TECHNOLOGIES DE L'INFORMATION

Par Mike Scherman, Jamie Parker, Oksana Migitko, Connor Bildfell et Keith Rose

TECHNOLOGIES DE L'INFORMATION

Contrôle des exportations de technologie

Au Canada, le contrôle des exportations de technologie est un mandat du gouvernement fédéral. L'exportation de certains équipements et logiciels et de certaines technologies peut être contrôlée par la *Loi sur les licences d'exportation et d'importation* (LLEI). Ces contrôles ne s'appliquent pas uniquement aux envois physiques, mais également aux transferts immatériels effectués notamment par l'intermédiaire de prestations de services ou de formations, de téléversements vers des serveurs, de téléchargements depuis des serveurs ou d'accès à des serveurs depuis l'étranger, d'autres transferts de fichiers électroniques, de courriels, de télécopies, de conversations téléphoniques, de téléconférences et d'entretiens individuels. De surcroît, des restrictions à l'exportation ou au transfert de certains logiciels et de certaines marchandises et technologies sont imposées en vertu des lois sur les sanctions, notamment la *Loi sur les Nations Unies* et la *Loi sur les mesures économiques spéciales.* Il peut arriver que les sanctions économiques fassent double emploi avec les contrôles à l'exportation, mais elles s'appliquent généralement de manière plus large, y compris dans des circonstances où il n'y a pas d'exportation ou de transfert de marchandises, de logiciels ou de technologies soumis à des restrictions à partir du Canada.

Établie sous le régime de la LLEI, la Liste des marchandises et technologies d'exportation contrôlée (LMTEC) identifie les marchandises, les logiciels et les technologies, y compris les produits de haute technologie, qui ne peuvent être exportés ou transférés à partir du Canada par des moyens matériels ou immatériels sans l'obtention préalable d'une licence d'exportation, sous réserve d'exemptions pour certains pays de destination. La LMTEC ne vise pas des produits en particulier; elle établit plutôt un ensemble de spécifications techniques qui sont pour la plupart neutres sur le plan technologique et qui constituent des descriptions fonctionnelles. Actuellement, la LMTEC contient des contrôles relatifs aux articles dotés d'une fonctionnalité cryptographique, aux logiciels d'intrusion, aux outils permettant de déjouer, d'affaiblir ou de contourner la sécurité de l'information, et aux outils de surveillance permettant aux forces de l'ordre de contrôler ou d'analyser le contenu des communications ou des métadonnées. Les logiciels généralement accessibles au public ne sont habituellement pas soumis à des restrictions. Les logiciels et autres éléments qui

comportent des fonctions de sécurité cryptographique sont, en règle générale, assujettis aux contrôles des exportations, sous réserve de certaines exceptions limitées concernant le marché de masse et le domaine public, à moins que la cryptographie n'utilise des longueurs de clés très courtes. De plus, toute la technologie venant des États-Unis qui doit être transférée à l'extérieur des États-Unis est assujettie aux contrôles des exportations.

Protection du consommateur — Conventions électroniques

Plusieurs mesures législatives ont conféré une plus grande certitude juridique au commerce électronique. En Ontario, par exemple, la *Loi de 2002 sur la protection du consommateur* (LPC) comprend des dispositions relatives au cybercommerce, une méthode utilisée par un grand nombre de consommateurs canadiens pour acheter et vendre des biens et des services, bien qu'elles s'appliquent généralement aussi en dehors du commerce électronique. Voir la section **Fabrication et vente de produits de consommation — Protection des consommateurs**.

Les fournisseurs sont réputés garantir, par exemple, que les services fournis aux termes d'une convention de consommation sont de « qualité raisonnablement acceptable ». La LPC étend également les garanties implicites prévues sous le régime de la *Loi sur la vente d'objets* aux marchandises fournies par location ou échange. Une autre disposition importante invalide toute exigence dans un contrat de consommation obligeant à soumettre les litiges à l'arbitrage, ce que certains commerçants utilisent pour tenter d'éviter un scénario de recours collectif. En outre, la LPC exige du commerçant qu'il divulgue et rend « accessible » au consommateur, avant la conclusion d'une convention électronique, une liste assez longue de renseignements « clairs, compréhensibles et bien en évidence ». Le commerçant doit également donner au consommateur la possibilité expresse d'accepter ou de refuser la convention électronique et d'en corriger les erreurs immédiatement avant de la conclure, et il doit remettre une copie de ladite convention électronique au consommateur dans les 15 jours suivant la conclusion de cette convention. Enfin, la LPC prévoit des règles relativement aux cartes prépayées, comme les cartes-cadeaux, qui constituent un segment de plus en plus important de l'économie axée sur la consommation, particulièrement en ligne. Ces règles prévoient diverses exigences et limites pour les émetteurs, par exemple la question de savoir si une carte-cadeau peut avoir une date d'expiration et si l'émetteur peut imputer des frais au consommateur. Des dispositions semblables réglementant les conventions électroniques

et les cartes prépayées ont été adoptées dans la majorité des provinces canadiennes.

Soulignons que les lois sur la protection des consommateurs sont actuellement en mutation et que les entreprises doivent être conscientes de l'évolution de la situation en ce qui a trait à la protection des consommateurs au Canada. À titre d'exemple, l'Ontario envisage de modifier considérablement la LPC en apportant des changements aux exigences en matière de divulgation des contrats et de consentement et en interdisant certaines clauses contractuelles[1], tandis que le Québec a proposé, le 1er juin 2023, une loi qui modifie ses règles de protection des consommateurs afin d'interdire la vente de produits dont l'obsolescence est planifiée et d'introduire une garantie légale de bon fonctionnement pour certains biens neufs couramment utilisés[2].

Lois sur la preuve

La plupart des provinces et territoires du Canada ont édicté des règles de preuve qui portent expressément sur les documents électroniques. Ces lois exigent en général, en ce qui concerne les documents électroniques, l'application de la règle de la meilleure preuve en démontrant l'intégrité du système d'archivage électronique qui a servi à enregistrer ou à mettre en mémoire les documents. Ces dispositions permettent également de conclure à l'intégrité du système d'archivage électronique en s'appuyant sur la preuve que le dispositif électronique sous-jacent fonctionnait correctement. Bref, ces modifications législatives soutiennent l'admissibilité des documents électroniques, tout en permettant à une partie de contester la fiabilité du système ou du réseau informatique qui a servi à produire les documents.

À l'ère numérique, l'observation stricte et littérale des règles régissant la communication préalable, comme la Règle 30 des *Règles de procédure civile* de l'Ontario, se révélerait souvent fort onéreuse, accablante et, dans une large mesure, inutile pour les parties au litige. C'est pourquoi les juges canadiens privilégient de plus en plus l'observation des lignes directrices en matière d'administration de la preuve électronique par les parties à un litige. Ces lignes directrices peuvent notamment exiger que

1 https://www.mccarthy.ca/en/insights/blogs/consumer-markets-perspectives/ontario-issues-consultation-paper-consumer-protection-legislation (article disponible en anglais seulement).

2 https://www.mccarthy.ca/fr/references/blogues/consumer-markets-perspectives/le-gouvernement-propose-des-changements-la-loi-sur-la-protection-du-consommateur-pour-interdire-lobsolescence-programmee.

les parties à un litige examinent les questions relatives à l'administration de la preuve électronique et, entre autres choses, qu'elles circonscrivent la portée de l'administration de la preuve électronique afin de respecter la Règle 30. Voir la section **Règlement des différends – Administration de la preuve électronique**. De plus, la pandémie de COVID-19 a accéléré l'adoption et l'utilisation des nouvelles technologies dans les tribunaux du Canada. De nombreux tribunaux canadiens ont continué à exiger ou à encourager le dépôt électronique de tous les documents relatifs aux litiges, avec des liens hypertextes vers la jurisprudence et les preuves pertinentes.

Lois sur le commerce électronique

Les provinces canadiennes ont adopté des lois sur le commerce électronique qui traitent d'un grand nombre de questions soulevées par la conduite d'activités commerciales par voie électronique, comme la validité des messages électroniques pour respecter les règles relatives à la forme écrite des documents juridiques. À titre d'exemple, la *Loi de 2000 sur le commerce électronique* de l'Ontario prévoit que l'obligation juridique selon laquelle un document doit se présenter par écrit est satisfaite par un document qui se présente sous forme électronique – comme un courriel – pourvu qu'il soit accessible de manière à être utilisable pour consultation ultérieure. Les lois provinciales sur le commerce électronique prévoient également que l'apposition d'une signature électronique est suffisante pour respecter toute exigence légale selon laquelle un document doit être signé. La définition de « signature électronique » est très large et comprend tous les renseignements électroniques qu'une personne crée ou utilise pour signer un document et qui se trouvent dans le document, y sont joints ou sont associés à celui-ci. La *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE) fédérale est un peu plus étroite et insiste sur les « signatures électroniques sécurisées », ce qui signifie actuellement pour le gouvernement un processus d'authentification fondé sur un système cryptographique à clé publique.

En plus des règles relatives à la signature et aux documents écrits, la plupart des lois provinciales sur le commerce électronique prévoient qu'une offre, l'acceptation d'une offre ou toute autre question liée à la formation ou à l'effet d'un contrat peut être exprimée au moyen de renseignements électroniques ou par un geste posé dans l'intention

de produire une communication électronique, comme toucher l'icône appropriée ou un autre endroit sur un écran d'ordinateur ou cliquer sur l'un ou l'autre, ou même parler. Ces règles sont utiles parce qu'elles confirment que les contrats conclus sur Internet ne seront pas non inexécutables du seul fait qu'ils se présentent sous forme électronique. Il existe au Canada une jurisprudence qui appuie le caractère exécutoire des consentements au moyen d'un simple clic sur un bouton. Le caractère exécutoire est cependant moins certain lorsque l'utilisateur n'est pas obligé de cliquer sur un bouton où il est expressément écrit « J'accepte », mais qu'il est plutôt dit, par exemple, que l'utilisation du site Web signifie que l'utilisateur en accepte les conditions.

Loi anti-pourriel

La *Loi canadienne anti-pourriel* (LCAP) est largement considérée comme l'une des plus strictes au monde. Cette loi met en œuvre un large éventail d'exigences visant à réduire les pourriels, l'usurpation d'identité, l'hameçonnage et l'utilisation de logiciels espions. Contrairement à la loi américaine *CAN-SPAM Act* qui permet aux entreprises d'envoyer des messages électroniques commerciaux sans le consentement préalable de leurs destinataires, pourvu qu'ils contiennent un mécanisme d'exclusion valide, la LCAP exige des entreprises qu'elles obtiennent un consentement valide avant même l'envoi du premier message électronique commercial aux destinataires prévus. Les infractions à la LCAP peuvent donner lieu à des sanctions administratives pécuniaires maximales de 1 million de dollars canadiens dans le cas de particuliers et de 10 millions de dollars canadiens dans le cas de tout autre contrevenant. Depuis l'entrée en vigueur de la LCAP, l'organisme chargé de la faire respecter, soit le Conseil de la radiodiffusion et des télécommunications canadiennes (CRTC), a reçu de nombreuses plaintes de Canadiens; toutefois, il n'a rendu jusqu'à présent que peu de décisions relativement à son application. Notamment, dans un cas au moins, le CRTC a attribué à un particulier la responsabilité, aux termes de la LCAP, d'infractions commises par une société. En avril 2019, le CRTC a imposé une sanction administrative pécuniaire de 100 000 dollars à un administrateur d'une société en lien avec l'envoi de courriels commerciaux à des destinataires au Canada. Pour en arriver à cette décision, le CRTC a évalué la capacité de payer de l'administrateur, son expérience en matière de plateformes de diffusion par courriel, ainsi que l'importance de cette méthode de marketing pour son entreprise. Le CRTC a insisté sur le fait que le but

de la sanction était de favoriser le respect de la LCAP et a imposé l'amende de 100 000 dollars afin de s'assurer que cet administrateur en particulier se conforme à la LCAP dans toute entreprise future.

Logiciels anti-espion / témoins de connexion

En vertu de l'article 8 de la LCAP, les entreprises doivent normalement obtenir le consentement de l'utilisateur si elles utilisent des programmes qui installent des logiciels ou d'autres programmes sur son système informatique. La LCAP prévoit qu'une demande de consentement explicite doit indiquer la raison pour laquelle le consentement est demandé ainsi que la fonction du programme informatique et le nom, l'adresse postale et le numéro de téléphone ou l'adresse électronique de l'entité qui demande le consentement. Toutefois, pour certains types de programmes tels que les témoins de connexion, le consentement explicite pour enregistrer des renseignements concernant des utilisateurs est réputé avoir déjà été obtenu sans en faire la demande, pour autant que le comportement de l'utilisateur permette raisonnablement de penser qu'il a consenti à l'installation du programme. À titre d'exemple, le consentement n'est pas présumé avoir été obtenu pour l'installation de témoins de connexion sur le système informatique d'un utilisateur si ce dernier désactive les témoins dans son navigateur[3].

Il convient de noter qu'à compter du 22 septembre 2023, en vertu de la loi modifiée du Québec sur la protection des renseignements personnels, les technologies qui recueillent des renseignements personnels et qui permettent d'identifier ou de localiser une personne ou d'établir son profil doivent être désactivées par défaut, et la personne doit être avisée de l'utilisation de ces technologies et des moyens disponibles pour activer les fonctions qui permettent de l'identifier, de la localiser ou d'établir son profil.

Libelle sur Internet

Le libelle sur Internet est défini comme étant la publication de renseignements portant atteinte à la réputation d'autrui au moyen d'un système informatique, sans excuse légitime. Dans des décisions récentes rendues par des tribunaux canadiens, d'importants dommages pécuniaires ont été accordés à des demandeurs victimes de libelle par des défendeurs qui envoyaient des courriels diffamatoires et qui

3 Idem.

affichaient en ligne d'autres propos de même nature au sujet des demandeurs. Le libelle sur Internet peut revêtir diverses formes. En février 2021, la Cour supérieure de justice de l'Ontario a même accordé une réparation novatrice pour le « délit de harcèlement sur Internet », devenant ainsi la première cour de common law en dehors des États-Unis à le faire[4]. L'affaire concernait la dissémination d'accusations fallacieuses et préjudiciables affichées en ligne par le défendeur au sujet du demandeur. Comme la Cour a conclu que les délits précédemment reconnus, tels que la diffamation, l'intrusion dans l'intimité (atteinte à la vie privée) et l'infliction intentionnelle de souffrance psychologique, n'étaient pas adaptés aux faits de l'espèce, elle a donc reconnu le délit de harcèlement sur Internet[5].

De plus en plus, la jurisprudence en matière de libelle sur Internet tend à diminuer la responsabilité potentielle des hôtes de forums de discussion en ligne. En règle générale, un hôte Internet sera traité comme un non-éditeur (instrument passif) jusqu'à ce qu'un demandeur potentiel notifie qu'il a été victime de libelle sur le site de l'hôte. Si l'hôte ne retire pas le contenu après la notification, le tribunal peut décider que l'hôte est responsable par omission[6].

Compétence

Dans les domaines du droit criminel, du droit quasi criminel et de la réglementation, les tribunaux et organismes de réglementation canadiens semblent peu hésiter à exercer leur compétence sur une conduite liée à Internet émanant de l'étranger qu'ils jugent nuisible à l'intérêt public, à condition qu'il y ait un lien réel et substantiel entre la compétence du tribunal ou de l'organisme de réglementation et les faits relatifs à la conduite.

Les organisations doivent se montrer transparentes quant à leurs pratiques de gestion des renseignements personnels. Cela implique notamment d'aviser les clients de la possibilité que leurs renseignements personnels soient envoyés dans un autre territoire pour y être traités et que les tribunaux, les forces de l'ordre et les autorités chargées de

4 https://www.mccarthy.ca/en/insights/blogs/techlex/tort-internet-harassment-new-tort-extraordinary-remedy (article disponible en anglais seulement).

5 https://www.canlii.org/en/on/onsc/doc/2021/2021onsc670/2021onsc670.html?resultIndex=1#document au paragraphe 171 (décision disponible en anglais seulement).

6 Emily B. Laidlaw et Hilary Young, Internet Intermediary Liability in Defamation, 2019 56-1 Osgoode Hall Law Journal 112, 2019 CanLIIDocs 3965, page 122, https://canlii.ca/t/sqlp.

la sécurité nationale de cet autre territoire puissent y accéder. De plus, les transferts de renseignements personnels hors du Québec (y compris vers une autre province) entraînent des obligations supplémentaires, telles que l'évaluation des facteurs liés au respect de la vie privée avant le transfert.

Droit criminel et rançongiciels

En général, le gouvernement canadien a fait des avancées utiles dans la lutte aux délits informatiques en apportant continuellement, depuis 20 ans, des modifications au *Code criminel du Canada* pour rivaliser avec les auteurs de délits informatiques. Les technologies et les pratiques technologiques et commerciales liées à Internet et à l'informatique soulèvent toutefois un grand nombre de nouvelles questions sur ces modifications et les anciennes dispositions du *Code criminel du Canada* qui font ressortir le défi que représente notamment l'application de lois pénales nationales à un environnement technologique de plus en plus planétaire. Alors que les technologies ne cessent d'évoluer, l'applicabilité du *Code criminel du Canada* à l'égard de certains comportements préjudiciables demeure incertaine.

Le Centre canadien pour la cybersécurité joue un rôle de premier plan dans la réponse du gouvernement en matière de cybersécurité et considère les rançongiciels comme l'une des formes les plus courantes de cyberattaques au Canada[7]. Les rançongiciels sont des logiciels malveillants utilisés par les cybercriminels pour infecter un appareil et bloquer l'accès à ses fichiers et données en échange d'une rançon. Une fois qu'un ordinateur ou un réseau est infecté par un rançongiciel, le logiciel est capable de restreindre l'accès au système ou de chiffrer les données qu'il contient.

L'idée selon laquelle les cyberattaques utilisent des rançongiciels en ciblant uniquement des « entreprises qui gèrent de données » est erronée. Toutes les sociétés conservent des données dans leurs systèmes et les cybercriminels ont commencé à cibler également les entreprises qui ne spécialisent pas dans la gestion de données[8]. Par conséquent, il est important de gérer adéquatement le risque posé par les rançongiciels en s'assurant de prendre les mesures de précaution appropriées avant qu'un incident ne se produise. Les entreprises peuvent agir de manière

7 https://www.cyber.gc.ca/fr/orientation/rancongiciels-comment-ne-pas-perdre-lacces-ses-appareils.

8 https://www.mccarthy.ca/en/insights/blogs/techlex/emerging-developments-ransomware (article disponible en anglais seulement).

proactive en établissant un solide cadre de cybersécurité composé de ressources organisationnelles qui sont en mesure d'évaluer et d'atténuer les risques de cybersécurité tels que les rançongiciels[9]. Une bonne gestion des risques passe également par l'élaboration de plans d'intervention en matière de cybersécurité en cas d'attaque par un rançongiciel. Le plan doit aborder des questions particulières comme la décision de payer ou non la rançon et la détermination du moment où il pourrait être nécessaire de faire appel à des avocats et des experts-conseils externes[10].

Intelligence artificielle (IA)

L'IA est en train de transformer la façon dont les affaires sont menées au Canada et dans le reste du monde. L'IA englobe un large éventail de technologies, allant des robots conversationnels et des outils de prise de décisions aux logiciels qui génèrent des documents entiers, des images et d'autres contenus. Bien que les gouvernements provinciaux et fédéral envisagent et élaborent des réglementations en matière d'IA, seul le Québec disposera, à compter du 22 septembre 2023, d'une législation en vigueur traitant directement des questions liées à l'IA, et dans ce cas, uniquement pour exiger des organisations qu'elles fassent certaines divulgations en rapport avec les décisions qu'elles prennent et qui sont fondées exclusivement sur le traitement automatisé des renseignements personnels d'un particulier.

Le gouvernement fédéral a proposé la *Loi sur l'intelligence artificielle et les données* (LIAD) pour réglementer la conception, le développement et l'utilisation de l'IA dans le secteur privé[11], loi qui devrait entrer en vigueur au plus tôt en 2025[12]. De nombreux détails de la LIAD devront être définis dans les réglementations futures, et les consultations avec les parties prenantes au cours de cette période pourraient modifier la LIAD de manière significative par rapport à son état actuel. Telle qu'elle est proposée, la LIAD imposera notamment des obligations de conformité importantes aux responsables des systèmes d'intelligence artificielle « à incidence élevée » (qui restent à définir) et donnera au ministre de l'Innovation, des Sciences et du Développement économique des pouvoirs étendus pour faire sanctionner les violations de la LIAD, y

9 https://www.mccarthy.ca/en/insights/blogs/techlex/ransomware-avoidance-and-response (article disponible en anglais seulement).
10 Idem.
11 https://www.parl.ca/DocumentViewer/fr/44-1/projet-loi/C-27/premiere-lecture.
12 https://ised-isde.canada.ca/site/innover-meilleur-canada/fr/loi-lintelligence-artificielle-donnees-liad-document-complementaire.

compris en imposant des amendes maximales de 10 millions de dollars ou de trois pour cent du revenu mondial brut, selon le montant le plus élevé. Bien qu'il soit difficile de prévoir la forme et l'effet définitifs de la LIAD, le secteur de l'IA continuera d'être une cible importante pour la réglementation et aura probablement une grande incidence sur la façon dont de nombreuses organisations mèneront leurs activités dans un proche avenir.

POUR EN SAVOIR PLUS,
VEUILLEZ COMMUNIQUER AVEC L'UNE DES PERSONNES SUIVANTES :

Christine Ing
christineing@mccarthy.ca
416-601-7713

Michael Scherman
mscherman@mccarthy.ca
416-601-8861