacités d'enquête du Canada dans un monde numérique. De plus, la majorité (70 %) du grand public qui a répondu au questionnaire de consultation en ligne considérait que les RBA étaient aussi privés que le contenu de ses communications; 48 % ont dit que les RBA [TRADUCTION] « devraient être fournis seulement dans des 'circonstances limitées' et avec l'agrément d'un tribunal », ce qui se rapproche de ce qui est actuellement exigé[22].

Le Livre vert a également proposé l'idée de créer des pouvoirs visant à relever les défis liés au chiffrement et à exiger que les FST et les fournisseurs d'Internet intègrent la capacité d'interception et de conservation des données dans leurs réseaux. Dans certains cas, les PSC pourraient ne pas être en mesure d'effectuer l'interception en réponse à une ordonnance d'un tribunal parce que la capacité technique d'interception des communications n'a pas été intégrée à leur infrastructure. Les consultations sur la sécurité nationale ont révélé que 78 % des répondants au questionnaire en ligne s'opposaient aux capacités d'interception prévues dans la loi[23]. Les points de vue s'opposaient tout aussi fermement au fait que les enquêteurs puissent obliger les particuliers ou les sociétés à les aider à déchiffrer des communications. De nombreuses organisations se sont opposées à l'utilisation de « moyens détournés » pour l'application de la loi parce qu'ils affaibliraient la sécurité du réseau et les laisseraient vulnérables aux attaques[24]. Selon les données recueillies dans le cadre de cette évaluation, les intervenants représentant les poursuivants et la police sont en faveur d'une telle loi.

En réponse aux consultations sur la sécurité nationale de mai 2017, le Comité permanent de la sécurité publique et nationale de la Chambre des communes a recommandé qu'aucun changement ne soit apporté au régime d'accès légal aux renseignements sur les abonnés et aux renseignements chiffrés, et qu'il (le Comité permanent) continue de se pencher sur les questions technologiques liées à la cybersécurité qui évoluent rapidement[25].

## 4.2 Rendement

### 4.2.1 Sensibilisation aux pouvoirs d'enquête et connaissance de ceux-ci

Les organismes d'application de la loi, les poursuivants et les FST connaissent très bien les pouvoirs d'enquête de l'Initiative PE21S. Les représentants de l'Initiative PE21S ont mené une vaste gamme d'activités visant à faire connaître les modifications législatives apportées au *Code criminel* et les obligations du Canada en vertu de la Convention de Budapest, tant au Canada qu'à l'étranger.

Bien qu'elle soit antérieure à l'Initiative PE21S, tous les informateurs clés représentant la police, les organismes d'application de la loi et les FST qui ont participé aux consultations qui ont mené à la LPCCC (c.-à-d. l'ancien projet de loi C-13 et ses prédécesseurs) ont déclaré que cette participation

[21] Gouvernement du Canada, *Notre sécurité, nos droits : Livre vert sur la sécurité nationale de 2016,* tiré de https://www.securitepublique.gc.ca/cnt/rsrcs/pblctns/ntnl-scrt-grn-ppr-2016/ntnl-scrt-grn-ppr-2016-fr.pdf
[22] Gouvernement du Canada, *Consultation sur la sécurité nationale : Rapport sur ce que nous avons appris*, p. 13, tiré de https://www.securitepublique.gc.ca/cnt/rsrcs/pblctns/2017-nsc-wwlr/2017-nsc-wwlr-fr.pdf
[23] *Ibid* p. 14.
[24] *Ibid* p. 14.
[25] Chambre des Communes Canada, *Rapport du Comité permanent de la sécurité publique et nationale - Protéger les canadiens et leurs droits : une nouvelle feuille de route pour la sécurité nationale du Canada*, mai 2017, p. 43, tirée de https://www.noscommunes.ca/Content/Committee/421/SECU/Reports/RP8874869/securp09/securp09-f.pdf

leur a permis de se familiariser avec les modifications législatives apportées au *Code criminel*. Par la suite, ils ont partagé ces connaissances avec leurs réseaux internes et externes.

Les représentants de l'Initiative PE21S ont entrepris une vaste gamme d'activités visant à faire connaître les modifications législatives et les obligations du Canada en vertu de la Convention de Budapest, tant au Canada qu'à l'étranger[26]. Par exemple, la SPDP de Justice a présenté plus de 40 exposés à divers groupes d'intervenants, a tenu des réunions ponctuelles avec des intervenants, et a répondu à de nombreuses demandes de renseignements de la part des organismes d'application de la loi et des poursuivants qui cherchaient à obtenir des conseils sur les nouveaux pouvoirs d'enquête. Environ 1 500 personnes ont bénéficié de ces présentations et réunions[27]. Le GEI de Justice a offert plus de 50 séances de formation aux policiers et poursuivants canadiens et étrangers sur les nouveaux pouvoirs disponibles et les circonstances dans lesquelles ils peuvent être utilisés[28]. De plus, le GEI organise des journées d'apprentissage annuelles, qui réunissent des policiers et des poursuivants canadiens et étrangers. La LPCCC et les discussions générales sur la coopération internationale dans un monde numérique ont constitué des sujets à l'ordre du jour de ces séances, compte tenu de la prévalence de telles demandes d'EJ adressées au Canada et par le Canada. Le GEI a également créé des guides et des guides d'introduction pour aider les partenaires concernés à comprendre les outils dont ils disposent pour rechercher des preuves numériques, à la fois par le processus d'EJ et d'autres moyens moins formels de coopération internationale[29] Des représentants de l'administration centrale du SPPC ont donné de la formation aux poursuivants dans les régions; ces poursuivants régionaux ont à leur tour donné de la formation aux poursuivants provinciaux, aux policiers et aux juges de paix dans les régions.

Peu d'informateurs clés représentant les organismes d'application de la loi et les poursuivants à l'extérieur du gouvernement fédéral ont pu faire des commentaires sur les activités de sensibilisation et de formation entreprises dans le cadre de l'Initiative PE21S. Cela est peut-être dû en partie au fait que plusieurs années se sont écoulées depuis que ces activités ont été menées à bien à la suite de la promulgation de la LPCCC.

### 4.2.2 Gestion des questions et cohérence de la mise en œuvre et de l'interprétation des pouvoirs d'enquête

Relativement peu de questions juridiques et opérationnelles ont été soulevées en ce qui a trait à la mise en œuvre des nouveaux pouvoirs d'enquête. Jusqu'à maintenant, très peu d'affaires judiciaires ont porté explicitement sur ces pouvoirs et aucune contestation fondée sur l'article 8 de la Charte n'a été couronnée de succès.

Une principale question juridique soulevée par les informateurs clés a trait au fait que les nouvelles dispositions visant les mandats pour enregistreurs de données de transmission ne donnent pas accès aux renseignements de base sur les abonnés. Les partenaires fédéraux suivent de près l'évolution de la jurisprudence dans ce domaine.

Enfin, les éléments probants de l'évaluation indiquent que les pouvoirs d'enquête ont été en grande partie mis en œuvre de façon uniforme partout au Canada.

L'Initiative PE21S visait à gérer les problèmes découlant de la mise en œuvre des nouveaux pouvoirs d'enquête ajoutés au *Code criminel* afin de veiller à ce que ces pouvoirs soient appliqués et interprétés

[26] Rapports annuels sur le rendement de l'Initiative PE21S, 2015-2016 à 2017-2018.
[27] *Ibid*
[28] *Ibid*
[29] Les documents de référence sur les GEI d'EJ sont disponibles au https://www.canada.ca/fr/services/police/justice/extradition.html

de façon uniforme. La présente section décrit les principales questions qui ont été soulevées et la mesure dans laquelle elles ont été gérées avec succès dans le cadre de l'Initiative PE21S.

**Questions juridiques**

À ce jour, très peu de questions juridiques liées aux pouvoirs d'enquête de l'Initiative PE21S ont été soulevées. Les ressources fournies aux partenaires fédéraux par l'Initiative PE21S les ont aidés à gérer les questions juridiques associées à la mise en œuvre des modifications législatives apportées au *Code criminel*. Par exemple, des fonctionnaires de Justice ont fourni des conseils juridiques à la suite de la décision de la Cour suprême dans l'arrêt *R. c Spencer* et relativement à plusieurs dossiers de litige dont est saisie la Cour suprême concernant la perquisition et la saisie (article 8 de la Charte)[30] et à la portée extraterritoriale des ordonnances de communication[31].

Même s'ils prévoyaient qu'il y aurait de nombreuses contestations en vertu de l'article 8 de la Charte, les représentants de l'Initiative PE21S ont indiqué qu'il y a eu très peu de litiges à quelque niveau que ce soit relativement aux pouvoirs d'enquête en particulier. Il n'y a pas eu non plus de contestations judiciaires liées à d'autres lois modifiées par la LPCCC, comme la LEJMC. Dernièrement, une demande dont était saisi un tribunal inférieur de l'Ontario contestait le critère des « motifs raisonnables de soupçonner » associé à un mandat d'enregistrement de données de transmission, mais cette demande a été rejetée et la décision n'a pas fait l'objet d'un appel jusqu'à maintenant[32].

L'absence relative de contestations judiciaires témoigne de la mesure dans laquelle les pouvoirs d'enquête ont été bien conçus et de façon à accroître la conformité à la Charte et à réduire la probabilité de contestations fructueuses fondées sur la Charte. De plus, certaines des dispositions les plus controversées incluses dans les tentatives législatives antérieures n'étaient pas incluses dans l'ancien projet de loi C-13 (p. ex., l'ancien projet de loi C-30 de 2012 comprenait des dispositions qui auraient donné accès aux RBA en vertu d'une autorisation administrative légale [et non d'une ordonnance du tribunal] dans des circonstances désignées et qui auraient édicté des exigences pour assurer une capacité d'interception dans les réseaux des FST).

La principale question juridique pendante soulevée par les organismes d'application de la loi et les poursuivants a trait au fait que les nouvelles dispositions sur les mandats pour enregistreurs de données de transmission (EDT) (paragraphe 492.2) du *Code criminel* ne donnent pas aux organismes d'application de la loi accès aux RBA. Au contraire, les pouvoirs conférés en vertu d'ordonnance générale de communication sont maintenant fréquemment utilisés pour les RBA, ce qui peut être fastidieux et poser des défis quant au respect des normes requises pour de telles ordonnances. À titre de solution de contournement, les organismes d'application de la loi de certaines provinces recourent aux ordonnances d'assistance (paragraphe 487.02) pour obtenir des renseignements sur le nom et l'adresse du client (NAC). En janvier 2019, la Cour d'appel de Terre-Neuve-et-Labrador a adopté une interprétation large des pouvoirs de la police en matière de données électroniques dans l'arrêt *Re: section 487.02 of the Criminal Code* (2019 NLCA 6)[33]. Dans cette affaire, la police avait demandé un mandat pour un EDT en vertu du paragraphe 492.2. Ce mandat permet seulement la collecte de « données de transmission ». Dans cette affaire, il a été utilisé pour identifier les numéros de téléphone à partir desquels des appels avaient été faits vers un téléphone cellulaire particulier en lien avec une enquête. La police a en outre présenté une requête en ordonnance d'assistance en vertu du paragraphe 487.02 exigeant que les FST fournissent également à la GRC les renseignements sur

---

[30] Voici des exemples d'affaires visant l'article 8 : arrêts *R. c Marakah*, *R. c Jones*, *R c Reeves* et *R. c Mills*.
[31] Voici des exemples d'affaires à ce sujet : arrêts *BC Attorney General v. Brecknell* et Terre-Neuve (*Newfoundland Court of Appeal Re: section 487.02 of the Criminal Code*).
[32] Cour supérieure de justice de l'Ontario, *R. v. Otto*, 2019 ONSC 2473.
[33] Association canadienne du droit de la technologie (CAN-TECH Law), « Transmission Data and Subscriber Information » [ANGLAIS SEULEMENT], 7 février 2019, tiré de https://www.cantechlaw.ca/news/transmission-data-and-subscriber-information

les abonnés associés à ces autres numéros de téléphone. La Cour a statué que le paragraphe 487.02 pouvait être invoqué pour ordonner la production de renseignements sur les abonnés. Justice et les partenaires fédéraux suivent de près l'évolution de la jurisprudence en ce qui a trait aux dispositions relatives aux mandats pour EDT et tiennent les intervenants internes au courant des répercussions des décisions des tribunaux sur les enquêtes et les poursuites.

**Questions opérationnelles**

Selon l'opinion d'ensemble des informateurs clés, la plupart des problèmes opérationnels associés à la mise en œuvre des pouvoirs d'enquête ont été résolus. Les représentants de l'Initiative PE21S ont travaillé avec les intervenants dans le but de fournir des conseils et du soutien au besoin.

La plupart des informateurs clés ont déclaré qu'il a fallu beaucoup de temps pour déterminer de quelle façon les pouvoirs d'enquête devraient être mis en pratique. Quelques personnes interrogées représentant les organismes d'application de la loi, les poursuivants et les FST ont déclaré qu'il y a eu de la confusion au sujet du recours aux ordonnances de communication au cours des deux premières années suivant l'adoption de la LPCCC. Par exemple, si les organismes d'application de la loi utilisaient une ordonnance générale de communication pour obtenir des renseignements sur le NAC et les comptes, il n'était pas certain s'ils devaient aussi obtenir d'autres ordonnances liées à l'enquête, telles que pour les données de transmission et de suivi. Bien que différents juges aient eu tendance à avoir des points de vue divergents sur cette question au cours des premières années, les tribunaux ont depuis statué que plusieurs ordonnances (notamment les mandats de localisation, les mandats pour enregistreur de données de transmission et les ordonnances d'assistance) peuvent être englobées par une « ordonnance omnibus » (ordonnance générale de communication en vertu du paragraphe 487.014)[34]. Les responsables de l'application de la loi et les poursuivants considèrent qu'il s'agit d'un aspect positif de la LPCCC.

Tous les FST interrogés ont déclaré avoir consacré des efforts à l'éducation des forces de l'ordre sur leur utilisation appropriée. Les principaux FST disposent de contentieux internes qui conseillent le personnel opérationnel en cas de questions sur les ordonnances qui ont été signifiées. Ils ont également souligné que les tribunaux ont été utiles en fournissant des conseils sur l'utilisation appropriée des pouvoirs d'enquête. Par exemple, en janvier 2016, la Cour supérieure de l'Ontario, dans la décision *R. v. Rogers Communications*, a fourni des précisions à la police et aux poursuivants sur la façon dont ils peuvent obtenir des renseignements sur les clients auprès des FST au moyen des « tours de téléphonie cellulaire », c'est-à-dire la production de tous les registres d'appels des tours de téléphonie cellulaire à un moment donné[35].

Le rapport annuel sur la transparence publié par TELUS indique que l'entreprise a contesté ou refusé de fournir des renseignements pour seulement 5 % des ordonnances judiciaires reçues en 2017, parce qu'elle croyait que l'ordonnance du tribunal était invalide ou outrancière. Le rapport indique également que les organismes d'application de la loi ont continué de préparer leurs demandes avec la plus grande circonspection[36].

La GRC a fait remarquer que les FST éprouvent des difficultés à exécuter les demandes et les ordonnances de conservation (en raison notamment de la complexité de la demande, des recherches de données requises, et du besoin d'atténuer les répercussions sur les serveurs et ses utilisateurs). Tous les FST interrogés se sont dits préoccupés par l'augmentation des coûts découlant de la

---

[34] Se référer notamment à la décision de la Cour supérieure de justice de l'Ontario, *R. v. Otto*, 2019 ONSC 2473.
[35] Pour de plus amples renseignements sur cette affaire, se référer à *E-Commerce Law Reports*, volume 16, numéro 01 [ANGLAIS SEULEMENT], tiré de http://www.mcinnescooper.com/wp-content/uploads/2016/06/ECLR-Jan-Feb-2016-pg-15-16.pdf
[36] TELUS, « Rapport sur la transparence », tiré de https://www.telus.com/fr/about/sustainability/sharing-our-progress/transparency-reporting

conformité au grand nombre d'ordonnances judiciaires. Les FST ne sont pas rémunérés par les organismes d'application de la loi pour ce faire. Un informateur clé représentant l'un des FST a expliqué que l'absence d'une politique d'indemnisation découle d'une décision rendue en 2008 par la Cour suprême (arrêt *Société Télé-Mobile c Ontario*, 2008 CSC 12), où TELUS Mobilité a demandé une indemnisation pour les coûts liés au respect des ordonnances de communication de tiers en vertu du *Code criminel*[37]. La Cour suprême a rejeté l'appel en se basant sur le concept de responsabilité civique. Un informateur clé représentant l'un des FST a fait valoir avec insistance que le Canada devrait se doter d'une loi sur l'« indemnisation équitable », selon laquelle les FST seraient indemnisés pour s'être conformés aux ordonnances des tribunaux, loi qui existe dans d'autres pays. Cet informateur clé a déclaré qu'un groupe de travail conjoint industrie-gouvernement étudie cette question.

**Problèmes liés à l'évolution rapide des technologies de l'informatique et des communications**

De nombreux informateurs clés ont fait remarquer que la technologie évolue à un rythme rapide et qu'elle crée des défis pour les organismes d'application de la loi lorsqu'ils enquêtent sur de présumés criminels qui ont commis ou prévoient commettre des crimes graves (terrorisme, exploitation des enfants, etc.). En voici des exemples :

- **Chiffrement** – Bien que le *Code criminel* puisse accorder aux organismes d'application de la loi le pouvoir, notamment, de saisir les ordinateurs portatifs et les téléphones cellulaires de présumés criminels ou d'intercepter des communications en temps réel, les données peuvent être chiffrées et donc illisibles. Les criminels présumés au Canada peuvent communiquer avec des collaborateurs d'autres pays au moyen d'applications de messagerie privée et de forums de clavardage en ligne protégés par chiffrement. Comme il est indiqué à la section 4.1.2, les organismes d'application de la loi souhaiteraient que des mesures législatives soient adoptées pour obliger les FST à leur fournir un accès « par moyen détourné » ou à déchiffrer les données.

- **Web invisible** – L'activité criminelle sur le Web invisible constitue une préoccupation importante pour les organismes d'application de la loi au pays et à l'étranger. L'anonymat du Web invisible pose des problèmes importants aux enquêteurs, car l'identité et l'emplacement des utilisateurs sont dissimulés. Le Centre européen de lutte contre la criminalité (EC3) Europol, avec le soutien du Federal Bureau of Investigation, de la Drug Enforcement Agency des États-Unis et de la police nationale néerlandaise, a mis un terme aux activités d'AlphaBay et de Hansa, qui étaient d'importants marchés d'activités criminelles sur le Web invisible[38]. Comme nous l'expliquons plus en détail à la section 4.2.4, le Canada est considéré par les intervenants internationaux comme un acteur important dans le soutien des efforts d'Europol pour lutter contre la criminalité sur le Web invisible.

- **Réseaux 5G** – Les principaux intervenants ont indiqué que les réseaux de 5G poseront des défis importants aux organismes d'application de la loi. Dans son évaluation annuelle de la menace du crime organisé[39], Europol a souligné que cette nouvelle technologie de communication présentera une menace pour les techniques existantes de suivi des criminels. L'organisme a déclaré que les outils et les techniques de surveillance des réseaux 4G représentent [TRADUCTION] « l'un des outils d'enquête les plus importants dont disposent les

---

[37] Pour de plus amples renseignements sur cette affaire, se référer à *Law Times*, « 2nd Opinion: Civic responsibility on the wane » [ANGLAIS SEULEMENT], tiré de https://www.lawtimesnews.com/article/2nd-opinion-civic-responsibility-on-the-wane-9682/

[38] Europol, *Internet Organised Crime Threat Assessment (IOCTA) 2018* [ANGLAIS SEULEMENT], tiré de https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2018

[39] *Ibid*

agents et les services de police », et que les forces policières ne seront peut-être pas en mesure de suivre efficacement les criminels sur les réseaux 5G[40]. Europol a déclaré que des discussions étaient en cours avec les entreprises technologiques et les gouvernements sur la façon de combler les lacunes en matière de surveillance.

**Problèmes de compétence transfrontalière**

Les représentants de l'Initiative PE21S consacrent des efforts considérables, comme en témoignent les rapports sur le rendement, à régler les questions de compétence transfrontalière liées aux enquêtes et aux poursuites relatives à la cybercriminalité transnationale et à la criminalité assistée par ordinateur[41]. À titre d'exemple, un crime peut avoir eu lieu au Canada, alors que les éléments de preuve numériques sont stockés dans le nuage ou sur des serveurs situés à l'extérieur du Canada (Facebook, par exemple, possède des centres de données aux États-Unis et dans plusieurs autres pays).

Il est difficile pour les organismes d'application de la loi au Canada et ailleurs dans le monde de signifier des ordonnances de communication à des entreprises situées à l'étranger. Certains partenaires nationaux et étrangers considèrent que le processus d'EJ prend trop de temps, de telle sorte que les organismes d'application de la loi et les poursuivants cherchent d'autres moyens d'obtenir des renseignements. Les organismes canadiens d'application de la loi et les poursuivants souhaiteraient avoir la capacité d'accéder directement aux données générées au Canada et stockées sur des serveurs étrangers; cependant, cette approche peut avoir d'importantes répercussions sur la souveraineté et les compétences, et nuire aux relations du Canada avec ses partenaires étrangers dans le domaine de l'EJ advenant le cas où le droit et la procédure étrangers n'étaient pas respectés lors de la recherche d'une coopération directe.

La Convention de Budapest contient des dispositions sur l'EJ; toutefois, le processus est parfois considéré comme inefficace, compte tenu de la présence de protections juridiques et procédurales visant à protéger la vie privée et d'autres droits de la personne. Dans certains cas, ces protections ont entraîné des retards dans l'application en temps opportun de l'EJ, surtout en ce qui concerne l'obtention d'éléments de preuve électroniques. Les États signataires de la Convention ont cherché des moyens de rationaliser le processus d'EJ. Un effort important est consacré à la rédaction du Deuxième Protocole additionnel, qui vise à relever les défis liés à l'obtention d'éléments de preuve numériques à des fins de justice pénale de façon plus efficace. Ce nouveau protocole est traité ci-après à la section 4.2.4.

En mars 2018, les États-Unis ont adopté la *CLOUD Act*, qui permet aux organismes fédéraux d'application de la loi d'obliger les entreprises de technologie dont le siège est aux États-Unis à fournir, au moyen d'un mandat ou d'une assignation, les données demandées stockées sur des serveurs, que les données soient stockées aux États-Unis ou à l'étranger. Elle offre également une solution de rechange au processus d'EJ sous forme d'« accords exécutifs » réciproques, dans le cadre desquels les pays étrangers qui concluent de tels accords avec les États-Unis peuvent signifier directement aux fournisseurs américains les demandes d'accès à leurs données présentées dans le cadre du processus juridique, et les États-Unis peuvent faire de même en retour. Il s'agit d'une évolution prometteuse qui pourrait permettre de relever, sur une base bilatérale, certains défis importants et qui comporte un certain nombre de mesures de protection importantes des droits de la personne. L'examen de la documentation révèle toutefois que, bien qu'elle soit appuyée par le gouvernement américain, le gouvernement britannique, le gouvernement australien, l'Union européenne ainsi que par les grandes entreprises américaines, la *CLOUD Act* n'est pas sans controverse. De nombreux groupes de défense des libertés civiles, comme l'American Civil Liberties Union, ont critiqué la loi.

[40] BBC News, « Police will struggle to track criminals via 5G » [ANGLAIS SEULEMENT], 19 juillet 2019, tiré de https://www.bbc.com/news/technology-49043822

[41] Rapports annuels sur le rendement de l'Initiative PE21S, 2015-2016 à 2017-2018.

Selon l'une des critiques présentées, la *CLOUD Act* ne contient aucun mécanisme permettant à un État de se soustraire rapidement aux accords exécutifs une fois qu'ils ont été conclus, même si l'un des États participants commence soudainement à violer les libertés civiles[42]. Les États-Unis et le Royaume-Uni ont récemment achevé leurs négociations en la matière et ont produit un accord final, qui est le premier accord exécutif en vertu de la *CLOUD Act*. Les représentants de l'Initiative PE21S ont déclaré que le Canada continuerait de suivre l'évolution de la situation dans ce domaine avec intérêt, étant donné que les accords exécutifs semblent prometteurs pour ce qui est de la résolution de certains problèmes pressants dans la lutte contre les crimes graves découlant de l'évolution de la technologie et des défis connexes en matière d'enquêtes transfrontalières. L'Association canadienne des chefs de police et l'Association internationale des chefs de police ont toutes deux demandé au gouvernement fédéral de poursuivre les discussions avec les États-Unis à ce sujet, étant donné la possibilité de créer un mécanisme utile en matière d'application de la loi[43].

**Uniformité de la mise en œuvre et de l'interprétation des pouvoirs d'enquête**

Le degré de cohérence de la mise en œuvre et de l'interprétation des pouvoirs d'enquête a été évalué à l'aune d'éventuelles contestations judiciaires des dispositions du *Code criminel*. Après l'entrée en vigueur de la LPCCC, la SPDP de Justice s'est efforcée d'appuyer une mise en œuvre uniforme en présentant plus de quarante exposés à des conférences d'enquêteurs et à des comités nationaux auxquels participaient des services de police à l'échelle nationale, provinciale et municipale[44]. Les partenaires fédéraux ont reçu des conseils juridiques sur les nouvelles dispositions destinées à appuyer les efforts déployés à l'échelle internationale, notamment ceux du Canada relativement au soutien de la rédaction du Deuxième Protocole additionnel.

Bien que les éléments probants de l'évaluation indiquent que l'Initiative PE21S a contribué à assurer la mise en œuvre des pouvoirs d'enquête en grande partie uniforme, les informateurs clés ont fait remarquer qu'il existe une incohérence quant à savoir si les tribunaux accorderont à la police une ordonnance de communication obligeant une entreprise non canadienne à produire des éléments de preuve numériques. L'examen de la documentation a révélé que les décisions des tribunaux ont divergé quant à savoir s'il était possible de signifier des ordonnances de communication contre des entreprises étrangères qui hébergent des données canadiennes sur des serveurs à l'extérieur du Canada. Certains tribunaux ont refusé d'accorder une ordonnance lorsque l'entreprise se trouve entièrement à l'extérieur du Canada, tandis que d'autres ont accordé de telles ordonnances au motif qu'une entreprise étrangère qui passe des contrats avec des utilisateurs au Canada et qui héberge leurs données est assujettie à la compétence des tribunaux canadiens[45]. Une décision de janvier 2018 de la Cour d'appel de la C.-B., l'arrêt *British Columbia (Attorney General) v. Brecknell*, a des répercussions sur les entreprises étrangères ayant une « présence virtuelle » au Canada[46]. En 2016, la GRC a déposé une requête en ordonnance de communication à la Cour provinciale de la C.B. obligeant Craigslist à produire certains renseignements sur l'un de ses utilisateurs, notamment le nom de l'utilisateur, son adresse, son adresse IP, son numéro de téléphone et tous les renseignements pertinents associés à un poste. La cour a refusé au motif que Craigslist n'avait qu'une présence

---

[42] *Canadian Lawyer*, « Dark Cloud », 16 avril 2018 [ANGLAIS SEULEMENT], tiré de https://www.canadianlawyermag.com/author/lisa-r-lifshitz/dark-cloud-15600/

[43] Association canadienne des chefs de police, Compte rendu sur les résolutions de l'ACCP, juin 2017 [ANGLAIS SEULEMENT], p. 9, tiré de https://www.cacp.ca/status-report-government-responses.html?asst_id=1433

[44] Rapports annuels sur le rendement de l'Initiative PE21S, 2015-2016 à 2017-2018.

[45] Se référer à l'analyse de cette question par Christopher P. Naudie et John Cotter, « Enquêtes transfrontalières : la Cour d'appel de la Colombie-Britannique affirme son vaste pouvoir de lancer un processus judiciaire contre des sociétés étrangères », tiré de https://www.osler.com/fr/ressources/transfrontaliers/2018/enquetes-transfrontalieres-la-cour-d-appel-de-la-colombie-britannique-affirme-son-vaste-pouvoir-de

[46] Pour consulter une analyse de l'arrêt *Brecknell*, voir David Fraser, « The Legal Reality: Canadian Appeal Court decides "Virtual Presence" is enough for production order for user information against non-Canadian company » [ANGLAIS SEULEMENT], *CanLII Connecte*, tiré de https://canliiconnects.org/en/commentaries/54673

virtuelle en C.B. La GRC a interjeté appel de cette décision à la Cour d'appel de la province, qui a fait droit à l'appel. Craigslist est [TRADUCTION] « présente dans la province de la C.B. et la police peut obtenir une ordonnance de communication à son endroit, même si l'entreprise n'a pas de présence physique au Canada ni d'adresse au Canada permettant l'exécution de l'ordonnance ».

Certains commentateurs juridiques ont été surpris par l'arrêt *Brecknell*, déclarant que la décision de la Cour semble donner un effet extraterritorial aux ordonnances de communication, ce qui, selon eux, n'était pas l'intention du Parlement lors de la rédaction de la législation[47]. Il y a aussi la question de savoir si, d'un point de vue pratique, de telles ordonnances peuvent être exécutées à l'extérieur du Canada.

Dans une autre affaire récente plaidée en Ontario (maintenant résolue), les services de police de London ont obtenu une ordonnance de communication canadienne obligeant Facebook à produire des données dans un procès pour meurtre en cours devant la Cour supérieure de l'Ontario. Facebook a volontairement produit les données sur les abonnés, mais a toutefois conseillé à la police canadienne de faire une demande d'EJ aux États-Unis pour le contenu des données recherchées, afin que les États-Unis puissent présenter une ordonnance américaine obligeant Facebook à les produire. Les autorités canadiennes tentaient toujours d'obtenir l'ordonnance de production auprès de Facebook, ce qui a mené Facebook à demander à la cour canadienne d'annuler l'ordonnance puisque celle-ci n'a pas force de loi aux États-Unis. Une demande d'EJ pour l'obtention de ces données a éventuellement été présentée et exécutée. Facebook a finalement retiré sa demande sur la base du caractère théorique, ce qui a mis fin à la question[48].

### 4.2.3 Amélioration de la capacité opérationnelle pour lutter contre la cybercriminalité et la criminalité assistée par ordinateur

L'Initiative PE21S a contribué à améliorer la capacité opérationnelle du Canada de lutte contre la cybercriminalité et d'autres types de criminalité assistée par ordinateur. Les responsables de l'Initiative PE21S ont collaboré étroitement les uns avec les autres et avec les intervenants externes pour soutenir la mise en œuvre des pouvoirs d'enquête liés à l'Initiative PE21S. La GRC a mis en place une fonction de triage spécialisée pour gérer les demandes de conservation des données reçues des organismes d'application de la loi étrangers. La GRC a également mis au point de nouveaux outils pour accéder à des éléments de preuve numériques provenant d'appareils saisis, les obtenir et les traiter, ainsi que des outils utilisés dans une situation d'interception réelle.

#### Formation de partenariats et renforcement de la collaboration

Les représentants de l'Initiative PE21S ont fait état d'une collaboration étroite entre eux et avec des organisations et des groupes externes pour appuyer la mise en œuvre de l'Initiative PE21S. Par exemple, la SPDP de Justice a établi une relation de travail étroite avec la police en participant à des tribunes comme l'assemblée annuelle des enquêteurs de l'exploitation des enfants et le Forum sur la sécurité nationale et le contre-terrorisme. À la suite de l'adoption de la LPCCC, de nombreuses

[47] Se référer notamment à Osler, « Enquêtes transfrontalières : la Cour d'appel de la Colombie-Britannique affirme son vaste pouvoir de lancer un processus judiciaire contre des sociétés étrangères », tiré de https://www.osler.com/fr/ressources/transfrontaliers/2018/enquetes-transfrontalieres-la-cour-d-appel-de-la-colombie-britannique-affirme-son-vaste-pouvoir-de

[48] CBC news, « London, Ont., court to decide if police can access Facebook messages » [ANGLAIS SEULEMENT], tiré de https://www.cbc.ca/news/canada/london/london-ontario-facebook-messages-legal-case-homicide-investigation-1.5149023

réunions ont eu lieu avec des représentants de l'industrie des télécommunications et les responsables fédéraux et provinciaux de l'application de la loi. Le Groupe d'entraide internationale (GEI) de Justice a établi des relations de travail étroites avec les organismes d'application de la loi et les poursuivants de tout le Canada et fait aussi de la sensibilisation auprès des fournisseurs de services Internet (FSI), dont les données sont souvent demandées par des partenaires étrangers pour faire progresser leurs enquêtes criminelles et leurs poursuites. À titre d'exemple, 43 % des demandes d'EJ entrantes en 2017-2018 visaient des éléments de preuve numériques.

**Mise en œuvre d'une fonction de triage réservée aux demandes internationales de conservation des données**

La GRC a élaboré et mis en œuvre une fonction de triage réservée à l'administration d'un nouveau système de conservation des données conforme aux dispositions juridiques de la LPCCC et visant à répondre aux demandes internationales de conservation des preuves numériques en vertu du *Code criminel*, en prévision de l'obtention de la preuve conservée par le pays étranger présentant la demande d'EJ au Canada. Cela a donné lieu à des activités telles que la dotation de la fonction, l'élaboration de procédures opérationnelles normalisées, et la conception d'un système de suivi.

La GRC (ainsi que d'autres services de police canadiens) reçoit des demandes de conservation des données de la part d'organismes d'application de la loi étrangers. Les demandes de conservation des données relatives aux enquêtes sur l'exploitation des enfants sont traitées par les Opérations techniques de la GRC (Centre national contre l'exploitation des enfants), tandis que toutes les autres demandes sont traitées par la Police fédérale. Dans la plupart des cas, la GRC transmettra une demande de conservation au FST canadien. Le FST informera ensuite la GRC de la période de conservation des données normalisée conformément à la politique de conservation des données du fournisseur. Dans les cas où les données ne seront pas sauvegardées assez longtemps pour que s'effectue le processus d'EJ, la GRC signifiera un ordre de conservation valide pendant 90 jours. Lorsque le processus d'EJ n'est pas achevé au cours de la période de 90 jours, la GRC signifiera, juste avant l'expiration de la période, une ordonnance de conservation au FST, ce qui prolongera de 90 jours la période visée par cette ordonnance.

L'examen des rapports de rendement de la GRC a révélé qu'en tout, 176 demandes de conservation de données ont été reçues en 2016, nombre qui est passé à 505 en 2017. De ce dernier total, 408 demandes ont été reçues par la Police fédérale, dont 286 (70 %) concernaient des demandes de conservation (l'étape initiale du processus, comme il a été mentionné ci-dessus), 117 (29 %) concernaient des ordres de conservation et 5 (1 %) concernaient des ordonnances de conservation. En 2018, le nombre de demandes de conservation des données reçues par la Police fédérale a considérablement diminué. Un FSI canadien qui avait fait l'objet du plus grand nombre de demandes a ouvert un bureau auxiliaire aux États-Unis. Par conséquent, les autorités américaines ont commencé à interagir avec ce bureau auxiliaire plutôt que de présenter des demandes au Canada.

**Amélioration du traitement des demandes d'entraide juridique**

Le financement accordé dans le cadre de l'Initiative PE21S a permis au GEI de Justice d'accroître sa capacité de traiter à la fois les demandes d'EJ entrantes et sortantes. Le niveau de collaboration avec la GRC a également augmenté. Ce point est discuté plus en détail à la section 4.2.4.

**Élaboration de nouveaux outils techniques**

L'Initiative PE21S a fourni du financement à la GRC, ce qui a contribué à l'élaboration de nouveaux outils pour accéder à des éléments de preuve numériques provenant d'appareils et de supports de stockage numérique (données inactives), les obtenir et les traiter, ainsi que d'outils utilisés pour les cas justifiés d'interception en temps réel des données de transmission (données en mouvement).

**Utilisation des pouvoirs d'enquête liés à l'Initiative PE21S**

La plupart des informateurs clés, notamment des représentants de l'Initiative PE21S et des organismes d'application de la loi, des poursuivants et des FST, ont confirmé que les pouvoirs d'enquête ajoutés au *Code criminel* sont utilisés. Les principaux intervenants représentant les organismes d'application de la loi et les poursuivants ont généralement convenu que ces pouvoirs sont maintenant bien intégrés dans la « boîte à outils » de l'enquêteur. Les représentants des FST ont déclaré que la plupart des ordonnances des tribunaux signifiées par les organismes d'application de la loi à l'égard des FST canadiens sont des ordonnances de communication (paragraphes 487,014 à 487,018). Les ordres et ordonnances de **con**servation représentent une plus petite proportion du total, ce qui correspond aux données sur le rendement de la GRC. Un informateur clé représentant les organismes d'application de la loi a fait remarquer que l'ordonnance de communication en vue de retracer une communication donnée (paragraphe 487.015) est rarement utilisée. Cette ordonnance est destinée à être utilisée pour retracer les communications réacheminées par l'intermédiaire de plusieurs FST, même si l'identité d'un ou de plusieurs fournisseurs n'est pas connue au moment où l'ordonnance fait l'objet d'une requête.

Deux des principaux FST, TELUS et Rogers, publient des rapports annuels sur la transparence conformément aux Lignes directrices concernant la production volontaire de rapports sur les mesures de transparence publiées par Innovation, Sciences et Développement économique Canada en 2015. Ces rapports fournissent des renseignements de haut niveau sur l'utilisation des pouvoirs d'enquête. (Les informateurs clés représentant les FST ont fait remarquer qu'il faut faire preuve de prudence dans l'interprétation de ces données, car les fournisseurs tiennent compte des ordonnances des tribunaux de différentes façons.) Le rapport de TELUS indique que le nombre d'ordonnances judiciaires qui lui ont été signifiées est passé de 3 550 en 2014 à 4 871 en 2018[49]. Les diverses dispositions du *Code criminel* n'offrent pas de ventilation de ces nombres. Le rapport de 2017 de Rogers montre que le nombre d'ordonnances judiciaires a diminué, passant de 115 954 en 2016 à 100 708 en 2017 (aucune explication n'a été fournie quant à la raison de cette baisse). Le nombre d'ordonnances de communication de tous les registres d'appels de tours de téléphonie cellulaire est passé de 191 en 2016 à 511 en 2017[50]. Les principaux intervenants représentant les principaux FST ont fait remarquer que les organismes d'application de la loi utilisent de plus en plus les registres d'appels de tours de téléphonie cellulaire.

### 4.2.4 Amélioration de la coopération internationale pour l'obtention d'éléments de preuve numériques

L'Initiative PE21S a aidé le Canada à accroître son niveau de coopération à l'échelle internationale pour l'obtention d'éléments de preuve numériques pour lutter contre la cybercriminalité et la criminalité assistée par ordinateur. Les intervenants internationaux considèrent que le Canada respecte les exigences de la Convention de Budapest. L'Initiative a également contribué à améliorer la coordination et l'uniformité de l'approche de la politique étrangère du Canada en matière de cybercriminalité et de criminalité assistée par ordinateur.

**Ratification de la Convention de Budapest**

Comme il a été mentionné précédemment, le Canada a signé la *Convention sur la cybercriminalité du Conseil de l'Europe* (Convention de Budapest) en novembre 2001 et l'a ratifiée le 8 juillet 2015. La Convention n'a pas été ratifiée plus tôt parce que le gouvernement avait besoin de temps pour mettre en vigueur la législation nationale visant à s'assurer que les lois canadiennes sont conformes à la

[49] TELUS, op. cit.
[50] Rogers Communications, « Rapport de 2017 sur la transparence », tiré de https://aproposde.rogers.com/nouvelles-et-idees/rapport-de-2017-sur-la-transparence/

Convention – ce qui a été accompli avec l'adoption de la LPCCC (l'ancien projet de loi C-13). Les intervenants internationaux considèrent que le Canada respecte les exigences de la Convention de Budapest.

**Deuxième Protocole additionnel**

La Convention de Budapest comporte des dispositions relatives à l'EJ, mais le processus est réputé surchargé par le volume croissant de demandes de production d'éléments de preuve numériques. Certains considèrent que le processus est trop lent pour permettre un accès efficace aux données dans le contexte moderne. Les États signataires de la Convention ont cherché à simplifier le processus, tout en préservant les mesures de protection nécessaires pour accéder à ces données. Ils ont envisagé de réglementer l'accès transfrontalier aux données stockées en élargissant l'interprétation de l'article 32 de la Convention; toutefois, cette tentative a pris fin sans résultats concrets en 2014. Le Groupe sur les preuves dans le nuage du Comité de la Convention sur la cybercriminalité (Conseil de l'Europe) (T-CY) a été créé en décembre 2014 pour étudier des solutions d'accès à des éléments de preuve dans le nuage à des fins de justice pénale, notamment par l'entremise de l'EJ. Le Groupe a produit un rapport en septembre 2016; la principale recommandation présentée au T-CY consistait à envisager la préparation d'un projet de protocole pour la Convention de Budapest. Le mandat pour la préparation d'une deuxième version du Protocole a été approuvé par le T-CY le 8 juin 2017[51]. Le protocole prévoit des dispositions visant à accroître l'efficacité de l'EJ (un régime simplifié pour les demandes d'EJ ayant trait aux abonnés, aux ordonnances de communication internationales et à la coopération directe entre les autorités judiciaires dans les demandes d'EJ), ainsi que des dispositions permettant une collaboration directe avec les fournisseurs de services d'autres territoires de compétence en ce qui concerne les demandes de renseignements sur les abonnés, les demandes de conservation et les demandes urgentes.

Le Canada joue un rôle important dans la rédaction du Deuxième Protocole additionnel. Deux séances plénières et de quatre à six séances de rédaction par des experts sont prévues chaque année. On a produit dix documents conceptuels qui clarifient des problèmes précis et, le cas échéant, proposent d'éventuelles dispositions de traité. Le Canada a pris en charge la rédaction de deux des documents conceptuels[52].

**Traitement des demandes d'entraide juridique**

La *Loi sur l'entraide juridique en matière criminelle* (LEJMC) confère au Canada le pouvoir légal d'obtenir des ordonnances judiciaires pour le compte d'États signataires d'accords d'entraide juridique avec le Canada. Il s'agit notamment de traités bilatéraux et de conventions multilatérales contenant des dispositions pour une EJ. Le Canada est également en mesure de conclure des ententes administratives visant des cas particuliers, et limitées dans le temps en vertu de la LEJMC afin d'aider les États non signataires à obtenir une EJ, notamment en ce qui concerne l'obtention d'éléments de preuve numériques du Canada. La LPCCC a apporté des changements importants à la LEJMC en y incorporant bon nombre des nouveaux pouvoirs d'enquête qui ont été ajoutés au *Code criminel*, permettant ainsi au Canada de fournir des éléments de preuve aux partenaires étrangers en vertu de ces dispositions dans des circonstances appropriées. Les représentants du GEI ont fait remarquer que la LPCCC et les modifications connexes apportées à la LEJMC ont procuré plusieurs avantages au processus d'EJ. Les principales modifications concernaient les dispositions ayant trait aux mandats pour un dispositif de localisation et aux mandats pour un enregistreur de données de transmission

[51] Centre d'excellence de cyberdéfense coopérative de l'OTAN (CCDCOE), « Council of Europe Ponders a New Treaty on Cloud Evidence » [ANGLAIS SEULEMENT], tiré de https://ccdcoe.org/incyder-articles/council-of-europe-ponders-a-new-treaty-on-cloud-evidence/

[52] La version provisoire de cette disposition et d'autres dispositions liées au Deuxième Protocole additionnel sont disponibles sur le site Web du Conseil de l'Europe à l'adresse https://www.coe.int/fr/web/cybercrime/t-cy-drafting-group

ainsi que les ordonnances de communication (ordonnances d'obtention des éléments de preuve) et l'inclusion des ordres et ordonnances de **con**servation dans le *Code criminel*, qui peuvent faire l'objet de requêtes par les autorités policières nationales et étrangères. Les nouvelles dispositions donnent au juge d'EJ qui délivre l'ordonnance ou le mandat le pouvoir discrétionnaire de faire abstraction de la tenue d'une audience distincte appelée « audience d'envoi », qui constitue généralement une exigence procédurale du processus d'EJ. Cette simplification du processus est importante étant donné qu'est souvent urgente l'obtention de dossiers au moyen de mandats pour un dispositif de localisation et de mandats pour un enregistreur de données de transmission ou en vertu de l'un des nouveaux pouvoirs d'ordonnance de communication. En somme, la LPCCC a modifié le *Code criminel* et la LEJMC de sorte que les ordonnances de communication et les ordres et ordonnances de conservation ajoutées au *Code criminel* sont maintenant disponibles pour faciliter les enquêtes à l'étranger.

Le Canada a signé des traités bilatéraux d'EJ avec 35 pays et a également ratifié plusieurs conventions internationales contenant des dispositions sur l'EJ, dont la *Convention des Nations Unies contre la criminalité transnationale organisée* et la *Convention des Nations Unies contre la corruption*[53]. La ratification par le Canada de la *Convention sur la cybercriminalité* du Conseil de l'Europe a attiré de nombreux nouveaux partenaires d'EJ, et ce nombre ne cesse de croître.

Le GEI de Justice coordonne toutes les demandes d'EJ présentées par le Canada et celles présentées au Canada. Pour traiter les demandes d'EJ, le GEI consulte les organismes d'application de la loi et les poursuivants canadiens et étrangers, ainsi que les autorités centrales d'autres pays. Le GEI examine les demandes et s'assure que les pièces justificatives et les éléments de preuve sont suffisants pour répondre aux exigences du traité et à celles du droit canadien, et que les autorisations requises ont été délivrées. On s'attendait à ce que le volume de demandes d'EJ augmente à la suite de l'adoption de la LPCCC et de la ratification de la Convention de Budapest. Le GEI tient des statistiques sur le nombre de demandes d'EJ présentées au Canada (entrantes) et par le Canada à l'étranger (sortantes). Sur un total d'environ 1 050 demandes d'EJ actives entrantes en 2017-2018, 43 % d'entre elles (soit 448 demandes) avaient trait à l'obtention d'éléments de preuve numériques. Le nombre total de demandes d'EJ a augmenté considérablement au fil des ans.

Le tableau 3 présente des statistiques sur le nombre de demandes d'EJ présentées pour obtenir des éléments de preuve numériques traitées par le GEI de Justice au cours de la période visée par l'évaluation.

**Tableau 3: Nombres de demandes d'entraide juridique entrantes et sortantes sollicitant des éléments de preuve numériques**

| Année | Nombres de demandes d'EJ entrantes sollicitant des éléments de preuve numériques traitées par le GEI | | | Nombres de demandes d'EJ sortantes sollicitant des éléments de preuve numériques présentées par le GEI | | |
|---|---|---|---|---|---|---|
| | En vertu de la Convention de Budapest | En vertu d'autres traités et ententes administratives | Total | En vertu de la Convention de Budapest | En vertu d'autres traités et ententes administratives | Total |
| 2015-2016 | 0 | 405 | 405 | 0 | 97 | 97 |
| 2016-2017 | 10 | 354 | 364 | 0 | 128 | 128 |
| 2017-2018 | 14 | 434 | 448 | 1 | 113 | 114 |

[53] Affaires mondiales Canada a dressé une liste des traités bilatéraux et multilatéraux à l'adresse https://treaty-accord.gc.ca/section.aspx?lang=fra

Le nombre total de demandes d'EJ entrantes visant l'obtention d'éléments de preuve numériques a fluctué au cours de la période de trois ans, atteignant un sommet de 448 demandes en 2017-2018. Le volume des demandes sortantes est beaucoup plus faible et a également fluctué au cours des trois années. Plusieurs représentants des organismes canadiens d'application de la loi ont déclaré qu'ils éviteront le long processus d'EJ, si possible. Bien que l'on ait l'impression que le processus d'EJ est relativement lent dans de nombreux pays, le Conseil de l'Europe ne compile pas de statistiques sur le temps que prennent les États signataires pour traiter les demandes d'EJ.

Relativement peu de demandes sont reçues en vertu de la Convention de Budapest, car les parties utilisent d'abord les traités existants et les autres conventions. Comme il a été mentionné précédemment, le Canada a conclu des accords bilatéraux avec de nombreux pays et a ratifié plusieurs conventions multilatérales.

Les statistiques du GEI indiquent qu'un peu plus de quatre mois sont nécessaires pour l'exécution des demandes d'EJ entrantes[54]. Les représentants du GEI ont fait remarquer que bon nombre des demandes simples provenant de pays ayant des systèmes juridiques similaires sont exécutées dans un délai plus court. La nature des demandes présentées dans le cadre de l'EJ devient de plus en plus complexe. Les demandes provenant de pays ayant des systèmes semblables, comme les États-Unis, sont généralement plus simples; les demandes ponctuelles provenant d'autres pays peuvent prendre plus de temps, car le pays peut ne pas connaître les exigences juridiques et procédurales du Canada, et aura besoin de conseils pour collaborer avec le Canada. En outre, il peut y avoir des problèmes de traduction, notamment. Le Canada connaît également des retards dans l'obtention d'éléments de preuve numériques d'autres pays.

Le financement fourni par l'Initiative PE21S a permis au GEI d'améliorer la gestion des demandes d'EJ. Le GEI a créé et doté une unité cyber d'EJ. De nombreux outils de formation ont été mis au point, notamment un guide étape par étape de l'EJ affiché sur le site Web public du GEI, ainsi que des guides d'introduction à la LPCCC en ce qui a trait au processus d'EJ et à la façon d'obtenir la conservation obligatoire des données. Les ébauches de demande sont communiquées à l'autorité compétente canadienne dès le début, de sorte que toute lacune ou question nécessitant des éclaircissements puisse être transmise à l'autorité centrale étrangère. La vaste campagne de sensibilisation menée par le GEI a également contribué à améliorer le fonctionnement général du processus d'EJ.

Enfin, le Canada est réputé être en conformité avec les dispositions d'EJ de la Convention de Budapest. Le Conseil de l'Europe (par l'intermédiaire de son Comité T-CY) a effectué trois séries d'évaluations du niveau de conformité de chaque État signataire. Le rapport d'évaluation de 2017[55] souligne que le Canada a mis en œuvre plusieurs pratiques exemplaires, comme l'établissement d'un point de contact 24 heures sur 24, 7 jours sur 7, pour les demandes d'EJ, la tenue d'une base de données sur les demandes d'EJ, l'établissement d'une cyber-unité au sein de l'autorité centrale (JUS-GEI), l'acceptation des demandes par voie électronique, et la tenue actualisée d'un site Web public complet fournissant des conseils de fond aux autorités étrangères sur la façon de présenter des demandes d'EJ efficaces. Des informateurs clés internationaux ont déclaré que d'autres pays peuvent bénéficier de l'expérience du Canada.

---

[54] Ce chiffre a trait aux demandes achevées; les communications avec l'autorité centrale qui fait la demande d'obtention des renseignements manquants et la clarification de tout problème peuvent nécessiter du temps supplémentaire.
[55] Conseil de l'Europe, « Évaluer la mise en œuvre de la Convention de Budapest », tiré de https://www.coe.int/fr/web/cybercrime/assessments

**L'approche de la politique étrangère du Canada envers la cybercriminalité**

Les ressources fournies à AMC (deux ETP en tout) par l'Initiative PE21S ont permis aux fonctionnaires de se concentrer sur le travail nécessaire pour aider à faire en sorte que le Canada adopte une approche intégrée et uniforme en matière de politique étrangère à l'égard de la cybercriminalité. AMC a mené des consultations et coordonné des activités interministérielles pour appuyer le travail en matière de politique étrangère. Les représentants d'AMC coordonnent la participation active du Canada aux initiatives internationales de lutte contre la cybercriminalité. Ce travail se déroule sur plusieurs tribunes, dont le G7, l'Office des Nations Unies contre la drogue et le crime, l'Organisation des États américains (OEA) et le Conseil de l'Europe.

Comme il a été mentionné précédemment, le Canada joue un rôle de premier plan en ce qui concerne le soutien à la Convention de Budapest. Les informateurs clés internationaux ont fait remarquer que la contribution du Canada a augmenté considérablement au cours des dernières années. Le fait de contribuer à l'application de la Convention exige un effort considérable. Des représentants fédéraux assistent aux réunions semestrielles du Comité de la Convention sur la cybercriminalité (T-CY), participent aux quatre à six séances de rédaction du protocole, ainsi qu'à la conférence périodique « Octopus »[56]. Un représentant de Justice a été élu au T-CY en 2016 et a été nommé pour un deuxième mandat en 2018. Le Canada joue également un rôle actif dans la promotion de la Convention auprès des pays qui ne l'ont pas encore ratifiée.

Bien que cela ne soit pas directement lié à l'Initiative PE21S, le Canada est réputé très mobilisé envers le travail du Centre européen de lutte contre la criminalité (EC3) d'Europol. Europol a mis en place l'EC3 en 2013 afin de renforcer les mesures prises par les forces de l'ordre envers la cybercriminalité dans l'Union européenne (UE) et ainsi aider à protéger les citoyens, les entreprises et les gouvernements européens contre la cybercriminalité. Le Canada, par l'entremise de la GRC, est membre du Groupe de travail conjoint sur la cybercriminalité qui traite les cas de cybercriminalité les plus importants qui touchent les États membres de l'UE. Un agent de liaison de la GRC est affecté à l'EC3 à La Haye, aux Pays-Bas; le Canada ajoutera en outre un deuxième effectif pour 2019-2020. Le Canada est considéré comme un chef de file dans la lutte contre l'exploitation sexuelle des enfants en ligne. Il est également un joueur à part entière dans « l'équipe du Web invisible» d'EC3.

**Soutien du renforcement des capacités**

L'Initiative PE21S affecte un petit montant (250 000 $ par année) pour augmenter le financement accordé à un projet dans le cadre du Programme d'aide au renforcement des capacités de lutte contre la criminalité d'AMC. Ce projet, mené par l'OEA, offre un soutien au Comité interaméricain contre le terrorisme afin d'offrir une formation technique aux intervenants en cybersécurité dans 26 États signataires d'Amérique latine et des Antilles.

### 4.2.5 Effets non prévus

Les principaux intervenants représentant les FST ont fait remarquer que le fait de se conformer aux ordonnances des tribunaux a une incidence réelle sur les coûts et estiment que cette incidence n'a pas été prise en compte lors de la rédaction des modifications législatives. Comme il a été mentionné précédemment, les FST demandent au GC de présenter un projet de loi prévoyant une indemnisation pour les coûts engagés.

Les principales répercussions inattendues relevées par les informateurs clés se rapportent aux conséquences de l'arrêt *Spencer* en 2014 et ne sont pas spécifiquement liées à la mise en œuvre des

[56] La Conférence Octopus est tenue par le Conseil de l'Europe tous les 12 à 18 mois et chaque conférence porte sur un problème particulier de cybercriminalité. Tiré dehttps://www.coe.int/fr/web/cybercrime/octopus-conference.

pouvoirs d'enquête liés à l'Initiative PE21S. Toutefois, elles ont affecté la façon dont ces pouvoirs sont utilisés. Par exemple, les FST ne fournissent plus de renseignements sur les abonnés aux organismes d'application de la loi sur une base volontaire (sauf en cas de circonstances contraignantes), et exigent plutôt une ordonnance générale de communication. Par conséquent, le nombre d'ordonnances de communication signifiées aux FST est probablement beaucoup plus élevé que ce à quoi l'on s'attendait au moment de la conception des modifications législatives.

## 4.3 Conception

### 4.3.1 Gestion horizontale de l'Initiative PE21S

L'Initiative PE21S a été bien coordonnée. Le plan d'activités de l'Initiative PE21S a fait l'objet d'une préparation rigoureuse et l'Initiative a évolué comme prévu.

Les représentants de l'Initiative PE21S interrogés ont indiqué que l'Initiative était bien coordonnée. Ils ont déclaré que l'analyse de rentabilisation du projet de l'Initiative PE21S avait fait l'objet d'une préparation rigoureuse. Il ressort clairement des constatations présentées dans le présent chapitre que l'Initiative a évolué comme prévu.

L'un des partenaires fédéraux a indiqué qu'il aimerait avoir plus d'information sur le travail effectué par d'autres représentants de l'Initiative PE21S en appui à l'Initiative. On a demandé s'il y a lieu de créer un groupe de travail interministériel sur la cybercriminalité; il a toutefois été souligné qu'un nouveau comité interministériel a été constitué dernièrement pour répondre à ce besoin.

Une stratégie de mesure du rendement a été élaborée au début de l'Initiative pour appuyer l'évaluation. Bien que quelques représentants de l'Initiative PE21S aient remarqué la présence de difficultés lors de la collecte des données en raison des limites d'extraction de l'information des systèmes de gestion des dossiers, ils ont été en mesure de fournir l'information requise sur une base annuelle.

# 5. CONCLUSIONS ET RECOMMANDATIONS

## 5.1 Conclusions

Les conclusions de l'évaluation horizontale de l'Initiative PE21S relativement aux questions d'évaluation sont résumées ci-dessous.

### 5.1.1 Pertinence

L'objectif global de l'Initiative PE21S, à savoir fournir les moyens de mettre en œuvre les modifications apportées au *Code criminel* et aux autres lois par la LPCCC et satisfaire les obligations internationales du Canada découlant de la ratification de la Convention de Budapest, demeure pertinent, alors que la cybercriminalité est en croissance rapide tant au Canada qu'à l'international, et que les criminels exploitent de plus en plus les technologies en évolution. Les activités principales soutenues par l'Initiative PE21S doivent se poursuivre.

Bien que les éléments probants de l'évaluation indiquent que la LPCCC a répondu à l'engagement pris par le GC en 2013 en matière de modernisation des pouvoirs d'enquête prévus dans le *Code criminel*, les lois canadiennes doivent continuellement évoluer afin que les organismes d'application de la loi et les poursuivants disposent des outils nécessaires pour lutter contre les crimes graves. La police et les poursuivants ont souligné en particulier les défis associés à l'accès aux RBA et aux données chiffrées.

### 5.1.2 Rendement

Les groupes cibles de l'Initiative PE21S, notamment les organismes d'application de la loi, les poursuivants et les FST, connaissent maintenant très bien les modifications législatives apportées au *Code criminel* et à d'autres lois. Les représentants de l'Initiative PE21S ont consacré des efforts considérables à la sensibilisation et à la connaissance des éléments clés de la LPCCC.

Relativement peu de questions juridiques et opérationnelles ont été soulevées relativement aux nouveaux pouvoirs d'enquête. On s'attendait à ce que les nouveaux pouvoirs d'enquête entraînent de nombreuses contestations fondées sur la Charte, mais cela ne s'est pas encore avéré. Les ressources fournies aux partenaires fédéraux par l'Initiative PE21S les ont aidés à gérer la mise en œuvre des pouvoirs d'enquête de diverses façons, allant de l'appui aux poursuites fondées sur ces pouvoirs à la prestation de conseils juridiques et stratégiques aux intervenants internes et externes. La principale question juridique soulevée par les informateurs clés a trait au fait que les nouvelles dispositions relatives au mandat pour enregistreurs de données de transmission ne donnent pas accès aux renseignements de base sur les abonnés. Les pouvoirs d'enquête ont été largement mis en œuvre partout au Canada.

L'Initiative PE21S a contribué à améliorer la capacité opérationnelle du Canada de lutte contre la cybercriminalité et d'autres types de criminalité assistée par ordinateur. Les responsables de l'Initiative PE21S ont collaboré étroitement entre eux ainsi qu'avec les intervenants externes pour soutenir la mise en œuvre des pouvoirs d'enquête liés à l'Initiative PE21S. La GRC a mis en place une fonction de triage réservée au traitement et au suivi des demandes de conservation des données reçues des organismes d'application de la loi étrangers. Elle a également mis au point de nouveaux outils pour accéder à des éléments de preuve numériques provenant d'appareils saisis, les obtenir et les traiter, ainsi que des outils utilisés dans une situation d'interception réelle.

L'Initiative PE21S a aidé le Canada à accroître son niveau de coopération à l'échelle internationale pour ce qui est de l'obtention d'éléments de preuve numériques pour lutter contre la cybercriminalité et la criminalité assistée par ordinateur. Les intervenants internationaux considèrent que le Canada respecte ses exigences. À l'échelle internationale, le Canada est réputé jouer un rôle important en ce qui concerne l'appui à la Convention de Budapest, déployant des efforts considérables à la rédaction du Deuxième Protocole additionnel. Le GEI de Justice a amélioré le traitement des demandes d'EJ visant à obtenir des éléments de preuve numériques reçues d'organismes d'application de la loi étrangers. L'Initiative a également contribué à améliorer la coordination et l'uniformité de l'approche de la politique étrangère du Canada en matière de cybercriminalité et de criminalité assistée par ordinateur.

### 5.1.3 Conception

L'Initiative PE21S a été bien coordonnée. Le plan d'activités de l'Initiative PE21S a fait l'objet d'une préparation rigoureuse et l'Initiative a évolué comme prévu.

## 5.2 Recommandations

Comme on l'a mentionné, l'Initiative PE21S découle des parties de l'IAL relatives aux modifications apportées au *Code criminel* et aux autres lois par la LPCCC et au respect des obligations internationales découlant de la ratification de la Convention de Budapest. Par conséquent, les partenaires de l'Initiative PE21S étaient déjà mobilisés dans les domaines opérationnels plus vastes dans lesquels se situent les activités spécifiques de l'Initiative PE21S.

Aucune recommandation n'est incluse, car l'Initiative a été mise en œuvre comme prévu, et on n'a relevé aucun obstacle à l'atteinte des résultats attendus. Bien que plusieurs questions aient été

soulevées, comme l’accès aux RBA et aux données chiffrées, elles dépassent la portée de l’Initiative ou ont été saisies par les tribunaux.

# ANNEXE A: PROFIL DU PROGRAMME

## A.1 Gouvernance

L'Initiative PE21S est supervisée par de hauts fonctionnaires de chaque ministère ou organisme partenaire qui sont conjointement responsables de la gestion de sa mise en œuvre, alors que chacun exerce ses activités particulières dans les systèmes de justice pénale et de politique internationale. Justice est responsable de la direction de la coordination de la stratégie et des conseils juridiques afin d'en assurer l'uniformité, tout en respectant l'indépendance des organisations fédérales dans l'exercice de leur propre mandat.

## A.2 Liens

L'Initiative PE21S est liée à la Stratégie de cybersécurité du GC, qui vise à rendre le cyberespace plus sécuritaire pour tous les Canadiens, et à l'IAL, qui vise à faire en sorte que les menaces à la criminalité et à la sécurité nationale soient repérées et traitées tout en respectant la vie privée des Canadiens.

## A.3 Rôles et responsabilités des partenaires de l'Initiative PE21S

### i) Ministère de la Justice du Canada

Le ministère de la Justice appuie les modifications apportées à la LPCCC et veille à ce que l'intégration au système de justice canadien des dispositions concernant les pouvoirs d'enquête liés aux éléments de preuve numériques soit une réussite. Cela passe notamment par l'élaboration et la prestation de formation aux responsables de l'application de la loi, aux poursuivants et aux fournisseurs de services, par la prestation de conseils juridiques et stratégiques à l'appui de la mise en œuvre, et par la prestation de connaissances spécialisées sur toute question liée à la Charte.

La Section de la politique en matière de droit pénal fournit des conseils juridiques et stratégiques pour appuyer la mise en œuvre des nouveaux pouvoirs d'enquête. Elle a participé à l'élaboration et à la prestation d'activités de sensibilisation et de formation pour veiller à ce que les modifications apportées à la LPCCC soient comprises, interprétées et mises en œuvre de façon uniforme afin de réduire le risque de mauvaise interprétation ou d'application erronée.

La Section des droits de la personne fournit des connaissances spécialisées liées à la Charte ainsi qu'un soutien des recours en justice connexe.

Le Groupe d'entraide internationale est responsable de l'examen et de l'exécution de toutes les demandes d'EJ présentées au Canada et par le Canada en matière criminelle et d'extradition.

L'Unité des services juridiques de la GRC (USJ) offre des conseils et du soutien juridiques à la GRC sur les questions juridiques et stratégiques découlant de la mise en œuvre et de l'application des dispositions de l'Initiative PE21S.

### ii) Service des poursuites pénales du Canada

Le SPPC est chargé de répondre aux demandes de conseils et de soutien juridiques des enquêteurs dans le contexte des enquêtes et des poursuites à la suite des modifications apportées aux paragraphes 492.1 et 492.2 du *Code criminel* et de la création de nouvelles ordonnances de communication et de conservation (surtout dans les cas très complexes et pour une grande proportion

des cas de complexité moyenne)[57]. Le SPPC participe également à l'étape préalable à l'inculpation. En outre, le SPPC intervient de plus en plus à l'étape postérieure à la mise en accusation, en raison de poursuites plus longues survenant lors de contestations constitutionnelles de la nouvelle loi, et de l'établissement de nouveaux précédents. Le SPPC offre également de la formation aux poursuivants et à certains agents de police. La formation a lieu périodiquement à l'École des poursuivants du SPPC et dans les bureaux régionaux. Des ateliers et des mises à jour continus du matériel de formation à l'intention des poursuivants et/ou de la police ont eu lieu à mesure que les nouvelles dispositions étaient mises en œuvre et interprétées par les tribunaux.

### iii) Gendarmerie royale de Canada

La GRC a un vaste mandat pour lutter contre la cybercriminalité, tant au pays qu'à l'étranger. Cela comprend la lutte contre la criminalité où Internet et les technologies de l'information sont utilisés dans la perpétration d'une infraction criminelle. En vertu de l'Initiative PE21S, la GRC est responsable des initiatives suivantes :

- Le développement d'une fonction de triage réservée à l'administration d'un nouveau système de conservation des données et à la réponse aux demandes d'aide des pays étrangers concernant l'Initiative PE21S, notamment en vertu de la Convention de Budapest. Une partie de cette fonction est intégrée au Centre national de lutte contre l'exploitation des enfants de la GRC et est liée aux secteurs opérationnels clés de la Police fédérale en ce qui concerne les demandes qui ne sont pas liées à l'exploitation des enfants. Le Centre national des opérations de la GRC sert de point de contact « 24 heures sur 24, 7 jours sur 7 » pour faciliter la prestation de conseils techniques et de renseignements juridiques, la conservation des données, la collecte de preuves, et le repérage des suspects relativement aux demandes internationales présentées en vertu de la Convention de Budapest.

- L'élaboration de nouveaux outils techniques et/ou de solutions pour l'interception en temps réel et justifiée des données de transmission et l'analyse des données saisies. Cela comprend les outils d'interception sur les réseaux, les autres outils de saisie des données, les outils de traitement, et le formatage des données à des fins d'enquête, d'analyse et de preuve. De nouveaux outils opérationnels ont été mis au point pour recueillir des données à partir de dispositifs de suivi en temps réel afin de localiser une personne, une transaction ou une chose. Ces outils appuient les enquêtes nationales et internationales portant sur les principaux services de télécommunications du Canada. Les activités de recherche et de développement sont intégrées aux programmes spéciaux « I » de la GRC et aux groupes intégrés de la criminalité technologique (GICT) situés en Ontario, au Québec et en Colombie-Britannique.

- De nouvelles ressources réservées pour accroître le nombre d'équipes d'enquête criminelle et mettre en œuvre des outils pour l'interception en temps réel des données de transmission, et l'analyse des données saisies liées aux pouvoirs d'enquête de l'Initiative PE21S; notamment les demandes internationales liées à la Convention de Budapest. Cet élément est axé sur la mise en œuvre opérationnelle et l'utilisation des nouveaux outils dans les enquêtes criminelles. Les ressources sont hébergées dans les programmes spéciaux « I » de la GRC et les GICT situés en Ontario, au Québec et en Colombie-Britannique.

Les USJ de la GRC appuient les rôles et les responsabilités de la GRC en ce qui concerne l'Initiative PE21S. Il y a eu une mobilisation continue des USJ de la GRC pour appuyer la formation de la GRC

[57] Parmi les autres modifications qui se sont traduites par une participation accrue du SPPC à l'étape préalable à l'inculpation, mentionnons les nouvelles dispositions de l'ordonnance omnibus des paragraphes 184.2(5), 186(8) et 188(6), plus précisément les mots « lié à l'exécution de l'autorisation », et la nouvelle disposition du paragraphe 187(7) sur l'ordonnance de mise sous scellés.

sur les nouveaux pouvoirs d'enquête en vertu de la LPCCC, les nouvelles obligations de la GRC découlant de la ratification de la Convention de Budapest, et les développements juridiques dans ce domaine du droit touchant les opérations de la GRC. La formation comprenait également des activités de formation à l'interne avec les secteurs opérationnels de la GRC, avec la participation des équipes de soutien à l'application des lois de la GRC[58].

### iv) Affaires mondiales Canada

AMC appuie la mise en œuvre de la LPCCC et de la Convention de Budapest en faisant progresser la coopération internationale en matière de cybercriminalité, et en veillant à ce que les intérêts du Canada en matière de cybercriminalité soient pris en compte dans la politique étrangère globale du Canada. Étant donné que la cybercriminalité est de nature internationale, un engagement supplémentaire a été entrepris avec des partenaires internationaux. Grâce à un financement sous forme de contribution, AMC fournit une assistance technique aux pays étrangers pour renforcer leurs capacités de lutte contre la cybercriminalité et/ou faciliter la ratification et la mise en œuvre de la Convention de Budapest. Le financement sous forme de contribution est fourni principalement en vertu des modalités du Programme visant à renforcer les capacités de lutte contre la criminalité. La Direction générale des affaires juridiques d'AMC, plus précisément la Division du droit criminel, de la sécurité et de la diplomatie (JLA), est responsable de veiller à ce que la politique et le droit canadiens soient conformes aux exigences de la Convention de Budapest et aux autres obligations internationales du Canada. JLA conseille Justice sur les questions de politique étrangère découlant des demandes d'EJ et d'extradition à destination et en provenance du Canada. AMC est responsable du Protocole concernant les enquêteurs étrangers au Canada. Il fournit des conseils juridiques sur les questions de souveraineté qui peuvent découler de la coopération transfrontalière en matière de cybersécurité liée à la Convention de Budapest, ainsi que des conseils juridiques sur les questions de droit international.

## A.5 Modèle logique

Un diagramme du modèle logique de l'Initiative PE21S est présenté à la figure A1 sur la page suivante. Il illustre la relation entre les activités prévues et les résultats attendus.

[58] Remarque : La formation interne est appuyée par les niveaux de ressources existants.

**Figure A1 : Modèle logique de l'Initiative sur les pouvoirs d'enquête au 21e siècle**