



14.

Technologies de
l'information et des
communications



Les entreprises qui souhaitent exercer leurs activités dans les secteurs canadiens des technologies de l'information et des communications devront satisfaire à un certain nombre d'exigences législatives et réglementaires. Ce chapitre vise à traiter des principales considérations législatives et réglementaires relatives au droit canadien des technologies de l'information et des communications.

Lois sur le commerce électronique

Chaque province et territoire possède sa propre législation sur le commerce électronique. La principale composante des lois sur le commerce électronique au Canada est la question d'« équivalence fonctionnelle ». Essentiellement, cela signifie que la législation sur le commerce électronique vise à atteindre trois objectifs : 1) veiller à ce que les contrats assujettis à la loi (certains contrats, tels que les testaments ou les contrats impliquant la vente ou le financement de biens immobiliers, sont exclus) soient traités en grande partie de la même façon que les contrats créés dans des formats tangibles, à condition que certains critères soient remplis; 2) établir quand les documents électroniques doivent répondre à une exigence légale selon laquelle un document doit être écrit, fourni par écrit, fourni dans un format non électronique particulier, ou conservé; et 3) établir qu'une exigence légale selon laquelle un document doit être signé peut être remplie au moyen d'une signature électronique qui répond à certains critères.

Au Québec, la *Loi concernant le cadre juridique des technologies de l'information* (la « LCCJTI ») a été adoptée en 2001 par l'Assemblée nationale afin de moderniser et d'uniformiser le traitement juridique des communications et des documents fondés sur les technologies. Elle établit une base juridique pour l'utilisation de documents numériques, de signatures électroniques et d'autres pratiques fondées sur les technologies dans les secteurs public et privé, en garantissant que les documents électroniques ont la même validité sur le plan juridique que les documents sur support papier, dans des conditions précises. Enfin, la LCCJTI établit un cadre juridique pour l'utilisation de technologies spécifiques en fixant des exigences pour des systèmes tels que la biométrie, la numérisation, la géolocalisation, l'identification, l'authentification et les signatures électroniques.

LCAP – Loi canadienne anti-pourriel

La Loi canadienne anti-pourriel (anciennement la *Loi visant à promouvoir l'efficacité et la capacité d'adaptation de l'économie canadienne par la réglementation de certaines pratiques qui découragent l'exercice des activités commerciales par voie électronique et modifiant la Loi sur le Conseil de la radiodiffusion et des télécommunications canadiennes, la Loi sur la concurrence, la Loi sur la protection des renseignements personnels et les documents électroniques et la Loi sur les télécommunications*, mais qui est mieux connue sous son acronyme informel LCAP) est en vigueur depuis maintenant plus d'une dizaine d'années.

La LCAP a une incidence importante sur l'utilisation de messages électroniques pour promouvoir des activités ou contacter des clients ou partenaires commerciaux, anciens ou potentiels, ainsi que sur l'installation de logiciels sur les systèmes informatiques de tiers.

La LCAP :

- vise à résoudre le problème des communications électroniques non sollicitées (soit les pourriels) et se penche principalement sur les messages électroniques commerciaux (MEC);
- introduit des règles pour traiter le problème de l'installation non sollicitée de programmes d'ordinateur, comme les témoins de connexion (même si leur désignation en tant que logiciels est techniquement discutable), et des règles pour traiter la modification non autorisée de données de transmission;
- prévoit un ensemble de règles à suivre pour obtenir un consentement valide permettant d'envoyer des MEC et d'installer des programmes d'ordinateur, y compris des exigences spécifiques concernant la procédure et le contenu du consentement, ainsi que diverses catégories de consentement implicite et certaines exceptions à l'exigence de consentement.
- impose diverses exigences concernant du contenu devant être inclus dans un MEC, y compris l'identification de la personne ou de l'entité qui envoie le message et un mécanisme d'exclusion qui répond à certains critères, et établit un régime strict et parfois complexe pour l'exécution des demandes de désabonnement;
- ne fait pas la distinction entre les messages envoyés à des fins légitimes et ceux envoyés à des fins malveillantes ni entre un petit nombre de messages et les messages de groupe;
- prévoit un cadre dont le champ d'application est beaucoup plus large que celui de ses équivalents américain et européen, et est considéré comme l'un des régimes anti-pourriel les plus stricts au monde.

Les exemples suivants présentent certaines des difficultés auxquelles les entreprises sont confrontées si elles veulent se conformer à la LCAP :

- **Application de la loi à l'extérieur du Canada – Messages électroniques commerciaux :** pour que les exigences anti-pourriel de la LCAP s'appliquent, il suffit qu'un MEC ait été envoyé ou ouvert à partir d'un ordinateur au Canada; par conséquent, les expéditeurs étrangers de MEC vers le Canada sont également assujettis à cette loi; Installation non sollicitée de programmes d'ordinateur : afin que les dispositions relatives aux programmes non sollicités s'appliquent, il faut que l'ordinateur ou la personne (ou la personne qui exerce un contrôle sur cette dernière) qui installe le programme se trouve au Canada au moment de l'installation; par conséquent, les installateurs étrangers qui déploient de tels programmes sur des systèmes informatiques au Canada sont assujettis à cette loi.
- **Critères d'application larges –** Un MEC qui est assujetti aux exigences anti-pourriel de la LCAP est défini comme tout message électronique « dont il est raisonnable de conclure [...] qu'il a pour but, entre autres, d'encourager la participation à une activité commerciale ». Il s'agit d'une définition élargie, qui englobe plus que ce qui est habituellement défini comme étant un pourriel. Ainsi, si au moins l'un des buts d'un message électronique est d'inciter une personne à participer à une « activité commerciale », même s'il ne s'agit pas de son seul but, les exigences anti-pourriel de la LCAP s'appliqueront.
- **Les messages visés n'incluent pas seulement les courriels –** La LCAP est couramment désignée comme une « loi anti-pourriel », mais elle s'applique à tout message électronique (ce qui inclut les messages textes ainsi que les messages sonores, vocaux ou visuels) envoyé à : a) un compte courriel; b) un compte de messagerie instantanée; c) un compte de téléphone; ou d) « tout autre compte similaire ».

- 
- **Régime d'adhésion volontaire** - À la différence d'autres lois anti-pourriel comme la CAN-SPAM Act aux États-Unis, la LCAP institue un régime à option d'adhésion. À de rares exceptions près, la LCAP interdit l'envoi de MEC sauf en cas de consentement exprès ou tacite. Le consentement exprès doit être obtenu sous la forme prescrite par la LCAP. Le consentement tacite n'est possible que pour certaines catégories énumérées, notamment les « relations d'affaires en cours » telles que définies dans la loi. Dans certaines catégories de consentement implicite, ce dernier n'est valable que pour une période déterminée. Les demandes de consentement à la transmission d'un MEC sont également considérées comme des MEC. Par conséquent, avant d'envoyer une telle demande, l'organisation doit étudier attentivement les exigences de la LCAP.
 - **Importance des liens ou de la relation avec le destinataire** - Selon les liens ou la relation entre l'expéditeur et le destinataire, un MEC peut être : a) exempté à la fois des exigences de consentement et de contenu; b) exempté seulement de l'exigence de consentement; ou c) assujéti au consentement tacite plutôt qu'au consentement exprès. Par exemple, la loi prévoit des exceptions pour les relations d'affaires en cours et les relations privées en cours prescrites, ainsi qu'à l'égard des employés d'une organisation qui se transmettent des MEC entre eux ou qui les transmettent à des employés d'autres organisations, s'ils ont une relation d'affaires avec ces derniers et que le message concerne les activités de l'organisation qui le reçoit. Comprendre à quels moments de telles exceptions peuvent s'appliquer demeure toutefois un défi de taille.
 - **Consentement exprès présumé pour l'installation de certains programmes d'ordinateur** - En plus des exigences anti-pourriel, la LCAP prévoit les règles concernant le consentement exprès devant être obtenu lorsque des logiciels sont installés sur l'ordinateur d'une autre personne dans le cadre d'activités commerciales. Ces règles exigent que certains renseignements soient communiqués au destinataire et qu'un mécanisme de consentement approprié soit mis en place. Toutefois, une personne sera réputée avoir consenti à l'installation de certains programmes mentionnés dans la loi (par exemple, lorsque ce programme est un témoin de connexion, un système d'exploitation ou une mise à jour ou une mise à niveau du réseau) s'il est raisonnable de croire, d'après son comportement, qu'elle consent à l'installation du programme.
 - **Le consentement exprès doit être donné au moyen d'un mécanisme de consentement actif et les demandes de consentement doivent être distinctes** - Le principe de base de la LCAP veut que le consentement exprès du destinataire soit obtenu pour transmettre des MEC et installer des programmes. Par exemple, la LCAP exige que le consentement soit donné au moyen d'un mécanisme de consentement actif (c.-à-d. que le destinataire indique explicitement son consentement), et que chaque demande de consentement soit distincte et ne soit pas regroupée avec d'autres demandes de consentement à d'autres fins, comme les demandes de consentements relatives aux conditions générales d'utilisation. En outre, une demande de consentement explicite doit répondre à certains critères pour être valable. Les entreprises doivent par conséquent s'assurer que leurs demandes de consentement sont préparées conformément aux exigences de la LCAP.

- **Les exigences relatives au contenu des MEC sont nuancées** – Outre les exigences en matière de consentement énoncées ci-dessus, le CRTC a fourni des directives détaillées sur la forme et la nature du contenu obligatoire d'un MEC pour qu'il respecte la LCAP. À titre d'exemple, les directives du CRTC comprennent des renseignements détaillés sur la façon dont un expéditeur de MEC doit identifier les tiers au nom desquels le MEC est envoyé ainsi que sur la façon dont le destinataire d'un MEC doit pouvoir « exécuter facilement » un mécanisme d'exclusion.

Toute contravention à la LCAP peut entraîner de graves conséquences. Elles prévoient notamment : a) l'imposition d'une sanction administrative pécuniaire d'un montant maximal de 1 000 000 \$ si l'auteur est une personne physique, et de 10 000 000 \$ dans le cas de toute autre personne; b) la prise d'un engagement par la partie contrevenante; c) la signification à la partie contrevenante d'un procès-verbal de violation; et d) un recours injonctif. Les dispositions prévoyant un droit privé d'action, qui devaient entrer en vigueur le 1^{er} juillet 2017, ont été suspendues indéfiniment.

De plus, en cas de contravention par une personne morale, les dirigeants, administrateurs ou mandataires qui l'ont ordonnée ou autorisée, ou qui y ont consenti ou participé, peuvent être tenus responsables de la contravention, que la personne morale fasse ou non l'objet de poursuites.

Au cours des dix années qui se sont écoulées depuis l'entrée en vigueur de la LCAP, les efforts d'exécution de la loi ont donné lieu à des sanctions administratives pécuniaires et à des engagements négociés allant de 15 000 \$ à 200 000 \$.

Outre les dispositions de la LCAP, les mesures d'application prises par le CRTC ont fourni des indications sur la manière dont les organisations doivent mener leurs activités afin de limiter les sanctions administratives pécuniaires potentielles en cas de manquement à la LCAP.

Compte tenu du risque de responsabilité personnelle associé aux contraventions à la LCAP, il est important que les entreprises s'assurent de mettre en œuvre des programmes de conformité à la LCAP, y compris des politiques concernant les pourriels et les programmes non sollicités, et qu'elles apportent les modifications nécessaires à leurs politiques de confidentialité.

Un bulletin du Conseil de la radiodiffusion et des télécommunications canadiennes publié le 5 novembre 2018 (CRTC, Bulletin d'information du secteur Conformité et Enquêtes 2018-415) présente aux parties intéressées des lignes directrices générales sur la conformité et les pratiques exemplaires concernant l'interdiction, en vertu de l'article 9, de faire accomplir, même indirectement, tout acte contraire aux exigences de la LCAP en ce qui concerne la transmission de MEC et l'installation de programmes d'ordinateur, ou d'aider ou d'encourager quiconque à accomplir un tel acte. Il semble que l'article 9 puisse s'appliquer aux particuliers et aux organisations : a) qui agissent à titre d'intermédiaires en fournissant des services habilitants qui permettent à une autre personne d'enfreindre la LCAP; ou b) qui bénéficient d'un avantage financier direct ou indirect découlant de telles contraventions. Les courtiers en publicité, les commerçants en ligne, les développeurs ou les distributeurs de logiciels et d'applications, les fournisseurs de services de télécommunication et de services Internet et les opérateurs de systèmes de traitement des paiements peuvent être à risque, selon certains facteurs, dont les suivants :

- le niveau de contrôle sur l'activité qui contrevient à la LCAP et la capacité d'empêcher ou de faire cesser cette activité;
- l'importance du lien entre les activités qui contreviennent à l'article 9 et celles qui contreviennent à la LCAP;
- les éléments de preuve établissant que des mesures raisonnables ont été prises pour prévenir les violations ou y mettre un terme.



Législation sur la preuve électronique

La législation canadienne en matière de preuve définit les conditions d'admissibilité des documents électroniques (données enregistrées ou mises en mémoire sur quelque support que ce soit par un système informatique ou un dispositif semblable). La législation vise principalement à adapter et à codifier les règles d'authentification de la common law et la règle de la « meilleure preuve » en matière de preuves électroniques.

En vertu de la *Loi sur la preuve au Canada*, il incombe à la personne qui cherche à faire admettre en preuve un document électronique d'établir son authenticité au moyen d'éléments de preuve permettant de conclure que le document est bien ce qu'il paraît être. À cette étape, l'objectif n'est pas de garantir l'authenticité du document électronique, mais simplement d'évaluer s'il semble être, à première vue, ce qu'il est censé être.

La règle de la « meilleure preuve » sert en quelque sorte à étayer l'authenticité d'un document; elle permet de valider (sans toutefois confirmer) son intégrité. L'intégrité, dans ce cas, renvoie à la question de savoir si les renseignements compris dans un document sont susceptibles de demeurer complets et inchangés entre le moment où ils sont recueillis et celui où ils sont présentés au tribunal. Tout document électronique satisfait à la règle de la « meilleure preuve » si la fiabilité du système d'archivage électronique au moyen duquel ou dans lequel le document est enregistré ou mis en mémoire est démontrée. La satisfaction à cette preuve, en l'absence de preuve du contraire, est démontrée au moyen d'éléments de preuve permettant de conclure que, à tout moment important, le système fonctionnait bien ou, s'il ne fonctionnait pas bien, que la défektivité n'a eu aucune incidence sur l'intégrité du document électronique, et qu'il n'existe aucun autre motif raisonnable de douter de l'intégrité du système ou du document électronique.

Comme les seuils d'authenticité et de meilleure preuve sont bas, il est possible d'utiliser comme preuve d'admissibilité des témoignages de témoins directs, indirects et parfois même profanes. Il est toutefois important de noter qu'aux yeux du tribunal, la facilité avec laquelle la preuve est admise n'a pas pour effet d'augmenter sa force probante. Les juges conservent le pouvoir d'évaluer la fiabilité et la crédibilité de la preuve au moment de prendre leur décision finale. Par conséquent, les documents électroniques de piètre qualité admis à des fins d'examen peuvent quand même finir par être jugés insuffisants et peu fiables.

Le fait de disposer d'un système d'archivage électronique fiable ne participe pas à lui seul à l'admissibilité de la preuve, car les méthodes de mise en mémoire, de copie, de transmission et de reproduction des relevés électroniques influent également sur la force probante des documents électroniques qui sont présentés devant le tribunal.

La législation en matière de preuve des provinces et les territoires de common law prévoit un régime similaire.

Lois visant la protection des consommateurs

Chaque province et territoire du Canada dispose de son propre régime de protection des consommateurs, composé de lois, de règles et de règlements, et dans certains cas, les régimes varient considérablement. Pour cette raison, un contrat électronique devant être signé par un « consommateur » (au sens donné dans les règlements de chaque province et territoire) doit respecter les exigences en matière de protection générale du consommateur (p. ex., l'interdiction de pratiques injustes) de même que les exigences relatives aux formalités du commerce électronique (selon lesquelles certains renseignements doivent être divulgués et certaines mesures doivent être prises à des moments précis pendant le processus de passation du contrat électronique).



D'autres raisons peuvent expliquer la complexité du régime canadien de protection des consommateurs. Les contrats en ligne sont souvent visés par plusieurs catégories de règlements dont les exigences se chevauchent. Par exemple, en Ontario, un contrat en ligne pourrait constituer une « convention électronique », « une convention à exécution différée » ou une « convention à distance ». En Colombie-Britannique, un contrat en ligne pourrait constituer une « convention à distance » ou une « convention à exécution différée ». Au Québec, à la suite des modifications apportées à la *Loi sur la protection du consommateur* en 2006 (articles 54.1 à 54.16), un contrat en ligne peut être qualifié de « contrat conclu à distance » et doit également respecter les exigences du *Code civil du Québec*, notamment celles s'appliquant aux contrats d'adhésion – contrats dont les stipulations essentielles ont été imposées par l'une des parties ou rédigées par elle et ne pouvant pas être librement discutées (p. ex. les modalités des contrats en ligne ou des « contrats d'achat au clic »). Il est important de noter que les clauses de limitation de responsabilité ne sont pas autorisées par la *Loi sur la protection du consommateur* du Québec.

Ces régimes exigent généralement que :

- a) certaines informations soient i) communiquées au consommateur au cours du processus contractuel et ii) incluses dans le contrat proprement dit;
- b) le contrat soit par écrit;
- c) le consommateur puisse valider les informations relatives à la transaction avant de finaliser l'achat;
- d) une copie du contrat soit fournie au consommateur dans un délai imparti.

Outre le droit de résilier le contrat et les autres recours dont dispose le consommateur, le non-respect de ces exigences peut entraîner des amendes ou des pénalités pour les fournisseurs en cas d'infraction. Les infractions aux lois provinciales sur la protection des consommateurs peuvent, en cas de condamnation, donner lieu à des amendes de 100 000 \$ à 250 000 \$ pour la première infraction d'une société. Certaines lois provinciales sur la protection des consommateurs contiennent également des dispositions relatives aux sanctions administratives pécuniaires qui pourraient donner lieu à des sanctions d'un montant inférieur. Les administrateurs de sociétés qui ont contrevenu à certaines règles des lois provinciales sur la protection des consommateurs peuvent également être tenus responsables, que la société ait été ou non poursuivie ou déclarée coupable.

De plus, une société pourrait être dénoncée et discréditée par les autorités de réglementation applicables. Par exemple, en Ontario, le ministère des Petites Entreprises et des Services aux consommateurs tient une « liste de mises en garde pour les consommateurs » dans laquelle les consommateurs peuvent facilement rechercher une entreprise et connaître la nature de l'infraction qu'elle a commise ou de la plainte qui a été déposée contre elle.

Ces dernières années, de nombreuses provinces ont mis à jour leurs lois et règlements pour répondre à l'évolution du paysage du commerce numérique et à la sensibilité accrue aux droits des consommateurs. Par exemple, l'Ontario a adopté la *Loi de 2023 sur la protection du consommateur*, qui s'appuie sur son régime législatif précédent en interdisant, entre autres, une nouvelle série d'actes abusifs de la part des fournisseurs et en offrant des recours supplémentaires aux consommateurs, y compris le droit de récupérer trois fois le montant du remboursement dans le cadre d'une action civile.



Noms de domaines

Les parties qui souhaitent obtenir un nom de domaine « .ca » doivent satisfaire aux « Exigences en matière de présence au Canada » de l'Autorité canadienne pour les enregistrements Internet. Au Canada, le nom de domaine principal est généralement offert aux citoyens, aux résidents permanents, aux sociétés constituées dans un territoire canadien et aux sociétés de personnes enregistrées au Canada, entre autres. En outre, le propriétaire d'une marque de commerce enregistrée au Canada a le droit d'utiliser un domaine « .ca » qui comprend la marque de commerce.

Accessibilité des sites Web

La plupart des lois provinciales sur l'accessibilité exigent que les organisations veillent à ce que leurs sites Web respectent certaines normes ou certains objectifs en matière d'accessibilité. En Ontario, par exemple, les organisations comptant cinquante (50) employés ou plus sont tenues, en vertu de la *Loi sur l'accessibilité pour les personnes handicapées de l'Ontario*, de veiller à ce que leur site Web soit conforme aux directives sur l'accessibilité du contenu Web (WCAG) 2.0 (niveau AA) ou à une version ultérieure.

Ententes relatives aux TI

Bien qu'il n'existe pas de lois d'application générale axées principalement sur la fourniture de services TI au secteur privé au Canada, d'autres lois canadiennes s'appliqueront invariablement à la fourniture de tels services. Il s'agit notamment des lois et règlements relatifs au traitement et à la protection des renseignements à caractère personnel (dans les secteurs public et privé) et des règlements et lignes directrices de l'industrie (p. ex., les exigences régissant la fourniture et l'utilisation de services TI par les institutions financières sous réglementation fédérale, examinées plus loin dans ce chapitre).

De plus, les entreprises qui souhaitent octroyer des licences à l'égard de technologies de l'information au Canada et les commercialiser doivent prendre connaissance du régime canadien de propriété intellectuelle (voir le [chapitre 13](#)).

Les « contrats de licence en ligne » ou les « concessions de licence par clic » peuvent être exécutoires si les acheteurs ont été informés des modalités au moment de la vente; autrement dit, l'acheteur doit avoir pu prendre connaissance des modalités avant que les parties ne concluent l'accord.

Exigences linguistiques en français

Le français est la seule langue officielle du Québec. C'est pourquoi la *Charte de la langue française*, récemment modifiée par le projet de loi 96, impose des exigences linguistiques visant à promouvoir l'utilisation du français dans tous les aspects de la vie publique, y compris le commerce et les communications d'entreprise. Si les logiciels peuvent être vendus dans d'autres langues s'il n'existe aucune version française, les contrats d'adhésion et les inscriptions sur les produits, en revanche, doivent respecter des exigences strictes en matière de langue française. Les contrats d'adhésion, lesquels sont non négociables et rédigés par une seule partie (p. ex., les conditions générales en ligne), doivent d'abord être fournis en français avant que les parties puissent accepter d'être liées par leur version dans une autre langue. Le non-respect de cette exigence pourrait entraîner la nullité ou l'inapplicabilité du contrat à l'égard de la partie qui y adhère.

Les inscriptions sur les produits (y compris les emballages, les instructions d'utilisation et les documents qui doivent les accompagner) doivent être fournies en français au même titre que toute autre version dans une autre langue. La même règle s'applique à la documentation commerciale comme les catalogues et les brochures sur les sites Web. L'affichage public et la publicité commerciale doivent être faits de façon à ce que le français y figure de façon nettement prédominante.



L'Office québécois de la langue française (OQLF) veille à l'application de la Charte et privilégie, de façon générale, une approche collaborative. Il peut toutefois renvoyer l'affaire devant les tribunaux, où l'auteur d'une première infraction est passible d'une amende de 3 000 \$ à 30 000 \$. Ce cadre souligne la volonté du Québec de préserver son patrimoine linguistique tout en fournissant aux entreprises des directives opérationnelles claires.

Intelligence artificielle

À l'heure actuelle, le Parlement du Canada examine le projet de loi C-27, lequel propose, entre autres, d'édicter la *Loi sur l'intelligence artificielle et les données* (la « LIAD »).

La LIAD et les initiatives connexes du gouvernement fédéral (examinées ci-dessous) s'articulent autour de six principes : i) responsabilité; ii) sécurité; iii) justice et équité; iv) transparence; v) supervision humaine et surveillance; et vi) validité et robustesse. Si elle est adoptée, la LIAD réglerait la conception, le développement et l'utilisation des systèmes d'IA dans le secteur privé et viserait à atténuer les risques de préjudice et de partialité dans l'utilisation des systèmes d'IA à « incidence élevée ». Dans sa version actuelle, la LIAD aurait notamment les effets suivants :

- établir les critères pour les systèmes d'IA à incidence élevée auxquels la loi s'appliquera;
- établir les exigences relatives à la réalisation d'évaluations des systèmes à incidence élevée, à la mise en place et au suivi de mesures d'atténuation des risques, à l'utilisation de données anonymes, à la tenue des registres, à la publication des renseignements sur le système d'IA et à certaines obligations de déclaration;
- exiger l'utilisation de cadres de responsabilisation par les organisations qui développent des systèmes d'IA à risque élevé.

- mettre en place un régime d'application visant, entre autres, à désigner et à habilitier un commissaire à l'intelligence artificielle et aux données, imposer des sanctions administratives pécuniaires en cas de non-respect (leur montant sera déterminé par des règlements futurs) et fixer le montant des amendes pour des infractions particulières en vertu de la LIAD (pouvant aller jusqu'à 25 M\$ ou 5 % du revenu global brut de l'organisation au cours de l'année précédente, selon le plus élevé des deux montants).

En novembre 2023, les membres du Parlement ont proposé des modifications à la LIAD qui auraient notamment les effets suivants :

- établir des classes de systèmes d'IA qui sont présumés être à incidence élevée (c.-à-d. les systèmes se rapportant aux questions suivantes : i) l'emploi; ii) les décisions relatives à l'accès aux services; iii) le traitement des données biométriques; iv) la modération du contenu sur les médias sociaux, les moteurs de recherche et d'autres plateformes de communication en ligne; v) les soins de santé et les services d'urgence; vi) la prise de décisions par un tribunal ou un organisme administratif; et vii) l'application de la loi);
- introduire le concept de « systèmes d'IA à usage général », qu'il faut différencier des « systèmes d'IA à incidence élevée », et le faire entrer dans le champ d'application réglementaire de la LIAD;
- clarifier davantage les cadres de responsabilité des organisations en fonction de leurs rôles et de leurs fonctions dans le cycle de vie des systèmes d'IA.

Un document complémentaire accompagnant la LIAD publié en mars 2023 prévoit un processus d'élaboration des règlements d'une durée de deux ans. La LIAD n'entrerait en vigueur qu'après cette période.



La LIAD a franchi l'étape de la deuxième lecture par la Chambre des communes et fait actuellement l'objet d'un examen par le Comité permanent de l'industrie et de la technologie (le « Comité ») dans le cadre duquel le gouvernement a fait part de son intention de proposer d'importantes modifications à la LIAD. Au moment de la rédaction du présent document, on ne sait pas encore quand et sous quelle forme la LIAD recevra la sanction royale.

En septembre 2023, Innovation, Sciences et Développement économique Canada (ISDE) a publié un « code de conduite volontaire visant un développement et une gestion responsables des systèmes d'IA générative avancés » (le « Code »). Le Code : a) définit les mesures volontaires destinées aux organisations qui développent et gèrent des systèmes d'IA générative à usage général visant à atténuer les risques que présentent ces systèmes; et b) cible des intervenants particuliers au sein de l'écosystème d'IA, des développeurs et des gestionnaires qui, en acceptant les engagements volontaires du Code, doivent refléter les six principes susmentionnés (c.-à-d. la responsabilité; la sécurité; la justice et l'équité; la transparence; la supervision humaine et la surveillance; et la validité et la robustesse) dans le cadre de leur travail. Bien qu'il se concentre principalement sur les systèmes d'IA générative avancés, le Code s'applique de façon plus générale à un large éventail de systèmes d'IA à incidence élevée. Les mesures définies dans le Code sont destinées à conseiller les organisations en prévision de la réglementation contraignante prise en application de la LIAD.

Au début de 2024, la période de consultation publique a pris fin en vue de la « Consultation sur le droit d'auteur à l'ère de l'intelligence artificielle générative » menée par le gouvernement du Canada. Cette consultation avait pour objectif d'orienter les futures modifications à la *Loi sur le droit d'auteur* du Canada compte tenu de l'utilisation de plus en plus répandue des systèmes d'IA, y compris la question de savoir si les systèmes d'IA peuvent être considérés comme les titulaires d'une œuvre.

Internet et autres moyens de télécommunication

Sous réserve de quelques exceptions, la prestation de services de télécommunications (y compris les services Internet de détail) aux clients résidentiels et professionnels n'est assujettie à aucune réglementation au Canada. Les exceptions comprennent notamment : a) un Code sur les services sans fil qui impose des obligations d'information et des limites relatives aux modalités des contrats de services sans fil pour les consommateurs et les petites entreprises; b) un Code sur les services Internet applicable aux grands fournisseurs de services Internet (FSI) désignés qui impose des obligations d'information et des limites relatives aux modalités contractuelles des services Internet fixes pour les consommateurs individuels; c) des règles de gestion du trafic Internet pour les FSI; d) des exigences en matière de transférabilité des numéros; e) des exigences en matière de transfert des consommateurs; f) des obligations en matière d'accessibilité; g) des obligations en matière de services d'urgence; et h) des obligations en matière de services de gros applicables aux entreprises de télécommunications désignées.

L'utilisation de services de télécommunications à des fins de télémarketing est assujettie à des listes de numéros de télécommunication exclus et à d'autres restrictions. L'utilisation de composeurs-messagers automatiques pour effectuer ce que l'on appelle communément des « appels robotisés » fait également l'objet de nombreuses restrictions. Le marketing par messages textes est régi par les restrictions de la LCAP mentionnées précédemment dans ce chapitre.

Les revendeurs de services de télécommunications ne sont pas soumis à des restrictions en matière de propriété étrangère. Dans certains cas, les entreprises de télécommunications doivent être constituées en vertu des lois canadiennes et peuvent être soumises à des exigences en matière de propriété étrangère (décrites au chapitre 3).

Obligations des secteurs réglementés

Le Bureau du surintendant des institutions financières (BSIF) est l'organisme de réglementation fédéral canadien chargé de superviser et de réglementer les banques et les assureurs sous réglementation fédérale, les sociétés de fiducie et de prêt et les régimes de retraite complémentaires assujettis à la surveillance fédérale.

Le 1^{er} mai 2024, la ligne directrice révisée B-10 sur la gestion du risque lié aux tiers (la « ligne directrice révisée ») du BSIF est entrée en vigueur, remplaçant l'ancienne ligne directrice B-10 sur l'impartition d'activités, de fonctions et de méthodes commerciales qui était en vigueur depuis longtemps. La ligne directrice révisée décrit les attentes plus élevées du BSIF à l'égard des institutions financières fédérales (IFF) en ce qui concerne la gestion d'un éventail élargi de risques liés aux tiers. De plus, elle met davantage l'accent sur les plans de gouvernance et de gestion du risque ainsi que sur des résultats et des principes précis. La ligne directrice révisée élargit la portée de l'application de la ligne directrice B-10 aux « ententes avec des tiers », qui comprennent toute entente commerciale ou stratégique avec des entités externes. La ligne directrice révisée continuera ainsi de s'appliquer aux contrats de technologie, y compris (comme il est expressément indiqué dans la ligne directrice révisée) : i) les relations impliquant la prestation de services pour le stockage, l'utilisation ou l'échange de données; et ii) les activités, les fonctions et les services impartis, de manière plus générale.

La ligne directrice révisée remplace le seuil d'« importance relative » dans la ligne directrice précédente et introduit une nouvelle « démarche axée sur le risque » qui exige un cadre de gestion du risque plus complet tenant compte du niveau de risque et de la « criticité » des ententes individuelles avec des tiers. Elle comprend également des exigences plus précises obligeant les IFF à élaborer des exigences s'appliquant à l'infonuagique et à prendre en considération la transférabilité infonuagique dans leurs contrats.

La ligne directrice B-10 précise que le BSIF s'attend, comme l'exigent la *Loi sur les sociétés de fiducie et de prêt* et la *Loi sur les sociétés d'assurances*, à ce que certains documents des IFF soient conservés au Canada. En outre, les IFF doivent veiller à ce que le BSIF ait accès, au Canada, à tout document dont il a besoin pour remplir ses fonctions.

Bien que la ligne directrice B-10 vise les entités fédérales, de nombreuses entités du secteur financier sous réglementation provinciale l'ont adoptée de façon volontaire. La ligne directrice B-10 s'applique également aux entités qui fournissent des produits et services aux IFF, car celles-ci risquent de négocier certaines dispositions contractuelles pour en tenir compte.

Outre la ligne directrice B-10, le BSIF a publié un préavis sur le signalement des incidents liés à la technologie et à la cybersécurité, énonçant ainsi ses attentes en matière de signalement immédiat et continu des incidents de cybersécurité dont les IFF doivent tenir compte dans leurs ententes avec les fournisseurs de services infonuagiques. Ces attentes s'ajoutent aux notifications obligatoires des atteintes à la protection des données prévues par les lois canadiennes sur la protection de la vie privée.

En juillet 2022, le BSIF a publié la version finale de la ligne directrice B-13 (intitulée « Gestion du risque lié aux technologies et du cyberrisque ») visant à compléter les lignes directrices existantes, y compris la ligne directrice B-10. Les IFF devraient lire et mettre en œuvre la ligne directrice B-13 dans une optique fondée sur le risque qui leur permet de concurrencer de façon efficace et de tirer pleinement parti de l'innovation numérique, et ce, tout en maintenant une saine gestion du risque lié aux technologies. La ligne directrice B-13 fournit des conseils technologiques impartiaux aux IFF pour les aider à produire des « résultats » précis dans trois domaines :

- technologies, cybergouvernance et gestion du risque;
- activités technologiques;
- cybersécurité.

La ligne directrice B-13 est entrée en vigueur le 1^{er} janvier 2024.

Recherche et développement

Les entreprises technologiques qui souhaitent s'implanter au pays doivent savoir que le Canada encourage la recherche et le développement (R&D) grâce au Programme de la recherche scientifique et du développement expérimental (RS&DE) – une initiative des autorités fiscales fédérales. Il s'agit de la plus importante source d'appui à la recherche et au développement accordée par le gouvernement fédéral aux contribuables. Ces crédits d'impôt constituent souvent un avantage important pour les entreprises technologiques, faisant du Canada une destination attrayante pour les celles qui souhaitent mener d'importantes activités de R&D dans le domaine des technologies. Aux termes du programme RS&DE, les demandeurs peuvent se prévaloir de crédits d'impôt à l'investissement, notamment pour les salaires, le matériel, la machinerie, les contrats et même une partie des coûts indirects de l'entreprise.

Pour être admissible, une société requérante doit être une « société privée sous contrôle canadien » (SPCC). En règle générale, une SPCC est une société privée dont au moins 50 % des actionnaires inscrits avec droit de vote sont des résidents canadiens. Autrement dit, 50 % des actionnaires de la société peuvent être des non-résidents et il n'y a aucune exigence de citoyenneté.

Les SPCC peuvent obtenir un crédit d'impôt à l'investissement remboursable de 35 % sur la première tranche de 3 M\$ de dépenses admissibles. Pour être admissibles au programme, ces dépenses doivent avoir été effectuées dans le cadre d'activités de RS&DE au Canada. Au-delà du montant initial, les SPCC peuvent obtenir un crédit d'impôt à l'investissement non remboursable de 15 %.

D'autres sociétés canadiennes qui ne sont pas admissibles à titre de SPCC sont admissibles à un crédit d'impôt de 15% sur les dépenses admissibles. Ces crédits ne sont pas remboursables, mais ils peuvent être utilisés pour réduire le fardeau fiscal.

Pour obtenir de plus amples renseignements sur les SCCP, consultez le [chapitre 7](#).

