mccarthy tetrault

Boîte à outils antipourriel

DERNIÈRE MISE À JOUR : FÉVRIER 2018

mccarthy tetrault

Table des matières

Boîte à outils antipourriel

Introduction

Cette boîte à outils a comme objectif d'aider les organisations à s'y retrouver dans la loi antipourriel du Canada. Il n'y a pas de nom abrégé pour désigner la loi antipourriel. Son nom officiel étant très long, pour des raisons de concision, nous utiliserons dans cette boîte à outils l'acronyme « LCAP » pour désigner la « Loi canadienne antipourriel »[1].

Le Parlement a adopté la LCAP le 15 décembre 2010 et la plupart de ses dispositions sont déjà en vigueur, à une exception près : le droit d'action. L'entrée en vigueur des dispositions relatives au droit d'action a été reportée indéfiniment pendant qu'un comité parlementaire examine la Loi[2].

La LCAP est sans doute la loi antipourriel/maliciel la plus sévère du monde. Afin de garantir la conformité, les organisations qui envoient des messages électroniques commerciaux aux Canadiens devront examiner la façon dont elles communiquent par voie électronique. Quiconque contrevient à la LCAP est passible d'une amende maximale de 10 millions de dollars[3]. Les dirigeants et les administrateurs peuvent également être tenus personnellement responsables s'ils ont autorisé une conduite attentatoire ou s'ils y ont acquiescé ou participé.

Si de nombreuses organisations connaissent les exigences réglementaires de la loi antipourriel américaine de 2003, la *CANSPAM Act*, elles doivent savoir que la loi canadienne est plus complexe et plus sévère. Dans la plupart des cas, il ne suffira pas de respecter les exigences de la loi américaine pour être conforme à la loi canadienne.

La portée de la LCAP s'étend bien au-delà de ce qu'on appelle généralement les « pourriels », et peut s'appliquer à certaines communications que la plupart des gens pourraient considérer comme des communications électroniques normales. Dès lors, les organisations doivent procéder à un examen attentif des messages qu'elles envoient par courriel et autres systèmes de messagerie électronique, y compris les SMS, ainsi que certains messages envoyés par l'intermédiaire de réseaux sociaux et de portails en ligne. Le seul fait d'envoyer un message électronique avec le moindre contenu commercial à une personne sans consentement préalable représente un risque important d'infraction pour les organisations.

La LCAP interdit aux organisations d'envoyer des messages électroniques commerciaux à un destinataire, à moins que celui-ci n'ait donné son consentement exprès ou qu'il ne s'agisse de messages dont le consentement est tacite visés par l'une des catégories fermées. Un « message électronique commercial » est un message électronique qui est envoyé à une adresse électronique et qui a pour but, entre autres, d'encourager la participation à une activité commerciale. Le terme « message électronique » est largement défini et comprend notamment quelque « message envoyé par tout moyen de télécommunication, notamment un message textuel, sonore, vocal ou visuel ». Une « adresse

---

[1] On peut trouver le texte intégral de la LCAP à l'adresse http://laws-lois.justice.gc.ca/fra/lois/E-1.6/index.html

[2] Pour plus de renseignements, voir l'article de Barry Sookman intitulé *CASL Private Right of Action delayed and Government to review CASL* à l'adresse http://www.barrysookman.com/2017/06/07/casl-private-right-of-action-delayed-and-government-to-review-casl/

[3] Les pénalités les plus importantes liées à la LCAP émises à ce jour concernent un règlement du Bureau de la concurrence contre des sociétés de location de voitures pour 3 millions de dollars; du côté des messages électroniques commerciaux, le CRTC a émis des avis d'infraction pour des montants allant jusqu'à 1,1 million de dollars.

électronique » s'entend notamment d'un compte courriel, d'un compte SMS, d'un compte messagerie instantané ou de tout compte similaire.

La LCAP stipule également que tout message électronique commercial doit présenter le nom de l'expéditeur, inclure les coordonnées de la personne-ressource ainsi qu'un mécanisme permettant au destinataire de faire connaître son désir de ne plus recevoir de messages. Ces exigences deviennent plus compliquées dans des situations où les fournisseurs de services ou les co-promoteurs sont impliqués dans la création du contenu d'un message ou dans la détermination de la liste des destinataires.

La LCAP modifie la *Loi sur la concurrence* pour empêcher toute déclaration fausse ou trompeuse quant à la description de l'expéditeur, à l'objet ou au contenu du message électronique, et ce, que ce soit dans l'adresse URL ou dans tout autre localisateur d'une page Web. L'expéditeur devra être particulièrement vigilant quant à l'utilisation de déclarations exagérées ou factuellement incomplètes contenues à l'objet du message dans le but de capter l'attention du destinataire car *tout* élément trompeur peut entraîner une responsabilité importante.

La loi comporte également des modifications à la législation fédérale sur la vie privée, soit la *Loi sur la protection des renseignements personnels et les documents électroniques* (« LPRPDE »). Ces modifications interdisent l'utilisation de programmes informatiques appelés « collecteurs d'adresse » et s'appliquent à l'utilisation de programmes de collecte d'adresses et d'adresses électroniques obtenues au moyen de l'usage de tels programmes. Cette dernière interdiction crée des problèmes pour les personnes qui ont obtenu ou utilisent des listes d'adresses de tiers.

Dans le but de contrer les logiciels espions et les logiciels malveillants, la LCAP interdit l'installation de programmes d'ordinateur sans le consentement préalable de l'utilisateur ou du propriétaire d'un ordinateur. Cependant, les dispositions sur les programmes d'ordinateur de la LCAP vont au-delà des logiciels malveillants et peuvent affecter les installations routines des programmes d'ordinateur à des fins inoffensives.

La LCAP accorde un droit d'action qui permet à une personne d'entamer une poursuite au civil contre quiconque viole la LCAP ou contrevient aux nouvelles dispositions de la *Loi sur la concurrence* en matière de déclarations fausses ou trompeuses. L'amende, dans de telles circonstances, pourrait atteindre un million de dollars par jour par catégorie de violation plus une indemnisation pour les dommages ou pertes réels. Comme nous l'avons mentionné ci-dessus, bien que le droit d'action ne soit pas encore en vigueur il pourrait être ressuscité suite à l'examen du gouvernement.

Cette boîte à outils donne aux organisations des conseils de base en matière de communication électronique afin qu'elles puissent se conformer aux exigences de la LCAP. L'annexe A établit une liste d'informations à recueillir pour un audit. En annexe B, on trouvera une liste de contrôle couvrant les principaux éléments de conformité à la loi, lesquels devront faire l'objet d'une vérification et d'une réévaluation à intervalles réguliers par l'organisation.

Cette boîte à outils ne constitue pas un avis juridique formel.

RESSOURCES ET CONSEILS SUPPLÉMENTAIRES

Bon nombre des dispositions de la LCAP sont visées par deux règlements gouvernementaux : l'un émanant du CRTC et l'autre d'Industrie Canada. En mars 2012, le CRTC a publié son règlement définitif. En décembre 2013, Industrie Canada a publié son règlement définitif[4]. Dans la présente boîte à outils, le renvoi au règlement du CRTC signifie son règlement définitif, tandis que le renvoi au Règlement IC signifie le règlement définitif publié en décembre 2013 par Industrie Canada[5].

De plus, le CRTC a publié trois Bulletins d'information de Conformité et Enquêtes en rapport avec la LCAP :

- CRTC 2012-548 Lignes directrices sur l'interprétation du Règlement sur la protection du commerce électronique (les « lignes directrices générales »)
- CRTC 2012-549 Lignes directrices sur l'utilisation des cases d'activation comme moyen d'obtenir le consentement exprès en vertu de la loi canadienne antipourriel (les « lignes directrices sur les cases d'activation »)
- CRTC 2014-326 Lignes directrices visant à aider les entreprises à élaborer des programmes de conformité (les « lignes directrices du programme »)

Le règlement du CRTC prescrit la forme et le contenu des messages électroniques commerciaux et des demandes de consentement relatives à l'envoi de messages électroniques commerciaux, à la modification des données de transmission des messages électroniques et à l'installation des programmes d'ordinateur. Les lignes directrices du CRTC portent sur l'interprétation que fait le CRTC du règlement du CRTC et des dispositions connexes de la LCAP et fournissent des exemples de pratiques que le CRTC estime conformes à son règlement[6].

Outre la loi, les règlements et les bulletins d'information sur la conformité et l'application de la loi, le CRTC, Industrie Canada et le Bureau de la concurrence ont fourni des lignes directrices sous diverses formes (les « documents d'orientation supplémentaires »), notamment :

- un résumé de l'étude d'impact de la réglementation (le « REIR »)[7], publié par Industrie Canada lors de l'entrée en vigueur du Règlement IC. Le REIR renferme des explications assez utiles d'importants aspects de la LCAP et du Règlement;
- la foire aux questions du CRTC au sujet de la LCAP (la « FAQ du CRTC »)[8];

---

[4] Pour un sommaire du Règlement IC, voir l'article de Barry Sookman intitulé *CASL Industry Canada regulations: summary and comments* à l'adresse http://www.barrysookman.com/2013/12/04/casl-industry-canada-regulations-summary-and-comments/ et l'article de Barry Sookman intitulé *The Industry Canada CASL Regulations and RIAS: a Lost Opportunity* à l'adresse http://www.barrysookman.com/2013/12/16/the-industry-canada-casl-regulations-and-rias-a-lost-opportunity/

[5] On trouve le Règlement du CRTC à l'adresse http://www.crtc.gc.ca/fra//archive/2012/2012-183.htm, le Règlement IC à l'adresse http://fightspam.gc.ca/eic/site/030.nsf/fra/00273.html et les lignes directrices sur les programmes de conformité à l'adresse http://crtc.gc.ca/fra/archive/2014/2014-326.htm

[6] Pour une analyse complète des lignes directrices du CRTC, voir l'article de Barry Sookman intitulé *CRTC Issues CASL (Canada's Anti-Spam Law) Guidelines, background and commentary* à l'adresse http://www.barrysookman.com/2012/10/16/crtc-issues-casl-canadas-anti-spam-law-guidelines-background-and-commentary/

[7] On peut trouver le REIR à l'adresse http://fightspam.gc.ca/eic/site/030.nsf/fra/00271.html. Pour une analyse et des commentaires portant sur le REIR, voir l'article de Barry Sookman intitulé *The Industry Canada CASL Regulations and RIAS: a Lost Opportunity* à l'adresse http://www.barrysookman.com/2013/12/16/the-industry-canada-casl-regulations-and-rias-a-lost-opportunity/. Pour d'autres commentaires sur la FAQ, voir l'article de Barry Sookman intitulé *CRTC FAQ on CASL* à l'adresse http://www.barrysookman.com/2013/12/18/crtc-faq-on-casl/

- la foire aux questions publiée sur le site combattrelepourriel.gc.ca[9];
- la foire aux questions du Bureau de la concurrence[10];
- une transcription de la vidéo de la séance d'information du CRTC sur la LCAP[11];
- la fiche d'information du CRTC intitulée *Exigences de la Loi canadienne anti-pourriel concernant l'installation de programmes informatiques* (les « lignes directrices sur l'installation de programmes informatiques »)[12];
- le document du CRTC *Avis d'application – Avis aux entreprises et aux particuliers sur la façon de conserver les preuves de consentement*[13]; et
- les lignes directrices du CRTC sur le consentement tacite (les « lignes directrices sur le consentement tacite »)[14].

IMPORTANT : Les indications figurant dans les documents d'orientation supplémentaires ci-dessus peuvent être prises en considération lorsque le CRTC ou un tribunal détermine la réparation qui s'impose en raison d'une contravention à la LCAP. Ces documents pourraient aussi être utiles pour établir des défenses de diligence raisonnable. Il faut cependant examiner ces documents sous réserve du fait important qu'une erreur de droit, c'est-à-dire une erreur quant à la teneur de la loi, a été rejetée comme moyen de défense aux infractions réglementaires. Par conséquent, les organisations ne peuvent pas simplement se fier aux énoncés figurant dans les documents d'orientation supplémentaires sans faire leurs propres évaluations afin de déterminer si les indications données sont correctes[15].

INDICATIONS ISSUES DES DÉCISIONS EN MATIÈRE D'APPLICATION : Bien que le CRTC ait publié une gamme de documents concernant la façon dont il a appliqué la LCAP à ce jour, ceux-ci fournissent peu d'indications supplémentaires sur les futures applications[16]. Le CRTC a émis plusieurs avis de violation, qui se sont généralement traduits par l'acceptation d'un engagement par la partie accusée. Jusqu'à présent, chacun des engagements comportait une sanction pécuniaire et un engagement à entreprendre un programme de conformité. Dans de tels cas, il y a très peu d'indications sur la nature de l'infraction et la façon dont le CRTC a interprété les dispositions ambiguës clés de la LCAP. Cependant, il y a eu au moins trois décisions publiées dans lesquelles des sanctions administratives pécuniaires (SAP)

---

[8] On peut trouver la FAQ du CRTC à l'adresse http://crtc.gc.ca/fra/com500/faq500.htm

[9] On peut trouver la FAQ du site combattrelepourriel.gc.ca à l'adresse http://fightspam.gc.ca/eic/site/030.nsf/fra/00304.html

[10] On peut trouver la FAQ du Bureau de la concurrence à l'adresse http://www.competitionbureau.gc.ca/eic/site/cb-bc.nsf/fra/03765.html

[11] On peut trouver la transcription à l'adresse http://www.crtc.gc.ca/fra/com500/videot1.htm

[12] On peut trouver les lignes directrices sur l'installation de programmes informatiques à l'adresse http://crtc.gc.ca/fra/internet/install.htm. Nous recommandons que ces lignes directrices soient évaluées avec prudence, car elles adoptent certaines interprétations concernant des installations qui ne semblent pas être ancrées dans le langage de la LCAP.

[13] On peut trouver l'avis d'application à l'adresse https://www.canada.ca/fr/radiodiffusion-telecommunications/nouvelles/2016/07/avis-d-application-avis-aux-entreprises-et-aux-particuliers-sur-la-faaon-de-conserver-les-preuves-de-consentement.html

[14] On peut trouver les lignes directrices sur le consentement tacite à l'adresse http://www.crtc.gc.ca/fra/com500/guide.htm

[15] Voir l'article de Barry Sookman intitulé *The Industry Canada CASL Regulations and RIAS: a Lost Opportunity* à l'adresse http://www.barrysookman.com/2013/12/16/the-industry-canada-casl-regulations-and-rias-a-lost-opportunity/

[16] Pour toutes les décisions, les sanctions administratives pécuniaires, les avis de violation et les engagements en cours, voir http://www.crtc.gc.ca/fra/dncl/dnclce.htm

ont été imposées.[17] Ces décisions fournissent des indications sur la manière dont le CRTC interprète la LCAP et ses règlements.

REMARQUE SUR L'APPLICATION : Le CRTC est l'autorité principalement responsable de l'application de la LCAP. Le commissaire de la concurrence et le commissaire à la protection à la vie privée du Canada sont chargés d'appliquer les modifications apportées dans la LCAP à la *Loi sur la concurrence* et à la LPRPDE. Le commissaire de la concurrence a également des pouvoirs d'application en matières civile et criminelle en vertu de la LCAP et de la *Loi sur la concurrence*. Le CRTC, le commissaire de la concurrence et le commissaire à la protection de la vie privée du Canada sont tenus de se consulter, et ils ont conclu un protocole d'entente afin de « faciliter la coopération, la coordination et l'échange d'information » pour l'application de la LCAP[18].

[17] Voir http://www.crtc.gc.ca/fra/archive/2017/2017-368.htm, https://www.crtc.gc.ca/fra/archive/2017/2017-65.htm, et https://www.crtc.gc.ca/fra/archive/2016/2016-428.htm

[18] Voir http://www.bureaudelaconcurrence.gc.ca/eic/site/cb-bc.nsf/fra/03643.html

Envoi de messages électroniques commerciaux

Les dispositions antipourriel de la LCAP visent principalement à empêcher que les « boîtes de réception » des utilisateurs canadiens soient remplies de messages électroniques commerciaux envoyés sans le consentement du destinataire et en violation des autres formalités. Ce document donne un aperçu des principales dispositions de la LCAP. Les représentants d'organisations qui jouent un rôle externe, notamment en vente ou en marketing, doivent connaître ces exigences et doivent y prêter une attention particulière.

Pour l'application de la loi, les organisations doivent pouvoir démontrer qu'elles ont pris des mesures afin de respecter les formalités liées à la LCAP, notamment en matière de consentement. Les mesures que prend une organisation pour empêcher ses employés et d'autres représentants d'envoyer des messages commerciaux non sollicités peuvent contribuer à établir ou à renforcer la défense de diligence raisonnable et peuvent être prises en considération dans la fixation du montant des sanctions administratives pécuniaires (SAP) ou des dommages-intérêts en cas de contravention à la LCAP. Par conséquent, il est essentiel que l'organisation élabore et mette en œuvre un programme de conformité à la LCAP afin de limiter sa responsabilité civile et son risque de contravention à la LCAP.

LE MESSAGE EST-IL UN « MESSAGE ÉLECTRONIQUE »?

La LCAP s'applique aux « messages électroniques » envoyés à une « adresse électronique ». Au sens de la LCAP, « message électronique » s'entend d'un message envoyé par « *tout* moyen de télécommunication, notamment un message textuel, sonore, vocal ou visuel ». Cette définition exclut toutefois les messages qui consistent en des communications vocales bilatérales qu'ont eues entre elles, en direct, des personnes physiques, les messages envoyés par fac-similé à un compte téléphone et les enregistrements de la parole envoyés à un compte téléphone.

Au sens de la LCAP, « adresse électronique » s'entend d'une adresse « utilisée relativement à la transmission d'un message électronique à l'un des comptes suivants : a) un compte courriel, b) un compte messagerie instantanée; c) un compte téléphone; ou d) *tout autre compte similaire* ». Cette définition englobe de nombreuses formes de systèmes de messagerie électronique, notamment les courriels, les messages texte et les messages instantanés, ainsi que certains services en ligne pour lesquels les utilisateurs détiennent un compte, notamment les sites de réseautage social, certains forums en ligne et les portails.

REMARQUE : Le Règlement IC a établi des exemptions applicables aux messages envoyés à des portails de commerce électronique sécurisés et à certains systèmes de messagerie. Pour plus de renseignements sur ces exemptions, voir ci-après la rubrique « Le message est-il absolument exclu de l'application de la loi? ». De plus, le REIR donne certaines indications relativement à la question de savoir si les messages envoyés à des adresses de protocole Internet (IP) ou dans le cadre d'annonces liées au comportement sont envoyés à des « adresses électroniques ». Le REIR énonce ce qui suit : « Pour autant que les adresses IP ne soient pas liées à une personne ou à un compte identifiable, les adresses IP ne sont pas des adresses électroniques aux fins de la LCAP. Par conséquent, les bannières publicitaires sur les sites Web ne relèvent pas de la LCAP. »

LE MESSAGE EST-IL UN « MEC »?

La LCAP ne s'applique qu'aux messages électroniques commerciaux (les « MEC »). Au sens de la loi, « est un message électronique commercial le message électronique dont il est raisonnable de conclure, vu son contenu, le contenu de tout site Web ou autre banque de données auxquels il donne accès *par hyperlien* ou l'information qu'il donne sur la personne à contacter, *qu'il a pour but, entre autres,*

d'encourager la participation à une activité commerciale et, notamment, tout message électronique qui, selon le cas : a) comporte une offre d'achat, de vente, de troc ou de louage d'un produit, bien, service, terrain ou droit ou intérêt foncier; b) offre une possibilité d'affaires d'investissement ou de jeu; c) annonce ou fait la promotion d'une chose ou possibilité mentionnée aux alinéas a) ou b); d) fait la promotion d'une personne, y compris l'image de celle-ci auprès du public, comme étant une personne qui accomplit – ou a l'intention d'accomplir – un des actes mentionnés aux alinéas a) à c) ». (Italiques ajoutés)

Au sens de la LCAP, « activité commerciale » s'entend aussi largement de « tout acte isolé ou activité régulière qui revête un caractère commercial, *que la personne qui l'accomplit le fasse ou non dans le but de réaliser un profit*, à l'exception de tout acte ou activité accompli à des fins d'observation de la loi, de sécurité publique, de protection du Canada, de conduite des affaires internationales ou de défense du Canada ». (Italiques ajoutés)

Dans les documents d'orientation supplémentaires, le CRTC et Industrie Canada ont fait des énoncés visant à préciser la définition de MEC. Bien qu'utiles, les explications sont parfois contradictoires et laissent toujours sans réponse d'importantes questions lorsqu'il s'agit de savoir si certains messages sont des MEC. En outre, les décisions d'application publiées et les résumés d'engagements du CRTC n'ont pas fourni de clarté sur les questions courantes des organisations qui essaient de comprendre la LACP.

La FAQ du CRTC énonce ce qui suit :

> « La question à se poser est la suivante : le message que j'envoie est-il un MEC? Un des buts du message est-il d'encourager le destinataire à participer à une activité commerciale?
>
> Pour déterminer si l'objectif du message est d'encourager la participation à une activité commerciale, voici les éléments du message à considérer :
>
> - le contenu du message;
> - tout hyperlien dans le message qui mène au contenu d'un site Web ou à une base de données;
> - les coordonnées dans le message.
>
> Ces éléments du message n'ont pas un effet déterminant.»

Le REIR énonce ce qui suit :

- « Le simple fait qu'un message soit lié à une activité commerciale donne accès par hyperlien au site Web d'une personne ou à de l'information électronique liée à des activités commerciales n'en fait pas pour autant un message électronique commercial en vertu de la Loi si aucun de ses buts ne vise à encourager le destinataire à participer à une activité commerciale. Si le message comporte une relation ou une activité commerciale préexistante et fournit des renseignements supplémentaires, des précisions ou complète une transaction liée à la réalisation d'une activité commerciale qui est déjà en cours, ce message ne serait pas considéré comme un message électronique commercial puisque, *plutôt que de promouvoir une activité commerciale, il représente sa mise en œuvre*. » (Italiques ajoutés)
- « Par ailleurs, les enquêtes, les sondages, les bulletins et les messages sollicitant des dons de bienfaisance, des contributions politiques, ou d'autres activités politiques qui n'encouragent pas la participation à une activité commerciale ne seraient pas visés par la définition. »

- « Cependant, les messages électroniques peuvent entrer dans la définition d'un message électronique commercial s'il est raisonnable de conclure qu'il a pour but, entre autres, d'encourager le destinataire à participer à des activités commerciales supplémentaires en fonction, par exemple, de la prévalence de contenu commercial, d'hyperliens ou de coordonnées. »
- « Autrement dit, si le but est d'annoncer, de faire la promotion, de commercialiser ou d'offrir un produit, un bien, un service, une possibilité d'affaires ou de jeu ou un intérêt foncier, ces messages sont sans contredit des messages électroniques commerciaux. Plus précisément, *la Loi vise à limiter les possibilités d'annoncer, de faire la promotion, de commercialiser ou d'offrir des produits ou des services sous le couvert d'un message électronique non commercial.* S'il est raisonnable de conclure que le message vise l'un de ces buts, alors le message serait considéré comme un message électronique commercial et, sauf exception, les dispositions de la Loi s'appliqueraient. » (Italiques ajoutés)

Le texte de la décision de Conformité et Enquêtes CRTC 2016-428 (« *Blackstone* »)[19] explique qu'un message peut constituer un message électronique commercial même s'il ne contient pas d'offre claire d'achat ou de vente :

> « Les messages envoyés faisaient état ou faisaient la promotion de programmes d'éducation et de formation dans des domaines comme la rédaction technique, la grammaire et la gestion du stress. Le coût de ces programmes n'était pas spécifiquement précisé, mais le langage utilisé, y compris des allusions à divers rabais et tarifs de groupe, faisait comprendre que ces cours étaient des services pouvant être achetés auprès de Blackstone. Le Conseil détermine donc que ces messages ont été envoyés pour assurer la promotion et la publicité de services disponibles commercialement auprès de Blackstone et qu'ils constituaient des messages électroniques commerciaux au sens du paragraphe 1(2) de la Loi. »

LE MESSAGE EST-IL ABSOLUMENT EXCLU DE L'APPLICATION DE LA LOI?

La LCAP prévoit plusieurs exemptions complètes à l'application de l'ensemble de ses dispositions, notamment :

1. si l'expéditeur et le destinataire ont entre eux des liens personnels ou familiaux au sens du Règlement (al. 6(5)a));
2. les demandes, notamment de renseignements, ont trait à une personne exerçant des activités commerciales (al. 6(5)b)).

Le Règlement IC prévoit neuf autres catégories d'exemptions. Ces exemptions, qui sont décrites plus en détail ci-dessous, sont :

1. Les messages envoyés au sein d'une organisation qui concernent les activités de l'organisation (Règlement IC – 3a)(i));
2. Les messages envoyés entre organisations entretenant des rapports qui concernent les activités de l'organisation à qui les messages sont envoyés (Règlement IC – 3a)(ii));
3. Les messages envoyés en réponse à une demande, notamment de renseignements, ou par suite d'une plainte (Règlement IC – 3b));

[19] Voir http://www.crtc.gc.ca/fra/archive/2016/2016-428.htm

4. Les messages envoyés pour satisfaire à une obligation juridique, notamment pour donner avis d'un droit existant ou pour faire valoir un droit (Règlement IC – 3c));
5. Les messages envoyés par l'entremise d'un service de messagerie électronique (i) si la forme, le contenu et le mécanisme d'exclusion requis sont publiés de façon à être visibles et facilement accessibles sur l'interface utilisateur du service et (ii) les destinataires ont consenti expressément ou tacitement à les recevoir (Règlement IC – 3d));
6. Les messages envoyés à un compte sécuritaire et confidentiel à accès restreint auquel les messages ne peuvent être envoyés que par la personne qui a fourni le compte à la personne qui reçoit les messages (Règlement IC – 3e));
7. Les messages que l'expéditeur (i) a des motifs raisonnables de croire qu'ils seront récupérés dans un État étranger mentionné à l'annexe et (ii) qu'ils seront conformes à une loi de cet État régissant les comportements essentiellement similaires à ceux visés par la LCAP (Règlement IC – 3f));
8. Les messages envoyés par ou pour un organisme de bienfaisance enregistré au sens du paragraphe 248(1) de la LIR si leur principal objet est de lever des fonds (Règlement IC – 3g));
9. Les messages envoyés par ou pour un parti politique, une organisation ou un candidat à une charge publique élective si leur principal objet est de demander des contributions. (Règlement IC – 3h)).

Messages entre organisations

Il y a deux exemptions entre organisations :

La première vise les messages envoyés au sein d'une organisation entre employés, représentants, consultants ou franchisés de l'organisation et concernant les activités de l'organisation.

La seconde vise les messages envoyés par l'employé, le représentant, le consultant, le franchisé ou l'entrepreneur d'une organisation à l'employé, au représentant, au consultant, au franchisé ou à l'entrepreneur d'une autre organisation si, d'une part, leurs organisations ont « des relations » au moment de l'envoi des messages et, d'autre part, les messages concernent les activités de l'organisation destinataire.

Messages envoyés en réponse à une demande

Les messages envoyés en réponse à une demande, notamment de renseignements, ou par suite d'une plainte, ou qui sont par ailleurs sollicités par le destinataire, sont exemptés de la LCAP. Cette exemption règle un problème fortuit du paragraphe 6(5) de la LCAP qui aurait rendu illégal l'envoi de messages en réponse à une demande d'information de consommateurs sans avoir obtenu un consentement supplémentaire.

Messages envoyés pour faire valoir un droit

Le Règlement IC exempte les MEC envoyés à une personne i) pour satisfaire à une obligation juridique, ii) pour donner avis d'un droit, d'une obligation, d'une ordonnance judiciaire ou d'un tarif existant ou à venir, iii) pour faire valoir un droit ou exécuter une obligation juridique, une ordonnance judiciaire, un jugement ou un tarif ou iv) pour faire valoir un droit découlant d'une règle de droit fédérale, provinciale, municipale ou étrangère.

Messages envoyés et reçus par l'entremise d'un service de messagerie électronique

Les messages envoyés et reçus par l'entremise d'un service de messagerie électronique sont exonérés si la forme, le contenu et le mécanisme d'exclusion requis par la LCAP *sont publiés de façon à être visibles et facilement accessibles* sur l'interface utilisateur au moyen de laquelle les messages sont récupérés et que les personnes à qui ils sont envoyés ont consenti expressément « *ou tacitement* » à les recevoir.

Messages envoyés à des portails de commerce électronique

Les messages envoyés « à un compte sécuritaire et confidentiel à accès restreint, auquel les messages ne peuvent être envoyés que par la personne qui a fourni le compte » sont aussi exemptés de la LCAP. L'application de cette exemption permettra aux banques, par exemple, de continuer à envoyer des messages aux utilisateurs de services bancaires en ligne, au moyen de comptes établis par la banque et accessibles grâce à de tels services.

Messages envoyés par une personne qui « a des motifs raisonnables de croire » qu'ils seront récupérés dans un État étranger

Les messages pour lesquels l'expéditeur a des motifs raisonnables de croire qu'ils seront récupérés dans un État étranger mentionné expressément dans une annexe au règlement sont exemptés de la LCAP dans la mesure où ils sont conformes aux lois de cet État portant sur une conduite similaire à la conduite interdite par la LCAP. Ce règlement a pour effet de rendre les expéditeurs de MEC du Canada responsables de la contravention à la LCAP si le message envoyé à l'État étranger contrevient à la loi antipourriel applicable de cet État.

Organismes de bienfaisance enregistrés, partis politiques, organisations et candidats

Les messages envoyés principalement en vue de la levée de fonds par des organismes de bienfaisance enregistrés et par des partis politiques, des organisations et des candidats sont exemptés de la LCAP. Les exemptions s'appliquent seulement aux organismes de bienfaisance enregistrés au sens du paragraphe 248(1) de la *Loi de l'impôt sur le revenu* et aux entités politiques, de sorte que tous les autres organismes à but non lucratif sont assujettis aux exigences de la LCAP.

Le CRTC a fourni d'autres indications pour les organismes de bienfaisance, en prenant la position de ne se concentrer que sur les organismes de bienfaisance où l'on tente de contourner la loi. La FAQ du CRTC énonce que « [é]tant donné que les messages légitimes envoyés par des organisations de bienfaisance enregistrées qui sollicitent des fonds sont exemptés en vertu de la Loi, le CRTC mettra l'accent sur les messages envoyés par ceux qui tentent de contourner les règles sous le couvert d'organismes de bienfaisance enregistrés[20]. »

[20] Pour une discussion plus détaillée sur la LCAP et les organismes de bienfaisance, voir l'article de Meghan Waters intitulé *CASL Guidance for Registered Charities* à l'adresse https://www.mccarthy.ca/en/insights/blogs/snipits/casl-guidance-registered-charities

LE DESTINATAIRE A-T-IL CONSENTI À RECEVOIR LE MESSAGE?

L'objectif de la LCAP est de s'assurer que les destinataires des messages électroniques commerciaux ont donné à l'expéditeur leur consentement. Ce consentement peut être soit exprès, soit tacite. Les dispositions de la LCAP relatives au consentement exprès ou tacite, de même que les exceptions à cet égard, sont décrites ci-dessous. L'obtention du consentement est essentielle. En fait, les trois premières décisions d'application qui ont abouti à des sanctions administratives pécuniaires concernaient une absence de consentement du destinataire.

Consentement exprès

La réglementation du CRTC stipule que le consentement à l'envoi de messages électroniques commerciaux peut être obtenu oralement ou par écrit. Bien qu'il ne soit pas obligatoire d'obtenir le consentement par écrit, les organisations préféreront certainement obtenir un consentement écrit afin de pouvoir en établir la preuve. Les lignes directrices du CRTC donnent certaines précisions sur les types de preuves qui suffiraient à démontrer un consentement oral. Les recommandations du CRTC sont sommairement décrites ci-après à la rubrique « Obtention du consentement ».

REMARQUE : Il convient de souligner qu'un message électronique qui constitue une demande de consentement est réputé être un message électronique commercial. Ainsi, l'expéditeur doit obtenir le consentement applicable avant d'envoyer un tel message, à moins que l'une des exceptions à l'exigence de consentement décrites ci-après ne s'applique.

REMARQUE SUR LA CONFORMITÉ : Le REIR et la FAQ du CRTC prévoient que les consentements exprès, obtenus avant l'entrée en vigueur de la LCAP, permettant la collecte ou l'utilisation d'adresses électroniques en vue de l'envoi de messages électroniques commerciaux sont considérés comme conformes à la LCAP même si les demandes de consentement ne respectaient pas les exigences de forme et de contenu de la LCAP (voir ci-après sous « Obtention du consentement »)[21]. Toutefois, d'autres consentements, comme ceux qui seraient conformes à la LPRPDE, ne seront pas considérés conformes à la LCAP, peu importe s'ils ont été obtenus avant ou après l'entrée vigueur de la LCAP. Les consentements déduits qui sont reconnus valides en Australie ne constituent pas des consentements exprès pour l'application de la LCAP.

Consentement tacite

La LCAP suppose le consentement tacite d'un message électronique commercial dans les trois cas suivants :

1. l'expéditeur et le destinataire ont des « *relations d'affaires en cours* » ou des « *relations privées en cours* »;
2. le destinataire a « *publié bien en vue* » l'adresse électronique sans aucune mention précisant qu'il ne veut recevoir aucun MEC non sollicité à cette adresse ET le message a un lien soit avec l'exercice des attributions du destinataire, soit avec son entreprise commerciale ou les fonctions qu'il exerce au sein d'une telle entreprise; et
3. le destinataire a communiqué l'adresse électronique à l'expéditeur sans aucune mention précisant qu'il ne veut recevoir aucun MEC non sollicité à cette adresse ET le message a un lien soit avec l'exercice des attributions du destinataire, soit avec son entreprise commerciale ou les fonctions qu'il exerce au sein d'une telle entreprise.

[21] Le CRTC estime que le consentement obtenu au moyen d'une case précochée n'est pas un consentement exprès. Voir les Lignes directrices sur l'utilisation des cases d'activation. Par conséquent, il n'est pas certain que ces consentements demeurent valides.

Une personne a « des relations d'affaires en cours » avec une personne qui reçoit un message si elles découlent, selon le cas :

a) de l'achat ou du louage par la seconde personne, au cours des deux ans précédant la date d'envoi du message, d'un bien, produit, service, terrain ou droit ou intérêt foncier de la première personne;

b) de l'acceptation par la seconde personne, au cours de cette période, d'une possibilité d'affaires, d'investissement ou de jeu offerte par la première personne;

c) du troc d'une chose mentionnée à l'alinéa *a*) intervenu entre elles au cours de cette période;

d) de tout contrat – toujours en vigueur ou venu à échéance au cours de cette période – conclu par écrit entre elles au sujet d'une chose non mentionnée aux alinéas *a*) à *c*); ou

e) d'une demande – notamment une demande de renseignements – présentée par la seconde personne à la première, au cours des six mois précédant la date d'envoi du message, relativement à une chose ou à une possibilité mentionnée aux alinéas *a*) ou *c*) (paragraphe 10(10)).

À l'égard de l'achat ou du louage d'un bien, produit, service, terrain ou droit ou intérêt foncier, s'il y a achat ou utilisation étalé sur une période donnée au titre d'un abonnement, d'un compte, d'un prêt ou de toute autre relation semblable, la période commence à la date d'expiration de l'abonnement, du compte, du prêt ou de la relation semblable en question, ce qui prolonge effectivement la période de deux ans pour les clients d'une entreprise qui ont un abonnement, un compte, un prêt ou toute autre relation semblable admissible (paragraphe 10(14)).

Une personne a « des relations privées en cours » avec une personne qui reçoit un message si elles découlent, selon le cas :

a) d'un don ou d'un cadeau offert par la seconde personne à la première au cours des deux ans précédant la date d'envoi du message, dans le cas où cette première personne est un organisme de bienfaisance enregistré au sens du paragraphe 248(1) de la *Loi de l'impôt sur le revenu*, une organisation ou un parti politiques ou un candidat – au sens de toute loi fédérale ou provinciale – à une charge publique élective;

b) du travail effectué à titre de bénévole par la seconde personne pour la première au cours des deux ans précédant la date d'envoi du message, dans le cas où cette première personne est un organisme de bienfaisance enregistré au sens du paragraphe 248(1) de la *Loi de l'impôt sur le revenu*, une organisation ou un parti politiques ou un candidat – au sens de toute loi fédérale ou provinciale – à une charge publique élective; ou

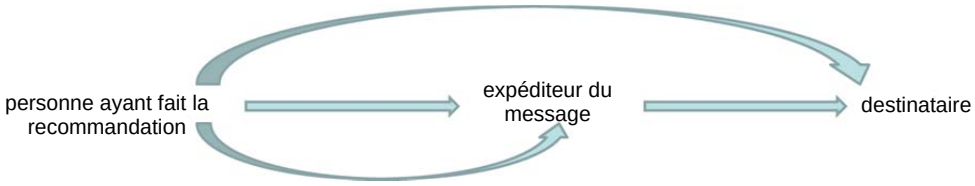
c) d'une adhésion, au sens des règlements, de la seconde personne auprès de la première au cours des deux ans précédant la date d'envoi du message, dans le cas où cette première personne est un club, une association ou un organisme bénévole, au sens des règlements (paragraphe 10(13)).

Aux fins du calcul d'une période susmentionnée à l'égard d'un don, d'un cadeau ou d'une adhésion, a) s'agissant d'un don ou d'un cadeau, s'il y a achat ou utilisation étalé sur une période donnée au titre d'un abonnement, d'un compte, d'un prêt ou de toute autre relation semblable, la période commence à la date d'expiration de l'abonnement, du compte, du prêt ou de la relation semblable en question; et b) s'agissant d'une adhésion, la période commence à la date d'expiration de celle-ci (paragraphe 10(14)).

Bien que, dans ces situations, le consentement puisse être tacite, nous recommandons tout de même que les organisations fassent les efforts nécessaires pour obtenir des destinataires un consentement exprès à l'envoi de messages électroniques commerciaux. Lorsqu'une entreprise a obtenu ce consentement, elle n'a plus à se soucier des conditions rattachées au consentement tacite, notamment

celle de s'assurer que la relation d'affaires ou la relation privée sont toujours existantes, de vérifier les dates de début et de fin de la période de deux ans ou de quelque autre période, ou de s'assurer que le message est lié à l'entreprise du destinataire.

Recommandations de tiers



Le Règlement IC prévoit une exception limitée aux dispositions de la LCAP sur le consentement, exception qui permet l'envoi de messages de recommandations de tiers. Aux termes de cette exception, les dispositions en matière de consentement de la LCAP « ne s'applique pas au premier message électronique commercial qui, d'une part, est envoyé par une personne à une personne physique en vue d'entrer en contact avec elle par suite d'une recommandation d'une ou de plusieurs personnes physiques ayant, avec l'expéditeur du message et avec son destinataire des relations d'affaires en cours, des relations privées en cours ou des liens familiaux ou personnels et si, d'autre part, ce message révèle le nom au complet de la ou des personnes physiques ayant fait la recommandation et comporte la mention qu'il est envoyé par suite d'une telle recommandation ».

Ces personnes ont des relations d'affaires en cours ou des relations privées en cours. Ainsi, bien que les dispositions en matière de consentement de la LCAP ne s'appliquent pas au premier message, elles s'appliquent relativement aux exigences quant à la forme et au mécanisme d'exclusion de la LCAP.

Exceptions quant au consentement

Certaines catégories de messages électroniques commerciaux sont dispensées des exigences de consentement de la LCAP, mais non pas des formalités et du mécanisme d'exclusion qui y sont prévus. Il s'agit des MEC énumérés au paragraphe 6(6) qui sont *uniquement*, selon le cas :

> *a*) des messages qui donnent, à la demande des personnes qui les reçoivent, un prix ou une estimation pour la fourniture de biens, produits, services, terrains ou droits ou intérêts fonciers;
>
> *b*) des messages qui facilitent, complètent ou confirment la réalisation d'une opération commerciale que les personnes qui les reçoivent ont au préalable accepté de conclure avec les personnes qui les ont envoyés ou, le cas échéant, celles au nom de qui ils ont été envoyés;
>
> *c*) des messages qui donnent des renseignements en matière de garanties, de rappels ou de sécurité à l'égard de biens ou produits utilisés ou achetés par les personnes qui reçoivent ces messages ou de services obtenus par celles-ci;
>
> *d*) des messages qui donnent des éléments d'information factuels aux personnes qui les reçoivent à l'égard :
>
> > i) soit de l'utilisation ou de l'achat par ces personnes, pendant une certaine période, de biens, produits ou services offerts par les personnes qui ont envoyé ces messages ou, le cas échéant, celles au nom de qui ils ont été envoyés au titre d'un abonnement, d'une adhésion, d'un compte, d'un prêt ou de toute autre relation semblable,
> >
> > ii) soit de cet abonnement, cette adhésion, ce compte, ce prêt ou cette autre relation;

e) des messages qui fournissent des renseignements directement liés au statut d'employé des personnes qui les reçoivent ou à tout régime de prestations auquel elles participent ou dont elles tirent des avantages;

f) des messages au moyen desquels sont livrés des biens, produits ou services, y compris des mises à jour ou des améliorations à l'égard de ceux-ci, auxquels les personnes qui reçoivent ces messages ont droit au titre d'une opération déjà conclue avec les personnes qui les ont envoyés ou, le cas échéant, celles au nom de qui ils ont été envoyés; ou

g) des messages envoyés à l'une des fins prévues par les règlements.

Le sens du terme « uniquement » au début de cette liste de messages partiellement exclus soulève quelques incertitudes. Des représentants du CRTC ont déclaré, officieusement, que ces messages ne sont pas réputés être des MEC. Le terme « uniquement » dispense plutôt ces messages des exigences de consentement de la LCAP si ces messages doivent en être dispensés parce qu'ils seraient par ailleurs, en raison de leur contenu, des MEC. Le REIR susmentionné visait également à préciser l'interprétation de cette disposition.

LE MESSAGE RESPECTE-T-IL LES EXIGENCES QUANT À LA FORME ET AU MÉCANISME D'EXCLUSION?

Même lorsque les conditions relatives au consentement en vertu de la LCAP ont été respectées, les messages électroniques commerciaux (sauf les quelques exceptions décrites ci-dessus) doivent comporter des éléments d'information spécifiques et permettre au destinataire de se désabonner ou de demander à ce que son nom soit retiré des listes d'envoi afin de ne plus recevoir de messages.

Renseignements prescrits à inclure dans les messages

En vertu de la LCAP, les messages électroniques commerciaux doivent comprendre des renseignements permettant d'identifier l'expéditeur. Cette boîte à outils renferme des directives à l'intention des entreprises qui souhaitent mettre à jour leur signature et les clauses de non-responsabilité de leurs courriels afin de se conformer aux nouvelles dispositions de la loi. De plus, il est important de souligner que ces dispositions s'appliquent non seulement aux communications par courriel, mais aussi à toute forme de message électronique commercial décrite ci-dessus.

Mécanisme d'exclusion

La LCAP stipule que tout message électronique commercial doit comprendre un mécanisme qui permet « à la personne qui reçoit le message électronique d'exprimer sans frais sa volonté de ne plus recevoir d'autres messages électroniques commerciaux de la personne qui l'a envoyé ». La présente boîte à outils contient d'autres renseignements sur la mise en œuvre d'un mécanisme d'exclusion conforme aux dispositions de la LCAP.

LE DESTINATAIRE S'EST-IL DÉSINSCRIT DE LA LISTE D'ENVOI DES MESSAGES ÉLECTRONIQUES COMMERCIAUX?

Les organisations sont tenues de mettre en œuvre un mécanisme efficace qui permet à leurs employés et à d'autres représentants de vérifier si un destinataire potentiel de message s'est désinscrit ou s'il a demandé de ne plus recevoir de messages de l'entreprise. Il peut s'agir d'un mécanisme automatisé appliqué au système des messages sortants, ou d'un système de gestion des relations avec la clientèle. Cette boîte à outils contient des renseignements sur la mise en œuvre d'un système efficace pour recevoir et enregistrer les demandes d'exclusion.

Obtention du consentement

Puisque l'obtention du consentement du destinataire est une exigence clé aux termes de la LCAP, il est important de connaître les diverses façons de l'obtenir.

Moyens d'obtenir le consentement

Comme il est indiqué ci-dessus, aux termes de la LCAP, est réputé être un MEC un message électronique qui contient une demande de consentement à l'envoi d'un MEC. Ainsi, dans la plupart des cas, une entreprise ne peut envoyer à une personne avec qui elle n'a encore eu aucun contact un message lui demandant son consentement à recevoir de futurs messages. Si une organisation entretient déjà une relation d'affaires ou privée avec le destinataire du message, ou si les dispositions relatives au consentement tacite s'appliquent au destinataire, alors l'organisation peut lui envoyer une demande électronique de consentement; en fait, on recommande aux entreprises de chercher à remplacer un consentement tacite (qui peut présenter une date d'expiration) par un consentement exprès, qui ne cesse d'être en vigueur que si le destinataire en fait la demande.

Lorsqu'une entreprise n'a pas de relations en cours ni quelque autre forme de consentement tacite, le consentement à l'envoi de messages électroniques commerciaux doit être obtenu d'autres manières.

Le consentement peut être obtenu oralement ou par écrit. Il revient aux expéditeurs de MEC de prouver le consentement.

Le CRTC estime que les types de preuves énoncés ci-dessous suffisent à démontrer que le consentement oral a été obtenu :

- le consentement oral peut être vérifié par une tierce partie indépendante; ou
- la personne qui sollicite le consentement ou le client de cette personne possède un enregistrement sonore complet et intégral du consentement accordé.

Le CRTC ajoute : « Par exemple, une personne peut demander et obtenir un consentement oral dans le cas où l'information est recueillie par téléphone (par exemple, centre d'appels) ou lorsqu'un client utilise un produit ou service (par exemple, achat à un point de vente). »

Le CRTC estime que, dans le consentement accordé par voie électronique, l'obligation d'obtenir le consentement par écrit est remplie si l'information est vérifiable. Les exemples suivants constituent des moyens acceptables d'obtenir un consentement par écrit : la personne indique son consentement en cochant une case sur une page Web, la date, l'heure et le but du consentement, ainsi que la manière dont ce dernier a été obtenu, étant enregistrés dans une base de données; et la personne remplit un formulaire de consentement à un point d'achat. Le CRTC, dans ses lignes directrices sur les cases d'activation, estime que le consentement obtenu au moyen d'une case précochée n'est pas un consentement exprès.

Le consentement doit être sollicité séparément pour chacun des actes visés par la LCAP (c.-à-d., l'envoi de messages électroniques commerciaux, la modification des données de transmission et l'installation d'un programme d'ordinateur), mais non pas chaque fois qu'a lieu un acte. Le consentement distinct doit aussi être obtenu pour chaque organisation ou membre de son groupe qui veut envoyer des messages au destinataire.

Comme il est indiqué ci-dessus, il revient aux expéditeurs de MEC de prouver le consentement. Dans le cadre de son travail de conformité, une société devrait donc veiller à la mise en place des processus adéquats et des systèmes nécessaires lui permettant de prouver le consentement. Dans cette optique,

les sociétés qui sollicitent le consentement peuvent choisir de le faire « par écrit », plutôt qu'oralement, afin de pouvoir prouver l'existence du consentement.

Renseignements prescrits dans le cadre d'une demande de consentement

Aux termes de la réglementation du CRTC, lorsqu'on demande le consentement exprès d'une personne à l'envoi d'un MEC, la demande doit contenir les renseignements suivants :

a) le ou les objets du consentement;

b) le nom de la personne qui sollicite le consentement et, le cas échéant, le nom de la personne au nom de laquelle il est sollicité;

c) si le consentement est sollicité au nom d'une autre personne, une mention indiquant le nom de la personne qui sollicite le consentement et le nom de la personne au nom de laquelle il est sollicité;

d) si la personne qui sollicite le consentement et celle au nom de laquelle le consentement est sollicité exercent leurs activités commerciales sous d'autres noms, les noms qu'elles utilisent pour exercer ces activités;

e) l'adresse postale municipale, et soit un numéro de téléphone donnant accès à un agent de service ou à un service de messagerie vocale, une adresse de courriel ou de site Web de la personne qui sollicite le consentement et, le cas échéant, de la personne au nom de laquelle le consentement est sollicité; et

f) une mention selon laquelle la personne qui donne son consentement peut le retirer en utilisant l'une ou l'autre des coordonnées mentionnées au point e).

Utilisation d'un tiers pour obtenir un consentement

Lorsqu'elles ont recours à un tiers pour obtenir un consentement, ou lorsqu'elles achètent des « listes d'envoi » d'agences de marketing, les entreprises canadiennes doivent veiller à ce que soient respectées les exigences quant à la forme du message pour l'obtention et l'utilisation du consentement. Les exigences prévues dans le Règlement IC sont ainsi rédigées :

> 5. (1) Pour l'application de l'alinéa 10(2)b) de la Loi, la personne qui a obtenu le consentement exprès au nom d'une autre personne dont l'identité était inconnue peut autoriser toute personne à utiliser le consentement à condition de veiller à ce que, dans tout message électronique commercial envoyé à la personne qui a donné le consentement :
>
> *a*) son identité soit établie à titre de personne ayant obtenu le consentement;
>
> *b*) la personne autorisée fournisse un mécanisme d'exclusion qui, en plus d'être conforme aux exigences de l'article 11 de la Loi, permet à la personne qui a donné le consentement de retirer celui-ci à la personne qui a obtenu un consentement ou à toute autre personne qui est autorisée à utiliser le consentement.
>
> (2) La personne qui a obtenu le consentement veille à ce que la personne autorisée à utiliser le consentement qui a envoyé le message l'avise dès qu'elle est informée que le consentement a été retiré à l'une ou l'autre des personnes suivantes :
>
> *a*) la personne qui a obtenu le consentement;
>
> *b*) la personne autorisée qui a envoyé le message; ou

c) toute autre personne autorisée à utiliser le consentement.

(3) Sur réception d'un avis de retrait du consentement concernant la personne visée à l'alinéa (2)*c*), la personne qui a obtenu le consentement avise sans délai l'intéressé.

(4) La personne qui a obtenu le consentement donne suite au retrait du consentement conformément au paragraphe 11(3) de la Loi et veille à ce que la personne visée à l'alinéa (2)*c*) fasse de même, le cas échéant.

Partage et obtention du consentement entre organisations du même groupe

La LCAP n'établit pas de distinction entre organisations membres du même groupe et organisations non membres du même groupe. Ainsi, lorsqu'une entreprise souhaite utiliser le consentement obtenu par une entreprise membre de son groupe pour envoyer des messages électroniques commerciaux, elle doit respecter les exigences susmentionnées relatives à l'obtention du consentement par un tiers. L'organisation a trois options :

- Chaque organisation du même groupe peut obtenir son propre consentement.
- Une organisation du même groupe peut obtenir le consentement au nom des autres membres du même groupe si les autres membres du même groupe sont nommés et que l'information prescrite est fournie pour chaque membre du même groupe au moment de la demande de consentement. Le REIR énonce ce qui suit : « Lorsqu'il est impossible d'inclure cette information dans le corps d'un message électronique commercial, un hyperlien vers une page sur Internet contenant cette information et facilement accessible sans frais peut être inclus dans le message électronique commercial. »
- L'organisation se fonde sur la réglementation d'Industrie Canada qui permet l'obtention de consentements au nom d'un tiers non identifié si les autres exigences de la réglementation sont respectées.

La gestion des consentements représentera un défi pour les entreprises qui ont de nombreuses sociétés affiliées. Ce défi sera d'autant plus grand lorsqu'une organisation vendra l'une de ses sociétés affiliées, car la liste des destinataires constitue un actif important, tant de la filiale vendue que de celles qui continuent d'être la propriété de l'organisation. Des dispositions devront être prises afin de permettre aux deux entreprises de poursuivre leurs activités respectives.

Transfert des consentements dans les transactions commerciales

Il est théoriquement possible pour une entreprise de transférer ses consentements à une autre dans le cadre de la vente de l'entreprise effectuant le transfert. Toutefois, cela risque d'être un exercice complexe.

En ce qui concerne le consentement exprès, le REIR énonce que « le consentement exprès sera transféré à la vente de l'entreprise, si le contrat de vente comprend des dispositions prévoyant ce transfert en tant qu'actif de l'entreprise. » Il convient toutefois de noter que le REIR fournit uniquement des indications sur le transfert des consentements exprès; le transfert direct des consentements tacites (tels que ceux découlant d'une relation commerciale en cours) n'est pas abordé.

Dans le cadre du consentement tacite sur la base d'une relation d'affaires, la LCAP prévoit que la relation d'affaires en cours sera transférée à la suite de la vente d'une entreprise à un acheteur. Cependant, elle ne précise pas spécifiquement que les consentements qui découlent de cette relation et qui sont détenus par l'entreprise peuvent également être transférés. Par conséquent, un enjeu important lié à la LCAP à aborder lors de la négociation d'une acquisition d'actifs porte sur l'obtention et le maintien des consentements des clients à recevoir des messages électroniques commerciaux sur cette base. Lors de l'achat de renseignements confidentiels utilisés pour distribuer des messages électroniques commerciaux, l'acheteur doit s'assurer que les consentements achetés auprès du vendeur sont validement détenus et transférables en vertu de la LCAP (et des lois sur la vie privée).

Les lignes directrices sur le consentement tacite ajoutent une autre couche d'interprétation :

> « Lors de la vente d'une entreprise, le consentement exprès est transféré avec l'entreprise, si le contrat de vente de cette dernière comprend une clause pour le transfert des consentements comme partie de l'ensemble des biens. Par conséquent, le nouveau propriétaire pourra continuer d'envoyer des MEC aux destinataires qui avaient donné leur consentement exprès, tant qu'il satisfait aux autres exigences de la LCAP. Au paragraphe 10(12), la LCAP indique aussi spécifiquement que, dans le cas de la vente d'une entreprise, le nouveau propriétaire de l'entreprise est réputé avoir les relations d'affaires en cours établies dans le cadre de l'entreprise. »

Les lignes directrices sur le consentement tacite semblent indiquer que les consentements tacites ne se transfèrent pas *en soi* et que c'est plutôt l'exemption de consentement créée par une relation d'affaires en cours valide qui peut être invoquée par une entreprise acheteuse. Cependant, il incombe à l'acheteur de s'assurer que ces relations d'affaires sous-jacentes sont en fait valides.

Une considération importante ici sera également de savoir quelle entité bénéficie de la relation d'affaires en cours. Les lignes directrices sur le consentement tacite énoncent que « dans le cas de la vente d'une entreprise, le nouveau propriétaire de l'entreprise est réputé avoir les relations d'affaires en cours établies dans le cadre de l'entreprise ». En d'autres mots, ces relations ne sont pas divisibles, ce qui crée une situation de tout ou rien.

Il existe peu de directives en ce qui concerne le transfert d'autres formes de consentement tacite, telles que le consentement tacite découlant de la publication bien en vue d'une adresse électronique.

Sur la base des indications actuellement disponibles, le transfert des consentements est une chose qu'il convient d'examiner soigneusement au cas par cas. Ceci est particulièrement vrai lorsque les consentements transférés sont des consentements tacites.

Exigences quant à la forme du message

Les organismes qui envoient des MEC doivent réviser l'information qui accompagne toutes leurs communications électroniques commerciales externes qui sont des MEC.

Ces exigences s'appliquent à tous les MEC (sauf les exceptions limitées dont il est question ci-dessus), même si le destinataire a consenti à l'envoi de cette catégorie de messages ou si le message lui a été envoyé en réponse à une demande qu'il a soumise.

Exigences quant à la forme du message

La LCAP stipule que tous les messages électroniques commerciaux doivent inclure les renseignements suivants :

a) le nom de la personne qui envoie le message et, s'il s'agit d'une autre personne, le nom de la personne au nom de laquelle le message est envoyé;

b) le nom que ces personnes utilisent dans le cadre de leurs activités commerciales;

c) les adresses municipale et postale de ces personnes; et

d) un numéro de téléphone pour communiquer avec ces personnes, une adresse de courrier électronique ou une adresse de site Web de ces personnes.

Lorsqu'il est impossible d'indiquer tous ces renseignements dans un message (par exemple si le support limite le nombre de caractères qu'il est possible d'inclure dans le message), la réglementation prévoit que ces renseignements peuvent figurer sur un site Web dont on aura placé l'adresse en hyperlien dans le message.

Les organisations devront réviser tous les types de messages électroniques qu'elles utilisent pour communiquer avec des tiers et veiller à ce que toutes leurs méthodes de communication soient configurées de manière à respecter les exigences de la loi.

CONSEIL : Plusieurs systèmes de courriel sont configurés de sorte que les renseignements de signature ne figurent que dans le premier message d'une chaîne de courriels. Pour des raisons d'espace, toutes les réponses de la chaîne n'indiquent pas la signature de l'expéditeur. Une telle configuration n'est pas conforme aux dispositions de la LCAP. Le premier message électronique commercial envoyé par une partie en réponse à un message doit désormais être conforme aux exigences et rédigé de façon à ce que l'information prescrite figure au moins une fois dans la chaîne de courriels.

Mécanisme d'exclusion

Aux termes de la LCAP, chaque message doit comporter un mécanisme d'exclusion permettant au destinataire de ne plus recevoir d'autres messages. Le mécanisme d'exclusion doit respecter les exigences suivantes :

a) permettre à la personne qui reçoit le message électronique d'exprimer sans frais sa volonté de ne plus recevoir d'autres messages électroniques commerciaux – ou certaines catégories de ceux-ci – de la personne qui l'a envoyé ou, le cas échéant, de celle au nom de qui il a été envoyé, en utilisant soit la méthode qui a été employée pour envoyer le message, soit, si cela est pratiquement impossible, toute autre méthode électronique qui lui permet d'exprimer cette volonté; et

b) fournir l'adresse électronique ou un lien à la page Web à laquelle la personne peut communiquer sa volonté.

La disposition relative au mécanisme d'exclusion indique que deux méthodes doivent être offertes aux destinataires de messages pour leur permettre d'exprimer leur volonté de ne plus recevoir d'autres messages. Pour certains types de messages, un mécanisme d'exclusion peut remplir ces deux exigences. Par exemple, un courriel qui indique une adresse électronique de réponse remplirait les deux exigences des alinéas a) et b) ci-dessus.

La réglementation du CRTC précise qu'un mécanisme d'exclusion doit pouvoir « s'exécuter facilement ». Au sens des lignes directrices générales, un mécanisme d'exclusion s'exécute facilement « s'il est simple, rapide et facile d'utilisation pour le consommateur et si l'accès se fait sans difficulté ni délai ». Le CRTC estime qu'un « hyperlien dans un courriel qui mène l'utilisateur à une page Web où ce dernier peut indiquer qu'il ne souhaite plus recevoir de MEC ou certains types de MEC de l'expéditeur » est un exemple de mécanisme d'exclusion qui s'exécute facilement. Dans le cas d'un message texte (SMS), l'utilisateur devrait avoir le choix entre la possibilité de répondre au message par le mot « STOP » ou « DÉSABONNEMENT » et la possibilité de cliquer sur un hyperlien qui mène à une page Web où ce dernier peut indiquer qu'il souhaite ne plus recevoir de MEC ou certains types de MEC de l'expéditeur.

Les entreprises peuvent créer un mécanisme d'exclusion qui permet au destinataire de retirer son nom de certains types de MEC uniquement, mais ce mécanisme doit également comprendre une option d'exclusion de tous les types de MEC.

Mise à jour des systèmes de messagerie

En vertu de la LCAP, les organisations devront implanter des systèmes leur permettant de retracer les consentements des destinataires et de traiter les demandes d'exclusion.

Idéalement, ces systèmes doivent être intégrés au système de messagerie ou au système de gestion des relations avec la clientèle. Lorsqu'un employé s'apprête à envoyer un MEC à un destinataire qui a demandé une exclusion ou qui n'a pas donné son consentement, le système doit bloquer l'envoi ou afficher un message indiquant que l'entreprise n'est pas autorisée à envoyer un message à ce destinataire.

Même si un tel système peut être extrêmement coûteux, les organisations devront tout de même s'assurer que les mécanismes de gestion des consentements et d'exclusion sont opérationnels, à jour et constamment activés.

Assurer le suivi des consentements

Un système de suivi des consentements peut être intégré de façon très simple, comme dans le cas d'une petite organisation où les consentements peuvent être inscrits sur une feuille électronique, ou encore de façon plus complexe, comme dans le cas d'une grande organisation qui constituerait une base de données intégrée.

Les organisations qui se fient aux dispositions de la LCAP en matière de consentement tacite pour l'envoi de messages électroniques commerciaux doivent avoir un système de gestion des consentements en mesure de repérer les dates d'expiration de chaque catégorie de consentement. Par exemple, si une société reçoit une demande d'un client potentiel à propos d'un de ses produits, le système de gestion des consentements doit prévoir qu'elle dispose de six mois, suivant la réception de cette demande, pour y donner suite.

Nous insistons sur le fait qu'en plus de mettre en œuvre un système qui permet de gérer tant les consentements tacites que les consentements exprès, les organisations devraient faire tous les efforts possibles, pendant la période de validité des consentements tacites, pour que ces consentements soient transformés en consentements exprès.

Donner suite aux demandes d'exclusion

Les organisations qui ne donnent pas suite aux demandes d'exclusion risquent des sanctions sévères. Pour cette raison, toutes les entreprises doivent mettre en œuvre un système qui reconnaît les adresses électroniques auxquelles elles ne peuvent envoyer de MEC. Idéalement, le système bloquera même l'envoi de messages à ces adresses. De plus, il convient de souligner que certains clients, après avoir retiré leur consentement, peuvent le redonner. Il faut donc prévoir la possibilité de retirer l'adresse de ces personnes de la liste d'envoi, puis de la remettre.

L'expéditeur doit traiter la demande d'exclusion au cours des 10 jours qui en suivent la réception. Pour plus de renseignements sur les exigences techniques relatives à cette question, reportez-vous aux sections précédentes.

Preuve de conformité

Être conforme à la LCAP ne suffit pas. Votre organisation doit être en mesure de prouver la conformité à l'aide de dossiers bien documentés. Le CRTC a publié des lignes directrices importantes sur le niveau de tenue de dossiers auquel il s'attend. Conformément au thème général de la LCAP, les attentes du CRTC sont élevées.

Poursuivant ce thème, dans ses premières décisions, le CRTC a souligné que le fardeau de preuve de la LCAP incombe à la personne qui allègue le consentement et a insisté pour qu'une preuve soit fournie pour chaque message faisant l'objet d'une enquête donnée.[22] Les organisations qui sont incapables de fournir des preuves à un niveau granulaire seront confrontées à des préoccupations importantes.

Les lignes directrices du CRTC sur les programmes de conformité énoncent que votre politique de conformité écrite doit prévoir « la tenue de dossiers, surtout en ce qui a trait au consentement ». Elles expliquent ensuite les avantages de la tenue de dossiers :

> « L'application de pratiques exemplaires en matière de tenue de dossiers peut aider l'entreprise à i) déceler d'éventuels problèmes de non-conformité, ii) analyser les plaintes des consommateurs et y répondre, iii) répondre aux questions sur les pratiques et procédures de l'entreprise, iv) surveiller le programme de conformité, v) déterminer si des mesures correctives s'imposent et prouver qu'elles ont bel et bien été mises en place, et vi) élaborer une défense fondée sur la diligence raisonnable en cas de plaintes formulées auprès du Conseil contre l'entreprise. »

Les lignes directrices sur le consentement tacite énumèrent les documents de base que les organisations devraient conserver :

- « les politiques et procédures relatives aux messages électroniques commerciaux;
- toutes les demandes de désabonnement et les mesures qui en résultent;
- toutes les preuves du consentement exprès (p. ex., les enregistrements audio ou les formulaires remplis) de consommateurs qui acceptent qu'on communique avec eux par des messages électroniques commerciaux;
- les registres de consentement à recevoir des messages électroniques commerciaux;
- les transcriptions des messages électroniques commerciaux;
- les dossiers relatifs aux campagnes des MEC;
- les documents relatifs à la formation des employés;
- les autres procédures de l'entreprise;
- les dossiers financiers officiels. »

Les lignes directrices sur le consentement tacite traitent également de la manière de prouver le consentement tacite au moyen d'une série d'exemples détaillés. L'un d'eux aborde un scénario courant selon lequel la publication d'une adresse électronique en ligne constitue un consentement tacite :

[22] Décision Compu-Finder (CRTC 2017-368) au para. 67: « 67.Comme le Conseil l'a fait remarquer dans la décision de Conformité et Enquêtes 2016-428, l'exemption relative à la publication bien en vue et les exigences qui en résultent fixent une norme plus exigeante que la simple disponibilité publique des adresses électroniques. Ces conditions n'accordent pas aux expéditeurs de MEC la liberté d'envoyer des messages à une adresse électronique qu'ils trouvent en ligne; elles établissent plutôt les circonstances limitées dans lesquelles le consentement peut être raisonnablement déduit, lesquelles **doivent être évaluées au cas par cas.** ».

> « Une société recueille des adresses de courriel sur des sites Web ou dans d'autres formes de publications de nature médiatique. Si la société souhaite invoquer la publication bien en vue comme une forme de consentement tacite, elle doit être en mesure de prouver que le site Web ou l'annonce d'où proviennent les adresses de courriel ne comportait aucun énoncé interdisant la réception de MEC et de démontrer le lien avec l'entreprise du destinataire, son rôle, ses fonctions ou ses tâches au sein d'une entreprise ou dans le cadre d'une fonction officielle; par exemple, afin de prouver l'absence d'énoncés interdisant la réception de MEC, une société pourrait enregistrer des captures d'écran ou établir un document au moment de la publication dans laquelle l'adresse apparaissait, incluant les renseignements, comme la date, l'adresse de courriel et l'URL. »

Des dossiers de conformité détaillés seront également utiles pour prouver la diligence raisonnable si le CRTC enquête sur une infraction non intentionnelle (comme on le décrit plus loin dans le présent document).

Anciens consentements

L'article 66 de la LCAP prévoyait une période transitoire de trois ans pour certains consentements qui pourraient être implicites en fonction d'une relation avec le destinataire. Cette période transitoire a pris fin en juillet 2017. Les organisations doivent veiller à ne pas utiliser les autorisations transitoires expirées, car celles-ci peuvent constituer une responsabilité cachée si elles n'ont pas été converties en un consentement valide pendant la période transitoire.

La FAQ du CRTC et le REIR suggèrent que les consentements exprès reçus avant le 1er juillet 2014 suffiront aux fins de la LCAP. Cependant, il n'y a pas de «droits acquis» pour d'autres formes de consentements existants, y compris des consentements implicites qui étaient «groupés» dans des modalités, ou des consentements qui contenaient des cases «J'accepte» précochées.

Maintenant que la période transitoire a expiré, les organisations voudront réexaminer la question de savoir si certaines de, ou toutes, leurs bases historiques de consentement restent valides.

Logiciels malveillants et logiciels espions

Les dispositions de la LCAP s'appliquent potentiellement à tous les programmes informatiques installés sur tout type d'ordinateur, de système, de machine, d'appareil ou de dispositif dans le cadre d'une activité commerciale[23]. Il n'est pas nécessaire que ces programmes causent quelque tort que ce soit. Les programmes visés par les dispositions relatives aux logiciels malveillants et aux logiciels espions peuvent aller des applications sur les ordinateurs personnels, les tablettes et les appareils mobiles aux programmes intégrés dans les produits de consommation dont les automobiles, les télévisions, les enregistreurs personnels de vidéo, les systèmes audio domestiques, les appareils électroménagers et les dispositifs utilisés dans les habitations comme les thermostats, les systèmes de sécurité, les contrôles d'éclairage et les systèmes de réseautage domestique, de même qu'un ensemble infini d'autres dispositifs, notamment les montres, les jouets, les systèmes d'apprentissage, les prothèses auditives et d'autres appareils médicaux. Ils sont aussi omniprésents dans les applications industrielles et commerciales.

Ces dispositions doivent être examinées avec un soin particulier, car les lignes directrices du CRTC sur l'installation de programmes informatiques semblent introduire des concepts d'interprétation qui pourraient être en contradiction avec le langage actuel de la LCAP. Par exemple, le CRTC suggère qu'«un logiciel installé soi-même n'est pas couvert par la LCAP», mais suggère ensuite qu'une personne peut causer l'installation d'un programme par une divulgation incomplète. Ces concepts ne suivent pas de près le langage de la LCAP elle-même et pourraient causer du faux réconfort à l'avenir si le CRTC change de point de vue ou si le droit privé d'action entre en vigueur.

Il est illégal en vertu de la LCAP d'installer ou de faire installer un programme d'ordinateur dans l'ordinateur d'une autre personne ou, après avoir ainsi installé ou fait installer un programme d'ordinateur, de faire envoyer un message électronique par cet ordinateur sauf a) si la personne a obtenu le consentement exprès du propriétaire ou de l'utilisateur autorisé de l'ordinateur et se conforme aux exigences de divulgation prévues par le paragraphe 11(5) ou b) la personne agit en vertu d'une ordonnance judiciaire (par. 8(1)).

Quiconque entend obtenir le consentement doit en indiquer les fins en termes simples et clairs. Cela comporte, de façon générale, la fonction et l'objet du programme d'ordinateur qui sera installé si le consentement est donné (par. 10(1) et (3)).

Si le programme effectue une des fonctions relatives aux logiciels malveillants ou aux logiciels espions mentionnées au paragraphe 10(5), la personne qui sollicite le consentement exprès doit, au moment de la sollicitation, en termes clairs et facilement lisibles et ailleurs que dans le contrat de licence, a) décrire les éléments du programme qui effectuent ces fonctions, notamment leur nature et objet et les conséquences prévisibles qu'ils auront sur le fonctionnement de l'ordinateur, et b) les porter à l'attention de l'autre personne de la façon prévue par règlement (par. 10 (4)). Le CRTC déclare qu'une reconnaissance provenant de l'utilisateur est exigée dans de tels cas.

Les exigences de consentement et de divulgation de base ne s'appliquent pas à une mise à jour ou à niveau a) si l'installation ou l'utilisation du programme a fait l'objet d'un consentement exprès initial, b) si la personne qui a donné le consentement a le droit de recevoir la mise à jour ou à niveau aux termes du consentement exprès et c) si la mise à jour ou à niveau est installée conformément à ce consentement (par. 10(7)). La mise à jour ou à niveau ne peut pas être installée sans l'obtention d'un nouveau

[23] Pour une analyse plus complète des dispositions relatives aux programmes d'ordinateur de la LCAP et du règlement connexe, voir l'article de Barry Sookman intitulé *The Industry Canada CASL regulations and RIAS: a lost opportunity* à l'adresse http://www.barrysookman.com/2013/12/16/the-industry-canada-casl-regulations-and-rias-a-lost-opportunity/

consentement exprès si elle contient l'une des fonctions de logiciel malveillant ou de logiciel espion énumérées au paragraphe 10(5).

La personne est réputée consentir expressément à l'installation d'un programme d'ordinateur si a) le programme relève de l'une des catégories énumérées au paragraphe 10(8), p. ex. il s'agit d'un témoin de connexion, d'un code HTML, d'un Java Script, d'un système d'exploitation ou de tout autre programme qui ne peut être exécuté que par l'entremise d'un autre programme auquel elle a déjà expressément consenti à l'installation ou à l'utilisation, mais seulement si b) il est raisonnable de croire, d'après le comportement de l'utilisateur, qu'il consent à l'installation du programme.

Un règlement peut allonger la liste des programmes pour lesquels le consentement exprès est réputé, mais tout ajout à la liste est assujetti à la réserve que le comportement de l'utilisateur soit tel qu'il est raisonnable de croire qu'il consent à l'installation du programme.

Les interdictions s'appliquent aux programmes installés à partir du Canada dans un autre pays ou vice versa.

Les systèmes d'exploitation et les témoins de connexion

Comme il a été mentionné, la personne est réputée consentir expressément à l'installation d'un programme d'ordinateur si a) le programme relève de l'une des catégories énumérées au paragraphe 10(8), p. ex. il s'agit d'un témoin de connexion, d'un code HTML, d'un java script, d'un système d'exploitation ou de tout autre programme qui ne peut être exécuté que par l'entremise d'un autre programme auquel elle a déjà expressément consenti à l'installation ou à l'utilisation, mais seulement si b) il est raisonnable de croire, d'après le comportement de l'utilisateur, qu'il consent à l'installation du programme.

Il peut être difficile d'appliquer la distinction entre un programme d'application et un programme de système d'exploitation. Dans le REIR, Industrie Canada a indiqué qu'un système de freinage pourrait être un système d'exploitation. Elle a aussi indiqué que le paragraphe 10(7) ne s'applique pas aux mises à jour ou à niveau des logiciels du type de ceux énumérés au paragraphe 10(8). Cette indication confirme que lorsqu'un programme fait l'objet d'une présomption de consentement exprès, cette présomption s'applique également à la mise à jour, dans la mesure où le comportement de l'utilisateur est tel qu'il est raisonnable de croire qu'il consent à l'installation du programme.

Dans le REIR, Industrie Canada a aussi indiqué que malgré le fait que le paragraphe 10(8) crée une présomption de consentement exprès à l'installation de témoins de connexion, il ne s'agit vraisemblablement pas de programmes visés par la Loi.

La sécurité des réseaux et les FST

Industrie Canada a souligné dans le REIR que les intervenants avaient exprimé la crainte que la LCAP les empêche de prendre les mesures nécessaires pour contrer les menaces à la sécurité de leurs réseaux, ce qui irait à l'encontre des objets de la Loi. Pour répondre à cette crainte, au moyen du pouvoir de réglementation prévu par le sous-alinéa 10(8)a)(vi) de la Loi, le Règlement IC a modifié l'ébauche précédente de manière à prévoir une présomption de consentement permettant aux fournisseurs de services de télécommunications (FST) d'installer des programmes d'ordinateur afin d'assurer la sécurité du réseau contre une menace actuelle et identifiable à la disponibilité, à la fiabilité, à l'efficacité ou à l'utilisation optimale de leur réseau.

La nouvelle exception précise les programmes suivants :

> le programme qui est installé par le télécommunicateur ou en son nom uniquement pour protéger la sécurité de la totalité ou d'une partie de son réseau d'une menace actuelle et identifiable à l'accessibilité, à la fiabilité, à l'efficacité ou à l'utilisation optimale du réseau.

Les mises à niveau du réseau

Comme l'a souligné Industrie Canada dans le REIR, des intervenants ont exprimé la crainte que la LCAP les empêche de mettre à jour ou à niveau leurs réseaux. Pour répondre à cette crainte, le règlement prévoit également une présomption de consentement permettant aux FST d'installer des logiciels sur des appareils pour tout ou partie d'un réseau aux fins de mise à jour et à niveau.

La nouvelle exception précise les programmes suivants :

> le programme qui est installé par le télécommunicateur qui possède ou exploite le réseau, ou en son nom, sur tous les ordinateurs faisant partie du réseau pour la mise à jour ou à niveau de ce réseau.

La correction de défaillances de programme

Le Règlement IC a aussi introduit une exception limitée concernant la correction de défaillances de programmes. Elle exempte les programmes suivants :

> « le programme qui est nécessaire à la correction d'une défaillance dans le fonctionnement de l'ordinateur ou d'un de ses programmes et qui est installé uniquement à cette fin. »

La sécurité publique

Le REIR souligne que même si des programmes sont installés dans le cadre d'une activité commerciale, ils ne sont pas visés par la LCAP s'ils sont nécessaires pour des raisons de sécurité publique. Selon le REIR :

> « Il convient de noter que la Loi s'applique uniquement aux programmes d'ordinateur installés dans le cadre d'une activité commerciale et exclut dans sa définition la sécurité publique et autres, par conséquent les questions de sécurité publique. Cependant, pour ce qui est de questions liées aux logiciels qui ne relèvent pas de la sécurité publique, le Règlement prévoit le consentement présumé pour l'installation de programmes d'ordinateur qui sont nécessaires pour corriger une défaillance liée au fonctionnement d'un système ou d'un programme d'ordinateur qui est déjà installé. »

La forme du consentement aux mises à jour et à niveau

Le REIR fournit également des indications sur la forme du consentement requis pour l'installation d'une mise à jour ou à niveau. Selon le REIR :

> « Pour les mises à jour ou à niveau des programmes d'ordinateur installés après l'entrée en vigueur de la LCAP, la Loi permet aux entreprises d'obtenir le consentement du propriétaire ou de l'utilisateur autorisé pour les futures mises à jour ou à niveau du programme d'ordinateur en même temps qu'ils obtiennent le consentement pour l'installation initiale, ou lorsque l'utilisateur effectue un téléchargement. Ainsi, lorsqu'un programme informatique est installé, le consentement doit en général être demandé conformément à la Loi, mais il n'existe aucune exigence relative à la forme d'une demande de consentement pour installer les mises à jour ou à niveau, que ce consentement soit demandé au préalable ou au moment de l'installation de la mise à jour ou à niveau. »

Même si l'énoncé n'y fait pas directement référence, il semble refléter les dispositions que renferme le paragraphe 10(7), qui prévoient qu'une mise à jour ou à niveau peut être installée avec consentement exprès si la personne qui a donné le consentement a le droit de recevoir la mise à jour ou à niveau aux termes des conditions du consentement et que l'installation est faite conformément à celles-ci. Cette approche est soutenue par les lignes directrices sur l'installation de programmes d'ordinateur, qui énoncent ce qui suit :

> « Une mise à jour ou à niveau consiste généralement à remplacer le logiciel par une version nouvelle ou améliorée pour mettre le système à jour ou en améliorer les caractéristiques. Habituellement, la mise à jour ou à niveau aura de nouvelles fonctions. Les mises à jour ou à niveau courantes comprennent le changement de version du système d'exploitation, de la suite bureautique, du logiciel antivirus ou d'autres outils variés.
>
> Une mise à jour ou à niveau apporte des modifications ou remplace des logiciels préalablement installés. Récupérer et afficher des renseignements courants à l'aide d'un programme n'est pas considéré être une mise à jour du programme dans le contexte de la LCAP. Par exemple, la mise à jour ou rafraîchir les renseignements affichés dans un programme, tel que l'actualisation des prévisions de la météo sur une application météorologique, ou l'actualisation des grilles horaires de télévision à l'aide du guide de programmation télévisuelle électronique, ne constituent pas une mise à jour ou à niveau au sens de la LCAP. »

Cas où les fonctions de logiciel malveillant et de logiciel espion d'un programme doivent être divulguées

En vertu du paragraphe 10(4), si le programme effectue l'une des fonctions de logiciel malveillant ou de logiciel espion énumérées au paragraphe 10(5), la personne qui sollicite le consentement exprès doit, au moment de la sollicitation, décrire les éléments du programme qui effectuent ces fonctions, notamment leur nature et objet et les conséquences prévisibles qu'ils auront sur le fonctionnement de l'ordinateur.

Les fonctions énumérées au paragraphe 10(5) sont ainsi décrites :

> (5) Les fonctions visées au paragraphe (4) sont celles mentionnées ci-dessous dont la personne qui sollicite le consentement sait qu'elles auront pour effet de faire fonctionner l'ordinateur d'une façon contraire aux attentes raisonnables du propriétaire ou de l'utilisateur autorisé de celui-ci et dont il entend qu'elles aient cet effet :
>
> a) la collecte de renseignements personnels sur l'ordinateur;
>
> b) l'entrave au contrôle de l'ordinateur par le propriétaire ou l'utilisateur autorisé de celui-ci;
>
> c) la modification des paramètres, préférences ou commandements déjà installés ou mis en mémoire dans l'ordinateur ou l'entrave à leur utilisation, à l'insu du propriétaire ou de l'utilisateur autorisé de l'ordinateur;
>
> d) la modification des données déjà mises en mémoire dans l'ordinateur ayant pour effet d'empêcher, d'interrompre ou d'entraver l'accès ou l'utilisation légitimes de ces données par le propriétaire ou l'utilisateur autorisé de celui-ci;
>
> e) la communication de l'ordinateur, sans l'autorisation de son propriétaire ou utilisateur autorisé, avec un autre ordinateur ou dispositif;
>
> f) l'installation d'un programme activé par un tiers à l'insu du propriétaire ou de l'utilisateur autorisé de l'ordinateur;

> g) toute autre fonction précisée dans les règlements.

Interprétés ensemble, les paragraphes 10(4) et 10(5) indiquent fortement que la divulgation est exigée à la fois lorsque l'un des éléments indiqués aux alinéas a) à g) existe et lorsque la personne qui sollicite le consentement exprès sait et veut que le système informatique fonctionne d'une manière contraire aux attentes raisonnables du propriétaire. C'est ce qu'a confirmé le REIR, qui énonce ce qui suit.

> Il convient de noter que le test de vraisemblance qui est intégré à la disposition relative au consentement présumé de la LCAP s'applique également comme un mécanisme visant à réduire le risque d'abus du consentement présumé dans ce Règlement. En outre, les exigences du paragraphe 10(4) de la Loi décrivant les fonctions du paragraphe 10(5) n'entrent en jeu que lorsque le consentement doit être sollicité. En outre, les obligations de notification au paragraphe 10(4) s'appliquent seulement lorsque la personne sollicitant le consentement sait que les fonctions visées au paragraphe 10(5) peuvent avoir pour effet de faire fonctionner l'ordinateur d'une façon contraire aux attentes raisonnables du propriétaire ou de l'utilisateur autorisé de celui-ci.

Les programmes existants et les dispositions transitoires

Il existe des centaines de milliers, voire même des millions, de programmes informatiques déjà installés sur des systèmes dans tout le pays. La LCAP s'applique à tous ces programmes, pour au moins deux raisons. Il est illégal d'installer des mises à jour ou à niveau à ces programmes sauf en cas de consentement exprès original d'installer les programmes comportant le consentement d'installer les mises à jour ou à niveau sauf si un nouveau consentement exprès est obtenu. Deuxièmement, il est illégal pour la personne qui a installé un programme de faire en sorte que ce programme lui transmette de l'information sans d'abord avoir obtenu un consentement exprès. De nombreux programmes existants sont régulièrement et automatiquement mis à jour (comme le désirent les consommateurs) ou nécessitent la transmission d'informations à une personne pour que le programme continue de fonctionner.

Pour la grande majorité des programmes déjà utilisés, les utilisateurs n'ont pas donné de consentements exprès à la réception de mises à jour ou à niveau. De plus, les fournisseurs originaux des programmes n'ont souvent pas de dossiers indiquant les coordonnées comme les adresses électroniques des personnes qui reçoivent les mises à jour ou à niveau. On ne peut pas non plus envoyer des courriels à de nombreux utilisateurs pour leur demander leur consentement, si cela s'inscrit dans une activité commerciale, sans contrevenir aux dispositions antipourriel de la LCAP.

Les dispositions transitoires visaient à atténuer temporairement ces problèmes. L'article 67 prévoit ce qui suit :

> Si des programmes ont été installés dans l'ordinateur d'une personne avant la date d'entrée en vigueur de l'article 8, cette personne est réputée avoir consenti à la mise à jour ou à niveau de ces programmes et ce consentement vaut jusqu'à ce qu'elle le retire ou, au plus tard, jusqu'à l'expiration des trois ans suivant l'entrée en vigueur de cet article.

La LCAP ne semble prévoir que deux façons de permettre l'installation d'une nouvelle mise à jour ou à niveau pour un programme existant. Si la mise à jour ou à niveau est considérée comme un nouveau programme, le consentement exprès est exigé. Si on se fonde sur un consentement antérieur lié à la première installation, il doit y avoir a) un consentement exprès original à l'installation ou à l'utilisation du programme, b) le droit de recevoir la mise à jour ou à niveau aux termes des conditions du consentement exprès et c) une installation de la mise à jour ou à niveau conformément à ces conditions.

À sa lecture, l'article 67 ne semble pas respecter les normes nécessaires pour permettre l'installation des mises à jour ou à niveau des programmes antérieurs, car seul le consentement tacite et non exprès est

réputé avoir été donné. Toutefois, dans le REIR, Industrie Canada soutient qu'une période transitoire de trois ans permet l'installation de mises à jour et à niveau pour les programmes installés avant l'entrée en vigueur de la LCAP.

Déclarations fausses ou trompeuses

La LCAP a modifié en outre la *Loi sur la concurrence* de façon à interdire l'inclusion, dans les messages électroniques, de déclarations fausses ou trompeuses qui viseraient à mousser les intérêts de l'entreprise et de ses produits. La *Loi sur la concurrence* comporte depuis longtemps des dispositions relatives aux déclarations fausses ou trompeuses (en matière de publicité trompeuse), et la LCAP a présenté des dispositions particulières s'appliquant aux courriels et autres messages électroniques.

En vertu des modifications apportées par la LCAP, la *Loi sur la concurrence* proscrit toute déclaration fausse ou trompeuse faite dans la description de l'expéditeur de tout message électronique, dans l'objet du message et dans son contenu, de même que dans l'URL ou tout autre localisateur de page Web.

Ces amendements ont été mises en évidence en mars 2015, lorsque le Bureau de la concurrence a déposé une réclamation de 30 millions de dollars contre trois agences de location de voitures pour des représentations fausses ou trompeuses dans divers documents de commercialisation destinés au public canadien. Les accusations portées contre les agences comprenaient des réclamations en vertu des amendements de la LCAP. L'affaire a été réglée par la suite au coût de 3 millions de dollars pour les agences.[24] Par la suite, en 2017, le Bureau de la concurrence a conclu un règlement de 1,25 million de dollars avec une autre paire d'agences de location de voitures dans une affaire qui concernait des courriers électroniques et des applications de téléphonie mobile.[25]

Les organisations conformes à la LCAP devront informer leurs employés et leurs autres représentants que les dispositions de la LCAP relativement aux déclarations fausses ou trompeuses s'appliquent de façon distincte à chaque section d'un message. Les employés des ventes ou du marketing ne pourront plus simplement invoquer les énoncés contenus dans le corps du message pour qualifier les déclarations de l'intitulé du message. Ainsi, si l'objet d'un message contient une déclaration fausse ou trompeuse, l'expéditeur contrevient à la *Loi sur la concurrence* malgré la présence, en petits caractères, d'un texte qui serait contenu au corps du message.

Messages électroniques à contenu faux ou trompeur

La LCAP interdit, en vue de promouvoir directement ou indirectement tout intérêt commercial ou tout produit, d'envoyer ou de faire envoyer un message électronique qui comporte une déclaration fausse ou trompeuse sur un point important. Le « message électronique » dans ce cas est l'ensemble du message.

CONSEIL : La mention d'une déclaration fausse ou trompeuse sur un point important peut laisser croire que certaines déclarations fausses ou trompeuses qui ne porteraient pas sur un point important pourraient être autorisées. Il faut ainsi mentionner que l'expression « sur un point important » ne s'applique pas à l'objet du message, à la description de l'expéditeur et au localisateur. Dès lors, les déclarations fausses ou trompeuses dans ces éléments seront interprétées de façon plus stricte.

Déclaration fausse ou trompeuse dans l'objet du message

La principale différence entre le marketing traditionnel et le marketing électronique se manifeste dans les dispositions de la LCAP relatives aux déclarations fausses ou trompeuses contenues à l'objet d'un message. Alors qu'un dépliant ou une affiche imprimée peuvent avoir un titre prétentieux ou exagéré si la portée en est réduite ailleurs dans le dépliant ou l'affiche, la LCAP stipule que toute déclaration fausse ou

[24] Voir http://www.bureaudelaconcurrence.gc.ca/eic/site/cb-bc.nsf/fra/03885.html et https://www.canada.ca/fr/bureau-concurrence/nouvelles/2016/06/avis-et-budget-s-assureront-que-les-prix-annonces-sont-exacts.html

[25] https://www.canada.ca/fr/bureau-concurrence/nouvelles/2017/04/hertz_et_dollar_thriftydevrontpayerunepenalitede125milliondedoll.html et http://www.ct-tc.gc.ca/CMFiles/CT-2017-009_Registered%20Consent%20Agreement_2_66_4-24-2017_7054.pdf

trompeuse dans l'objet d'un message électronique constitue une infraction, peu importe ce que peut contenir le corps ou tout autre élément du message.

Prenons l'exemple d'une compagnie aérienne qui enverrait à ses abonnés un courriel présentant des « vols aller-retour Ottawa-Calgary à 299 $ ». Un dépliant imprimé pourrait porter un tel titre s'il comporte une mention précisant que ce prix ne comprend pas les frais additionnels, ni les taxes ou d'autres frais d'admissibilité. Mais dans le cas d'un message électronique, la déclaration faite dans l'objet du message doit être complète par elle-même. En conséquence, il peut être risqué d'inclure des déclarations prétentieuses ou exagérées dans l'objet d'un message.

Conseil : La LCAP n'impose pas de taille ou de nombre limite de caractères contenu à l'objet d'un message. Les organisations doivent donc prévoir la possibilité d'inclure dans l'objet une mention telle que « certaines conditions s'appliquent » ou, encore, « voir les conditions ci-dessous » afin de se conformer aux nouvelles dispositions de la *Loi sur la concurrence*.

Renseignements faux ou trompeurs sur l'identité de l'expéditeur

Les dispositions relatives aux renseignements faux ou trompeurs sur l'identité de l'expéditeur ne doivent pas préoccuper outre mesure les organisations légitimes. De façon générale, ces dispositions concernent le champ « Message de » d'un courriel, et elles ont pour but d'empêcher l'envoi de messages sous une fausse identité.

Localisateur de page Web faux ou trompeur

Une pratique courante chez les expéditeurs de pourriels consiste à créer une adresse Web qui semble, à première vue, représenter une organisation légitime. Par exemple, en ajoutant un « c » au nom McCarthy et en créant le site Web www.mcccarthy.ca, il est facile de tromper certains destinataires de courriels et de leur faire croire que ce lien mène au site Web de McCarthy Tétrault S.E.N.C.R.L., s.r.l. La LCAP interdit de telles pratiques et le fait d'envoyer une fausse URL ou un faux localisateur de page Web dans le but de promouvoir un intérêt commercial ou un produit constitue une infraction. Cette nouvelle disposition n'est évidemment pas une préoccupation pour les organisations légitimes.

Droit d'action

Il convient de noter que le droit d'action s'appliquera également aux infractions à l'article 74.011, ce qui en fait la seule disposition de la *Loi sur la concurrence* qui fait l'objet d'un droit d'action[26]. Comme il est indiqué ci-dessus, aucune nouvelle date n'a été prévue pour l'entrée en vigueur du droit d'action.

[26] Pour une discussion sur les problèmes présentés par le droit d'action dans le contexte des dispositions de la *Loi sur la concurrence*, voir l'article de Donald Houston et Jonathan Bitra intitulé *Misguided Policy: CASL's Private Right of Action for Competition Act Reviewable Conduct* à l'adresse https://www.mccarthy.ca/en/insights/blogs/snipits/misguided-policy-casls-private-right-action-competition-act-reviewable-conduct

Conformité technique

En plus des dispositions relatives aux pourriels et aux logiciels espions, la LCAP interdit toutes les autres formes d'activité malveillante menées sur Internet ou sur les autres réseaux numériques. Bien que les organisations légitimes ne soient pas intentionnellement engagées dans ce type d'activités, la portée des dispositions de la LCAP est suffisamment grande pour qu'elles s'y attardent.

Modifier les données de transmission

Il est interdit, en vertu de la LCAP, de modifier les données de transmission d'un message électronique de façon à ce que ce message soit acheminé à un destinataire autre que le destinataire prévu par l'expéditeur. Cette disposition vise à assurer que les courriels et autres messages électroniques ne soient pas acheminés ou copiés vers un destinataire autre que celui prévu par l'expéditeur. Bien qu'il soit peu probable qu'une entreprise canadienne légitime achemine subrepticement des messages en modifiant les données de transmission, il peut arriver que le recours à certains modes d'envois automatiques ou autres procédés techniques fasse en sorte que l'entreprise contrevienne à cette disposition.

En vertu de la LCAP, les données de transmission sont celles qui, à la fois :

a) concernent les fonctions de composition, de routage, d'adressage ou de signalisation en matière de télécommunication;

b) sont transmises pour identifier, activer ou configurer un appareil ou un dispositif (notamment un programme d'ordinateur) en vue d'établir ou de maintenir une communication, ou sont produites durant la création, la transmission ou la réception d'une communication et indiquent, ou visent à indiquer, le type, la direction, la date, l'heure, la durée, le volume, le point d'envoi, la destination ou le point d'arrivée de la communication; et

c) ne révèlent pas la substance, le sens ou l'objet de la communication.

Collecte d'adresses

La LCAP modifie la LPRPDE, soit la législation canadienne sur la protection de la vie privée, de façon à interdire l'utilisation de programmes d'ordinateur pour la collecte d'adresses. Il s'agit de programmes destinés à rechercher et recueillir des adresses de courriel ou d'autres adresses électroniques dans le but de créer des listes d'envoi. L'interdiction touche tant l'utilisation de programmes de collecte d'adresses que l'utilisation des adresses électroniques obtenues grâce à ces programmes. Dès lors, il est important que les organisations qui se procurent des listes d'envoi auprès d'un tiers s'assurent que ces listes ont été obtenues selon les dispositions de la LCAP. Même si la LCAP n'interdit pas aux organisations d'obtenir des listes d'envoi d'autres parties, nous recommandons fortement qu'elles ne fassent affaire qu'avec des fournisseurs dont la réputation est établie et qui ont mis en œuvre toutes les mesures de conformité requises. Mentionnons que la présente boîte à outils contient d'autres conseils relativement au recours à des tiers.

Il faut souligner que la seule utilisation de programmes de collecte d'adresses contrevient à la LCAP. L'interdiction d'utiliser des programmes de collecte automatique d'adresses électroniques vaut même lorsque l'utilisation n'est pas liée à l'envoi de pourriels.

Collecte de renseignements personnels

La LCAP interdit l'utilisation de systèmes informatiques destinés à recueillir, outre les adresses électroniques, des renseignements personnels.

La LCAP interdit toute collecte de renseignements personnels, par tout moyen de télécommunication, si la collecte est faite en utilisant un système informatique en violation d'une loi fédérale. En d'autres mots, lorsqu'une personne pirate illégalement un système informatique, un réseau ou une base de données, la LCAP interdit la collecte de tout renseignement personnel qui s'y trouverait ainsi que l'utilisation de ces renseignements pour quelque fin que ce soit. Ces dispositions confirment l'importance de se procurer des listes d'envoi auprès de fournisseurs dont la réputation est sans tache et de conclure des ententes afin de prévenir les risques liés à l'utilisation de renseignements personnels obtenus illégalement.

Balayage des réseaux « zombies »

Très peu d'organisations légitimes sont engagées dans des activités de pollupostage de masse. Toutefois, les organisations qui se livrent à de telles pratiques illicites réussissent souvent à prendre le contrôle des systèmes informatiques d'entreprises tout à fait légitimes. Les systèmes informatiques ainsi piratés et infestés par des virus ou des logiciels malveillants sont appelés des « zombies », car les polluposteurs sont capables d'utiliser les vastes réseaux de ces systèmes, appelés réseaux zombies, pour envoyer des milliards de pourriels.

Les organisations devraient s'assurer que leurs systèmes ne sont pas utilisés à titre de systèmes zombies. Avant l'entrée en vigueur de la LCAP, les entreprises devraient procéder à un balayage technique de leurs systèmes, en prêtant une attention particulière aux serveurs de courriel et en utilisant des programmes antivirus et antimalveillants à jour et performants. De telles mesures réduiront le risque d'être victime de piratage, une éventualité qui pourrait s'avérer fort coûteuse, tant en argent qu'en temps. De plus, dans le cas où une entreprise ferait l'objet d'une enquête sur des activités de type zombie provenant de son système informatique, elle serait en mesure de démontrer qu'elle a pris toutes les mesures raisonnables pour se protéger.

Travail avec des tiers

De nombreuses organisations recourent aux services de tiers dans le cadre de leurs activités de marketing par courriel ou en ligne. Certains tiers offrent un service de prise en charge de l'ensemble des activités de marketing numérique d'une entreprise. D'autres vendent des listes de clients potentiels à des entreprises qui souhaitent accroître leur clientèle.

Les organisations qui ont recours à des tiers ne doivent pas ignorer les nouvelles dispositions de la LCAP, dispositions auxquelles sont soumis tant l'expéditeur de messages électroniques commerciaux que celui au nom duquel ces messages sont envoyés. Cela signifie que les entreprises qui confient à un tiers l'envoi de messages peuvent être tenues responsables dans le cas où ces messages contreviendraient aux dispositions de la LCAP sur l'envoi de pourriels. La LCAP oblige également que soit divulguée l'identité tant de celui qui envoie le message que de l'expéditeur pour lequel le message est envoyé.

Exigences relatives à la double divulgation

Nous avons traité, précédemment, des renseignements qu'une organisation doit divulguer sur son compte dans tout message électronique commercial, de même que des renseignements qu'elle doit divulguer lorsqu'elle sollicite un consentement à recevoir des messages électroniques commerciaux. Dans les deux cas, lorsqu'une organisation utilise les services d'un tiers pour envoyer des messages ou solliciter le consentement d'une personne, la LCAP exige une double divulgation. Ainsi, tout renseignement que l'expéditeur doit divulguer sur lui-même dans ses messages électroniques commerciaux doit également être divulgué par l'organisation au nom de laquelle un consentement est sollicité.

Les deux parties doivent s'assurer que les renseignements qu'elles divulguent sur elles-mêmes demeureront valides pendant au moins 60 jours suivant la date d'envoi du message.

Exigences relatives à l'exclusion lorsqu'un tiers sollicite un consentement

La LCAP pose des exigences additionnelles relativement à l'exclusion lorsqu'une organisation confie à un tiers la sollicitation du consentement à recevoir des messages électroniques commerciaux. Ces exigences s'appliquent dans le cas où l'organisation a embauché un tiers pour obtenir en son nom le consentement ou qu'elle a simplement acheté une liste d'envoi regroupant les coordonnées de personnes qui ont présumément donné leur consentement à ce tiers. Pour plus de renseignements sur ces exigences, veuillez vous reporter aux sections précédentes de cette boîte à outils.

Dispositions contractuelles

Lorsqu'une organisation confie à un tiers certaines des activités relevant de sa stratégie de marketing numérique, elle s'attend à ce que ce tiers connaisse les dispositions de toutes les lois applicables, y compris les lois et règlements antipourriel, et qu'elle s'y conforme. Toutefois, lorsqu'elle embauche un tiers, l'organisation doit s'assurer par contrat que le tiers assume l'entière responsabilité de se conformer aux dispositions des diverses lois et qu'il s'engage à indemniser l'organisation si celle-ci est reconnue coupable de violation des lois.

Une accusation d'infraction à la LCAP pourrait provenir d'un organisme gouvernemental, principalement le CRTC, ou d'une personne détenant un droit privé d'action (que ce soit par recours individuel ou collectif). Dès lors, les contrats régissant les services externes devraient protéger l'entreprise contre la violation des lois par le fournisseur de services, et contenir notamment :

- une déclaration et des garanties que les services sont et seront fournis en conformité avec les dispositions de la LCAP et les règlements afférents;
- un engagement à indemniser l'entreprise en cas de perte ou dommage subi en raison d'une violation présumée ou réelle de la LCAP.

Recours, pénalités et droit d'action

L'une des raisons pour lesquelles les organisations doivent être diligentes afin de se conformer à la LCAP est le fait que les pénalités, en cas d'infraction, pourraient être importantes. La LCAP prévoit l'imposition de « sanctions administratives pécuniaires » qui ne sont pas proportionnelles aux dommages causés par l'infraction. De plus, la LCAP autorise les personnes à demander, en leur conférant un droit d'action, que soient imposées des sanctions pécuniaires en plus des dommages. L'importance des amendes qui pourraient être imposées de même que la menace toujours présente d'un recours collectif confirment la sévérité de la loi et les graves conséquences d'une violation.

REMARQUE : Les dispositions établissant le droit d'action seront les dernières dispositions de la LCAP à entrer en vigueur. Ces dispositions devaient initialement entrer en vigueur en juillet 2017. Toutefois, un décret a suspendu le droit d'action et une nouvelle date n'est pas encore prévue.

SANCTIONS ADMINISTRATIVES PAR LE CRTC

Toute infraction aux dispositions de la LCAP en matière de pourriels et de logiciels espions (ces derniers n'étant pas abordés dans cette boîte à outils) est considérée comme une violation de la loi et est sujette à des « sanctions administratives pécuniaires ». Ces sanctions consistent essentiellement en des amendes qui peuvent atteindre jusqu'à un million de dollars pour les particuliers, et 10 millions de dollars pour les entreprises. Ces amendes peuvent être infligées par le CRTC. Voici quelques exemples d'infraction :

- envoi d'un courriel de nature commerciale sans consentement préalable, exprès ou tacite, du destinataire;
- envoi d'un message texte de nature commerciale avec omission d'indiquer l'identité de l'expéditeur ou d'offrir un mécanisme d'exclusion;
- envoi par un service d'envoi ou de redistribution de messages, ou autre service mandataire, d'un message électronique commercial à une personne qui n'est pas le destinataire original du message, sans consentement exprès de l'expéditeur ou du destinataire.

Dans la décision écrite de Conformité et Enquêtes dans l'affaire Blackstone[27], le CRTC a établi une série de considérations pour l'évaluation des sanctions administratives pécuniaires (SAP) imposées dans ce cas :

- « l'effet de la dissuasion générale associée à la SAP peut favoriser la conformité à la Loi;
- la conduite non conforme observée s'est manifestée par un grand nombre de messages électroniques commerciaux envoyés à des destinataires d'un éventail d'organisations, sur une période d'environ cinq mois, et s'est poursuivie jusqu'au jour précédant l'émission du procès-verbal de violation;
- certaines personnes ont acheté des services de Blackstone au cours de la période où les messages ont été envoyés et Blackstone pourrait avoir retiré un avantage financier en conséquence directe des messages envoyés en infraction à la Loi, mais il est impossible de le calculer avec les renseignements disponibles;

[27] Voir http://www.crtc.gc.ca/fra/archive/2016/2016-428.htm. Pour une analyse plus approfondie de la décision, voir l'article de Keith Rose, Daniel G.C. Glover, Charles Morgan et Kirsten Thompson intitulé *Seven Practical Lessons from CRTC's First CASL Enforcement Decision* à l'adresse https://www.mccarthy.ca/en/insights/blogs/cyberlex/seven-practical-lessons-crtcs-first-casl-enforcement-decision

- la capacité de payer de Blackstone n'a pu être évaluée parce que l'entreprise n'a pas présenté de renseignements financiers, tel qu'exigé dans l'avis de communication;
- Blackstone a fait preuve d'un manque de coopération en refusant de se conformer à l'avis de communication et n'a pas démontré de probabilité d'autocorrection. »

À ce jour, seul un petit nombre de sanctions administratives pécuniaires ont été imposées en vertu des dispositions sur les messages de la LCAP. Le montant le plus élevé de dommages demandés était de 1,1 million de dollars au moyen d'un procès-verbal (qui a était réduit à 200 000 $ en appel au CRTC)[28]. Le montant le plus bas a été de 15 000 $, mais il est remarquable du fait qu'il a été émis à l'égard d'une seule personne relativement à 58 courriels seulement (Décision de Conformité et Enquêtes CRTC 2017-65 ou « *Rapanos* »)[29].

Les contrevenants à la messagerie présumés ont généralement accepté un engagement qui a toujours inclus un paiement en espèces. En ce qui concerne les organisations, ces paiements ont varié de 48 000 $[30] à 200 000 $[31]. Une seule personne a pris un engagement, qui consistait en un paiement de 10 000 $[32]. Dans tous les cas, les engagements ont également comporté une obligation de mettre en œuvre un plan de conformité.

Procédures administratives

Les enquêteurs désignés par le CRTC peuvent exiger qu'une entreprise prenne des mesures visant à protéger ses données et que celles-ci soient divulguées. Ils peuvent obtenir un mandat afin d'effectuer une vérification, en entreprise, de la conformité à la LCAP. Ils peuvent également collaborer à des enquêtes. Le CRTC s'est appuyé sur son pouvoir de demander des mandats dans au moins une situation[33].

Le CRTC a également le pouvoir de publier des avis de communication. Le Conseil a démontré sa volonté d'utiliser libéralement ce pouvoir[34]. Par exemple, dans la décision *Rapanos*, on établit que des avis de communication ont été émis à l'égard de la partie visée par l'enquête (deux fois), de sa conjointe, de la propriétaire de la maison où il résidait, de l'hôte de son domaine de site Web et des deux sociétés qui lui fournissaient des services de téléphone cellulaire (et ce ne sont que les avis mentionnés dans la décision). Les avis initiaux à produire ont établi des échéanciers serrés, fourni peu ou pas de divulgation quant à la nature des infractions présumées et ont exigé des divulgations détaillées selon les formats précisés par le CRTC. Ils sont très onéreux par nature.

Les enquêteurs du CRTC peuvent émettre un « procès-verbal de violation » lorsqu'ils ont des motifs raisonnables de croire qu'une personne ou une entreprise a violé une disposition de la LCAP. Ce procès-verbal doit être émis au cours des trois années qui suivent la découverte de cette présumée violation.

---

[28] Voir http://www.crtc.gc.ca/fra/archive/2015/vt150305.htm

[29] Voir http://www.crtc.gc.ca/fra/archive/2017/2017-65.htm. Pour une analyse plus approfondie de la décision, voir l'article de Jade Buchanan intitulé *In New CASL Case, CRTC Sends $15,000 Message* à l'adresse https://www.mccarthy.ca/en/insights/blogs/cyberlex/new-casl-case-crtc-sends-15000-message

[30] Voir http://www.crtc.gc.ca/fra/archive/2015/ut150325.htm

[31] Voir http://www.crtc.gc.ca/fra/archive/2015/ut151120.htm

[32] Voir http://www.crtc.gc.ca/fra/archive/2017/ut170612.htm

[33] Pour une analyse de ce mandat, voir l'article de Keith Rose intitulé *CRTC Executes CASL Warrant as Part of Botnet Take-down* à l'adresse https://www.mccarthy.ca/en/insights/blogs/snipits/crtc-executes-casl-warrant-part-botnet-take-down

[34] Pour une discussion sur le pouvoir du CRTC à émettre des avis de communication, voir l'article de Kirsten Thompson intitulé *CASL Enforcement: Much Ado About Nothing?* à l'adresse https://www.mccarthy.ca/en/insights/blogs/snipits/casl-enforcement-much-ado-about-nothing

Une personne qui reçoit un procès-verbal de violation doit payer l'amende qui y est indiquée ou encore, présenter des observations auprès du CRTC. Ces observations peuvent concerner les actes ou les omissions faisant l'objet de l'avis : ainsi, la personne peut plaider qu'il y a une erreur de fait ou de droit, ou simplement contester le montant de l'amende. Le Conseil pourra alors déterminer, sur prépondérance des probabilités, s'il y a réellement eu violation. Dans ce cas, il peut imposer la sanction prévue dans le procès-verbal ou une sanction moindre s'il le juge à propos. Le Conseil peut également annuler ou la suspendre la sanction, en posant des conditions qui permettront à la personne ou à l'entreprise de se conformer à la loi. Le CRTC doit alors signifier sa décision à la personne ou à l'entreprise, accompagnée d'un avis relatif au droit d'appel.

Droit d'appel

La personne ou l'entreprise dispose d'un droit d'appel à la Cour fédérale des décisions du CRTC en vertu de la LCAP. Si l'appel concerne une question de fait, l'autorisation de la Cour est requise. Cette autorisation doit être accordée au cours des 30 jours suivant la décision ou l'ordonnance, et la cause doit être portée en appel au cours des 30 jours suivant la décision de la Cour d'accorder l'autorisation d'en appeler.

Injonctions

Les enquêteurs nommés par le CRTC peuvent également soumettre, à un tribunal compétent, une demande d'injonction destinée à prévenir toute violation d'une disposition de la LCAP relative aux pourriels. Pour qu'une telle injonction soit accordée, le tribunal doit conclure à « l'imminence ou la probabilité d'un fait constituant une contravention ». L'injonction peut exiger ou empêcher une action. Ainsi, le tribunal peut, dans le but d'éviter que soit commise une infraction à la loi, enjoindre à une personne d'accomplir ou de s'abstenir d'un acte. L'injonction doit être précédée d'un avis de 48 heures aux personnes concernées. En cas d'urgence, toutefois, lorsque l'avis n'est pas dans l'intérêt public, le tribunal peut accorder l'injonction ex parte.

SANCTIONS ADMINISTRATIVES EN VERTU DE LA LOI SUR LA CONCURRENCE

Le Bureau de la concurrence est responsable de l'application des dispositions de la *Loi sur la concurrence* en matière de pratiques commerciales trompeuses, dispositions qui, en vertu de la LCAP, s'appliqueront désormais aux messages électroniques faux ou trompeurs. Le Bureau de la concurrence détient d'importants pouvoirs d'enquête. Il peut poursuivre les contrevenants devant le Tribunal de la concurrence, un tribunal qui régit certaines infractions en vertu de la *Loi sur la concurrence*. Si l'infraction est confirmée, des amendes substantielles peuvent être imposées, soit jusqu'à 750 000 $, dans le cas d'individus, et 10 millions $ dans le cas d'entreprises (les amendes sont encore plus élevées en cas de récidive). Dans le cas où des déclarations fausses ou trompeuses sont faites « sciemment ou sans se soucier des conséquences », des poursuites criminelles peuvent être intentées en vertu de la *Loi sur la concurrence*.

Tel qu'indiqué ci-dessus, le Bureau de la concurrence a adopté des approches agressives à l'égard des dossiers de publicité fausse ou trompeuse comportant des composantes de messagerie de la LCAP, entraînant des règlements de 3 M$ et de 1,25 M$ pour les agences de location de voitures. La norme de non-matérialité pour les en-têtes de sujet fait des messages électroniques une cible très attrayante et un important domaine de préoccupations en matière de conformité pour les organisations.

DROIT D'ACTION

Enfin, tel qu'il est indiqué plus haut, le gouvernement a suspendu indéfiniment l'entrée en vigueur d'un article de la LCAP qui prévoit un droit d'action privé pour les personnes lésées par une infraction à la LCAP. Tel que rédigé, ce droit d'action privé s'applique aux violations de la LCAP, ainsi qu'aux

dispositions de la LCAP qui ont été exportées dans la *Loi sur la concurrence* et la LPRPDE. La personne lésée peut demander au tribunal d'imposer une réparation pécuniaire. La demande doit être faite au cours des trois années suivant la découverte de l'infraction présumée. Il n'y a pas d'interdiction de regrouper plusieurs demandeurs dans un recours collectif.

Les pratiques sujettes à un droit d'action peuvent être notamment :

- la collecte, à des fins commerciales et en utilisant un programme d'ordinateur conçu à cette fin, des coordonnées d'une personne sans avoir obtenu le consentement de cette personne;
- l'utilisation, à des fins commerciales, d'une liste d'envoi constituée grâce à un programme d'ordinateur sans le consentement des personnes dont les coordonnées figurent sur cette liste;
- la fausse déclaration quant à l'identité de l'expéditeur d'un message électronique commercial; ou
- une promesse fausse ou fallacieuse contenue à un message électronique commercial.

Si le tribunal est d'avis qu'une entreprise a commis une infraction à la LCAP, il peut ordonner à cette entreprise de payer des dommages :

- égaux aux pertes réelles et aux dépenses engagées; et
- d'une somme statutaire de 200 dollars par infraction jusqu'à un maximum d'un million de dollars par jour d'infraction.

L'imposition de ces sommes a pour but non pas d'imposer des dommages punitifs, mais d'inciter les entreprises à se conformer à la loi. Lorsqu'il détermine le montant des dommages, le tribunal doit tenir compte de plusieurs facteurs, dont :

- l'objet de l'ordonnance;
- la nature et l'étendue de la pratique fautive ou susceptible d'examen;
- les antécédents, notamment les infractions et engagements précédents;
- tout avantage financier obtenu par la personne ou les personnes par la pratique fautive ou susceptible d'examen;
- la capacité de payer de la personne ou des personnes;
- le dédommagement reçu par le demandeur lésé par la pratique fautive ou susceptible d'examen;
- les facteurs prévus dans le règlement; et
- tout autre facteur pertinent.

CONSEIL : Si le droit d'action privé est réintroduit, les organisations doivent évaluer la pertinence de faire une déclaration volontaire au CRTC relativement à toute infraction aux dispositions de la LCAP en matière de pourriels, d'altération des données de transmission et de logiciels espions. Dans un tel cas, le droit privé d'action ne peut être exercé lorsque le CRTC a pris les mesures contre l'auteur de l'infraction ou qu'il a obtenu de ce dernier un engagement.

AUTRES RESPONSABILITÉS

Les dirigeants, administrateurs, agents ou mandataires d'une entreprise sont tenus personnellement responsables de toute infraction à la LCAP commise par l'entreprise s'ils ordonnent ou autorisent l'infraction, ou encore s'ils consentent, acquiescent ou participent à cette infraction. Les employeurs sont

responsables du fait de leurs employés. Cette responsabilité s'applique à toutes les infractions aux dispositions de la LCAP, y compris les sanctions administratives, les dommages découlant du droit privé d'action ou les sanctions prévues par la *Loi sur la concurrence*.

Jusqu'à présent, au moins un dirigeant d'une cible du CRTC a été exposé à une responsabilité personnelle[35]. Dans ce cas, le chef de la direction d'une entreprise qui a envoyé des MEC sans respecter les exigences relatives à l'ajout d'un mécanisme d'exclusion a accepté de payer 10 000 $.

MOYENS DE DÉFENSE

La LCAP prévoit un moyen de défense contre les violations alléguées qui consiste à prouver qu'on a pris toutes les précautions voulues pour prévenir la violation. Afin de faciliter le recours à une telle défense, nous conseillons aux organisations de prendre les mesures requises pour se conformer à la loi (notamment implanter des politiques et procédures concernant les messages électroniques commerciaux indésirables), d'informer leurs employés des dispositions de la LCAP et de nommer un agent chargé de s'assurer que l'entreprise respecte la loi et de traiter les plaintes provenant des destinataires de messages. Enfin, il convient de souligner que la *Loi sur la concurrence* permet d'invoquer la diligence raisonnable dans le cas de déclarations fausses ou trompeuses.

Les lignes directrices du CRTC sur les programmes de conformité comprennent des détails sur ce que le CRTC considère être un programme de conformité approprié. Elles devraient être utiles pour établir une défense de diligence raisonnable. Voici quelques-unes des principales recommandations des lignes directrices sur les programmes de conformité :

- avoir une seule personne ultimement responsable de la conformité; dans le cas d'une grande organisation, cette personne devrait faire partie de l'équipe de direction;
- avoir une politique de conformité écrite;
- fournir une formation aux employés, accompagnée de mesures correctives pour les infractions;
- effectuer un suivi et un audit régulier de la conformité; et
- mettre en place un système de traitement des plaintes des clients.

[35] Voir http://www.crtc.gc.ca/fra/archive/2017/ut170612.htm.

Renseignements supplémentaires

Pour de plus amples renseignements sur la Loi canadienne antipourriel, prière de communiquer avec :

TORONTO :

Barry Sookman
416-601-7949
bsookman@mccarthy.ca

Dan Glover
416-601-8069
dglover@mccarthy.ca

Keith D. Rose
416-601-7913
krose@mccarthy.ca

MONTRÉAL :

Charles Morgan
514-397-4230
cmorgan@mccarthy.ca

CALGARY :

Cathy Samuel
403-206-5528
csamuel@mccarthy.ca

VANCOUVER :

David Crane
604-643-5891
dcrane@mccarthy.ca

Jade Buchanan
604-643-7947
jbuchanan@mccarthy.ca

Annexe A : Renseignements à recueillir pour un audit de conformité

La loi canadienne antipourriel a, de plusieurs façons, une incidence sur les communications des organisations avec leurs clients, les autres entreprises et les tiers. Avant de mettre en œuvre un audit de conformité, l'entreprise doit pouvoir répondre aux questions suivantes :

1. Qui est le responsable de la conformité antipourriel de votre organisation ou toute autre personne responsable de la conformité?
2. Votre organisation a-t-elle une politique de conformité à la LCAP et un processus de conformité à la LCAP documenté?
3. Quelles formes de communications électroniques votre organisation utilise-t-elle dans ses communications externes de nature commerciale?
    a) Courriel
    b) Messagerie instantanée
    c) Messagerie texte
    d) Réseaux sociaux (Facebook, etc.)
    e) Autres services en ligne (p. ex. : forums et portails Web)
    f) Autres formes de communications électroniques
4. Pour chacune de ces formes de communication, quels renseignements, quant à l'identité de votre organisation, figurent dans chacun des messages envoyés (p. ex. : signature d'un courriel)?
5. Pour chacune de ces formes de communication, comment votre organisation sollicite-t-elle le consentement des destinataires à recevoir des messages électroniques?
6. Pour chacune de ces formes de communication, comment votre organisation enregistre-t-elle les consentements à recevoir des messages électroniques?
7. Quel consentement exprès votre organisation détient-elle pour continuer d'envoyer des MEC? Une documentation appropriée est-elle constituée?
8. Votre organisation peut-elle se fonder sur un consentement tacite pour continuer d'envoyer des MEC?
9. Pour chacune de ces formes de communication, comment votre organisation reçoit-elle les demandes d'exclusion provenant des destinataires qui ne souhaitent plus recevoir de messages?
10. Pour chacune de ces formes de communication, comment ces demandes d'exclusion sont-elles traitées ou enregistrées?
11. Comment votre organisation s'assure-t-elle que les personnes qui ont demandé une exclusion ne reçoivent plus de messages?
12. Comment votre organisation assure-t-elle le suivi des coordonnées qu'elle recueille des destinataires de ses messages (p. ex. : cartes professionnelles, inscription à des événements, sondages, etc.)?

13. Votre organisation a-t-elle un processus établi pour traiter les plaintes des clients concernant la LCAP?

14. Comment votre organisation assure-t-elle le suivi des dates d'inscription des destinataires à la base de données?

15. Comment votre organisation ajoute-t-elle à ses listes d'envoi les coordonnées des destinataires avec qui elle n'a aucune relation préalable (par exemple, en recueillant les adresses électroniques à partir de sites ou de répertoires en ligne)?

16. Votre organisation utilise-t-elle des programmes de collecte d'adresses électroniques pour établir ses listes d'envoi?

17. Votre organisation a-t-elle confié à un tiers la tâche de communiquer par voie électronique, en son nom, avec des clients potentiels?

18. Votre organisation achète-t-elle de tiers des listes d'envoi électroniques afin de faire parvenir des communications à des clients potentiels?

19. Votre organisation envoie-t-elle des messages électroniques au nom de tiers, ou transmet-elle ses listes d'envoi électroniques à des tiers?

20. Votre organisation dispense-t-elle à ses employés qui envoient des messages électroniques à l'extérieur une formation sur les déclarations fausses ou trompeuses?

21. Votre organisation effectue-t-elle des balayages de routine pour s'assurer que ses serveurs de courriels ne sont pas piratés et utilisés par des tiers pour envoyer des pourriels?

22. Quelle formation votre organisation fournit-elle aux employés en ce qui concerne la LCAP?

23. Quelles mesures correctives votre organisation prend-elle contre les employés qui enfreignent votre politique de conformité à la LCAP?

Annexe B : Liste de contrôle aux fins d'audit de conformité à la LCAP

Après avoir examiné ses pratiques en matière de communications électroniques commerciales, une entreprise peut s'informer quant aux exigences de la loi canadienne antipourriel (LCAP) afin d'évaluer ses politiques, ses processus et ses systèmes sous l'angle de la conformité. La liste de contrôle suivante aidera l'entreprise à vérifier dans quelle mesure ses pratiques sont conformes à la LCAP :

- ❑ L'organisation a désigné un responsable de la conformité à la LCAP chargé de s'assurer que ses pratiques sont conformes aux dispositions de la LCAP, la *Loi sur la concurrence* et la LPRPDE et de traiter toute plainte des membres du public. Le responsable de la conformité de la LCAP devrait faire partie de l'équipe de direction.

- ❑ L'organisation a informé ses employés en détail des exigences de la LCAP, dont les façons de prévenir l'envoi de messages électroniques commerciaux indésirables.

- ❑ Le programme de formation de l'organisation comprend la formation des employés sur une politique de zéro tolérance pour des déclarations fausses ou trompeuses dans les messages électroniques commerciaux qu'ils envoient, y compris en omettant tous les faits pertinents. Le programme doit mettre en évidence les normes strictes applicables aux messages électroniques en vertu de la *Loi sur la concurrence*.

- ❑ Le programme de formation de l'organisation explique les conséquences de la non-conformité, y compris les conséquences pour l'organisation et les mesures correctives qui seront prises à l'égard de l'employé.

- ❑ L'organisation a implanté un système qui enregistre les consentements à recevoir des messages électroniques, et ses employés connaissent la procédure pour recueillir et enregistrer ces consentements. L'organisation a apporté tous les changements nécessaires à ses processus opérationnels et à sa base de données relativement à la gestion de ses relations avec la clientèle, afin de s'assurer que les demandes des clients sont respectées.

- ❑ Les signatures des courriels (et de tout autre moyen de communication électronique) destinés à l'extérieur contiennent les renseignements prescrits par la loi.

- ❑ L'organisation a mis en œuvre un mécanisme d'exclusion afin que les destinataires qui le demandent ne reçoivent plus de messages électroniques commerciaux. Cette exclusion entre en vigueur au cours des 10 jours qui suivent la demande.

- ❑ L'organisation a veillé à ce que, conformément aux dispositions de la LCAP, les données de transmission de ses courriels et autres systèmes de messagerie ne soient pas modifiées.

- ❑ L'organisation a veillé à n'être engagée dans aucune activité de collecte d'adresses de courriel visée au sens de la LCAP.

- ❑ L'organisation a veillé à ne pas utiliser de systèmes ordinés pour recueillir des renseignements personnels au sens de la LCAP.

- ❑ L'organisation a revu les modalités de ses ententes contractuelles avec des tiers afin de s'assurer que les organisations à qui elle confie des activités d'envoi de messages électroniques

commerciaux à des clients ou à des personnes externes le font dans le respect des dispositions de la LCAP.

- ❑ L'organisation a procédé à une vérification technique afin de s'assurer que ses serveurs de courriel ne sont pas utilisés par un tiers pour envoyer des pourriels.

- ❑ L'organisation a une politique de conformité à la LCAP qu'elle met à jour régulièrement. La politique doit être conçue de manière à pouvoir invoquer en défense que toutes les précautions voulues ont été prises pour prévenir toute violation de la LCAP.

mccarthy tetrault

VANCOUVER

Suite 2400, 745 Thurlow Street

Vancouver BC V6E 0C5

Tel: 604-643-7100 Fax: 604-643-7900

CALGARY

Suite 4000, 421 7th Avenue SW

Calgary AB T2P 4K9

Tel: 403-260-3500 Fax: 403-260-3501

TORONTO

Suite 5300, TD Bank Tower

Box 48, 66 Wellington Street West

Toronto ON M5K 1E6

Tel: 416-362-1812 Fax: 416-868-0673

MONTRÉAL

Suite 2500

1000 De La Gauchetière Street West

Montréal QC H3B 0A2

Tel: 514-397-4100 Fax: 514-875-6246

QUÉBEC CITY

500, Grande Allée Est, 9e étage

Québec QC G1R 2J7

Tel: 418-521-3000 Fax: 418-521-3099

LONDON, UK

125 Old Broad Street, 26th Floor

London EC2N 1AR

UNITED KINGDOM

Tel: +44 (0)20 7786 5700 Fax: +44 (0)20 7786 5702