Traverser 2025 : Tendances clés du secteur des technologies

FASKEN

Traçons l'avenir

Traverser 2025 : Tendances clés du secteur des technologies

En 2025, les fournisseurs et les utilisateurs de technologies doivent composer avec un environnement complexe regorgeant de défis et de possibilités. La dynamique du marché, stimulée par l'innovation technologique, la recherche de rentabilité, le changement d'attitude à l'égard du risque, l'importance accrue accordée aux initiatives environnementales, sociales et de gouvernance (ESG), les préoccupations grandissantes en matière de géopolitique et de cybersécurité, ainsi que les nouvelles modifications législatives et réglementaires, est en train de remodeler le visage des technologies de l'information (TI).

Pour vous aider à traverser ces changements, l'équipe de droit des technologies de Fasken a préparé ce guide qui met en lumière les principales tendances qui façonneront le secteur canadien des technologies en 2025.

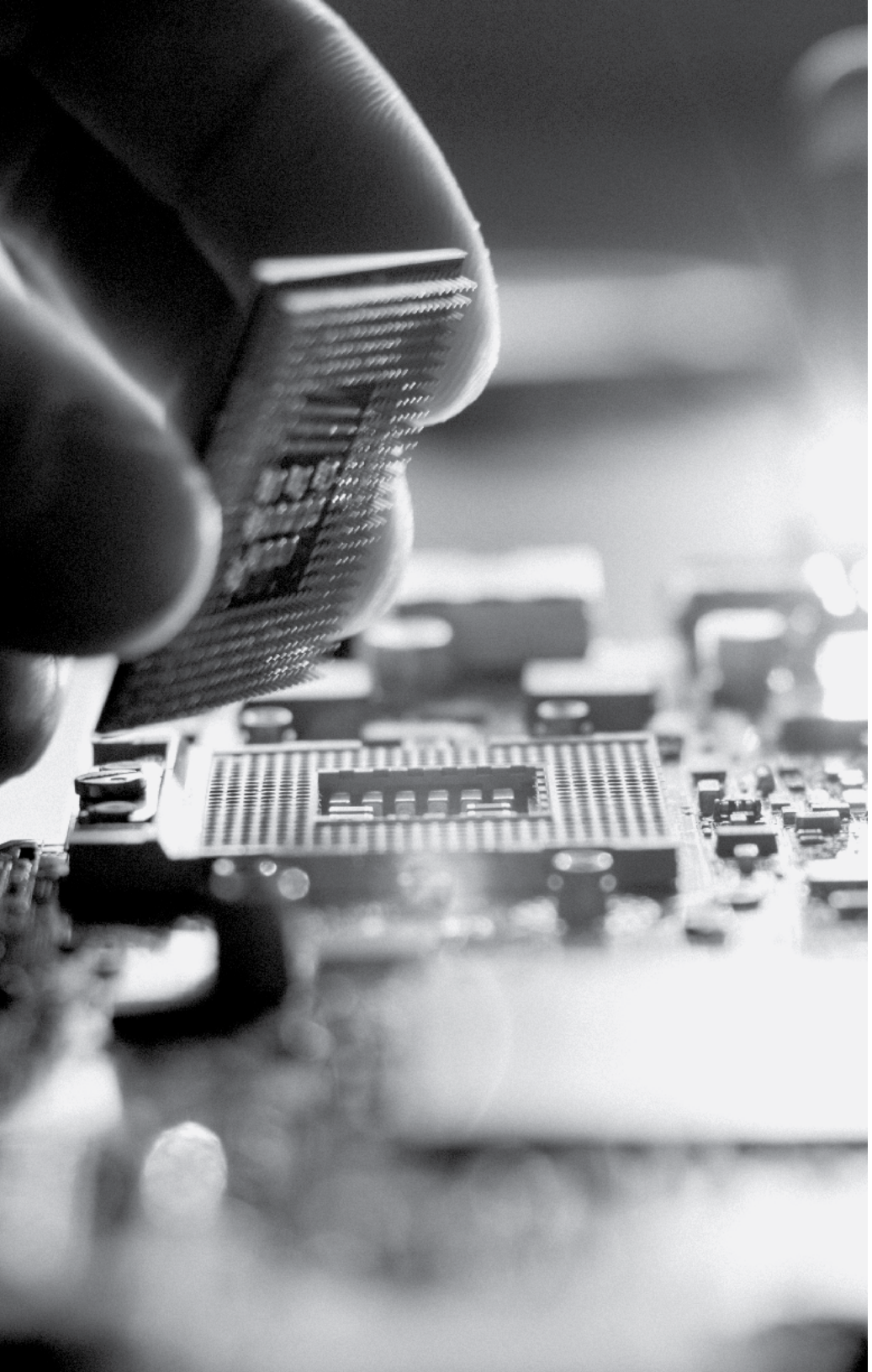


Table des matières

Tendance 1 : Le secteur des technologies restera au centre des activités de fusions et acquisitions au Canada

Les transactions technologiques devraient continuer à être au cœur des activités de fusions et acquisitions en 2025. L'augmentation du nombre de fusions et acquisitions dans le secteur des technologies devrait être stimulée par l'innovation dans les industries émergentes, les efforts continus des acteurs du secteur pour améliorer leurs capacités en matière d'intelligence artificielle (IA) et l'assouplissement prévu des contraintes réglementaires pour ce secteur, conséquence probable de la nouvelle administration américaine.

THÈMES ÉMERGENTS ET POSSIBILITÉS EN MATIÈRE DE F&A TECHNOLOGIQUES

Une analyse des activités de fusions et acquisitions dans le secteur des TI au Canada au cours des dernières années[1] a révélé les perspectives et les thèmes suivants :

- **Logiciels de productivité d'entreprise et impartition des TI** : Ces domaines demeurent prédominants lorsqu'on analyse les volumes d'opérations, ce qui reflète l'intérêt croissant des entreprises pour les outils et les services qui améliorent l'efficacité et réduisent la complexité opérationnelle.

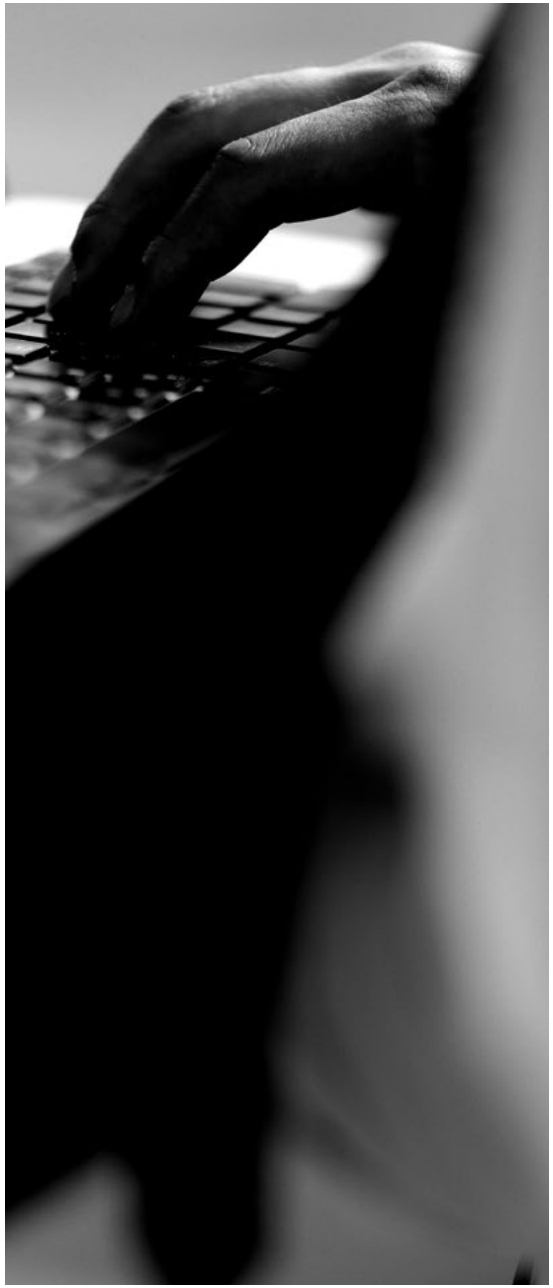
- **Logiciels-services** : Les logiciels-services restent le principal secteur vertical des fusions et acquisitions dans le secteur des technologies, avec une croissance régulière du volume d'opérations au cours des trois dernières années. Cette tendance souligne la demande soutenue de solutions évolutives, basées sur le nuage, qui prennent en charge les environnements de travail hybrides et favorisent l'efficacité à l'échelle de l'entreprise.

- **Semi-conducteurs à application spécifique** : Ce secteur vertical est devenu beaucoup plus dynamique en 2024. Bien que les volumes d'opérations soient relativement faibles, on constate une croissance notable. Cela reflète l'importance des semi-conducteurs et leur contribution aux progrès de l'IA et d'autres technologies nécessitant un traitement intensif des données.

- **Intelligence artificielle et apprentissage automatique** : Ce secteur vertical clé représentait 7,03 % des opérations de fusion et acquisition dans le secteur des technologies en 2022, puis 12,66 % en 2023, et a conservé une forte part de marché d'environ 11,79 % en 2024, malgré une baisse plus générale du nombre total d'opérations. Cette croissance souligne le rôle central de l'IA dans la stimulation de l'innovation et la création de valeur dans tous les secteurs.

Il est important de noter que ces secteurs verticaux sont complétés par d'autres secteurs verticaux connexes et ne sont pas le seul centre d'intérêt des fusions et acquisitions. Par exemple, l'augmentation du nombre d'opérations dans le secteur des semi-conducteurs sera complémentaire avec celles visant les minéraux stratégiques au sein du marché nord-américain.

1. Les données de cette analyse proviennent de PitchBook et reflètent les opérations de fusions et acquisitions et de changement de contrôle au Canada dans le secteur des TI pour 2022, 2023 et 2024.



ÉLÉMENTS À CONSIDÉRER LORS DE F&A TECHNOLOGIQUES AXÉES SUR L'IA

L'intégration de l'IA dans les modèles d'affaires a stimulé les activités de fusions et acquisitions, présentant à la fois des occasions et des défis uniques. Ces défis, qui vont de la responsabilité des modèles à l'examen réglementaire, façonnent le processus de vérification diligente ainsi que les déclarations et garanties dans les conventions d'acquisition.

Vérification diligente

La relative émergence de l'IA nécessite un processus de vérification diligente plus complet pour évaluer correctement la valeur et les risques d'une cible d'acquisition. Si la cible est dans le domaine de l'IA, des approches sur mesure sont nécessaires pour couvrir les questions propres à l'IA telles que la qualité des données, les droits sur celles-ci et la conformité aux réglementations en constante évolution. Cela inclut l'évaluation de l'intégrité et de la légalité des données utilisées pour l'entraînement des modèles d'IA et la garantie de l'exactitude et de la fiabilité de ceux-ci.

La portée de la vérification diligente propre à l'IA varie en fonction de la nature de la cible. Par exemple, si une entreprise fournit une infrastructure d'IA ou des centres de données, la vérification diligente peut correspondre davantage aux considérations standard en matière de fusions et acquisitions, à quelques exceptions près, comme la garantie de capacités de production suffisante d'électricité ou l'accès à des puces spécialisées. Inversement, l'exercice d'une vérification diligente sur les fournisseurs d'apprentissage automatique et d'IA générative peut nécessiter une approche visant à mieux comprendre les caractéristiques et les risques uniques de l'entreprise et de sa technologie. Cela peut consister à mener des enquêtes ciblées sur le personnel et les systèmes d'IA dans le but d'évaluer des domaines critiques comme l'intégrité des données, la robustesse des modèles, les processus de conception éthique et l'expertise du personnel spécialisé.

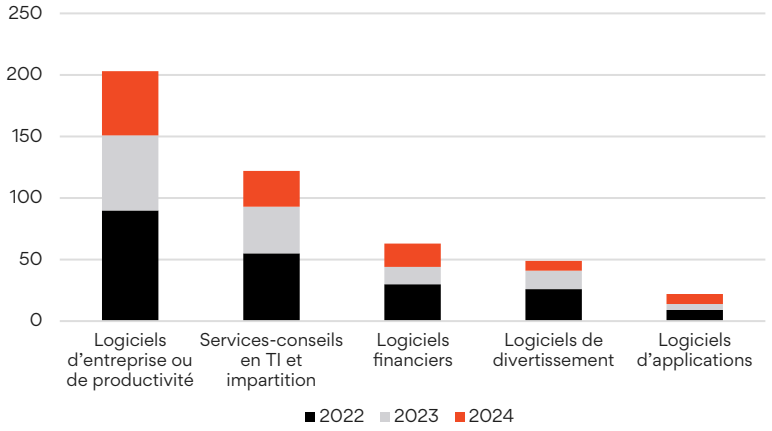
Déclarations, garanties et engagements

Les opérations de fusion et acquisition impliquant des technologies d'IA comprennent souvent des déclarations et garanties utilisées normalement dans le cadre d'opérations de fusion et acquisition dans le secteur des technologies. Des exemples? Les déclarations et garanties relatives aux droits de propriété intellectuelle, à la confidentialité des données et à la cybersécurité, entre autres. Cependant, les acquéreurs récents privilégient de plus en plus les déclarations propres à l'IA, en particulier lorsque l'évaluation d'une cible dépend d'un aspect précis de cette technologie ou lorsqu'il s'agit de faire face aux risques uniques posés par une situation juridique incertaine. Certains assureurs de déclarations et de garanties accordent également une attention particulière aux compétences et à l'expertise des personnes qui évaluent les technologies d'IA et exigent une prise en compte délibérée dans le processus de vérification diligente. Alors que de plus en plus d'entreprises commencent à inclure des déclarations et garanties propres à l'IA, nous anticipons une augmentation similaire du nombre d'assureurs mettant en œuvre cette pratique ou élaborant des polices avec des garanties et exclusions spécialement adaptées à l'IA.

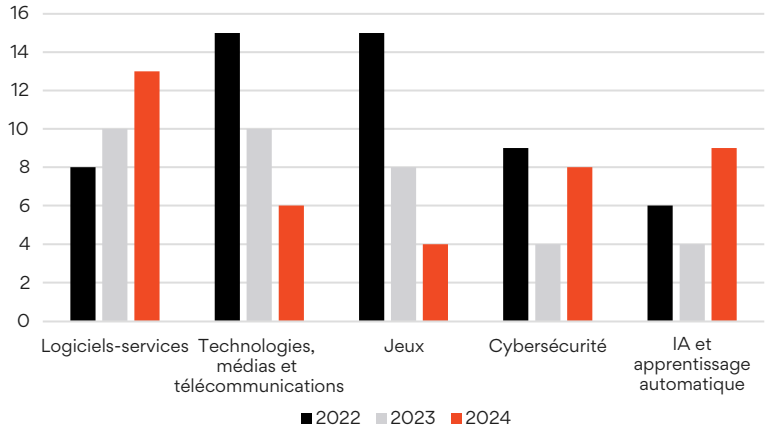
Dans les situations où la loi sur la technologie d'IA reste incertaine, comme dans le cas de l'IA générative ou de l'utilisation de données collectées sur le Web, les déclarations standard peuvent ne pas être suffisantes. Les acquéreurs peuvent exiger des déclarations précises pour s'assurer que les modèles d'IA ont été entraînés à l'aide de données autorisées ou que les systèmes d'IA sont conformes à leur tolérance au risque en matière de biais, d'explicabilité et de fiabilité. Ils peuvent également négocier des indemnités particulières et d'autres conditions uniques, comme des clauses relatives à l'IA qui interdisent de modifier les données d'entraînement d'une société cible ou les fournisseurs, modèles ou politiques de conformité en matière d'IA entre la signature et la clôture de l'accord pour maintenir la valeur de l'entreprise ou de l'actif. Inversement, les sociétés cibles peuvent chercher à obtenir une assurance de déclarations et de garanties ou à inclure des exclusions dans les déclarations et les garanties pour éviter toute violation due à des changements législatifs indépendants de leur contrôle.

Au bout du compte, les risques uniques associés à l'IA nécessitent une vérification diligente, des déclarations, des garanties et des engagements sur mesure pour se protéger et gérer adéquatement les incertitudes dans le cadre d'opérations de fusion et acquisition dans le secteur des technologies.

Répartition par secteur
(Les 5 principaux secteurs, 2022-2024)



Répartition par secteur vertical
(Les 5 principaux secteurs verticaux, 2022-2024)



Tendance 2 : La dynamique du marché modifiera les prix des fournisseurs et les possibilités d'économies des clients

DYNAMIQUE FAVORISANT LES AUGMENTATIONS DE PRIX DES FOURNISSEURS

Comme les clients le savent, certains changements dans le marché ont conduit les fournisseurs de technologies à exercer une pression croissante pour augmenter les prix. Voici des exemples :

1. **Les fusions et acquisitions ont entraîné une pression accrue sur les fournisseurs pour qu'ils génèrent des rendements financiers** : Le secteur des technologies a connu une augmentation importante des activités de fusions et acquisitions, en particulier grâce aux sociétés de capital-investissement qui rachètent des entreprises technologiques pour créer des synergies, consolider leurs positions sur le marché et, finalement, augmenter leurs marges (p. ex. l'acquisition de VMware par Broadcom à la fin de 2023). Les entreprises nouvellement acquises sont souvent soumises à une forte pression pour améliorer leurs résultats financiers, ce qui contribue à des hausses de prix généralisées.

2. **Modifications des modèles de tarification des fournisseurs** : Les fournisseurs de technologies redéfinissent la manière dont ils établissent le prix de leurs produits. Par exemple, Oracle a récemment décidé de fixer le prix de Java en fonction du nombre d'*employés* plutôt que du nombre de *licences*.

3. **Transition vers des modèles de licence par abonnement** : Dans le même ordre d'idées, les fournisseurs continuent de passer d'un modèle de licence perpétuelle à un modèle de logiciel-service basé sur un abonnement et un paiement récurrent. Par exemple, a) Guidewire, fournisseur de technologies pour le secteur de l'assurance incendie, accident et risques divers, est récemment passé d'un modèle de licence sur site à un modèle de logiciel-service, et b) en 2025, IBM fera de même pour ses produits clés tels que Maximo et Cognos. Tout cela s'inscrit dans une stratégie plus large visant à faire passer les clients à des modèles de paiements récurrents. Non seulement ces modèles hébergés par le fournisseur suscitent de nouvelles préoccupations chez les clients – concernant la sécurité du fournisseur et les obligations en matière de violation de données –, mais chaque expiration d'une période d'abonnement devient une nouvelle occasion pour les fournisseurs d'augmenter leurs prix.

4. **Cycles de fin de vie accélérés** : Les fournisseurs accélèrent l'arrêt de la prise en charge des anciennes versions de logiciels, ce qui oblige les clients à effectuer des mises à niveau et à supporter des coûts plus élevés. Avec le modèle de licence sur site, qui était auparavant largement répandu, les éditeurs de logiciels comptaient beaucoup sur les frais de maintenance (qui pouvaient représenter 20 % ou plus du coût de la licence) pour générer des revenus récurrents. Le modèle de licence sur site étant en voie de disparition, les fournisseurs ont accéléré le cycle de fin de vie des produits, notamment pour maintenir leurs revenus en incitant les clients à acheter les versions successives mises à niveau.

5. **Augmentation du nombre de vérifications de conformité** : Les fournisseurs procèdent à des vérifications rigoureuses pour détecter les cas de licences non conformes. Ces vérifications peuvent entraîner des coûts imprévus et nécessiter des investissements supplémentaires dans des mesures de conformité. Par exemple, les pratiques de vérification d'IBM s'avèrent toujours très strictes. En 2025, IBM prévoit non seulement effectuer des vérifications auprès de tous les clients chez qui il n'y a pas eu de vérifications au cours des quatre dernières années, mais aussi imposer des vérifications obligatoires (des vérifications effectives, en réalité) à la fin de la durée de chacun de leurs contrats de licence pour entreprise. Pareillement, Oracle devrait intensifier ses activités de vérification des licences auprès de ses clients tout au long de l'année 2025. Cette société a en effet reconnu que les vérifications constituaient une source de revenus essentielle, et a notamment renforcé la surveillance des licences OCI Cloud, Oracle Java et des logiciels locaux.

DYNAMIQUE CONTRANT LES AUGMENTATIONS DE PRIX DES FOURNISSEURS

D'autres forces sont à l'œuvre et viennent s'opposer à ces tendances. Les incertitudes pesant sur le marché ont entraîné un ralentissement du nombre de demandes de propositions et de renseignements sur lesquels les fournisseurs peuvent soumissionner. Les clients ont ainsi signalé que, dans certains cas, les fournisseurs ont rapidement fait des compromis en réponse à la résistance de la clientèle aux augmentations de prix demandées. La justification donnée par les fournisseurs était qu'il valait mieux conserver une part de marché que de la perdre en cherchant à augmenter les prix. Dans d'autres secteurs, le plafonnement des revenus des clients, par exemple dans le secteur des assurances, a entraîné un effort de réduction des coûts accru, créant une nouvelle dynamique pour contrer la pression des fournisseurs de technologies en faveur d'une augmentation des frais.

La capacité d'un client à résister aux augmentations de prix dépend toutefois de l'importance du logiciel à ses yeux. Par exemple, il est plus facile de se tourner, ou de menacer de se tourner, vers un autre fournisseur moins cher lorsque le produit concerné est davantage une commodité. Cela devient beaucoup moins envisageable lorsque le produit fait partie d'une mise en œuvre très importante ou complexe de progiciel de gestion intégré (PGI).

Les clients peuvent chercher à améliorer leur capacité à négocier de meilleurs prix avec chaque fournisseur en mettant en œuvre des stratégies proactives, notamment : a) l'analyse de l'obsolescence ou la prévision de la fin de vie de leur stock technologique, de manière à recenser les composants dont la fin de vie est imminente; et b) l'adoption d'une stratégie de « seconde source », où le client recherche et engage un autre fournisseur secondaire en tant que solution de secours au fournisseur principal, s'assurant ainsi de ne pas dépendre d'un seul fournisseur.

LES PROBLÈMES PERSISTANTS POSÉS PAR LES CONTRATS T&M

Les procès liés à des projets qui ont échoué continuent de suggérer qu'il peut y avoir une dépendance excessive aux contrats de temps et de matériel (T&M) dans le domaine des projets PGI et technologiques, ce qui peut présenter des défis. Pour ne citer qu'un exemple, dans l'affaire *Hertz Corporation v Accenture LLP*, 1:19-cv-03508 (SD NY 2019), le client l'a appris à ses dépens lorsqu'il a engagé le fournisseur pour réaliser un projet de canaux numériques selon un contrat T&M. Mais après avoir payé au fournisseur plus de 32 millions $ US en frais et honoraires, il a fait valoir qu'il n'avait jamais reçu de site Web fonctionnel ni d'application mobile.

Les clients doivent être très prudents lorsqu'ils envisagent d'accepter des structures de facturation en T&M pour des projets technologiques de grande envergure. Dans certains cas, les clients, sachant que les frais imprévus sont intégrés dans un prix forfaitaire, peuvent penser qu'ils « déjouent » le fournisseur en acceptant un contrat T&M qui leur évite de payer les frais imprévus. Cependant, cela n'est pas nécessairement le cas et peut représenter un défi de taille.

Du point de vue du client, un contrat à prix fixe présente l'avantage d'une liste plus précise des justifications du fournisseur en cas de dépassement des coûts du projet. Par exemple, le fournisseur peut justifier les dépassements de coûts par un manquement du client à ses obligations ou par un élargissement de la portée du projet. En revanche, dans le cadre d'un contrat T&M, le fournisseur n'a pas besoin de se référer à une telle liste de justifications, car les honoraires sont simplement calculés en fonction du temps passé.

Pour le client, un deuxième avantage d'un projet à prix fixe est qu'il oblige le fournisseur à s'investir. Le client fera valoir que si un fournisseur prétend avoir une expérience et une expertise approfondies pour le projet technologique concerné, il devrait être en mesure de proposer un prix fixe pour le réaliser. Le vendeur peut toujours se protéger en définissant clairement la portée du projet et en prévoyant un montant pour faire face aux imprévus, ainsi qu'en énumérant les hypothèses particulières et les obligations du client afin de justifier ce montant forfaitaire. Néanmoins, dans l'ensemble, le prix fixe pourrait encore répartir plus équitablement les risques liés au projet.

Du point de vue du fournisseur, un contrat T&M peut être préférable dans diverses circonstances, y compris pour les contrats de portée limitée, mais avec un degré élevé d'incertitude. Par exemple, le contrat T&M pourrait être plus adapté a) à l'étape préliminaire de planification d'un projet, plutôt qu'à l'étape de « construction », b) à une « étape 0 » initiale de la vérification diligente d'un projet, ou c) à un projet impliquant plusieurs fournisseurs et où le succès du fournisseur dépendra de la performance d'autres tiers sous-traitants indépendants de son contrôle. Nous nous attendons à une pression continue de la part des fournisseurs pour obtenir des mandats facturés en T&M lorsqu'ils ne disposent pas de renseignements adéquats ou qu'ils n'ont pas de contrôle sur les facteurs externes dont dépend la réussite du projet.

Tendance 3 : Les limitations de responsabilité continueront d'être adaptées pour faire face à des risques complexes et précis

Les clauses de limitation de responsabilité sont une pierre angulaire des ententes relatives aux TI. Elles sont utilisées pour répartir les risques entre les parties contractantes et limiter les responsabilités potentielles. À mesure que les technologies continuent d'évoluer et que le champ d'application des services TI s'élargit, ces clauses sont devenues de plus en plus complexes et mieux adaptées pour répondre à des risques bien précis. Cette section examine les tendances récentes des clauses de limitation de responsabilité dans diverses ententes de TI. Elle traite plus spécialement des limites de responsabilité, de la portée des exclusions et des clauses de limitation de responsabilité particulières.

LIMITES DE RESPONSABILITÉ

En 2024, les limites et les super-limites ont continué à prendre différentes structures, la plus courante étant basée sur la valeur du contrat ou un multiple des frais payés sur une période donnée. Par exemple, certaines ententes plafonnaient la responsabilité au total des sommes reçues pour le produit ou le service, tandis que d'autres fixaient des plafonds à un montant négocié, qui était lié à la valeur totale du contrat, avec des révisions annuelles. En 2024, les rajustements au titre du coût de la vie ont fait l'objet d'une attention accrue en raison des préoccupations liées à l'inflation et à la hausse des taux d'intérêt. Ces préoccupations pourraient s'atténuer légèrement cette année, la Banque du Canada prévoyant une baisse de l'inflation en 2025 et ayant réduit ses taux d'intérêt depuis[2].

L'utilisation de mécanismes de réinitialisation des limites a également gagné du terrain sur le marché. Ces mécanismes réinitialisent effectivement la limite de responsabilité à son montant initial en cas de manquements déterminés ou lorsque le paiement des dommages-intérêts dépasse un seuil particulier (50 %) dans un délai défini (12 à 36 mois).

Pour 2025, nous nous attendons à ce que ces clauses continuent à prendre des formes et des montants variés, reflétant les nuances de la nature particulière des services TI concernés et les différents niveaux de risque associés aux différents types d'ententes.

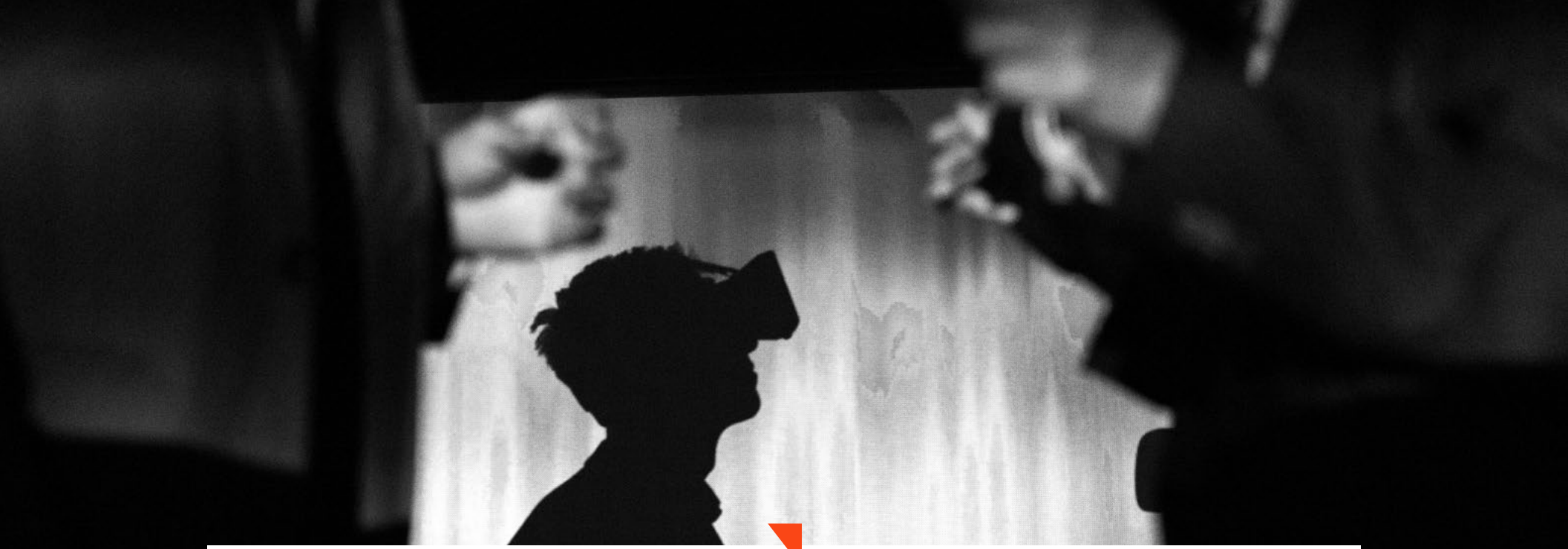
2. https://www.banqueducanada.ca/publication/rpm/rpm-2024-10-23/projections/?theme_mode=light&_gl=1*vswktf*_ga*MTMyMTc1NDc1NC4xNzQzNDUwOTk1*_ga_D0WRRH3RZH*MTc0MzQ1MDk5NC4xLjAuMTc0MzQ1MDk5NC42MC4wLjA. https://marchesdescapitaux.bmo.com/fr/ressources/perspectives-conomiques-du-canada-pour-2025-la-situation-samliore/

EXCLUSIONS DE RESPONSABILITÉ

Un autre élément clé des clauses de limitation de responsabilité est l'exclusion de la responsabilité pour certains types de dommages. Les exclusions de responsabilité pour les dommages indirects, exemplaires, punitifs et particuliers sont restées une pratique courante en 2024. Les pertes de profits, les pertes d'exploitation et les pertes de données étaient également des exclusions courantes. Cependant, il y avait des variations notables dans la façon dont elles étaient appliquées. Dans certains cas, les dommages indirects peuvent constituer un recours approprié et, par conséquent, n'ont pas été exclus de la responsabilité. Certaines ententes prévoyaient des exceptions pour des types précis de violations ou d'obligations d'indemnisation, garantissant que certains risques critiques n'étaient pas visés par l'exclusion de responsabilité. Par exemple, les violations du secret professionnel, de la confidentialité et des obligations de sécurité ont souvent été soustraites à ces exclusions. Cela reflète l'importance accrue de ces questions au sein du secteur des TI, en particulier avec l'avènement de l'intelligence artificielle ainsi que la prévalence et le risque financier accru que représentent les violations de données. Nous prévoyons que ces tendances se poursuivront tout au long de l'année 2025.

CLAUSES DE LIMITATION DE RESPONSABILITÉ PARTICULIÈRES

Outre les éléments plus traditionnels des clauses de limitation de responsabilité, les ententes relatives aux TI contiennent souvent des dispositions distinctes adaptées aux risques opérationnels propres à ce secteur. Une telle disposition est le concept de dommages directs réputés, qui pourrait s'appliquer à des scénarios où certaines défaillances entraînent des pertes financières déterminées. Par exemple, les dommages directs réputés peuvent inclure les pertes de revenus résultant de pannes de système ou d'autres perturbations. De même, certaines ententes prévoient des dépenses pour retenir les services de tiers stratégiques pour répondre à des situations ou à des violations telles que celles impliquant des renseignements personnels, la confidentialité ou les obligations de sécurité, ou pour fournir des conseils à cet égard. Étant donné les nombreuses perturbations informatiques notables survenues en 2024, nous prévoyons que ces dispositions resteront très pertinentes en 2025. Certains services TI sont essentiels et les parties chercheront probablement à s'assurer qu'elles sont indemnisées pour des types précis de pertes qui pourraient autrement être exclues en vertu des dispositions traditionnelles de limitation de responsabilité.



CONCLUSION

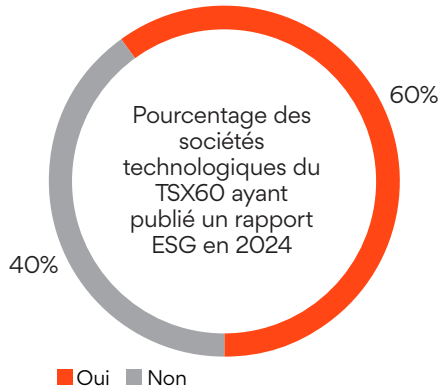
L'analyse des récentes ententes relatives aux TI révèle plusieurs tendances clés dans les clauses de limitation de responsabilité. Largement utilisées pour gérer l'exposition financière, les limites de responsabilité se situent généralement dans une large fourchette en fonction de la valeur du contrat ou des frais payés. Les exclusions pour dommages indirects sont courantes, bien qu'on y fasse souvent exception pour les risques critiques. En outre, des clauses propres aux limitations de responsabilité, comme les dommages directs réputés, reflètent la nature évolutive des services TI et la nécessité de traiter des risques opérationnels bien précis.

Ces tendances soulignent l'importance de rédiger et de négocier soigneusement les clauses de limitation de responsabilité pour s'assurer qu'elles répartissent efficacement les risques et offrent une protection adéquate aux deux parties. À mesure que progressera l'année 2025, ces clauses continueront d'être révisées pour refléter les risques émergents et atténuer les responsabilités potentielles des entreprises qui recherchent un environnement commercial plus stable et prévisible.

Tendance 4 : Le paysage réglementaire des facteurs ESG continuera d'évoluer et de trouver du soutien et des défis dans l'innovation technologique

Les facteurs environnementaux, sociaux et de gouvernance (ESG) restent au cœur des stratégies d'affaires au Canada. Cela s'explique par les préoccupations mondiales en matière de développement durable et par les pressions réglementaires croissantes. Au Canada, les pratiques ESG sont de plus en plus formalisées, et on a vu des changements importants dans le paysage réglementaire au cours de l'année écoulée. La *Loi sur la lutte contre le travail forcé et le travail des enfants dans les chaînes d'approvisionnement*, entrée en vigueur le 1er janvier 2024, oblige les entreprises à divulguer les efforts qu'elles déploient pour éliminer le travail forcé et le travail des enfants dans leurs chaînes d'approvisionnement[3]. Le non-respect de ces nouvelles règles pourrait entraîner des sanctions pouvant aller jusqu'à 250 000 $ CA pour les entités, dirigeants ou administrateurs non conformes[4].

En outre, les modifications apportées à la *Loi sur la concurrence*, en vigueur depuis juin 2024, interdisent expressément l'écoblanchiment et exigent que les déclarations environnementales des entreprises soient étayées par des tests appropriés et des normes mondialement reconnues[5]. Cette loi aura une incidence encore plus importante sur la manière dont les entreprises technologiques communiquent leurs initiatives environnementales. Parallèlement, le sentiment anti-ESG croissant, en particulier aux États-Unis, influence l'environnement commercial au sens large, créant des sensibilités politiques que les organisations doivent gérer avec prudence[6]. Pour rester compétitives et conformes, les entreprises technologiques doivent se tenir informées des changements législatifs et de l'évolution des attitudes du public à l'égard des questions ESG. Ce faisant, elles s'assurent de pouvoir trouver un équilibre entre les exigences de transparence et les défis potentiels posés par les courants opposés.



3. ***Loi sur la lutte contre le travail forcé et le travail des enfants dans les chaînes d'approvisionnement*** (L.C. 2023, ch. 9)
4. Ibid, para. 19(1)
5. https://bureau-concurrence.canada.ca/fr/comment-nous-favorisons-concurrence/education-sensibilisation/declarations-environnementales-ecoblanchiment
6. https://www.thomsonreuters.com/en-us/posts/esg/anti-esg-legislation/ (en anglais seulement)

IA ET INNOVATION : POSSIBILITÉS ET DÉFIS POUR L'AVENIR

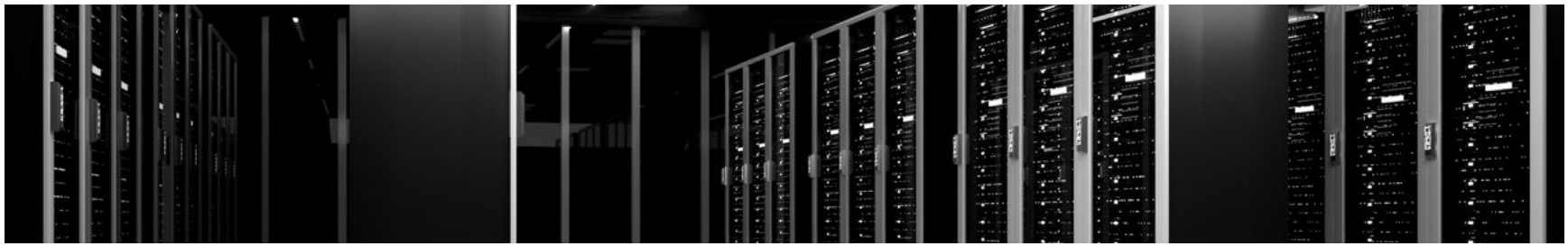
L'intelligence artificielle est de plus en plus au cœur des discussions sur l'ESG, les entreprises et les investisseurs reconnaissant son influence croissante. D'un point de vue ESG, l'IA offre des possibilités pour améliorer la transparence et l'efficacité, en particulier dans le suivi, l'analyse et la comparaison des données ESG. Or, l'IA introduit aussi de nouveaux défis, notamment les risques pour la vie privée, les biais algorithmiques et les impacts environnementaux des systèmes d'IA à grande échelle.

L'un des principaux défis est la demande croissante de centres de données alimentés par l'IA, qui consomment de grandes quantités d'énergie et d'eau. Par exemple, l'électricité consommée par un robot conversationnel doté d'une intelligence artificielle, tel que ChatGPT, peut être jusqu'à dix fois supérieure à celle d'une recherche Google classique. L'Agence internationale de l'énergie estime que la consommation d'électricité des centres de données et de l'IA pourrait dépasser 1 000 TWh d'ici 2026, soit à peu près l'équivalent de la consommation d'électricité totale du Japon[7].

Cependant, les progrès réalisés au niveau de l'infrastructure des centres de données ont permis de réduire considérablement la demande en énergie. L'essor des centres de données écologiques, qui privilégient l'efficacité énergétique et la durabilité, joue un rôle clé à cet égard. Ces installations utilisent des systèmes de refroidissement efficaces, des sources d'énergie renouvelables et des solutions de réutilisation de la chaleur résiduelle pour optimiser la consommation d'énergie. De plus, des innovations comme l'optimisation des modèles d'IA et le matériel écoénergétique contribuent à réduire l'empreinte carbone de l'IA. À l'avenir, il sera important de voir comment les pays, y compris le Canada, trouveront un équilibre entre ces avancées technologiques et les mesures réglementaires visant à gérer l'explosion de la demande énergétique.

En ce qui concerne la gouvernance et les enjeux sociaux, les investisseurs sont de plus en plus préoccupés par les risques liés à l'IA et font pression pour que soient mis en place des cadres de gouvernance responsables en la matière. Cela a conduit à une augmentation des propositions d'actionnaires, en particulier aux États-Unis, exhortant les entreprises à présenter de l'information sur leur utilisation de l'IA, à établir des directives éthiques et à assurer une surveillance adéquate de la part du conseil d'administration. À mesure que l'adoption de l'IA se généralise dans tous les secteurs, les entreprises technologiques doivent répondre à la fois aux exigences réglementaires et aux demandes croissantes des investisseurs quant à la transparence et aux pratiques éthiques en matière d'IA. Les organisations qui gèrent ces risques de manière proactive et font preuve d'une utilisation responsable de l'IA sont plus susceptibles de gagner la confiance des investisseurs et de conserver un avantage concurrentiel.

À terme, le paysage ESG au Canada évoluera rapidement, en raison de nouvelles réglementations et des attentes croissantes des investisseurs qui façonneront les stratégies des entreprises. Pour assurer leur réussite à long terme, les entreprises technologiques devront se tenir informées de ces changements réglementaires, relever les défis posés par l'IA et répondre aux préoccupations croissantes concernant les critères ESG.



7. https://iea.blob.core.windows.net/assets/18f3ed24-4b26-4c83-a3d2-8a1be51c8cc8/Electricity2024-Analysisandforecastto2026.pdf à la page 8 (en anglais seulement).

Tendance 5 : Les mesures gouvernementales renforceront l'impératif de cybersécurité pour les entreprises

L'introduction de nouvelles exigences fédérales et provinciales en matière de cybersécurité représente une étape importante dans l'encadrement de ce secteur au Canada. Si elles entrent en vigueur en 2025, les modifications législatives et réglementaires fédérales et provinciales décrites dans cette section auront un effet considérable sur les pratiques de sécurité des organisations des secteurs privé et public, nécessitant une réévaluation considérable des politiques internes de cybersécurité et des accords avec des tiers.

FÉDÉRAL – *PROJET DE LOI C-26, LOI CONCERNANT LA CYBERSÉCURITÉ, MODIFIANT LA LOI SUR LES TÉLÉCOMMUNICATIONS ET APPORTANT DES MODIFICATIONS CORRÉLATIVES À D'AUTRES LOIS* (PROJET DE LOI C-26)

À la fin du mois de décembre 2024, le Parlement fédéral était sur le point d'adopter le projet de loi C-26, le Sénat du Canada ayant achevé sa troisième lecture du projet de loi et la Chambre des communes étant prête à adopter les amendements du Sénat et à envoyer le projet de loi pour la sanction royale. Le projet de loi C-26 est néanmoins « mort » au Feuilleton à la suite de la décision du premier ministre de proroger le Parlement le 6 janvier 2025. En effet, les projets de loi qui n'ont pas reçu la sanction royale avant la prorogation sont abrogés et doivent normalement être présentés à nouveau comme s'ils n'avaient jamais existé. Étant donné l'avancement de l'examen du projet de loi par le Parlement, il est toutefois possible que la même législation soit présentée à nouveau[8] et rapidement adoptée par un nouveau gouvernement (ou le prochain Parlement) en 2025.

Si elle est adoptée, la loi :

1. Apportera des modifications à la *Loi sur les télécommunications* (notamment pour interdire l'utilisation des produits et services de certains fournisseurs au moyen d'ordonnances de sécurité émises par le gouvernement canadien ou le ministre de l'Industrie).

2. Édictera la *Loi sur la protection des cybersystèmes essentiels*, qui s'appliquerait à certains opérateurs désignés de « systèmes et services critiques » (p. ex. systèmes bancaires, systèmes de transport sous réglementation fédérale, réseaux électriques interprovinciaux). Les obligations concernent généralement la mise en place d'un programme de cybersécurité, le signalement des incidents de cybersécurité, le respect des directives du gouvernement canadien et la conservation des documents relatifs à la conformité et aux incidents.

8. Les projets de loi peuvent être déposés à nouveau au début d'une nouvelle session au même stade qu'ils avaient atteint à la fin de la session précédente. Cela se fait soit avec le consentement unanime de la Chambre, soit par l'adoption d'une motion à cet effet. Voir : « Incidences de la prorogation » https://www.noscommunes.ca/procedure/procedure-et-les-usages-3/ch_08_6-f.html.

3. Imposera des dispositions relatives aux pénalités importantes. Par exemple, la *Loi sur la protection des cybersystèmes essentiels* introduira des sanctions pour chaque type de violation à définir par la loi (c.-à-d. mineure, grave ou très grave). Le montant des pénalités pour chaque violation est plafonné à 1 000 000 $ dans les cas de personnes physiques et à 15 000 000 $ pour les autres personnes.

Le projet de loi C-26 représente une affirmation importante de la compétence fédérale en matière de réglementation de la cybersécurité au Canada. Compte tenu du stade avancé auquel le projet de loi C-26 était parvenu avant la prorogation et de l'attitude agressive de la nouvelle administration américaine à l'égard des questions de cybersécurité et de sécurité nationale, les organisations devraient se préparer à l'éventualité où cette loi serait remise sur le tapis et adoptée en 2025.

ONTARIO – *PROJET DE LOI 194 (LOI DE 2024 VISANT À RENFORCER LA CYBERSÉCURITÉ ET LA CONFIANCE DANS LE SECTEUR PUBLIC)*

Le projet de loi 194 (*Loi de 2024 visant à renforcer la cybersécurité et la confiance dans le secteur public*) a reçu la sanction royale le 25 novembre 2024. À une date qui sera communiquée ultérieurement, le projet de loi 194 :

1. Édictera la *Loi visant à renforcer la sécurité et la confiance en matière de numérique*, qui permet au gouvernement de l'Ontario d'exiger des entités du secteur public qu'elles élaborent et mettent en œuvre des programmes de cybersécurité et soumettent des rapports sur ce sujet, entre autres exigences liées à la protection de la vie privée et à l'utilisation des systèmes d'IA par les entités du secteur public.

2. Apportera des modifications à la *Loi sur l'accès à l'information et la protection de la vie privée* (dont seule une partie est entrée en vigueur lors de la sanction royale relative aux « renseignements liés au service à la clientèle »).

Le regard tourné vers 2025

L'année 2025 sera une année critique pour les organisations qui devront faire le point sur leurs programmes de cybersécurité, y compris les politiques qu'elles utilisent pour protéger les renseignements confidentiels et personnels. Les organisations devront également revoir leurs ententes avec les fournisseurs de services et évaluer si des mesures suffisantes sont en place pour assurer la conformité aux nouvelles réglementations en matière de cybersécurité en Ontario (et, potentiellement, dans tout le Canada). Bien que les institutions du secteur public soient au cœur du projet de loi 194 en Ontario, les organisations du secteur privé devraient suivre de près les développements fédéraux et provinciaux. Il sera important pour elles de surveiller l'évolution des normes de l'industrie en fonction de la surveillance réglementaire fédérale et provinciale croissante de la cybersécurité dans les secteurs public et privé.

Tendance 6 : Les clients et les fournisseurs de services se tourneront de plus en plus vers les assurances pour atténuer les risques technologiques

L'évolution du risque numérique au cours de l'année 2025 conduira davantage d'entreprises à exiger de leurs fournisseurs de services qu'ils souscrivent une assurance erreurs et omissions technologiques et une assurance cyberrisque (ou assurance cybersécurité), et ces fournisseurs jugeront prudent de le faire. Cela sera particulièrement vrai lorsque les risques pertinents seront connus ou accrus. Dans ce cas, il ne sera pas suffisant de se fier uniquement aux dispositions contractuelles de limitation de responsabilité ou d'indemnisation, en particulier lorsque l'on peut s'attendre à ce que les fournisseurs de services redoublent d'efforts pour limiter leur exposition à ces risques connus. Lorsque le risque d'un événement augmente, les clients avertis cherchent souvent à atténuer leur exposition en souscrivant une assurance (entre autres), et les fournisseurs avertis peuvent chercher à réaffecter entièrement ou partiellement le risque à leur client.

ASSURANCE ERREURS ET OMISSIONS TECHNOLOGIQUES

Les clients continueront à attendre de leurs prestataires de services qu'ils souscrivent une assurance erreurs et omissions technologiques. Ces derniers pourraient également avoir besoin de se prévaloir d'une telle assurance. Les entreprises de logiciels-services, plus particulièrement, continueront à bénéficier de l'assurance erreurs et omissions technologiques, car elles exercent leurs activités dans un environnement hautement dynamique et concurrentiel où la fiabilité et la sécurité de leurs services sont primordiales. Ces entreprises fournissent des applications logicielles sur l'Internet public ou des réseaux privés tout en traitant de grandes quantités de données. Elles doivent aussi garantir un accès relativement ininterrompu à leurs services. Par conséquent, les entreprises de logiciels-services et leurs clients continueront de compter sur l'assurance erreurs et omissions technologiques, en 2025 et dans les années à venir. Cela s'explique notamment par les raisons suivantes : simple prudence, obligation contractuelle, exigences en matière d'innovation et obligations de conformité réglementaire.

Prudence des fournisseurs de logiciels-services : L'utilisation de l'assurance erreurs et omissions technologiques est appelée à se développer pour faire face à la complexité croissante des écosystèmes numériques modernes, compte tenu de sa couverture des frais de justice et des responsabilités financières découlant des risques couverts liés au stockage et au traitement des renseignements sensibles des clients. Elle permet également d'assurer la disponibilité continue des services de logiciels-services dont les clients dépendent pour leurs opérations quotidiennes.

Attentes relatives aux obligations contractuelles : Lorsque les contrats de logiciel-service incluent des accords sur les niveaux de services (ANS) stricts qui garantissent des mesures de performance précises, y compris le temps de disponibilité et les temps de réponse, le non-respect de ces obligations contractuelles peut entraîner des pénalités, des obligations de remboursement et des poursuites judiciaires de la part de leurs clients. L'assurance erreurs et omissions technologiques aide les entreprises de logiciels-services à couvrir les coûts associés à ces violations contractuelles.

Elle leur offre un filet de sécurité qui leur permet de se concentrer sur le maintien de normes de service élevées.

Pressions continues pour innover et se développer : Le secteur des logiciels-services se caractérise par une innovation rapide et le développement continu de nouvelles caractéristiques et fonctionnalités. Cependant, l'introduction de nouvelles technologies et de mises à jour peut générer des bogues supplémentaires et d'autres problèmes techniques imprévus. L'assurance erreurs et omissions technologiques couvre les réclamations liées aux défauts des logiciels et aux erreurs de développement. Cela permet aux entreprises de logiciels-services d'innover en toute confiance, sachant qu'elles sont protégées contre d'éventuelles responsabilités.

Conformité réglementaire : Le non-respect des règlements en matière de protection des données et de cybersécurité peut entraîner des amendes importantes et donner lieu à des litiges longs et coûteux. Les organismes réglementaires restent attentifs aux conséquences des violations de données, des interruptions de service imprévues et des cas de non-conformité générale à la loi. L'atténuation des risques que l'assurance erreurs et omissions technologiques offre pour les frais juridiques et les pénalités liées aux infractions réglementaires sera un outil de plus en plus utile pour atténuer le risque dans un paysage réglementaire complexe.

ASSURANCE CYBERRISQUE

Nous nous attendons à ce que la tendance à la hausse des cyberattaques se poursuive en 2025, avec un transfert proportionnel de ce risque des clients vers les fournisseurs de logiciels-services en vertu de contrats exigeant de ces derniers qu'ils mettent en œuvre des cadres de cybersécurité complets, tels que des évaluations régulières des risques, la formation des employés et des plans d'intervention en cas d'incident. La conformité réglementaire sera également un facteur particulièrement important en 2025. Les contrats s'adapteront pour répondre aux exigences strictes des lois sur la protection des données et des organismes de réglementation en matière de protection de la vie privée, d'autant plus que de nouvelles lois et réglementations sur la confidentialité sont élaborées et mises en œuvre. Nous nous attendons également à une évolution vers des polices plus personnalisées qui continuent à couvrir les risques propres à chaque secteur d'activité et à fournir une couverture pour la cyberresponsabilité, y compris la réponse aux incidents, l'interruption des activités et la violation des données.

ASSURANCE RESPONSABILITÉ EN MATIÈRE DE PI

Nous prévoyons une augmentation de la demande de produits d'assurance contre les risques liés à la propriété intellectuelle, notamment les violations de brevets, de marques de commerce et de droits d'auteur, au cours de l'année 2025. Les clients continueront d'imposer aux fournisseurs de services l'obligation de souscrire une assurance pour couvrir les risques liés à la propriété intellectuelle, en particulier lorsqu'un fournisseur de services utilise la propriété intellectuelle appartenant à des sous-traitants tiers ou lorsque la propriété intellectuelle utilisée dans les offres de services technologiques externalisés a fait l'objet d'un litige pour violation de propriété intellectuelle (que ce soit au pays ou ailleurs dans le monde). Les parties contractantes peuvent aussi se tourner vers l'assurance responsabilité en matière de PI pour atténuer le risque posé par les nouvelles technologies, telles que l'intelligence artificielle, l'apprentissage automatique, et les nouveaux défis en matière de propriété intellectuelle qu'elles introduisent. Parmi les caractéristiques de l'assurance contre la responsabilité en matière de PI qui peuvent intéresser les clients comme les fournisseurs de services, citons la couverture multiterritoriale, qui aide les entreprises à gérer les complexités de la mise en application et de la protection de la PI à l'échelle mondiale.

Tendance 7 : L'industrie devra traverser les défis et les possibilités découlant de l'IA sans point de repère

L'année 2024 a été celle des tests, de la mise en œuvre et de l'adoption de l'IA générative. Les propriétaires de produits visaient à améliorer leur fiabilité, à répondre aux implications sociétales, à instaurer la confiance, à trouver l'adéquation produit-marché et à en faire une partie intégrante de la vie quotidienne. Les organisations utilisatrices ont quant à elles présenté des scénarios de cas d'utilisation posant un risque réduit, axés sur la création de politiques, la gouvernance éthique et la formation. Or, le cadre juridique canadien visant à réglementer l'IA n'a pas évolué au même rythme que la croissance explosive de l'IA générative et l'investissement de 2,4 milliards de dollars dans l'IA prévu par le gouvernement canadien en 2024. En 2022, le gouvernement canadien a déposé la *Loi sur l'intelligence artificielle et les données* (LIAD), et des amendements ont été proposés en 2023. Par la suite, la LIAD a été adoptée en deuxième lecture à la Chambre des communes et a fait l'objet d'un examen par le Comité permanent de l'industrie et de la technologie de la Chambre. Le Parlement canadien ayant été prorogé début janvier, la LIAD est morte au Feuilleton.

Pourtant, la complexité et la sophistication des systèmes d'IA et le paysage de risques en constante évolution, combinées à l'absence d'un cadre législatif normalisé, exigent que les fournisseurs et les utilisateurs de systèmes d'IA adoptent des mesures proactives. D'une part, les fournisseurs doivent mettre en œuvre des mesures de protection qui rendent les systèmes d'IA éthiques, fiables et sécurisés. Cela implique de traiter les questions de partialité, de donner la priorité à l'équité et à la transparence des résultats, de mettre en œuvre des mesures de sécurité robustes, de se conformer aux lois sur la protection de la vie privée, de procéder à des tests continus pour détecter les vulnérabilités, les erreurs et les résultats inattendus, et de mettre en œuvre des correctifs. D'autre part, les utilisateurs doivent mettre en place des mesures préventives visant à réduire les risques. Cela inclut la vérification de leur infrastructure de données, la conformité aux réglementations en matière de protection de la vie privée, l'amélioration des compétences et la formation de leur personnel, ainsi que la mise en œuvre de politiques et de cadres clairs pour une utilisation responsable de l'IA, de systèmes de surveillance de cette utilisation et de mécanismes permettant de résoudre les problèmes rapidement.

DÉVELOPPEMENTS EN MATIÈRE DE PROTECTION DES DONNÉES PERSONNELLES

Bien que la LIAD n'ait pas vu le jour, les lois fédérales et provinciales sur la protection de la vie privée continuent de s'appliquer à l'utilisation de l'IA par les organisations. La LPRPDE et les lois provinciales exigent que les organisations obtiennent le consentement pour la collecte, l'utilisation et la communication de renseignements personnels en lien avec les systèmes d'IA et que les organisations s'en portent responsables dans le cadre de leur utilisation de ces systèmes. Vous pouvez lire notre bulletin sur une récente décision de la Cour d'appel fédérale concernant l'obtention d'un consentement valable et la nécessité pour les organisations de fournir des avis précis, directs et à plusieurs niveaux aux personnes afin qu'elles puissent donner leur consentement éclairé à la collecte et à l'utilisation de ces renseignements. En outre, lorsque des systèmes d'IA sont utilisés pour prendre des décisions concernant des individus, les lois existantes en matière de protection de la vie privée

exigent que les organisations conservent les renseignements personnels afin que les personnes concernées aient un accès raisonnable à ces renseignements sur demande. La loi révisée du Québec sur la protection des renseignements personnels comprend également des exigences particulières relatives aux décisions prises uniquement de manière automatisée, en accordant aux individus le droit d'être informés de ces décisions et de demander des renseignements supplémentaires sur la manière dont la décision a été prise.

L'année 2025 pourrait aussi voir les organismes de réglementation canadiens appliquer pour la première fois à l'IA générative les lois canadiennes en vigueur sur la protection de la vie privée. Cela dépendra des conclusions de l'enquête menée par les commissaires à la protection de la vie privée du Canada, de l'Alberta, de la Colombie-Britannique et du Québec sur OpenAI. Les commissaires à la protection de la vie privée enquêtent sur OpenAI afin de déterminer si la société : i) a obtenu un consentement valable pour collecter, utiliser et communiquer des renseignements personnels au moyen de ChatGPT; ii) a respecté ses obligations en matière d'ouverture, de transparence, d'accès, d'exactitude et de responsabilité; et iii) a recueilli, utilisé et/ou communiqué des renseignements personnels à des fins appropriées, raisonnables et légitimes, et a tâché de ne recueillir que des renseignements nécessaires. L'enquête pourrait aborder des questions fondamentales de confidentialité pour l'IA générative, par exemple si l'entraînement constitue une utilisation des renseignements personnels et si les grands modèles de langage eux-mêmes contiennent des renseignements personnels. En Europe, une décision récente du Comité européen de la protection des données a estimé que les modèles d'entraînement utilisant des données incluant des données personnelles et les modèles qui en résultent impliquent le traitement de données personnelles au sens du *Règlement général sur la protection des données*. Les résultats de l'enquête des commissaires pourraient avoir des répercussions importantes sur la manière dont l'IA générative peut être développée, mise à disposition et déployée au Canada.

ÉVOLUTION DE LA RÉGLEMENTATION INTERNATIONALE EN MATIÈRE D'IA

L'année dernière, l'Union européenne a introduit la loi sur l'IA, qui est entrée en vigueur le 1er août 2024 et dont les dispositions ont pris effet le 2 février 2025. La loi sur l'IA de l'UE classe les systèmes d'IA en fonction des risques et impose des restrictions et des interdictions aux différentes catégories de systèmes et d'utilisations de l'IA. Vous pouvez consulter notre bulletin pour en savoir plus sur la loi sur l'IA et son calendrier de mise en œuvre.

Aux États-Unis, il n'existe actuellement aucune législation fédérale complète en matière d'IA. Plusieurs projets de loi portant sur un large éventail de questions relatives à l'IA sont actuellement examinés par le Congrès américain, dont plusieurs insistent sur le développement de lignes directrices volontaires et de bonnes pratiques pour ces systèmes. En septembre 2023, le Sénat américain a tenu des auditions publiques (article en anglais) pour étudier les moyens d'accroître la transparence de l'IA pour les consommateurs, de déterminer les utilisations bénéfiques ou « à haut

risque » et d'évaluer la portée potentielle des politiques en matière d'IA visant à accroître la fiabilité et augmenter la confiance du public. Parallèlement, les législateurs américains ont tenu des séances d'écoute à huis clos (article en anglais) avec des développeurs d'IA, des acteurs technologiques de premier plan et des groupes de la société civile. Malgré l'absence de législation fédérale, des cadres et lignes directrices sur l'IA ont été adoptées par l'administration Biden, mais ces initiatives ont été abrogées dès l'investiture du président Donald Trump.

NORMES INDUSTRIELLES ET AUTRES MESURES DE SÉCURITÉ

D'importantes organisations de normalisation du secteur, dont le National Institute of Standards and Technology (NIST) et l'Organisation internationale de normalisation (ISO), ont cherché à combler davantage le vide législatif en publiant des normes et des principes pouvant être adoptés volontairement par les organisations qui s'impliquent dans la conception, le développement, l'utilisation et l'évaluation des systèmes d'IA. On peut citer à titre d'exemple le Artificial Intelligence Risk Management Framework (cadre de gestion des risques liés à l'intelligence artificielle) du NIST, qui vise à doter les fournisseurs et les utilisateurs de systèmes d'IA d'approches qui augmentent la fiabilité de ces systèmes et favorisent la conception, le développement, le déploiement et l'utilisation responsables de ces systèmes. Il y a aussi la norme ISO/IEC 42001, qui fournit des conseils sur la manière d'établir, de mettre en œuvre, de maintenir et d'améliorer continuellement la gestion des systèmes d'IA et de traiter les considérations éthiques et les risques tels que la traçabilité, la transparence et la fiabilité. Les fournisseurs participant au développement et à la commercialisation de systèmes d'IA peuvent adopter entièrement ou partiellement ces normes pour démontrer leur engagement en faveur d'une conception responsable de l'IA et des meilleures pratiques de l'industrie. Les organisations qui cherchent à se procurer des systèmes d'IA peuvent exiger de leurs fournisseurs qu'ils respectent ces normes de la même manière qu'ils peuvent exiger le respect des normes de sécurité informatique et de l'information du NIST ou de l'ISO.

Il est important de noter que les mesures de protection juridiques élémentaires continuent de s'appliquer à l'adoption des systèmes d'IA. La prise de décision assistée par l'IA qui s'avère discriminatoire ou qui enfreint d'une autre manière les droits fondamentaux de la personne reste soumise à la *Charte canadienne des droits et libertés* et à la législation fédérale et provinciale sur les droits de la personne, comme ce serait le cas si la décision était prise par un être humain. De même, les lois fédérales et provinciales sur la protection des consommateurs et l'emploi continuent de protéger les consommateurs et les employés, quelle que soit l'ampleur de l'utilisation des systèmes d'IA par les fournisseurs et les employeurs avec lesquels ils traitent.

Tendance 8 : Les gouvernements imposeront des règles de plus en plus strictes pour protéger les consommateurs dans l'environnement en ligne

Le commerce électronique a connu une popularité fulgurante au cours des cinq dernières années et est devenu le principal canal de vente pour une part importante du marché des produits et services de consommation. Les entreprises qui ne vendaient jamais en ligne ont commencé à le faire et d'autres qui évoluaient dans cet espace ont commencé à explorer de nouvelles possibilités comme les services d'abonnement. Cette migration vers le commerce numérique ne ralentira pas de sitôt.

Se lancer dans le commerce électronique au Canada signifie devoir naviguer dans un dédale complexe de cadres réglementaires. La *Loi sur la protection des renseignements personnels*, la *Loi canadienne anti-pourriel* (LCAP), la *Loi sur la concurrence* et les lois provinciales sur la protection des consommateurs d'application générale ne sont que quelques-uns des cadres réglementaires à connaître pour acheter ou vendre en ligne. Ces lois et règlements étant adaptés pour protéger les consommateurs contre des risques en constante évolution, les entreprises doivent comprendre ce que ces changements impliquent pour leurs activités et comment s'assurer de leur conformité sans contraintes ni coûts excessifs.

Toute entreprise canadienne qui vend aux consommateurs doit veiller à respecter les lois sur la protection des consommateurs. Toutes les provinces et tous les territoires ont leurs propres lois d'application générale sur la protection du consommateur. Les organisations doivent se conformer à ces lois, quel que soit leur emplacement géographique. Les lois sur la protection du consommateur s'appliquent généralement aux entreprises situées au Canada, mais aussi aux entreprises qui fournissent des produits ou des services aux consommateurs canadiens.

Au début de l'année 2025, l'Ontario et le Nouveau-Brunswick ont adopté des lois modernisées sur la protection des consommateurs. Ces nouvelles lois ont reçu la sanction royale, mais ne sont toujours pas entrées en vigueur. Quoi qu'il en soit, elles reflètent les tendances législatives en matière de commerce électronique. Un certain nombre de changements à venir en Ontario en vertu de la nouvelle *Loi de 2023 sur la protection du consommateur* (la nouvelle LPC) sont révélateurs :

1. **Examens publics** : En vertu de la nouvelle LPC, un concept a été emprunté à la *Loi sur la protection des consommateurs et consommatrices de l'Alberta*, qui interdit aux fournisseurs d'empêcher les consommateurs de publier des commentaires sur le fournisseur ou ses produits. Deux provinces ont maintenant modifié leurs lois pour lutter contre les pratiques susceptibles d'induire le public en erreur par le biais de commentaires de consommateurs. Ces modifications suggèrent une sensibilité accrue des autorités de réglementation à la transparence des commerçants quant à la manière dont leurs produits et services sont commercialisés.

2. **Conditions interdites en tant qu'infractions** : En vertu de la loi ontarienne actuelle, les dispositions des conventions de consommation (y compris les conditions de service) qui ne sont pas exécutoires ne sont généralement et simplement pas appliquées. Cependant, la nouvelle LPC va plus loin et prévoit que l'inclusion de conditions interdites dans les contrats est également considérée comme une infraction, exposant potentiellement les entreprises à des mesures d'application de la réglementation. Cela suggère l'adoption possible du modèle déjà en place au Québec, selon lequel les dispositions qui ne sont pas exécutoires au Québec sont expressément exclues. Une telle tendance renforce la nécessité pour les entreprises de faire preuve de diligence dans la rédaction de leurs conditions générales de vente en ligne pour ne pas s'exposer à des responsabilités non désirées.

3. **Modifications de contrat** : La nouvelle LPC établit une distinction entre la « prorogation » et la « modification » d'un contrat de consommation. L'intention et l'effet de ces concepts ne sont pas encore clairs, mais au début de 2025, le gouvernement de l'Ontario a entamé un processus de consultation sur le contenu des règlements qui permettront de clarifier ces concepts. Ces consultations permettront de déterminer dans quels cas les contrats de consommation devraient seulement nécessiter une modification avec préavis par opposition à ceux où le consentement peut être requis.

4. **Méthodes d'annulation** : La question de savoir comment les contrats de consommation peuvent être annulés est liée à celle de leur modification. Bien qu'il ne s'agisse pas d'une question expressément abordée dans la nouvelle LPC, le processus de consultation susmentionné soulève la possibilité d'introduire des règlements qui contribueraient à simplifier le processus d'annulation. Par exemple, il pourrait être obligatoire que les contrats puissent être annulés de la même manière qu'ils ont été conclus (p. ex. les contrats en ligne doivent pouvoir être annulés en ligne) ou qu'il soit interdit aux entreprises de dissuader les consommateurs d'annuler les contrats. Étant donné que des initiatives similaires sont en cours ailleurs (notamment une règle de « cliquer pour annuler » pour les abonnements aux États-Unis), une telle réglementation des processus commerciaux est un sujet que les fournisseurs de commerce électronique doivent surveiller.

La modernisation du régime ontarien de protection du consommateur illustre la nécessité pour les entreprises de suivre l'évolution des lois régissant le commerce électronique et de s'y conformer. Alors que l'Ontario et d'autres provinces canadiennes continuent de faire évoluer leurs lois sur la protection du consommateur, les entreprises auraient intérêt à obtenir des avis juridiques sur la manière de s'y retrouver dans ce nouveau paysage.

Tendance 9 : L'innovation des technologies financières se poursuivra et leur adoption progressera malgré les défis actuels

Les produits de technologie financière (fintech) innovent rapidement pour répondre aux attentes des consommateurs en matière de services pratiques et rentables facilitant les paiements numériques, les placements, la mobilisation de capitaux et d'autres services financiers numériques. Malgré une croissance récente, le secteur des technologies financières au Canada continue d'accuser un retard par rapport à certains autres pays du G7 en ce qui concerne l'adoption et la taille du marché. En 2023, seulement 13 % des consommateurs de services bancaires canadiens utilisaient des services de technologie financière, contre 32 % au Royaume-Uni et 42 % aux États-Unis[9]. La tendance est toutefois à la hausse, les données indiquant qu'en comparaison avec 2020, les Canadiens étaient en 2023 trois fois plus disposés à partager des données avec des fournisseurs de services financiers avec lesquels ils avaient déjà une relation[10]. Nous nous attendons à ce que cette tendance se soit poursuivie en 2024 et perdure en 2025. L'évolution du cadre juridique devrait jouer un rôle important dans la croissance du secteur des technologies financières au Canada, comme ce fut le cas au Royaume-Uni et aux États-Unis.

LES SERVICES BANCAIRES OUVERTS AU CANADA

Les services bancaires ouverts (ou services bancaires axés sur le consommateur) constituent un cadre qui permet aux utilisateurs de communiquer à des fournisseurs de services tiers les données du compte bancaire d'un consommateur. Traditionnellement, les banques conservaient les données financières de leurs clients dans leurs propres systèmes fermés. Les services bancaires ouverts permettent aux consommateurs de partager en toute sécurité leurs renseignements financiers avec des entreprises de technologie financière. Il est ainsi possible d'élargir l'accès aux services financiers comme les transferts d'argent, la gestion de comptes agrégés et les renseignements financiers personnalisés.

Pour proposer des services de technologie financière innovants, les institutions financières établies se sont tournées vers des acquisitions stratégiques d'entreprises œuvrant dans ce domaine, ou vers des partenariats avec celles-ci, dans le but d'améliorer l'expérience client sur leurs propres plateformes. Nous nous attendons à ce que cette tendance persiste.

9. L'essor de la technologie financière au Canada? | McKinsey
10. Canadians are 3x more likely to share data with their financial service providers today than 2020, finds EY survey EY - Canada. (en anglais seulement)
Voir également : https://www2.deloitte.com/content/dam/Deloitte/ca/Documents/financial-services/ca-les-services-bancaires-ouverts-au-canada-accro%C3%AEtre-la-sensibilisation-la-transparence-et-a-confiance-aoda.pdf

La majorité des entreprises de technologie financière ne sont cependant pas en mesure d'accéder en toute sécurité aux renseignements concernant les clients des institutions financières établies, car le Canada n'a pas d'exigences les obligeant à le faire. Par conséquent, ces entreprises doivent recourir à une pratique appelée « capture de données d'écran », qui consiste, pour le client, à fournir à l'entreprise de technologie financière ses identifiants bancaires afin que celle-ci puisse se connecter par intermittence au compte bancaire du client pour accéder à ses renseignements financiers. Cette pratique comporte des risques importants en matière de sécurité et de responsabilité en cas de transactions non autorisées ou de violation des données. Les chefs de file du secteur des technologies financières ont publiquement exprimé leurs préoccupations quant à la lenteur du Canada à adopter des lois sur les services bancaires ouverts par rapport à d'autres économies développées. Les institutions financières établies ont pour leur part soulevé des préoccupations fondamentales concernant la réglementation, ou l'absence de réglementation, applicable aux entreprises de technologie financière, de même que des inquiétudes quant aux coûts élevés de mise en conformité.

En avril 2024, le gouvernement fédéral a annoncé qu'il élaborait un cadre régissant les services bancaires ouverts dans le budget fédéral et a alloué plus de 5 millions de dollars à cette initiative répartis sur les trois prochaines années. En juin, la *Loi sur les services bancaires axés sur les consommateurs* a été adoptée[11]. Cette loi élargit le mandat de l'Agence de la consommation en matière financière du Canada pour y inclure la supervision d'un nouveau cadre de services bancaires axés sur le consommateur. L'énoncé économique de l'automne du gouvernement fédéral de décembre 2024 a annoncé que le cadre devrait être lancé au début de l'année 2026, avec un budget de mise en œuvre revu à la hausse qui s'élèvera à 44,3 millions de dollars sur trois ans, à compter de l'exercice 2025-2026[12].

Les priorités politiques peuvent changer et un nouveau gouvernement fédéral en 2025 pourrait consacrer son énergie à d'autres initiatives dans le secteur financier. Cela dit, nous nous attendons à ce que le secteur des technologies financières continue d'innover et de croître en 2025, et à ce que les partenariats favorables aux consommateurs entre les entreprises de technologies financières et les institutions financières continuent de jouer un rôle important.

11. Budget de 2024
12. Énoncé économique de l'automne de 2024

Tendance 10 : La prochaine vague de transformation numérique sera portée par l'innovation et la nécessité d'unifier les offres de services

Le rythme toujours plus rapide de la transformation numérique en 2025 sera caractérisé par plusieurs tendances clés. Les organisations investiront dans l'unification des plateformes et exploiteront des technologies telles que l'intelligence artificielle, l'informatique en nuage et les plateformes à faible code pour automatiser les processus, améliorer l'expérience utilisateur, gagner en efficacité et en innovation, et responsabiliser leurs employés.

UNIFICATION DES PLATEFORMES : TOUT RASSEMBLER POUR POUVOIR PROFITER DE POSSIBILITÉS INFINIES

Pilier central de la transformation numérique, l'unification des plateformes simplifie les écosystèmes informatiques complexes, améliore l'efficacité opérationnelle et l'agilité, réduit la fragmentation et les coûts, et permet d'améliorer la gestion et la prise de décision. Vous trouverez ci-dessous quelques-uns des principaux domaines dans lesquels le processus d'unification est en plein essor et continuera de l'être :

- Les systèmes PGI et CRM unifiés deviennent de plus en plus la norme pour rationaliser les opérations, les interactions avec les clients et la gestion des ressources de l'entreprise. Ces systèmes permettent la consolidation des données entre les services, l'élimination des redondances et offrent une vision globale des opérations internes et des interactions avec les clients. Ils favorisent ainsi l'amélioration de l'efficacité, de la collaboration et de la prise de décision.

- L'unification des logiciels et des API répond aux besoins croissants d'interopérabilité entre des systèmes contrastés (tels que les systèmes existants et les systèmes plus récents). L'unification des API réduit la complexité de l'intégration, accélère les cycles de développement et améliore l'évolutivité. Alors que les entreprises adoptent des environnements hybrides et à nuages multiples, les API unifiées permettent flexibilité et portabilité. Elles garantissent que les applications peuvent s'adapter à l'évolution des technologies et des exigences réglementaires sans nécessiter de remaniement important.

- L'architecture en nuage évoluera en raison de la forte augmentation des solutions hybrides et à nuages multiples utilisant des plateformes de gestion en nuage. Gartner prévoit que les dépenses des utilisateurs finaux pour les services en nuage passeront de 595,7 milliards de dollars US en 2024 à 723,4 milliards de dollars US en 2025, soit une augmentation de 21,5 % (article en anglais). Les solutions hybrides et à nuages multiples répartissent les risques en réduisant la dépendance vis-à-vis d'un seul fournisseur, permettent l'intelligence artificielle et l'apprentissage automatique à grande échelle, et augmentent la résilience du nuage face aux cybermenaces. Le supernuage (couche de gestion unifiée) apportera simplicité, harmonie et contrôle au chaos des environnements hybrides et offrira la même gouvernance et le même accès aux données dans l'environnement local, public et en nuage privé.

Tableau 1 : Prévisions des dépenses des utilisateurs finaux de services de nuage public à l'échelle mondiale (en millions de dollars US)

	Dépenses 2023 ($)	2023 Croissance (%)	Dépenses 2024 ($)	2024 Croissance (%)	Dépenses 2025 ($)	2025 Croissance (%)
Infrastructure d'applications en tant que service en nuage (plateforme-service)	142 934	19,5	172 449	20,6	211 589	22,7
Logiciel en tant que service en nuage (logiciel-service)	205 998	18,1	247 203	20,0	295 083	19,4
Processus d'affaires en tant que service en nuage (BPaaS)	66 162	7,5	72 675	9,8	82 262	13,2
Bureau en tant que service en nuage (DaaS)	2 708	11,4	3 062	13,1	3 437	12,3
Services d'infrastructure de systèmes en nuage (infrastructure-service)	143 302	19,1	180 044	25,6	232 391	29,1
Marché total	**561 104**	**17,3**	**675 433**	**20,4**	**824 763**	**22,1**

Attention : Les totaux ayant été arrondis, leur somme peut ne pas correspondre au total indiqué.
Source : Gartner (mai 2024)

AUTOMATISATION DE L'IA : RÉALISER DE NOUVEAUX GAINS EN EFFICIENCE

Opérationnalisation de l'IA générative : L'opérationnalisation de l'IA générative restera un processus graduel en 2025, en particulier pour les organisations des secteurs réglementés, qui sont aux prises avec les défis de l'intégration de cette technologie transformatrice. Si les grands modèles de langage et autres outils génératifs offrent un potentiel important pour rationaliser la rédaction de documents, automatiser le service client et améliorer les flux de travail créatifs, de nombreuses entreprises n'ont pas encore pleinement réalisé ces gains d'efficacité. Les obstacles juridiques et de conformité, tels que les préoccupations relatives aux droits de propriété intellectuelle, la responsabilité en cas d'erreurs générées par l'IA et le respect des lois sur la protection de la vie privée, restent des préoccupations majeures pour les entreprises.

Agents d'IA (l'application révolutionnaire?) : Les agents autonomes dotés d'une intelligence artificielle et capables de gérer des flux de travail, de prendre des décisions et d'apprendre à partir d'interactions gagnent du terrain dans des domaines tels que la logistique, la finance et les relations clients, pour n'en citer que quelques-uns. Cependant, leur déploiement au sein des organisations présente des risques et des défis juridiques majeurs, notamment le fait d'être tenu responsable des erreurs ou des résultats préjudiciables des systèmes d'IA, le respect de la confidentialité des données, les biais potentiels dans les processus décisionnels, les questions de propriété intellectuelle et le respect des réglementations et normes applicables.

Gouvernance des données – assurer la qualité et la conformité : L'essor des applications d'IA met en évidence la nécessité d'une gouvernance des données solide pour garantir la conformité et tirer le meilleur parti de ces technologies. Il est essentiel de disposer de données de haute qualité, car des données inexactes ou incohérentes peuvent conduire à de mauvais résultats et à une perte de confiance envers le contenu généré par l'IA. Les organisations qui utilisent des outils propulsés par l'IA doivent s'adapter aux lois changeantes sur la protection de la vie privée tout en s'assurant que leurs données sont exactes et fiables. Pour ce faire, elles peuvent par exemple conclure des ententes appropriées de partage des données, mettre en œuvre des pratiques adéquates de tenue des dossiers et intégrer des considérations relatives à la protection de la vie privée dans leur utilisation et leur adoption des systèmes d'IA en vue d'en assurer la conformité et obtenir le meilleur rendement.

ADOPTION PLUS LARGE DES PLATEFORMES À FAIBLE CODE OU SANS CODE

Il existe des plateformes (Microsoft Power Apps, OutSystems, Appian, Mendix, entre autres) qui permettent au personnel n'ayant pas de compétences techniques de créer et de déployer rapidement des applications, ce qui réduit considérablement les délais de développement. Si ces outils démocratisent l'innovation, ils soulèvent aussi des préoccupations en matière de sécurité, de conformité et de propriété intellectuelle. En 2025, les équipes juridiques devront guider les entreprises avec soin dans la mise en œuvre de politiques d'utilisation et la sécurisation de contrats de licence et de services solides.

Personnes-ressources

Le groupe Technologies de Fasken est un chef de file reconnu et l'une des équipes juridiques les plus importantes et les plus anciennes en droit des technologies au Canada. Notre équipe nationale a acquis une solide expérience en résolution de problèmes complexes auprès de clients en TI. Nous avons représenté des fournisseurs et des utilisateurs de technologies, et ce, dans le cadre du développement, de la protection et de la commercialisation de produits et services technologiques. De plus, nous avons accompagné des acheteurs et des vendeurs dans l'acquisition et la vente d'entreprises technologiques.

Nous fournissons des conseils sur tous les sujets, que ce soit les transactions informatiques commerciales complexes, y compris les ententes d'impartition, les contrats XaaS, les modèles d'affaires Internet, le commerce électronique, les nouvelles technologies (comme l'informatique quantique, l'intelligence artificielle et les chaînes de blocs), les acquisitions ou dessaisissements technologiques et la protection des données.

Notre équipe est là pour vous aider à attendre vos objectifs d'affaires. Pour obtenir plus de renseignements ou pour aborder un sujet en particulier, veuillez communiquer avec nous.

Andrew S. Nunes
Associé | Toronto
+1 416 865-4510
anunes@fasken.com

Andrew C. Alleyne
Associé | Toronto
+1 416 868-3338
aalleyne@fasken.com

John Beardwood
Associé | Toronto
+1 416 868-3490
jbeardwood@fasken.com

Daniel Fabiano
Associé | Toronto
+1 416 868-3364
dfabiano@fasken.com

Gabriel M.A. Stern
Associé | Toronto
+1 416 865-5494
gstern@fasken.com

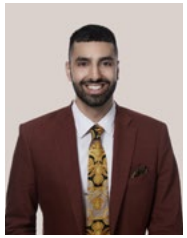
Christopher Ferguson
Associé | Toronto
+1 416 865-4425
cferguson@fasken.com

Ariel Laver
Associé | Vancouver
+1 604 631-3201
alaver@fasken.com

Karam Bayrakal
Associé | Vancouver
+1 604 631-4850
kbayrakal@fasken.com

Jocelyn Auger
Associé | Montréal
+1 514 397-7694
jauger@fasken.com

Paul Burbank
Avocat | Toronto
+1 416 865-4427
pburbank@fasken.com



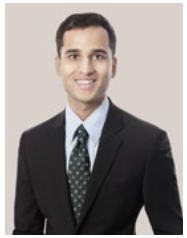
Shan L. M. Arora
Avocat | Toronto
+1 416 865-5412
sarora@fasken.com

Anagha Nandakumaran
Avocate | Toronto
+1 416 865-5412
anandakumaran@fasken.com

Summer Lewis
Avocate | Toronto
+1 416 865-5490
slewis@fasken.com

Julie He
Avocate | Toronto
+1 416 865-5407
jhe@fasken.com

Keihgan Blackmore
Avocat | Toronto
+1 416 868-7870
kblackmore@fasken.com



Aniket Bhatt
Avocat | Toronto
+1 416 868-7871
abhatt@fasken.com

Hannah Im
Stagiaire en droit | Toronto
+1 416 865-5439
him@fasken.com

Dongwoo Kim
Stagiaire en droit | Toronto
+1 416 865-5168
dwkim@fasken.com

FASKEN

Traçons l'avenir

À propos du cabinet

Situé à l'intersection de l'excellence et de l'expertise, Fasken est un cabinet d'avocats de premier plan comptant plus de 950 avocats et avocates à l'échelle mondiale.

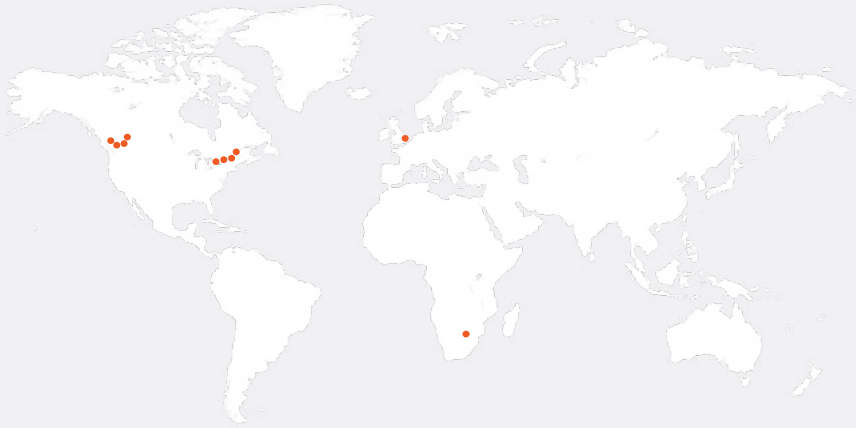
Avec 10 bureaux au Canada, au Royaume-Uni et en Afrique du Sud, nous travaillons à résoudre des problèmes complexes dans un large éventail de secteurs et de domaines de pratique.

Nous nous engageons auprès de nos clients à façonner l'avenir qu'ils imaginent, précisément au moment où cela compte le plus.

fasken.com/fr

Situé à l'intersection de l'excellence et de l'expertise, Fasken est un cabinet d'avocats de premier plan comptant plus de 950 avocats et avocates à l'échelle mondiale. Nous nous engageons auprès de nos clients à façonner l'avenir qu'ils imaginent, précisément au moment où cela compte le plus.

Pour plus de renseignements, visitez fasken.com.



VANCOUVER	550 Burrard Street, Suite 2900	+1 604 631 3131	vancouver@fasken.com
SURREY	13401 - 108th Avenue, Suite 1800	+1 604 631 3131	surrey@fasken.com
TSUUT'INA	11501 Buffalo Run Boulevard, Suite 211	+1 587 233 4113	tsuutina@fasken.com
CALGARY	350 7th Avenue SW, Suite 3400	+1 403 261 5350	calgary@fasken.com
TORONTO	333 Bay Street, Suite 2400	+1 416 366 8381	toronto@fasken.com
OTTAWA	55, rue Metcalfe, bureau 1300	+1 613 236 3882	ottawa@fasken.com
MONTRÉAL	800, rue du Square-Victoria, bureau 3500	+1 514 397 7400	montreal@fasken.com
QUÉBEC	365, rue Abraham-Martin, bureau 600	+1 418 640 2000	quebec@fasken.com
LONDRES	6th Floor, 100 Liverpool Street	+44 20 7917 8500	london@fasken.com
JOHANNESBURG	Inanda Greens, 54 Wierda Road West, Sandton 2196	+27 11 586 6000	johannesburg@fasken.com

FASKEN

Traçons l'avenir

fasken.com/fr