Innovation, Sciences et Développement économique Canada

Innovation, Science and Economic Development Canada

Canada

# LA LOI CANADIENNE ANTI-POURRIEL (LCAP)

## + RAPPORT DE MESURE DU RENDEMENT 2020-2021

Cette publication est également offerte en ligne :
https://www.ic.gc.ca/eic/site/030.nsf/fra/00027.html

Pour obtenir un exemplaire de cette publication ou un format substitut (Braille, gros caractères, etc.), veuillez remplir le formulaire de demande de publication : www.ic.gc.ca/demande-publication ou communiquer avec :

Centre de services Web
Innovation, Sciences et Développement économique Canada
Édifice C.D.-Howe
235, rue Queen
Ottawa (Ontario) K1A 0H5
Canada

Téléphone (sans frais au Canada) : 1-800-328-6189
Téléphone (international) : 613-954-5031
TTY (pour les personnes malentendantes) : 1-866-694-8389
Les heures de bureau sont de 8 h 30 à 17 h (heure de l'Est)
Courriel : ISDE@canada.ca

## Autorisation de reproduction



N° de catalogue Iu170-2F-PDF
ISSN 2562-3273

N.B. Dans cette publication, la forme masculine désigne tant les femmes que les hommes.

Also available in English under the title *Canada's Anti-Spam Legislation (CASL) Initiative performance measurement report.*

# Table des matières


**1. Introduction** 4

**2. Partenaires** 5

**3. Aperçu des résultats** 6

**4. L'environnement** 7

4.1 Contexte international 7

4.2 Tendances, indicateurs et défis 8

**5. Les résultats** 9

5.1 Politiques et coordination 9

5.2 Promotion de la conformité 9

5.3 Coopération internationale et nationale 11

5.4 Surveillance de la conformité 14

5.5 Application de la loi 14

**Annexe A : Modèle logique de la LCAP** 18

# 1. Introduction

Le rapport annuel 2020-2021 de mesure du rendement de la *Loi canadienne anti-pourriel* (LCAP) vise à mieux faire connaître l'initiative de la LCAP. Il fournit des renseignements pertinents sur l'initiative, son environnement, son rendement et les rôles et activités de ses partenaires.

Dans un monde de plus en plus numérique, l'objectif de la LCAP est d'aider l'économie canadienne à être aussi efficace et adaptable que possible en réglementant les pratiques commerciales qui pourraient dissuader les consommateurs de faire des affaires par voie électronique. Plus précisément, la LCAP vise à protéger les entreprises et les consommateurs canadiens contre les pourriels, les maliciels et les autres menaces électroniques émergentes qui :

- nuisent à la disponibilité, à la fiabilité, à l'efficacité et à l'utilisation optimale des moyens électroniques pour mener des activités commerciales;
- engendrent des coûts supplémentaires pour les entreprises et les consommateurs;
- compromettent la vie privée ou la sécurité des renseignements confidentiels;
- minent la confiance des Canadiens face à l'utilisation des plateformes électroniques pour effectuer des activités commerciales au pays et à l'étranger.

La LCAP joue un rôle important dans l'atteinte d'un équilibre entre le potentiel d'une économie axée sur les données et le droit des Canadiens à la protection de leurs données et de leur vie privée. Dans le contexte d'une activité commerciale, les règles de la LCAP interdisent, entre-autres, ce qui suit :

- pourriel – envoyer des messages électroniques commerciaux sans consentement préalable;
- pratiques commerciales trompeuses – donner des indications fausses ou trompeuses en ligne, y compris dans les adresses de sites Web;
- maliciels – installer des logiciels sans consentement préalable;
- piratage – modifier des données de transmission;
- collecte d'adresses – faire la collecte d'adresses électroniques à l'aide d'ordinateurs sans consentement préalable;
- atteintes à la vie privée – utiliser des logiciels espions et des outils semblables pour recueillir ou utiliser les renseignements personnels d'individus par l'accès illégal à leurs systèmes informatiques.

# 2. Partenaires

L'initiative de la LCAP mobilise de multiples partenaires fédéraux aux mandats différents mais complémentaires. Comme l'illustre le diagramme suivant, Innovation, Sciences et Développement économique Canada (ISDE), qui comprend le Bureau de la consommation (BC), supervise l'initiative, tandis que le Conseil de la radiodiffusion et des télécommunications canadiennes (CRTC), le Commissariat à la protection de la vie privée du Canada (CPVP) et le Bureau de la concurrence appliquent différents articles de la Loi ou en rapport avec celle-ci dans d'autre Lois, notamment la Loi sur la protection des renseignements personnels et les documents électroniques, la Loi sur la concurrence et la Loi sur les télécommunications.

## Initiative de la LCAP

### Non-application (ISDE)

**Organe national de coordination (ONC)**

**L'ONC relève de la Direction de la politique sur la vie privée et la protection des données d'ISDE. Il :**

- assure la surveillance des politiques, y compris la surveillance et la production de rapports sur l'efficacité globale du régime
- supervise les activités de communication publique et de sensibilisation

**Bureau de la consommation**

**Le Bureau de la consommation assure la promotion des intérêts et la protection des consommateurs canadiens. Il :**

- coordonne les efforts d'éducation et de sensibilisation des consommateurs et des entreprises
- gère le site Web combattrelepourriel.gc.ca

### Application

**Conseil de la radiodiffusion et des télécommunications canadiennes (CRTC)**

**Le CRTC est un tribunal administratif indépendant du gouvernement fédéral. Il :**

- s'acquitte de ses responsabilités de mise en application et fait enquête sur les violations potentielles aux interdictions de la LCAP relatives à l'envoi de pourriels, à la modification des données de transmission et à l'installation de logiciels sur des systèmes informatiques ou des réseaux sans consentement
- encourage la conformité par de la sensibilisation, des sanctions et des recours en cas d'infraction, comme les sanctions administratives pécuniaires (SAP)
- héberge le Centre de notification des pourriels, lieu central permettant aux gens de signaler des pourriels, de déposer des plaintes et d'alerter les organismes d'application de la loi au sujet d'infractions présumées à la LCAP

**Bureau de la concurrence**

**Le Bureau de la concurrence est un organisme d'application de la loi indépendant. En vertu de modifications à la Loi sur la concurrence, il :**

- s'acquitte de ses responsabilités de mise en application et fait enquête sur les cas d'indications fausses ou trompeuses et les pratiques commerciales trompeuses dans le marché électronique, y compris les indications fausses ou trompeuses contenues dans les renseignements sur l'expéditeur ou dans l'objet d'un message électronique, dans un message électronique et dans un localisateur tel que les URL et les métadonnées
- encourage la conformité par de la sensibilisation, la promotion, et l'application de la Loi. En vertu de la Loi sur la concurrence, les affaires peuvent être réglées par des accords par consentement, des ordonnances de la cour, des amendes et des sanctions administratives pécuniaires

**Commissariat à la protection de la vie privée du Canada (CPVP)**

**Le CPVP est un agent du Parlement. En vertu de modifications à la Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE), il :**

- s'acquitte de ses responsabilités de mise en application et fait enquête sur la collecte et l'utilisation non autorisées d'adresses électroniques au moyen de programmes informatiques et de renseignements personnels des individus par tout moyen d'accès illégal à leurs systèmes informatiques et via tout moyen de télécommunication
- encourage la conformité aux dispositions de la LPRPDE en rapport avec la LCAP par de la sensibilisation et des recours (à l'exclusion des SAP)

# 3. Aperçu des résultats

## Promotion

Les partenaires de la LCAP échangent de l'information visant à promouvoir l'éducation et la conformité à la Loi, comme des FAQ et d'autres conseils pour les Canadiens et les entreprises, sur le site Web combattrelepourriel.gc.ca, sur leurs sites Web respectifs et par l'entremise d'activités d'éducation et de sensibilisation. Les partenaires explorent régulièrement des moyens d'atteindre divers publics tels que des publications officielles, des billets de blogue et les médias sociaux.

En 2020–2021 :

- Le site Web combattrelepourriel.gc.ca a reçu 148 464 visites.
- Le site Web du CRTC lié à la LCAP a fait l'objet de plus de 199 184 pages vues uniques (17 % de plus que l'année précédente) et de 238 250 pages vues (15 % de plus que l'année précédente).
- Les pages Web du CPVP liées à la LCAP ont été consultées plus de 55 983 fois.
- Le Bureau de la concurrence a publié 2 alertes aux consommateurs et aux entreprises en lien avec la LCAP afin de les aider à détecter et à éviter les arnaques courantes.
- Le Centre de notification des pourriels a reçu 285 505 signalements (soit environ 7,5 % de plaintes de moins que l'année précédente).
- Les partenaires en application de la LCAP ont collaboré à la tenue d'une campagne de sensibilisation et à la rédaction d'une lettre conjointe à l'intention de 36 compagnies de l'industrie des applications mobiles pour leur rappeler leurs obligations en matière de conformité à la LCAP.

## Application

Les organismes chargés de faire respecter la LCAP, ou des articles en rapport avec celle-ci, sont le CRTC, le Bureau de la concurrence et le CPVP. Ils ont des outils efficaces pour intervenir en cas de non-conformité, comme des lettres d'avertissement, des procès-verbaux de violation, des engagements et des accords de consentement. Le CRTC peut imposer des sanctions administratives pécuniaires (SAP) et le Bureau de la concurrence peut demander que des SAP soient imposées en vertu d'ordonnance ou d'ententes par consentement, tandis que le CPVP peut faire des recommandations, conclure des accords de conformité avec les répondants et demander des ordonnances de la cour. Ces outils visent à promouvoir et à faire respecter la Loi et ses règlements afférents.

En 2020-2021, le CRTC :

- a rendu 1 décision;
- a conclu 1 engagement assorti d'un montant à payer de 100 000 $;
- a envoyé 1 procès-verbal de violation assorti d'une SAP de 75 000 $;
- a envoyé 400 avis de communication;
- a envoyé 34 ordonnances de préservation;
- a envoyé 12 lettres d'avertissement.

Le Bureau de la concurrence :

- a réglé 1 dossier à l'aide d'un plaidoyer de culpabilité et 2 dossiers à l'aide d'un consentement enregistré assorti d'une SAP;
- a pris des mesures dans 1 dossier pour faire cesser de la publicité fausse ou trompeuse pendant qu'il enquêtait;

- a envoyé plus de 40 lettres d'avertissement à des vendeurs qui donnaient des indications potentiellement fausses ou trompeuses au sujet de la pandémie de COVID-19.

Le CPVP a enquêté sur :

- 1 allégation selon laquelle un logiciel d'outil d'accès à distance (RAT) avait été installé secrètement sur l'ordinateur portatif d'une personne par une entreprise de services informatiques (un rapport a été publié);
- 1 allégation de marketing par courriel non sollicité contre une compagnie d'assurance (résolue par règlement rapide).

# 4. L'environnement

## 4.1 Contexte international

Les entreprises, les gouvernements et les citoyens du monde entier s'efforcent à s'adapter à l'ampleur et au rythme grandissants des changements technologiques. Comme l'a souligné le Centre canadien pour la cybersécurité, la technologie transforme nos sociétés et modifie le contexte des cybermenaces au fur et à mesure de la dépendance croissante du monde à Internet. Un nombre grandissant d'activités quotidiennes importantes telles que les transactions bancaires, les services gouvernementaux, les services de santé, le commerce et l'éducation se font maintenant en ligne pour des raisons de commodité et d'efficacité. Dans le contexte de la COVID-19, cette tendance s'est accélérée pour permettre aux Canadiens de travailler, de magasiner et de socialiser à distance tout en respectant les directives émises par la santé publique. Toutefois, cette transition a également été marquée par l'ouverture de nouvelles possibilités pour, et l'utilisation de nouvelles tactiques par, de cyberacteurs malveillants. Une fois en ligne, les appareils, l'information et les activités deviennent vulnérables aux menaces. En même temps, l'offre de services de cybercriminalité et de rançongiciels sur les marchés du Web invisible a réduit les entraves à l'accès pour de nouveaux acteurs malveillants, ce qui leur a permis de mener plus facilement des cyberattaques. Ces acteurs adaptent leurs activités afin de trouver des informations de valeur, de les obtenir, de les garder en échange d'une rançon ou de les détruire.

Les cybermenaces font fi des frontières nationales et leur omniprésence démontre toute la nécessité pour les agences de mises en applications de la Loi, nationales et internationales, de collaborer pour réduire les problèmes de cybersécurité. Cela témoigne également du rôle essentiel que les partenariats public-privé doivent jouer dans ce domaine. Ainsi, la LCAP s'inscrit dans une vaste gamme de cadres juridiques et stratégiques nationaux et internationaux dans les domaines du spectre, des télécommunications, de la protection de la vie privée et de la cyberrésilience, y compris la cybersécurité. La LCAP aide à maintenir un cadre de protection de la vie privée et des données qui fournit des mécanismes permettant d'améliorer l'interopérabilité à l'échelle nationale et internationale à l'aide de lois sur la protection de la vie privée et la protection électronique.

## 4.2 Tendances, indicateurs et défis

Le contexte des cybermenaces évolue au Canada, et les auteurs de cybermenaces continuent de s'adapter à l'évolution de l'environnement. Tel que décrit précédemment, la pandémie de COVID-19 a incité ces acteurs à innover et à trouver de nouvelles façons de lancer des attaques. Durant la pandémie, selon le rapport *Internet Organised Crime Threat Assessment 2020* d'Europol, les contrevenants ont conçu de nouveaux modus operandi et adapté ceux qui existaient pour exploiter la situation et cibler de nouvelles victimes. Par exemple, ces acteurs ont peaufiné les formes existantes d'infractions liées à cybercriminalité pour les adapter à la pandémie et ont exploité l'incertitude de la situation et la soif d'information du public. Les courriels malveillants, les pièces jointes, les sites Web sur le thème de la pandémie et même les fausses applications de recherche de personnes risquant d'avoir été exposées à la COVID-19 étaient monnaie courante.

Toutefois, le comportement opportuniste des cyberacteurs malveillants durant la pandémie ne devrait pas éclipser le contexte global des cybermenaces. Dans bien des cas, la pandémie de COVID-19 a amplifié les faiblesses de sécurité existantes, qui se sont accentuées et multipliées lorsqu'un nombre important de personnes ont commencé à travailler à domicile. Il s'est fait un nombre record de cyberattaques en 2020.

En 2020, au Canada :

- La plupart des Canadiens (87 %) étaient préoccupés par la protection de leur vie privée; 70 % ont refusé de fournir leurs renseignements personnels à une organisation ou à une entreprise pour des raisons liées à la protection de la vie privée; et 74 % ont ajusté les paramètres de confidentialité d'un compte de médias sociaux.
- Le commerce électronique est devenu le principal moyen de magasiner des Canadiens, et les cyberboutiques sont devenues les cibles les plus fréquentes des attaques par hameçonnage (18 %).
- 40 % des Canadiens ont supprimé un compte de médias sociaux pour des raisons liées à la protection de la vie privée ou ont cessé de faire affaire avec une entreprise qui a subi une atteinte à la vie privée.
- Les organisations étaient moins susceptibles d'informer un organisme de réglementation d'une atteinte à la protection des données, à peine 36 % l'ayant fait (comparativement à 58 % en 2019).
- On estime que les paiements de rançon et la perte de productivité attribuables aux rançongiciels ont coûté 5 milliards de dollars aux organisations canadiennes.

En 2020, à l'échelle mondiale :

- 50 % des courriels, soit 6 % de moins qu'en 2019, étaient des pourriels.
- 85 % de toutes les organisations ont fait l'objet d'au moins une attaque d'hameçonnage.
- 95 % de toutes les attaques visant les réseaux d'entreprise ont été causées par des tentatives réussies de harponnage ciblé.
- 30 % des courriels d'hameçonnage ont été ouverts par les utilisateurs, et 12 % de ces utilisateurs ciblés ont cliqué sur le lien malveillant ou sur la pièce jointe malveillante.
- Environ 1,5 million de nouveaux sites d'hameçonnage ont été créés chaque mois.
- Le nombre de courriels d'hameçonnage renfermant une forme quelconque de rançongiciel s'est accru de 97 %.
- 80 % des pourriels reçus par les internautes en Amérique du Nord et en Europe peuvent être attribués à une centaine d'opérations de pourriels répertoriées dans la base de données du Spamhaus Project's Register of Known Spam Operations (en anglais seulement).
  - En 2020, aucune n'était canadienne, ce qui signifie que la plupart des attaques ciblant des Canadiens proviennent de l'extérieur du pays.
  - Aucune opération provenant du Canada ne figurait dans la base de données Spamhaus ou dans la liste 10 Worst Spammers (en anglais seulement).
  - Le Canada ne figurait pas dans les listes 10 Worst Spam Countries (en anglais seulement) ou 10 Worst Botnet Countries (en anglais seulement) de Spamhaus.

# 5. Les résultats

## 5.1 Politiques et coordination

### Organe national de coordination

L'Organe national de coordination (ONC) se tient au fait des derniers développements dans les domaines du pourriel, des menaces en ligne, de la cybersécurité et du commerce électronique en effectuant des analyses de renseignement stratégique, menant des recherches et analysant les paramètres et les tendances. Il travaille également avec des partenaires nationaux et internationaux en vue d'harmoniser les cadres législatifs et réglementaires avec les pratiques exemplaires internationales en matière de lutte contre le pourriel et les logiciels malveillants.

En 2020-2021, l'ONC a :

- a collaboré à l'élaboration du *Rapport de mesure du rendement 2019-2020* de la LCAP avec tous les partenaires de celle-ci;
- a participé au Messaging Malware Mobile Anti-Abuse Working Group (M3AAWG) – un forum international sur le pourriel – aux côtés de ses partenaires canadiens;
- a informé et conseillé ISDE (le département responsable de la LCAP) au sujet de tous les développements liés à la gestion et aux politiques de la LCAP;
- a coordonné les activités de gouvernance de la LCAP, comme le Comité des directeurs généraux et les groupes de travail, et collaboré avec les partenaires de la LCAP pour discuter de politiques et de stratégies;
- a collaboré avec les partenaires de la LCAP pour mettre à jour le site Web combattrelepourriel.gc.ca,
- a collaboré avec les partenaires de la LCAP pour mieux faire connaître l'initiative de la LCAP en coordonnant les activités afférentes de communication, d'éducation et de sensibilisation.

## 5.2 Promotion de la conformité

### Bureau de la consommation

Le Bureau de la consommation gère les produits de communication de la LCAP destinés aux particuliers et aux entreprises du Canada, y compris combattrelepourriel.gc.ca, le site Web de la LCAP.

En 2020-2021, le Bureau de la consommation a régulièrement mis à jour la page Nouvelle sur les pourriels de combattrelepourriel.gc.ca en en y ajoutant des liens vers les derniers rapports des partenaires de la LCAP et les plus récentes mesures d'application de la loi de ceux-ci. Le Bureau s'est aussi assuré de l'entretien courant du site Web, y compris en mettant son contenu à jour, en y corrigeant les liens brisés et en y ajoutant des messages d'alerte liés à la COVID-19.

Combattrelepourriel.gc.ca fait la promotion d'informations liées à la LCAP. En 2020-2021, le site Web a reçu 148 464 visites.

### Conseil de la radiodiffusion et des télécommunications canadiennes

En complément de combattrelepourriel.gc.ca, le site Web du CRTC fournit également de l'information sur la LCAP aux Canadiens et aux intervenants pour qu'il soit plus facile à chacun d'obtenir l'aide requise. L'expérience en ligne comprend des alertes, des vidéos, des infographies, des politiques et des lignes directrices faciles à consulter visant à renseigner les Canadiens sur la LCAP et pour aider les entreprises à s'y conformer. Le CRTC éduque et informe également les intervenants et les Canadiens par l'entremise de ses plateformes de médias sociaux.

En 2020-2021, le CRTC :

- a publié 28 gazouillis (qui ont généré 5847 impressions) et 60 partages;
- a téléchargé sur Facebook 12 messages qui ont généré 61 889 impressions et qui ont été republiés 19 fois;
- a publié sur LinkedIn 12 messages qui ont généré 8 232 impressions;
- a interagi plus de 24 fois avec des intervenants dans le cadre d'activités générales de sensibilisation, de rencontres vidéo, de séances d'information des partenaires par vidéo, de présentations par vidéoconférence et de webinaires;
- a participé à des séances de clavardage hebdomadaires sur Twitter pendant le Mois de la prévention de la fraude (mars) afin de sensibiliser les consommateurs et les entreprises aux méthodes de prévention de la fraude;
- a tenu une discussion informelle avec le cadre en chef de la conformité et des enquêtes du CRTC au sommet canadien sur le courriel;
- a fait une présentation à et échangé des idées avec le Canadian University Council of Chief Information Officers;
- a publié des mises à jour des documents d'orientation du CRTC concernant l'article 8 de la LCAP (exigences concernant l'installation de programmes informatiques);
- a publié 2 tableaux de bord d'application de la LCAP sur son site Web;
- a publié 2 résumés de cas relatifs à un procès-verbal de violation et à un engagement;
- a publié un communiqué annonçant les résultats d'une enquête importante sur une campagne de pourriels de type « hailstorm » (consistant à envoyer un très grand nombre de courriels sur une courte période avant que les filtres antipourriel ne puissent réagir et les bloquer);
- a mis à jour les messages sur son site Web et dans les médias sociaux afin d'inclure les arnaques liées à la pandémie de COVID-19.

En raison des restrictions engendrées par la pandémie de COVID-19, l'équipe de Conformité et Enquêtes du CRTC a communiqué virtuellement avec les entreprises, les associations et les organisations pour les sensibiliser à l'application de la LCAP aux communications non sollicitées.

En février 2021, le CRTC a participé, avec ses partenaires du Centre antifraude du Canada, du Bureau de la concurrence et de la GRC, à une séance de clavardage hebdomadaire sur Twitter afin de sensibiliser les consommateurs et les entreprises aux méthodes de prévention de la fraude.

### Bureau de la concurrence

Le Bureau de la concurrence a recours à plusieurs moyens importants pour sensibiliser le plus grand nombre possible de consommateurs et d'entreprises au Canada à certains enjeux liés à la LCAP.

En 2020-2021, le Bureau :

- a publié 2 alertes aux consommateurs et aux entreprises en lien avec la LCAP afin de les aider à détecter et à éviter des fraudes liées à la non-livraison et des arnaques courantes visant les entreprises;
- a lancé un avertissement général à l'industrie de ne pas donner d'indications fausses ou trompeuses voulant que leurs produits et services puissent prévenir, traiter ou guérir la COVID-19, demandant à toutes les entreprises d'examiner leur marketing et leur étiquetage et de se conformer immédiatement;
- a publié 146 gazouillis, 90 messages sur Facebook et 60 messages sur LinkedIn pour éduquer les Canadiens au sujet des pratiques commerciales trompeuses, les mettre en garde contre les arnaques en ligne et les encourager à signaler les pratiques trompeuses et à être vigilants lorsqu'ils sont en ligne;
- a coprésidé le Mois de la prévention de la fraude avec la GRC et le Centre antifraude du Canada pour sensibiliser à la fraude en ligne.

### Commissariat à la protection de la vie privée du Canada

Le CPVP a continué de fournir des conseils de conformité à la LCAP aux entreprises et aux particuliers par différents canaux. Il utilise principalement la page La Loi canadienne anti-pourriel (LCAP) pour informer les particuliers et les entreprises. Il s'agit d'ailleurs de son moyen le plus efficace de promouvoir les activités liées à la LCAP.

Le CPVP a également mené des activités de sensibilisation à la LCAP tout au long de l'année telles que : le partage de contenu sur les médias sociaux et l'organisation d'une campagne de sensibilisation des entreprises ainsi que l'envoi d'une lettre à celles-ci; la publication et la distribution de matériel éducatif; et la diffusion de messages radiophoniques partout au pays. En raison de la pandémie, certaines activités de sensibilisation telles que les promotions en personne et les expositions ont été suspendues.

En 2020-2021, le CPVP s'est associé à l'Agence du revenu du Canada pour envoyer par la poste un encart imprimé au sujet de la LCAP à 477 350 petites et moyennes entreprises du Canada inscrites au « Compte de programme d'employeur ». L'objectif était d'informer les entreprises au sujet des pourriels et des menaces de cybermarketing, comme ceux liés au courriel, à la messagerie instantanée et aux médias sociaux, y compris la collecte de messages électroniques. La campagne visait également à resserrer la conformité des entreprises à la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE) et à la LCAP.

Le CPVP :

- a imprimé un nouveau guide intitulé Guide sur la protection de la vie privée à l'intention des entreprises comprenant une section au sujet de la LCAP.
- a répondu à 45 demandes de renseignements sur la LCAP, le plus souvent sur le consentement, de la part de particuliers et d'entreprises.

## 5.3 Coopération internationale et nationale

### Conseil de la radiodiffusion et des télécommunications canadiennes

À l'instar de ses partenaires de la LCAP, le CRTC a forgé des partenariats avec des organisations du monde entier afin de mieux remplir son mandat. La Commission continue de faire partie du Unsolicited Communications Enforcement Network (UCENet). Les membres de celui-ci proviennent plus de 26 pays et travaillent ensemble à promouvoir la coopération internationale en matière de lutte contre les pourriels et à s'attaquer aux problèmes liés aux pourriels et aux télécommunications non sollicitées.

En 2020-2021, le CRTC s'est associé au CPVP et au Bureau de la concurrence dans le cadre de la première initiative conjointe de conformité à la LCAP. Les partenaires d'application de la LCAP ont envoyé des lettres à 36 entreprises de l'industrie des applications mobiles au Canada afin de leur rappeler leurs obligations en vertu des lois fédérales. Les lettres insistaient sur le fait que les entreprises qui offrent des applications doivent veiller à ce que leurs produits respectent la LCAP. Cette initiative comprenait également une campagne de sensibilisation à l'intention des consommateurs qui a atteint environ 77 500 personnes dans les médias traditionnels et 40 918 dans les médias sociaux, avec 2 238 visites sur le site Web.

Cette initiative visait à soulever des préoccupations concernant :

- des applications comportant des indications fausses ou trompeuses visant à promouvoir un produit, un service ou un intérêt commercial;
- des applications qui recueillent ou utilisent des renseignements personnels, comme les logiciels malveillants d'enregistrement de frappe, sans consentement;
- des applications qui ne décrivent pas de manière appropriée leurs fonctions afin d'obtenir le consentement éclairé de l'utilisateur avant l'installation;
- des applications conçues pour envoyer des pourriels aux amis et aux contacts de l'utilisateur.

Ces activités exposent les Canadiens à des risques de fraude, de vol d'identité et de perte financière, entre autres problèmes. Les 36 entreprises offrant des applications mobiles sont particulièrement bien placés pour détecter et prévenir de telles pratiques et pour empêcher qu'elles nuisent aux consommateurs.

Enfin, la lettre encourageait les entreprises à passer en revue leurs pratiques et à prendre des mesures de prévention et de correction au besoin.

## Bureau de la concurrence

En plus de répondre aux demandes d'aide provenant de l'étranger, le Bureau demeure actif auprès d'un certain nombre de partenaires et de groupes de travail internationaux et nationaux, dont :

- l'Organisation de coopération et de développement économiques
- le Réseau mondial de lutte contre la fraude, anciennement connu sous le nom de Groupe de travail international sur la fraude par marketing de masse
- le Centre antifraude du Canada, équipe de cogestion
- le Partenariat stratégique de Toronto
- le Partenariat de l'Alberta contre la fraude transfrontalière
- le Partenariat du Pacifique contre la fraude transfrontalière
- l'International Consumer Protection Enforcement Network (ICPEN)

L'ICPEN est un réseau d'organismes de protection des consommateurs et d'application de la loi de plus de 65 pays dont l'objectif est de protéger les consommateurs en encourageant la coopération mondiale entre les organismes d'application de la loi et l'échange d'information au sujet des défis transfrontaliers qui touchent les consommateurs.

Le 1er juillet 2020, le Bureau a commencé son mandat d'un an à la présidence de l'ICPEN. Durant l'année qui s'est écoulée, le Bureau et d'autres membres de l'ICPEN ont exploré des moyens de dissuader le recours à des pratiques commerciales trompeuses en mettant l'accent sur les thèmes suivants :

- examen des pratiques exemplaires mondiales en matière de protection des consommateurs et d'enquêtes à distance afin de mieux s'adapter aux activités commerciales trompeuses et frauduleuses liées à la pandémie de COVID-19;
- exploration des avantages et des inconvénients de l'intelligence artificielle (IA), qui peut être à la fois un puissant outil d'enquête et un moyen pour les entreprises de tromper les consommateurs;
- examen des défis de mise en application, des préoccupations en matière de confidentialité des données et de la responsabilité des tiers relativement aux plateformes numériques;
- examen des moyens de lutter contre les activités trompeuses qui tentent d'exploiter les préoccupations environnementales des consommateurs.

De plus, en tant que président de l'ICPEN, le Bureau a tenu en février 2021 une série de quatre webinaires sur les pratiques exemplaires, dont une sur la protection des données des consommateurs en collaboration avec le CPVP par l'entremise du Global Privacy Enforcement Network (GPEN).

## Commissariat à la protection de la vie privée du Canada

Tout au long de 2020-2021, les organismes d'application de la LCAP ont travaillé avec leurs pendants nationaux et internationaux à promouvoir le respect de celle-ci. Étant donné la nature sans frontières de l'Internet, les violations de la LCAP peuvent provenir de l'extérieur des frontières canadiennes. Par conséquent, la coopération internationale est souvent nécessaire pour enquêter sur les menaces en ligne. Il est essentiel d'échanger des renseignements et de collaborer avec des gouvernements et des organismes étrangers pour assurer la prise de mesures efficaces et cohérentes à l'échelle mondiale à l'égard des contrevenants à la LCAP.

En avril 2011, la LCAP a modifié des dispositions de la LPRPDE, ce qui a permis au CPVP de collaborer et d'échanger de l'information avec ses pendants provinciaux et internationaux chargés de la protection des données. Depuis, le CPVP a pris un certain nombre de mesures d'application conjointes et concertées avec des partenaires en concluant des protocoles d'entente avec eux et en participant à des réseaux de réglementation. En fait, une telle collaboration est maintenant la façon normale de faire les choses. En témoignent les nombreuses enquêtes concertées qui ont été lancées ou réalisées au cours de la dernière année (voir la section 5.5, Application de la loi, Commission à la protection de la vie privée du Canada).

Le CPVP est membre du comité exécutif du GPEN. À ce titre, il participe à des activités concertées d'application de la loi, héberge et administre le site Web du GPEN et prend part aux téléconférences mensuelles et aux réunions du réseau au sujet de la protection de la vie privée.

- En mars 2021, les membres du GPEN (y compris le CPVP) ont collaboré avec l'ICPEN à la tenue du tout premier atelier conjoint sur les pratiques exemplaires. Cet événement virtuel réunissait des praticiens internationaux de l'application de la loi des deux sphères de réglementation venus discuter du recoupement important entre la protection de la vie privée et la protection des consommateurs et explorer des stratégies visant à faire progresser la

coopération intersectorielle en matière d'application de la réglementation.

- La toute première activité de collaboration entre le GPEN et l'ICPEN, dans le cadre de laquelle le GPEN a approuvé l'envoi d'une lettre de 27 organismes de l'ICPEN à l'intention d'Apple et de Google, a porté fruit en 2020-2021, les deux entreprises ayant apporté des changements pour améliorer l'information que les applications fournissent aux utilisateurs sur la façon dont leurs données sont recueillies et utilisées.
- En réponse à la pandémie de COVID-19, le GPEN a tenu une discussion virtuelle et un sondage subséquent afin de jauger l'impact de celle-ci sur les activités des autorités de protection des données et d'échanger sur les moyens d'appliquer la loi pendant la pandémie et au sortir de celle-ci.

La Global Privacy Assembly (GPA), auparavant appelée International Conference of Data Protection and Privacy Commissioners, est un forum à l'intention des autorités de protection de la vie privée et des données du monde entier.

- En octobre 2020, le CPVP a assisté à la 42e conférence virtuelle de la GPA et y a fait une présentation.
- Le CPVP copréside également l'International Enforcement Collaboration Working Group (IEWG) de la GPA, dont les membres travaillent à faire progresser la coopération en matière d'application de la loi dans le monde et à établir des mesures pratiques à l'appui. En 2020-2021, l'IEWG a organisé plusieurs réunions virtuelles entre les autorités de la protection de la vie privée afin de discuter et d'échanger sur des questions telles que les applications de dépistage de la COVID-19, la technologie de reconnaissance faciale et le bourrage de justificatifs (une forme courante de cyberattaque).
- En juillet 2020, le CPVP et cinq autres membres de la GPA, réunis par l'entremise de l'IEWG, ont publié une déclaration commune sur les attentes mondiales en matière de protection de la vie privée à l'endroit des entreprises de vidéoconférence. Bien que destinée à toutes ces entreprises, la lettre a été envoyée directement à cinq d'entre elles. Quatre y ont répondu en décrivant les mesures qu'elles avaient prises pour se conformer aux exigences en matière de protection des données et de la vie privée. Les signataires conjoints ont publié une déclaration mise à jour en décembre 2020 et recommuniqueront avec chacune de ces entreprises pour mieux comprendre leurs plateformes et leurs pratiques de protection de la vie privée en 2021-2022.
- Le CPVP copréside également le groupe de travail Citoyens et consommateurs numériques, composé de 13 membres, de la GPA. Ce groupe étudie l'intersection de la protection de la vie privée et de la protection des données et l'intersection de la protection des consommateurs et des mesures de protection antitrust en plus de promouvoir la coopération entre ces sphères de réglementation. En 2020-2021, il a donné une présentation et animé des séances en petits groupes lors du tout premier atelier conjoint de l'ICPEN et du GPEN sur les pratiques exemplaires. Il a également réalisé des entrevues auprès d'organismes de réglementation de la concurrence afin d'obtenir des renseignements sur l'intersection entre la protection de la vie privée et la réglementation de la concurrence et a commandé un examen indépendant des recherches universitaires sur cette intersection.

Le CPVP est membre du UCENet, qui n'a pas tenu d'assemblée annuelle en 2020. Mais le CPVP a participé à des appels des membres en plus d'assister à la réunion annuelle virtuelle du Messaging, Malware and Mobile Anti-Abuse Working Group en octobre. L'événement réunissait également des organismes de réglementation de lutte contre le pourriel, de protection des consommateurs et des télécommunications et des experts en sécurité des TI.

En juin et en décembre 2020, le CPVP a participé aux 53e et 54e forums des autorités de protection de la vie privée de l'Asie-Pacifique. Les participants au 53e forum se sont penchés sur les défis en matière de protection de la vie privée que présentent la pandémie de COVID-19, les renseignements biométriques et les questions entourant la notification des atteintes à la sécurité des données. Lors du 54e forum, ils ont continué d'examiner les répercussions de la pandémie sur la vie privée et ont discuté de la technologie de reconnaissance faciale, de l'IA et de l'avenir des cadres de protection de la vie privée.

Enfin, lors d'un webinaire sur la COVID-19 organisé par les autorités en septembre 2020, le CPVP a présenté les techniques qu'il utilise pour tirer parti des outils virtuels et continuer de collaborer avec d'autres organismes par l'entremise de l'IEWG durant la pandémie.

## 5.4 Surveillance de la conformité

### Conseil de la radiodiffusion et des télécommunications canadiennes

Le CRTC héberge le Centre de notification des pourriels (CNP), qui recueille des renseignements pouvant servir de preuve d'infractions potentielles à la LCAP.

En 2020-2021 :

- les Canadiens ont fait 285 505 signalements au Centre, soit 7,5 % de moins que l'année précédente;
- 8 413 de ces signalements ont été faits à l'aide du formulaire Web et 277 092 l'ont été par retransmission de courriels.

Les signalements par les Canadiens sont importants, en particulier lorsqu'ils sont faits par l'entremise du formulaire Web, car les renseignements ainsi obtenus sont généralement plus détaillés. Le CRTC utilise ces renseignements pour :

- analyser les données recueillies au sujet des plaintes et effectuer des analyses de l'environnement;
- cerner les tendances et les menaces;
- lancer des enquêtes et prendre des mesures d'application de la loi.

Par exemple, l'analyse des données du CNP a permis au CRTC de détecter une campagne de pourriels de type « hailstorm » durant laquelle une personne envoyait un très grand nombre de courriels sur une courte période avant que les filtres antipourriel ne puissent réagir et bloquer les messages.

### Bureau de la concurrence

L'Unité de vérification de la conformité de la Direction des pratiques commerciales trompeuses du Bureau de la concurrence suit les dossiers – y compris ceux liés à la LCAP – qui ont été réglés au moyen d'accords de consentement, d'ordonnances de détermination de la peine, d'autres instruments de résolution ou d'autres ordonnances des tribunaux.

### Commissariat à la protection de la vie privée

L'Unité de la vérification de la conformité du CPVP continue de collaborer avec les organisations pour veiller à ce qu'elles honorent les engagements qu'elles ont pris envers le Commissariat et prennent des mesures satisfaisantes pour donner suite aux recommandations de celui-ci découlant de rapports de conclusions et d'accords de conformité.

## 5.5 Application de la loi

### Conseil de la radiodiffusion et des télécommunications canadiennes

Le CRTC est chargé d'assurer la conformité aux articles 6 à 9 de la LCAP. Il a le pouvoir de mener des enquêtes et de prendre des mesures contre les contrevenants et il peut fixer des SAP.

En général, le CRTC se concentre sur ceux qui envoient des messages électroniques commerciaux sans le consentement du destinataire ou qui installent des programmes sur des ordinateurs ou des réseaux sans consentement. Cela comprend les programmes informatiques malveillants, les pourriels et les hyperliens infectés.

Le CRTC publie ses mesures d'exécution de la loi. En 2020-2021, comme le mentionne la section 3, Aperçu des résultats, celles-ci comprenaient :

- 1 décision;
- 1 engagement assorti d'un montant à payer de 100 000 $;
- 1 procès-verbal de violation assorti d'une SAP de 75 000 $;
- 400 avis de communication;
- 34 ordonnances de préservation;
- 12 lettres d'avertissement.

En juin 2020, le CRTC a publié la Décision de Conformité et Enquêtes CRTC 2020-196, qui confirmait l'obligation pour Hydro-Québec de fournir des renseignements liés à 10 adresses de service et aux comptes clients associés.

En septembre 2020, le CRTC a publié un engagement comprenant un montant à payer de 100 000 $ et la mise en œuvre d'un programme de conformité en relation avec des violations présumées à la LCAP. Le CRTC a conclu une entente avec Notesolution Inc. (qui fait affaire sous le nom de OneClass) pour régler les violations présumées. OneClass a accepté de faire un paiement de 100 000 $ et s'est engagé à élaborer et à mettre en œuvre un programme de conformité à la LCAP.

En mars 2021, le CRTC a imposé la sanction la plus importante en vertu de la LCAP à ce jour à une personne. À la lumière des renseignements recueillis au cours de l'enquête, le cadre en chef de la conformité et des enquêtes a donné un procès-verbal de violation assorti d'une SAP de 75 000 $ à Scott William Brewer pour avoir envoyé des messages électroniques commerciaux sans le consentement des destinataires.

## Bureau de la concurrence

Le Bureau de la concurrence est chargé de faire appliquer la Loi de la concurrence et de mener des enquêtes dans les cas d'indications électroniques fausses ou trompeuses et de pratiques commerciales trompeuses sur le marché électronique.

En 2020-2021, comme le mentionne la section 3, Aperçu des résultats, le Bureau :

- a réglé 1 dossier à l'aide d'un plaidoyer de culpabilité et 2 dossiers à l'aide d'un consentement enregistré assorti d'une SAP;
- a pris des mesures dans 1 dossier pour faire cesser de la publicité fausse ou trompeuse pendant qu'il enquêtait;
- a envoyé plus de 40 lettres d'avertissement à des vendeurs qui donnaient des indications potentiellement fausses ou trompeuses au sujet de la pandémie de COVID-19.

Le 13 mai 2020, à la suite de mesures judiciaires prises par le Bureau, NuvoCare Health Sciences et son président-directeur général, Ryan Foley, ont accepté de conclure un consentement temporaire interdisant à l'entreprise de donner des indications non fondées relativement à la perte de poids et à l'effet brûle-graisse lors de la promotion de certains produits de santé naturels, dont « WheightOFF Max! » et « Forskolin Nx ».

Le 19 mai 2020, le Bureau est parvenu à une entente avec Facebook après avoir conclu que l'entreprise avait donné des indications fausses ou trompeuses au sujet de la protection des renseignements personnels des Canadiens sur Facebook et Messenger.

Le 28 janvier 2021, à la suite de mesures judiciaires prises par le Bureau, une entreprise canadienne faisant affaire sous le nom de Revive You Media (1806369 Alberta Limited), a plaidé coupable devant la Cour provinciale de l'Ontario d'avoir fait la promotion d'offres trompeuses pour des essais gratuits de compléments alimentaires et de suppléments de santé, qui piégeaient en fait les consommateurs dans un abonnement mensuel. L'entreprise a écopé d'une amende de 15 millions de dollars.

Le 24 février 2021, le Bureau a enregistré un consentement conclu avec l'exploitant de FlightHub.com et de JustFly.com pour résoudre les préoccupations du Bureau quant aux pratiques commerciales de celui-ci. Le Bureau a conclu que les agences de voyages en ligne avaient facturé aux consommateurs des frais cachés, rédigé des évaluations positives de consommateurs afin de promouvoir leurs services et donné de nombreuses indications fausses ou trompeuses au sujet de leurs prix et de services. Cela s'est traduit par une SAP de 5 millions de dollars pour FlightHub Group Inc. et par une SAP de 400 000 $ pour chacun de ses deux directeurs, Matthew Keezer and Nicholas Hart.

Enfin, le Bureau a envoyé plus de 40 lettres d'avertissement à des vendeurs qui donnaient des indications potentiellement fausses ou trompeuses au sujet de la COVID-19. Les avertissements visaient, entre autres, des indications concernant des masques, des aliments et des produits naturels de même que des produits de ventilation et de purification d'air. La plupart des entreprises ont pris des mesures correctives en retirant des étalages les produits soulevant des préoccupations ou en mettant fin à leurs indications.

## Commissariat à la protection de la vie privée

En 2020-2021, le CPVP a reçu deux nouvelles plaintes potentielles liées à la LCAP. Dans un cas, le dossier a été fermé au moment de sa réception, n'étant pas du ressort du CPVP, tandis que dans l'autre, le dossier a fait l'objet d'un règlement rapide.

Comme le mentionne brièvement la section 3, Aperçu des résultats, le CPVP a réalisé des enquêtes sur :

- 1 allégation selon laquelle un logiciel d'outil d'accès à distance (RAT) avait été installé secrètement sur l'ordinateur portatif d'une personne par une entreprise de services informatiques (un rapport a été publié);
- 1 allégation de marketing par courriel non sollicité contre une compagnie d'assurance (résolue par règlement rapide).

En 2011, la LCAP a modifié des dispositions de la LPRPDE et permis ainsi au CPVP de collaborer et d'échanger de l'information plus facilement avec d'autres autorités provinciales et internationales de protection des données sur des questions liées à la conformité et à l'application de la loi.

Malgré l'impact de la pandémie tout au long de 2020-2021, le CPVP a multiplié ses efforts visant à échanger de l'information et à collaborer avec ses pendants nationaux chargés de protéger la vie privée. Il a continué à collaborer sur des questions d'intérêt commun avec le Commissariat à l'information et à la protection de la vie privée de l'Alberta (CIPVP ALB), le Commissariat à l'information et à la protection de la vie privée de la Colombie-Britannique (CIPVP C.-B.), la Commission d'accès à l'information du Québec (CAI) et le Bureau du commissaire à l'information et à la protection de la vie privée de l'Ontario (BCIPVP), y compris un nombre sans précédent d'enquêtes conjointes, en l'occurrence :

- En juin 2020, le CPVP, de concert avec le CPVP ALB, le CIPVP C.-B. et la CAI, a lancé une enquête conjointe sur une application mobile de Tim Hortons à la suite de préoccupations soulevées par les médias quant à la manière dont cette application pourrait recueillir et utiliser les données sur les déplacements des personnes alors qu'elles vaquent à leurs occupations quotidiennes. Cette enquête était toujours en cours à la fin de l'exercice.
- En octobre 2020, le CPVP, le CIPVP C.-B. et le CIPVP ALB ont publié leurs conclusions dans l'affaire de l'utilisation par Cadillac Fairview de caméras discrètes dans les bornes d'orientation numérique du centre commercial. Les caméras avaient recueilli 5 millions d'images de clients et utilisé la technologie de reconnaissance faciale pour chercher à déterminer leur âge et leur sexe.
- En décembre 2020, le CPVP et ses homologues à la Commission de l'accès à l'information du Québec (la « CAI ») ont publié les conclusions d'enquêtes distinctes mais coordonnées sur une atteinte importante à la vie privée chez Desjardins.
- En février 2021, de concert avec le CIPVP ALB, le CIPVP C.-B. et la CAI, le CPVP a annoncé les résultats d'une enquête conjointe sur l'application de reconnaissance faciale de Clearview AI. Il s'agissait de sa première enquête menée conjointement avec les trois provinces en vertu de leurs lois respectives sur la protection des renseignements personnels applicables au secteur privé.
- Enfin, en mars 2021, le CPVP a publié les conclusions de son enquête sur la conformité de CoreFour Inc. à ses propres mesures de sécurité, mesures de déclaration et de notification d'atteintes et pratiques en matière de responsabilité concernant Edsby, son application d'apprentissage de la maternelle à la 12e année. Au cours de l'enquête, le CPVP a communiqué des renseignements au BCIPVP, qui menait une enquête distincte mais complémentaire sur un conseil scolaire provincial qui avait adopté Edsby.

Au cours de l'exercice écoulé, le CPVP a échangé de l'information et collaboré avec divers pendants internationaux, dont le Commissariat à l'information du Royaume-Uni, la Federal Trade Commission des États-Unis et le Commissariat à l'information de l'Australie, à la réalisation d'une gamme d'activités de conformité. Cela comprenait des enquêtes actives et confidentielles de portée internationale du CPVP.

## Résumé

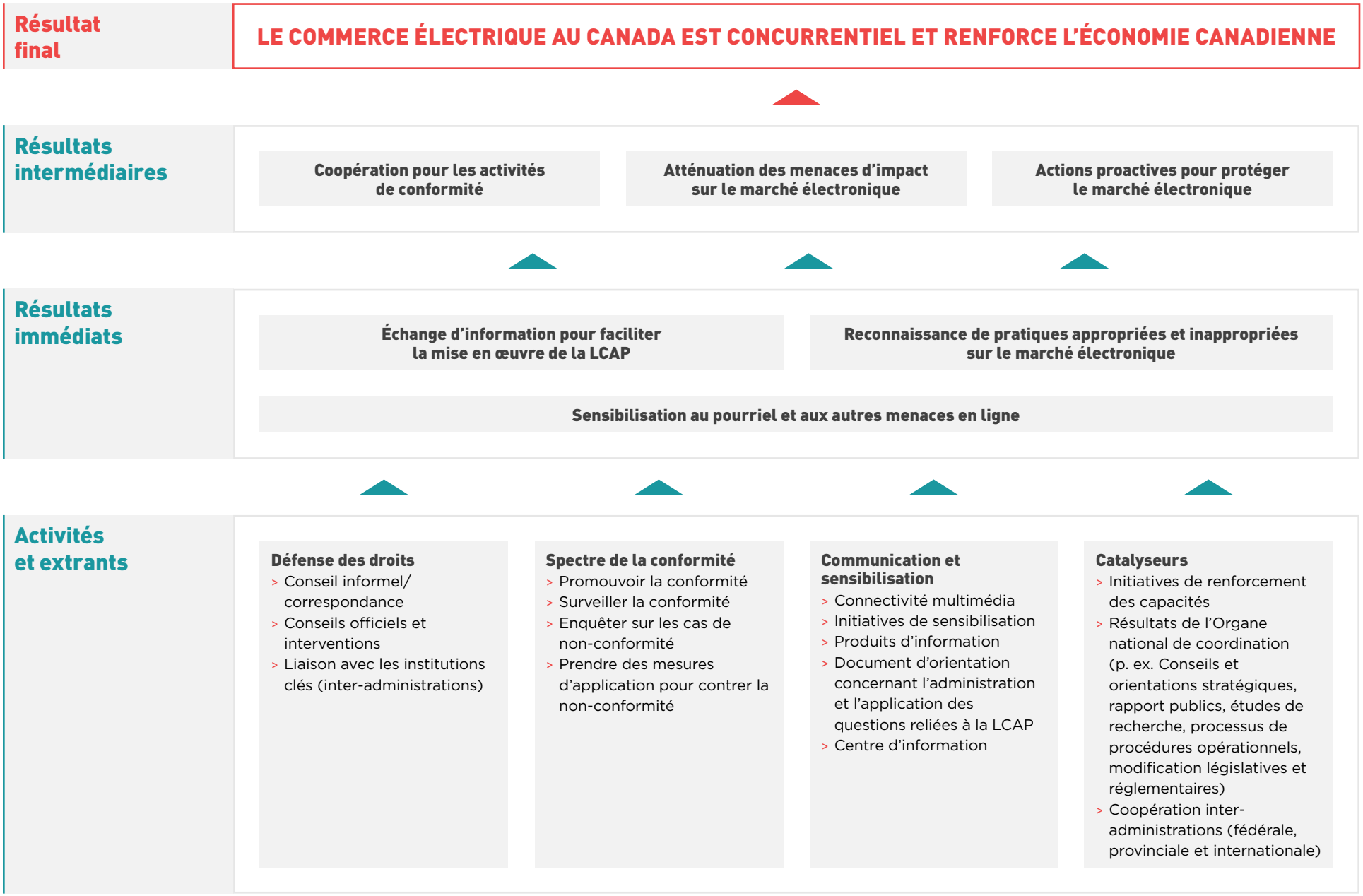
Dans un contexte de cybermenaces en constante évolution, la LCAP continue d'aider à protéger les Canadiens contre les pourriels et les autres menaces électroniques qui mènent au harcèlement, au vol d'identité et à la fraude, tout en veillant à ce que les entreprises puissent continuer d'être concurrentielles sur le marché mondial en établissant des règles conformes aux pratiques exemplaires internationales et aux lois anti-pourriel.

L'année 2020 a été une année record en termes de cyberattaques. Dans de nombreux cas, la pandémie de COVID-19 a amplifié les faiblesses existantes en matière de sécurité, et les cybermenaces sont devenues plus importantes et plus nombreuses à mesure que les gens transitionnaient vers le travail à distance. De plus, l'avènement de la cybercriminalité en tant que service a réduit les obstacles d'entrée à de nouveaux acteurs malveillants, ce qui leur a permis de mener plus facilement des cyberattaques. L'omniprésence des cybermenaces démontre à quel point il est nécessaire que les autorités nationales et internationales coopèrent pour atténuer les problèmes de cybersécurité, ce que les partenaires de la LCAP ont toujours fait avec succès.

En 2020-2021, les partenaires de la LCAP ont continué d'assurer l'efficacité du régime de la LCAP pour lutter contre les pourriels, les logiciels malveillants, les pratiques commerciales trompeuses, le piratage, la collecte d'adresses et les atteintes à la vie privée en ligne. Les partenaires de la LCAP ont entrepris de nombreuses actions unilatérales et collaboratives pour promouvoir la sensibilisation et la conformité à la LCAP. Ils ont également continué à forger des partenariats avec des organisations du monde entier pour mieux remplir leur mandat respectif.

Le présent rapport de performance souligne les résultats des efforts des partenaires de la LCAP. De grands progrès ont été réalisés en 2020-2021 et les partenaires de la LCAP continueront de bâtir une initiative de la LCAP encore plus efficace.

# Annexe A : Modèle logique de la LCAP



## Description

L'annexe présente un modèle logique de la LCAP. Un modèle logique montre la façon dont les activités de programme sont censées produire des extrants et dont ceux-ci devraient permettre d'obtenir différents niveaux de résultats.

Il y a quatre séries d'activités et d'extrants :

1. La défense des droits, soit les conseils informels ou la correspondance, les conseils officiels et les interventions, et la liaison avec des institutions clés (à l'échelle pangouvernementale)
2. Le spectre de la conformité, soit la promotion de la conformité, la surveillance de la conformité, la tenue d'enquêtes sur les cas de non-conformité et la prise de mesures d'application pour contrer la non-conformité
3. Les communications et la sensibilisation, soit la connectivité multimédia, les initiatives de sensibilisation, les produits d'information, les documents d'orientation concernant l'administration et l'application des questions liées à la LCAP, et les centres d'information
4. Les catalyseurs, soit les initiatives de renforcement des capacités, les résultats de l'Organe national de coordination (p. ex. les conseils et orientations stratégiques, les rapports publics, les études de recherche, les processus et procédures opérationnels et les modifications législatives et réglementaires) ainsi que la coopération pangouvernementale (fédérale, provinciale et internationale)

Les quatre séries d'activités et d'extrants mènent à trois résultats immédiats :

1. Sensibilisation au pourriel et aux autres menaces en ligne
2. Échange d'information pour faciliter la mise en œuvre de la LCAP
3. Reconnaissance de pratiques appropriées et inappropriées sur le marché électronique

Les trois résultats immédiats mènent à trois résultats intermédiaires :

1. Coopération pour les activités de conformité Atténuation des menaces d'impact sur le marché électronique
2. L'atténuation des menaces d'impact sur le marché électronique
3. Les actions proactives pour protéger le marché électronique

Les résultats intermédiaires mènent à un résultat final : le commerce électronique au Canada est concurrentiel et renforce l'économie canadienne.