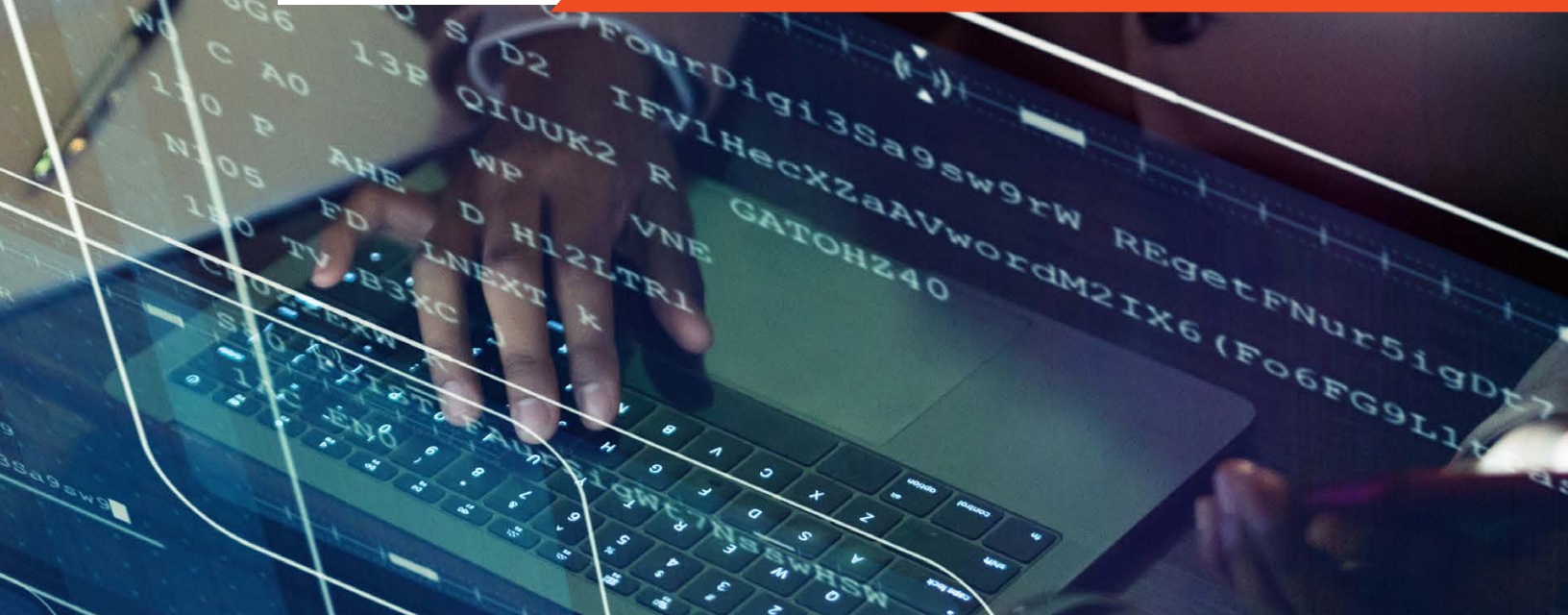
Prendre une longueur d'avance en matière de protection de la vie privée, de gestion des données et de cybersécurité

Bilan et perspectives en Cyber/Données (2021-2022)



Message des membres de notre équipe éditoriale, Marissa Caldwell, Dan Glover et Charles Morgan :

Le groupe Cyber/Données de McCarthy Tétrault est fier de vous présenter le rapport **Bilan et perspectives en Cyber/Données (2021-2022): Prendre une longueur d'avance en matière de protection de la vie privée, de gestion des données et de cybersécurité**.

Il s'agit du premier rapport de la série Perspectives présenté par le groupe Cyber/Données. Dans ce rapport, notre équipe pluridisciplinaire intégrée souligne les principaux faits saillants survenus en matière de protection des renseignements personnels, de cybersécurité et de traitement des données au Canada et ailleurs dans le monde et présente les grandes tendances et ses réflexions pour 2022 et au-delà. Pour en savoir plus, veuillez consulter la page d'accueil du groupe Cyber/Données ou communiquer avec l'un de nos talentueux auteurs.

Le présent article ne contient que des renseignements généraux et n'est pas destiné à fournir des conseils juridiques. Pour obtenir de plus amples renseignements, veuillez communiquer avec l'une de nos personnes-ressources.

Table des matières

Introduction

2021 a été une année marquante dans les domaines de la protection des renseignements personnels, de la cybersécurité et du traitement des données au Canada. Le Québec a proposé, peaufiné et adopté une nouvelle loi phare, et d'autres textes législatifs pourraient suivre. La pandémie mondiale de COVID-19 a continué à transformer notre façon de vivre et de travailler, nous amenant à investir toujours plus nos vies (et nos renseignements personnels) dans le monde numérique. Les avancées technologiques ont continué à se succéder à un rythme effréné, ouvrant des possibilités sans limites et présentant des risques complexes. Les organismes de réglementation en matière de concurrence se sont intéressés à la valeur des données ainsi qu'à leurs effets anticoncurrentiels potentiels. Nous avons assisté à des atteintes majeures à la sécurité des données et à une forte croissance des attaques par rançongiciel. Les tribunaux ont réaffirmé leur rôle de remparts dans le cadre d'actions collectives en matière de protection de la vie privée. Les assureurs ont été durement touchés et ont changé leurs pratiques.

Dans le présent rapport, notre groupe Cyber/Données dresse un bilan des principaux événements survenus au Canada et dans le reste du monde en 2021 et analyse leur portée pour 2022 et au-delà.

Projet de loi no 64 : une réforme majeure du régime de protection des renseignements personnels du Québec

Le 22 septembre 2021, la *Loi modernisant des dispositions législatives en matière de protection des renseignements personnels* (le « projet de loi no 64 ») a reçu la sanction royale et a acquis force de loi. Le projet de loi no 64 propose des changements radicaux au régime de protection des renseignements personnels du Québec, notamment en modifiant en profondeur la *Loi sur la protection des renseignements personnels dans le secteur privé* (la « Loi sur le secteur privé »). Ces modifications doivent entrer en vigueur en trois étapes, le 22 septembre 2022 pour la première série de dispositions, le même jour en 2023 pour la deuxième, et en 2024 pour la dernière.

> **Les entreprises doit obtenir d'un individu un consentement manifeste, libre, éclairé et non équivoque pour utiliser ses renseignements personnels.**

Les entreprises qui conservent les renseignements personnels de résidents du Québec se verront ainsi imposer un ensemble de nouvelles obligations et des amendes très élevées en cas de non-conformité inspirées du *Règlement général sur la protection des données* (le « RGPD ») de l'Union européenne Le texte ci-dessous présente les grandes lignes des changements les plus significatifs pour les entreprises.

PROJET DE LOI NO 64 : CONSENTEMENT ET FONDEMENTS DE LA COLLECTE DE RENSEIGNEMENTS

Le projet de loi no 64 prévoit de nouvelles exigences en matière de consentement pour les entreprises qui recueillent des renseignements personnels. L'exigence fondamentale est qu'une entreprise doit obtenir d'un individu un consentement manifeste, libre, éclairé et non équivoque pour utiliser ses renseignements personnels.

Lorsqu'une entreprise obtient un consentement, elle ne peut utiliser les renseignements personnels visés qu'aux fins pour lesquelles le consentement avait été initialement obtenu, à quelques rares exceptions, y compris si la nouvelle fin est compatible avec la fin prévue à l'origine, si la nouvelle fin est nécessaire pour détecter une fraude ou améliorer des mesures de sécurité, ou si l'utilisation est nécessaire pour fournir un produit ou un service demandé par la personne en cause.

Les exigences applicables au consentement entreront en vigueur le 22 septembre 2023. Les entreprises doivent mettre à jour leurs politiques et ententes sur la collecte afin d'y intégrer les éléments susmentionnés et veiller à ce que le consentement approprié, précis et explicite requis pour les pratiques en matière d'utilisation de données de l'entreprise soit pris en compte sur le plan opérationnel.

PROJET DE LOI NO 64 : MODIFICATIONS APPORTÉES AUX REQUÊTES BASÉES SUR LES DROITS INDIVIDUELS

Le projet de loi no 64 accorde aux individus un ensemble de nouveaux droits qu'ils peuvent faire valoir à l'encontre des entreprises qui détiennent leurs renseignements personnels. Ces demandes ne peuvent être refusées que pour des raisons valables. Dans tous les cas, que la demande soit acceptée ou refusée, les entreprises doivent y répondre par écrit dans un délai de 30 jours. À l'exception du nouveau droit à la portabilité (qui prendra effet le 22 septembre 2024), ces changements doivent entrer en vigueur le 22 septembre 2023.

Droit à la portabilité

Auparavant, une personne pouvait demander d'avoir accès à une copie des renseignements personnels qu'une entreprise conservait à son sujet et obtenir la confirmation de l'existence des renseignements personnels détenus par une entreprise à son sujet.

En vertu du projet de loi no 64, un individu peut à présent demander une copie des renseignements personnels détenus à son sujet sous une forme structurée et d'usage technologique courant et la transmission à des tiers des renseignements personnels informatisés le concernant.

Droit de demander la désindexation, la ré-indexation ou la cessation de la diffusion des renseignements personnels

Un individu peut à présent demander à une entreprise de cesser la diffusion d'un renseignement, ou encore de désindexer ou de réindexer les renseignements le concernant, lorsque les conditions suivantes sont réunies :

- la diffusion cause un préjudice grave relativement à son droit au respect de sa réputation ou de sa vie privée;
- ce préjudice est supérieur à l'intérêt du public ou au droit à la libre expression; et
- la cessation de la diffusion, la ré-indexation ou la désindexation demandée n'excède pas ce qui est nécessaire pour éviter la perpétuation du préjudice.

OBLIGATIONS EN MATIÈRE DE GOUVERNANCE D'ENTREPRISE

Le projet de loi no 64 impose une série de nouvelles obligations en matière de gouvernance d'entreprise. Les principales modifications sont présentées ci-dessous.

Responsable de la protection des renseignements personnels

Chaque entreprise doit nommer un « responsable de la protection des renseignements personnels », qui est chargé de superviser le traitement des renseignements personnels par l'entreprise et d'agir comme principal point de contact à cet égard. Par défaut, la personne ayant la plus haute autorité au sein de l'entreprise remplit la fonction de responsable de la protection des renseignements personnels. Cette responsabilité peut cependant être déléguée à toute autre personne par écrit, y compris à des personnes extérieures à l'entreprise. Les coordonnées et le titre du responsable de la protection des renseignements personnels doivent être publiés sur le site Web de l'entreprise. Il incombe également au responsable de la protection des renseignements personnels de répondre à toute demande basée sur les droits individuels transmise par un individu.

De plus, le responsable de la protection des renseignements personnels doit être consulté pour tout projet d'acquisition, de mise en œuvre ou de remaniement d'un système mettant en cause des renseignements personnels. Lorsqu'une évaluation des facteurs relatifs à la vie privée est réalisée, le responsable de la protection des renseignements personnels doit donner son avis sur les questions relatives à la protection de la vie privée. Les obligations se rapportant au responsable de la protection des renseignements personnels entreront en vigueur le 22 septembre 2022, ce qui en fait un élément hautement prioritaire pour toute entreprise recueillant des renseignements personnels.

Communication des politiques et des pratiques de gouvernance en matière de renseignements personnels

Les entreprises doivent établir et mettre en œuvre des politiques et des pratiques de gouvernance internes et publier de l'information à leur sujet en termes simples et clairs. Ces politiques doivent contenir des renseignements de base sur les aspects suivants des pratiques de l'entreprise en matière de renseignements personnels :

- le cadre de conservation et de destruction des renseignements personnels recueillis;
- les rôles et les responsabilités des membres du personnel tout au long du cycle de vie des renseignements personnels; et
- le processus de traitement des plaintes.

Les entreprises doivent également rendre publique leur politique de protection des renseignements personnels (communément appelée « politique de confidentialité ») et veiller à ce qu'elle soit rédigée de manière simple et claire, y compris pour les modifications ultérieures qui y sont apportée.

Exigences d'enregistrement des incidents et d'avis en cas d'incident

Les entreprises devront consigner tout incident de confidentialité dans un registre interne des incidents et fournir ce registre, sur demande de la Commission d'accès à l'information (la « CAI »). Lors de l'inscription au registre des incidents de confidentialité, les moyens utilisés pour corriger la vulnérabilité ou y remédier doivent être précisés dans le rapport d'incident interne. De plus, tout membre d'une entreprise qui a des motifs de croire qu'il s'est produit un incident de confidentialité doit prendre des

mesures raisonnables afin de réduire les risques pour les renseignements personnels des personnes.

Lorsqu'un incident présente un risque de « préjudice sérieux », l'entreprise doit, avec diligence, aviser la CAI, ainsi que toute personne dont les renseignements personnels sont concernés par l'incident, sauf si cela est susceptible d'entraver une enquête s'y rapportant.

Les exigences en matière de registre pour les atteintes aux données doivent entrer en vigueur le 22 septembre 2022; il s'agit donc d'un élément hautement prioritaire en termes de conformité. Soulignons que des obligations similaires existent déjà dans la *Loi sur la protection des renseignements personnels et les documents électroniques* (la « LPRPDE ») à l'échelle fédérale et dans la loi de l'Alberta intitulée *Personal Information and Protection of Privacy Act*.

Lorsqu'un incident présente un risque de « préjudice sérieux », l'entreprise doit, avec diligence, aviser la CAI, ainsi que toute personne dont les renseignements personnels sont concernés par l'incident.

Évaluation des facteurs relatifs à la vie privée

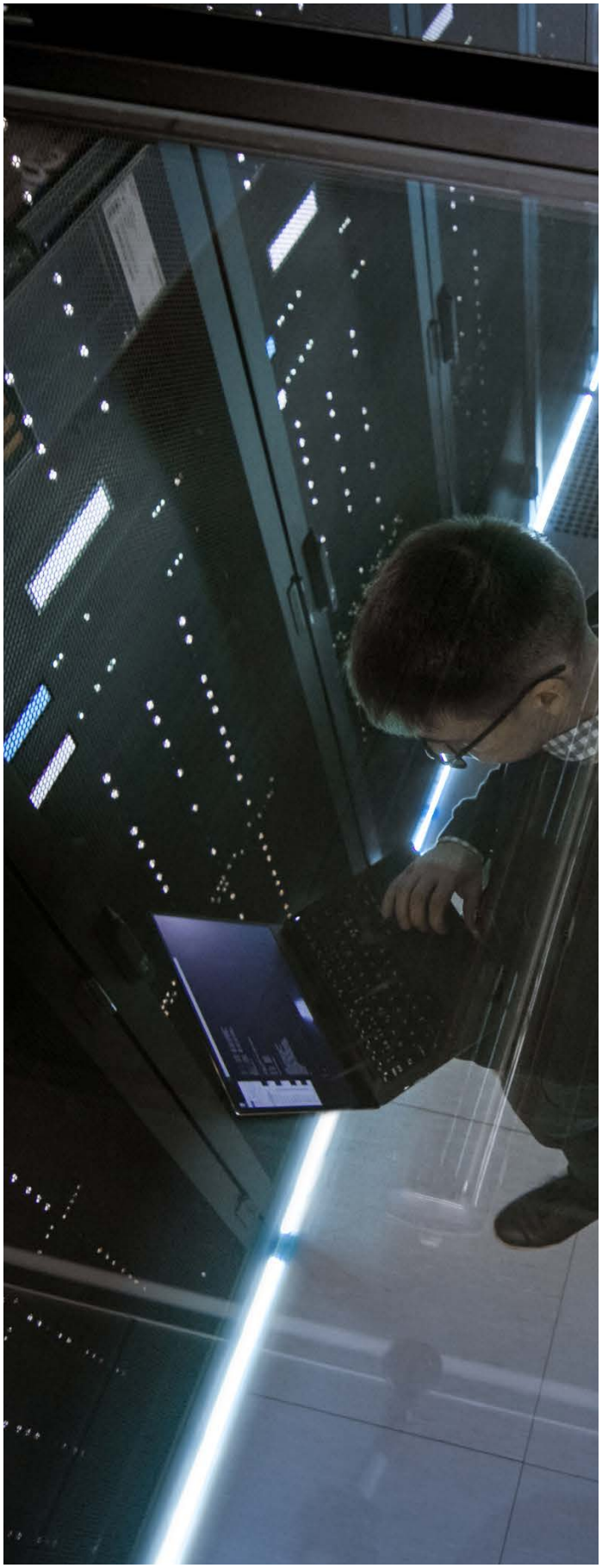
Le projet de loi no 64 ajoute l'obligation pour les entreprises de réaliser une évaluation des facteurs relatifs à la vie privée avant de communiquer des renseignements personnels à l'extérieur du Québec. En plus de l'obligation d'obtenir un consentement ou d'établir une entente contractuelle par écrit précisant les modalités de communication à des tiers *avant* la collecte, l'évaluation des facteurs relatifs à la vie privée doit déterminer si les renseignements personnels bénéficieraient d'une protection adéquate dans le territoire cible du transfert.

Les entreprises sont également tenues de réaliser une évaluation des facteurs relatifs à la vie privée pour tout projet d'acquisition, d'élaboration ou de remaniement d'un système d'information ou de prestation électronique de services mettant en cause la collecte, l'utilisation, la communication, la conservation ou la destruction de renseignements personnels. Cette obligation aura probablement des conséquences sur la passation de contrats pour bon nombre d'outils technologiques et de solutions de stockage utilisés par la plupart des entreprises.

L'évaluation des facteurs relatifs à la vie privée doit notamment tenir compte des éléments suivants :

- la sensibilité des renseignements;
- les fins auxquelles les renseignements seront utilisés;
- les mesures de protection, y compris les mesures contractuelles, qui s'appliqueraient; et
- le régime juridique applicable dans le territoire où ces renseignements seraient communiqués.

L'évaluation des facteurs relatifs à la vie privée doit être proportionnée à la sensibilité des renseignements évalués.



De plus, la communication de renseignements personnels à des tiers doit être assujettie à une entente écrite permettant d'atténuer les risques relevés dans le cadre de l'évaluation des facteurs relatifs à la vie privée.

Les obligations applicables à la communication de renseignements personnels à des tiers entrent en vigueur le 22 septembre 2023, ce qui laisse plus de temps aux entreprises pour s'y préparer.

DES PÉNALITÉS PLUS LOURDES

L'un des principaux changements instaurés par le projet de loi no 64 est la possibilité d'imposer des pénalités importantes en cas de non-conformité aux dispositions de la Loi sur le secteur privé. Les sanctions administratives et pénales pouvant être imposées sont comparables, et dans certains cas supérieures, aux lourdes amendes prévues par le RGPD.

La CAI peut imposer des sanctions administratives pécuniaires en cas de non-respect des dispositions de la Loi sur le secteur privé. Les entreprises qui contreviennent à ces dispositions peuvent s'engager auprès de la CAI à remédier au défaut et ainsi éviter une sanction administrative pécuniaire. Dans les autres cas, la CAI impose une pénalité maximale de 10 000 000 $ ou du montant correspondant à 2 % du chiffre d'affaires mondial de l'exercice financier précédent, selon le plus élevé de ces montants.

La CAI impose une pénalité maximale de 10 000 000 $ ou du montant correspondant à 2 % du chiffre d'affaires mondial de l'exercice financier précédent, selon le plus élevé de ces montants.

Dans l'éventualité d'un défaut de déclarer un incident de confidentialité, d'un refus de se conformer à un engagement auprès de la CAI, ou de l'utilisation, de la collecte ou de la communication de renseignements personnels en contravention de la Loi sur le secteur privé, la CAI peut intenter une poursuite pénale devant les tribunaux, d'un maximum de 25 000 000 $ ou du montant correspondant à 4 % du chiffre d'affaires mondial de l'exercice financier précédent, selon le plus élevé de ces montants.

En cas de récidive du non-respect des dispositions de la Loi, les montants des pénalités ci-haut peuvent être doublés pour toute violation ultérieure.

Modifications prévues aux lois sur la protection de la vie privée au Canada

Auparavant, la protection de la vie privée était un processus simple se résumant à cocher les bonnes cases, puisqu'il suffisait en général de publier un formulaire de consentement et une politique de confidentialité appropriés sur un site Internet, mais ce monde est révolu. Nous sommes actuellement les témoins d'une véritable explosion à l'échelle mondiale des lois régissant les données. Avec un risque de chevauchement, voire de conflits entre les différentes lois, alors que les flux de données gagnent en complexité, les organisations sont maintenant contraintes de composer avec les lois sur la protection de la vie privée de différents territoires et de différents paliers de gouvernement, sans oublier les règles et les lignes directrices propres à chaque industrie, qui s'accompagnent d'amendes de plus en plus lourdes en cas de non-conformité.

Rester informé des évolutions dans ce milieu vous permettra d'éviter les sables mouvants sans pour autant renoncer à utiliser des données pour des fins d'affaires légitimes. Les pages qui suivent présentent un résumé des modifications prévues touchant la législation relative à la protection des renseignements personnels, les transferts transfrontaliers des données et les exigences applicables aux données sensibles comme les données biométriques et les décisions automatisées.

À QUOI S'ATTENDRE AU CANADA?

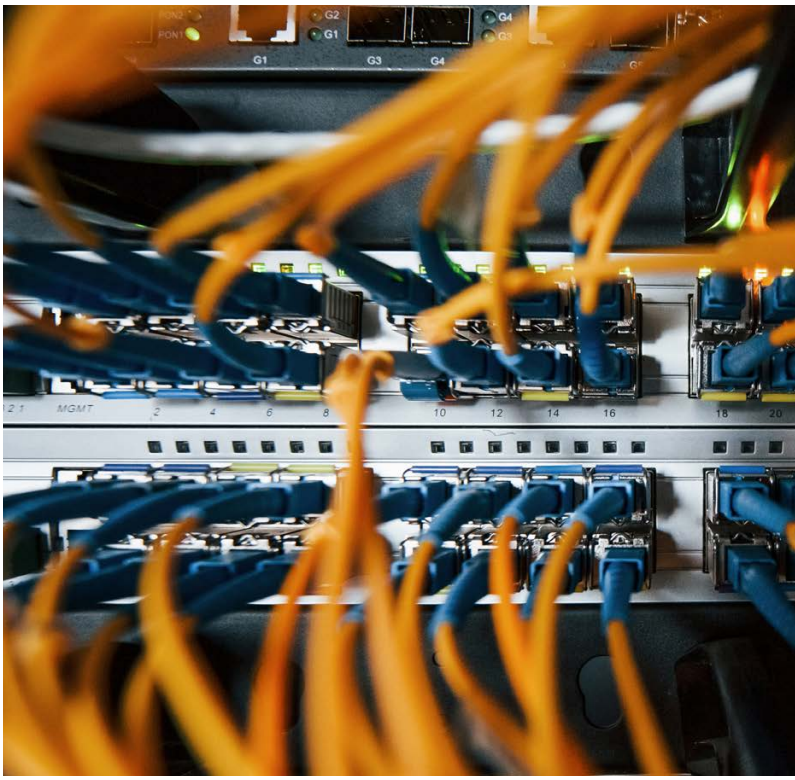
Québec : Adopté en septembre 2021, le projet de loi no 64 du Québec va révolutionner le paysage canadien de la protection de la vie privée avec une loi fondamentalement nouvelle inspirée du RGPD prévoyant, en cas de non-conformité, de lourdes pénalités pouvant représenter jusqu'à 8 % du chiffre d'affaires mondial pour les contrevenants récidivistes. Le projet de loi no 64 introduit des obligations uniques de déclaration des incidents de cybersécurité, y compris celles d'aviser les individus si un incident de confidentialité pose un « risque de préjudice sérieux » et de prendre les mesures raisonnables pour réduire le risque de préjudice et prévenir les nouveaux incidents. Aux termes des nouvelles normes en matière de transparence et de consentement, le consentement doit être manifeste, libre, éclairé et être donné à des fins spécifiques, ce qui constitue une norme plus exigeante que celle imposée par la loi fédérale actuelle sur la protection des renseignements personnels au Canada, la LPRPDE. Les exigences opérationnelles pour les transferts transfrontaliers de renseignements personnels du projet de loi no 64 imposent aux entreprises l'obligation de réaliser des évaluations de certains facteurs relatifs à la vie privée avant de communiquer des renseignements personnels à l'extérieur du Québec. Les dispositions sur la protection des données par défaut et sur la protection des données dès la conception exigeront un changement radical de mentalité lors de l'acquisition de technologies et de la mise au point de nouveaux programmes. Les nouveaux droits des utilisateurs exigeront l'adoption de nouvelles approches en matière de conformité. Le projet de loi no 64 commencera à

prendre effet en septembre 2022, tandis que les pénalités et la plupart des principales dispositions entreront en vigueur en septembre 2023.

Fédéral : Proposé en 2020 et susceptible d'être remis à l'ordre du jour sous une forme similaire au cours de la prochaine année, le projet de loi C-11 abrogerait la LPRPDE et édicterait à sa place la *Loi sur la protection de la vie privée des consommateurs* (« LPVPC ») et la *Loi sur le Tribunal de la protection des renseignements personnels et des données* (« LTPRPD »). La LPVPC vise à instaurer de nouvelles exigences applicables à la protection des données au Canada et s'appliquerait aux renseignements personnels collectés au Canada. Le projet de loi C-11 qui, de l'avis du Commissaire à la protection de la vie privée du Canada, constitue un « recul », s'il est déposé de nouveau et adopté sous une forme similaire, modifierait sensiblement le paysage canadien de la protection de la vie privée, car il assortirait les principales obligations d'amendes conséquentes pouvant aller jusqu'à 5 % des recettes globales brutes de l'organisation.

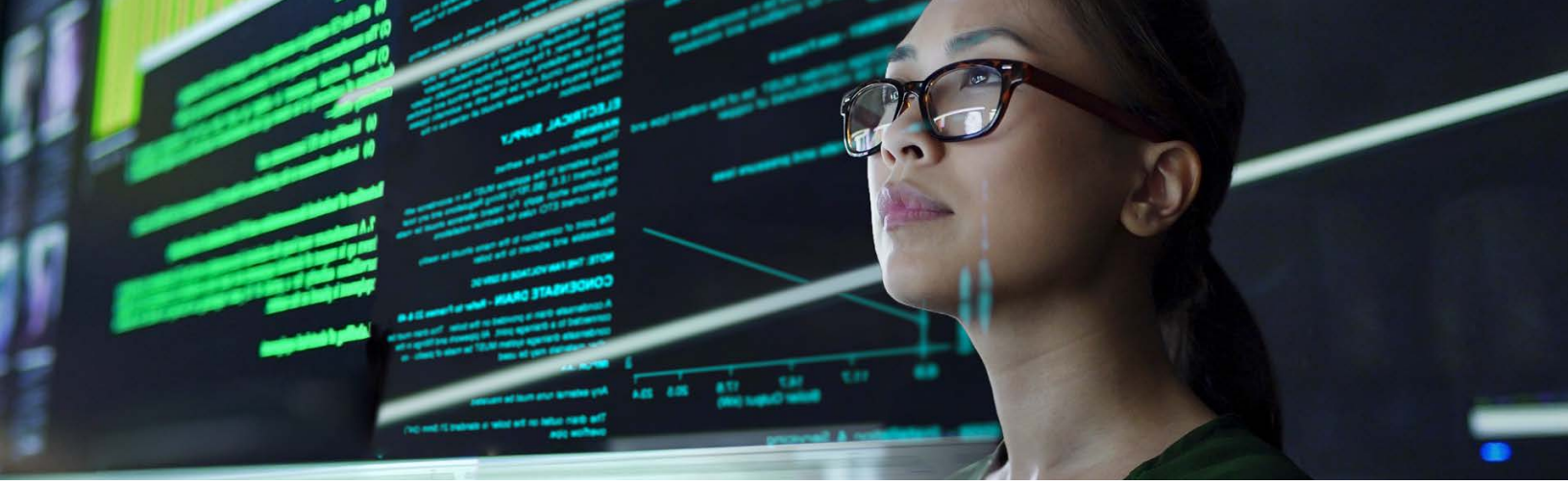
Ontario : Publié en juin 2021, le livre blanc *Modernisation de la protection de la vie privée en Ontario* propose des changements importants pour instaurer un nouveau régime législatif provincial en matière de protection des renseignements personnels. De manière générale, les propositions présentées dans le livre blanc suggèrent la mise en œuvre d'exigences plus strictes et moins souples que celles figurant dans la LPVPC. Bien que la rumeur veut qu'il ait été mis en veilleuse pendant que le gouvernement provincial se penche sur d'autres priorités, le modèle décrit dans le livre blanc *Modernisation de la protection de la vie privée en Ontario*, s'il est déposé et adopté, instaurerait des droits, des mesures d'application et des pénalités inspirés du RGPD, y compris à l'égard des renseignements personnels des employés, qui tombent à l'heure actuelle dans une zone grise pour la plupart des entreprises de l'Ontario. Un autre document intéressant est la réponse du Commissaire à l'information et à la protection de la vie privée (CIPVP) de l'Ontario au livre blanc *Modernisation de la protection de la vie privée en Ontario*. Celle-ci dresse une longue liste de souhaits, notamment celui d'habiliter le CIPVP à créer des outils de soutien à la conformité tels que des services consultatifs, des codes de pratique sectoriels et des programmes de certification, en mettant particulièrement l'accent sur une réglementation « souple » à l'intention des petites et moyennes entreprises. De plus, le CIPVP réclame le pouvoir d'imposer des sanctions administratives prenant en compte « toute mesure réglementaire déjà prise par d'autres territoires de compétence comme facteur atténuant possible, assurant une approche harmonisée, équitable et proportionnée ».

Colombie-Britannique : Cet automne, le projet de loi 22 modifiant la loi intitulée *Freedom of Information and Protection of Privacy Act* (« FIPPA ») a été présenté et adopté en Colombie-Britannique. Un changement majeur susceptible de toucher les organismes publics de la province est l'élimination de l'obligation de conserver les renseignements personnels et d'autoriser l'accès à ces renseignements uniquement à partir du territoire canadien. Il en résulterait une hausse du nombre de prestataires de services auxquels pourrait avoir accès le gouvernement, car bon nombre de ces fournisseurs n'ont pas de présence physique au Canada. Le projet de loi 22 ouvre la porte à des transferts transfrontaliers de données qui sont régis par règlement et autorisés.



TENDANCES ACTUELLES

Classification de la nature des droits relatifs à la protection de la vie privée : Non seulement certains droits individuels – tels que le droit à l'oubli et le droit à la portabilité des données – sont expressément énumérés dans les textes de lois sur la protection des renseignements personnels, mais il semble que certains projets de loi pourraient reconnaître le caractère fondamental du droit à la vie privée. Par exemple, dans le cadre de la modernisation de ses lois sur la protection



des renseignements personnels, le livre blanc de l'Ontario envisage la possibilité de reconnaître un droit fondamental à la protection de la vie privée dans le préambule de la législation provinciale. À l'heure actuelle, le Québec est la seule province reconnaissant un droit au respect de la vie privée, qui est expressément énoncé à l'article 5 de la *Charte des droits et libertés de la personne* du Québec. Le Commissariat à la protection de la vie privée a critiqué l'absence de préambule axé sur les droits et de clause énonçant l'objet de la loi dans d'autres projets de loi, y compris la LPVPC, mais n'a pas encore vu ses efforts de lobbying porter ses fruits à l'échelle fédérale.

Cette question est soulevée à un moment intéressant, où les tribunaux semblent remettre en question le traitement de la vie privée comme un « droit quasi constitutionnel ». En 2021, la Cour suprême du Canada a décrit « la nature des limites à la vie privée comme étant dans un état de confusion […] sur le plan théorique » en précisant que « la reconnaissance d'un intérêt important à l'égard de la notion générale de vie privée pourrait s'avérer trop indéterminée et difficile à appliquer ». La Cour a souligné que « [c]ela dépend en grande partie du contexte dans lequel la vie privée est invoquée ». Ces déclarations font suite à d'autres décisions de la Cour suprême rendues au cours de la dernière décennie (*Banque Royale du Canada c. Trang, Alberta (Information and Privacy Commissioner) c. Travailleurs et travailleuses unis de l'alimentation et du commerce, section locale 401*), dans lesquelles le droit à la vie privée a dû céder le pas devant des intérêts opposés jugés plus convaincants, ce qui montre que l'évaluation contextuelle du droit à la vie privée est l'approche privilégiée par les tribunaux. Compte tenu du vaste éventail des protections des renseignements personnels, qui vont du nom et de l'adresse postale aux renseignements plus intimes et ayant une incidence, et de la probabilité élevée de conflits entre la vie privée et les droits et valeurs fondamentaux, la réticence à traiter la vie privée comme un concept unitaire semble être une approche empreinte de sagesse.

Des pénalités beaucoup plus lourdes : À l'heure actuelle, la LPRPDE permet seulement l'imposition d'amendes maximales de 100 000 $ dans le cas d'une infraction punissable par mise en accusation. Aux termes du projet de loi C-11, les tribunaux pourraient imposer des amendes d'un montant allant jusqu'à 10 millions de dollars ou 4 % des recettes globales brutes de l'organisation, et les contraventions plus graves pourraient donner lieu à des pénalités allant jusqu'à 25 millions de dollars ou 5 % des recettes globales brutes de l'organisation, selon le plus élevé de ces montants. Au Québec, les clauses pénales du projet de loi no 64 sont encore plus sévères, puisque les contrevenants récidivistes sont passibles d'une amende dont le montant peut atteindre 50 millions de dollars ou 8 % des recettes globales brutes, selon le plus élevé de ces montants. Malheureusement, les facteurs servant à déterminer la pénalité en vertu de la loi ne tiennent pas compte de la possibilité que d'autres pénalités fondées sur les mêmes faits soient imposées par d'autres instances, ce qui pourrait conduire à une multiplication des risques pour un incident de confidentialité ayant un caractère transfrontalier et attirant l'attention de plusieurs organismes de réglementation.

Aux termes du projet de loi C-11, les tribunaux pourraient imposer des amendes d'un montant allant jusqu'à 10 millions de dollars ou 4 % des recettes globales brutes de l'organisation.

Séparation des pouvoirs d'enquête et de décision : Si elle est déposée de nouveau et adoptée sous une forme similaire, la LPVPC accorderait un pouvoir de surveillance accru au commissaire à la protection de la vie privée du Canada par l'intermédiaire de divers pouvoirs, notamment de procéder à des vérifications, de mener des enquêtes et de rendre des ordonnances. La principale différence par rapport aux régimes de protection de la vie privée en vigueur tant au pays qu'à l'étranger serait la mise en place d'un tribunal pour

entendre les appels administratifs par suite des décisions rendues par le commissaire à la protection de la vie privée du Canada. Le tribunal aurait également compétence pour imposer des sanctions pécuniaires. Le tribunal constituerait une instance indépendante comparativement aux structures existantes au Canada, car certains soupçonnent les organismes de réglementation d'exercer simultanément les fonctions de « juge, jury et bourreau ». Les complexités de ce régime sont abordées plus en détail sur notre blogue dans l'article intitulé The CPPA's Privacy Law Enforcement Regime. Par contre, au Québec, la CAI prend en charge les questions liées à l'application de la loi en vertu du projet de loi 64 et est habilitée à imposer des amendes allant jusqu'à 2 % du chiffre d'affaires mondial ou 10 millions de dollars. L'organisme a promis d'élaborer et de rendre public un cadre général d'application des sanctions administratives pécuniaires avant l'entrée en vigueur du projet de loi n° 64.

COMPLEXITÉ DES QUESTIONS LIÉES AU TRANSFERT TRANSFRONTALIER DE DONNÉES

Décision d'adéquation de l'Union européenne relative au Canada : Aux termes d'une décision adoptée en 2001 par la Commission européenne (récemment réaffirmée en mai 2018), le Canada est considéré comme offrant un niveau adéquat de protection des données personnelles transférées de l'Union européenne (UE) à des destinataires assujettis à la LPRPDE; par contre, en 2014, le Groupe de travail « Article 29 » de l'UE n'a pas recommandé que le Québec reçoive une évaluation favorable quant à son adéquation tant que certaines améliorations ne seraient pas apportées à sa Loi sur le secteur privé. Aux termes du paragraphe 45(4) du RGPD, la Commission doit faire un suivi continue de l'évolution des questions touchant la vie privée au Canada pouvant porter atteinte au fonctionnement de la décision d'adéquation adoptée pour le Canada. Sauf s'il modifie sa législation fédérale sur la protection des renseignements personnels avant le prochain examen (qui est effectué tous les quatre ans, le prochain devant commencer en mai 2020), on s'attend généralement à ce que le Canada ne conserve pas son statut d'adéquation actuel. En l'absence de décision d'adéquation, une évaluation de l'impact du transfert doit être réalisée (voir la version intégrale des recommandations en format PDF).

Approches divergentes : Les exigences du projet de loi n° 64 applicables aux transferts transfrontaliers de données contrastent fortement avec l'approche libérale de la LPVPC, qui n'impose aux organisations ni restriction du transfert de renseignements personnels à l'extérieur du Canada ni obligation de réaliser une évaluation des impacts de tels transferts. Aux termes du projet de loi no 64, avant de communiquer des renseignements personnels à l'extérieur du Québec, une organisation doit procéder à une évaluation des facteurs relatifs à la vie privée, puis conclure une entente écrite qui tient compte des résultats de cette évaluation et définit les mesures de protection adéquates compte tenu de la sensibilité des renseignements personnels, des fins auxquelles les renseignements seront utilisés, des mesures de protection et du régime juridique applicable dans le territoire de destination.

TENDANCES EN MATIÈRE DE BIOMÉTRIE ET PRISE DE DÉCISION AUTOMATISÉE

Prise de décision automatisée : Depuis l'adoption du projet de loi n° 64, le Québec est la première province canadienne à instaurer un droit d'être informé d'une décision fondée exclusivement sur un traitement automatisé. Être informé d'une décision fondée exclusivement sur un traitement automatisé comprend le

droit d'être informé des principaux facteurs et paramètres, ayant mené à la décision et le droit de présenter des observations à l'égard de la décision ou de s'y opposer. Autrement dit, les entreprises doivent se préparer à expliquer leurs décisions fondées exclusivement sur un traitement automatisé. La LPVPC propose des exigences similaires pour les décisions fondées exclusivement sur un traitement automatisé, y compris l'obligation pour les organisations de fournir une explication générale de leur utilisation des systèmes décisionnels automatisés pour faire des prédictions, des recommandations ou prendre des décisions qui pourraient avoir une incidence importante sur les individus concernés.

Le Québec est la première province canadienne à instaurer un droit d'être informé d'une décision fondée exclusivement sur un traitement automatisé.

La proposition faite par l'Ontario dans son livre blanc va un peu plus loin en interdisant les décisions fondées exclusivement sur un traitement automatisé lorsque la décision aurait des effets significatifs pour un individu, sauf si son consentement exprès est obtenu ou si une telle décision est autorisée par la loi ou exigée en vertu d'un contrat. Cette approche est conforme à l'article 22 du RGPD, aux termes duquel (sous réserve de certaines exceptions) la personne concernée a le droit de ne pas faire l'objet d'une décision fondée exclusivement sur un traitement automatisé, y compris le profilage, produisant des effets juridiques ou l'affectant sensiblement de façon similaire. Cette disposition interdit également les décisions fondées sur des « catégories particulières » de données à caractère personnel comme les origines raciales, l'opinion politique et les données biométriques aux fins d'identifier une personne physique de manière unique. Les décisions automatisées sont autorisées dans les cas où la décision est nécessaire à la conclusion ou à l'exécution d'un contrat, est autorisée par le droit de l'Union ou de l'État membre ou est fondée sur le consentement explicite de la personne concernée.

Comment se préparer : Les organisations qui utilisent actuellement ou qui prévoient utiliser des systèmes d'IA pour leurs activités doivent accorder la priorité à trois mesures :

(i) réaliser une évaluation de l'incidence algorithmique en vue de déterminer le niveau d'incidence que pourrait avoir le système décisionnel automatisé et en évaluer les préjudices possibles;

(ii) communiquer les décisions du système décisionnel automatisé de façon à assurer qu'un consentement soit donné; et

(iii) prévoir un mécanisme d'examen du système décisionnel automatisé par un être humain.

Au Canada, seule la *Directive sur la prise de décisions automatisée* impose de procéder à une évaluation de l'incidence algorithmique. Malgré sa portée étroite et le fait qu'elle ne s'applique qu'au secteur privé, la Directive est en phase avec la demande croissante dont font l'objet les évaluations des incidences dans un large éventail de contextes.

Biométrie : En phase avec la tendance croissante à l'élargissement des pouvoirs en matière d'application de la loi prévus dans la législation sur la protection de la vie privée, la *Loi concernant le cadre juridique des technologies de l'information* (la « LCJTI ») du Québec impose un nouveau délai de 60 jours pour déclarer à la CAI la création d'une banque de caractéristiques ou de mesures biométriques avant son déploiement. Un consentement exprès est exigé avant l'utilisation de données biométriques.

Comment se préparer : Ces deux éléments – surveillance et consentement – s'inscrivent dans la continuité de l'approche fondée sur des principes qui est appliquée au Canada et qui, selon toute vraisemblance, continuera de l'être. Si votre

organisation envisage d'utiliser des données biométriques, assurez-vous d'élaborer un plan prêt à être appliqué en utilisant comme guide le cycle de vie des données.

STRATÉGIES DE RÉUSSITE

Les lois sur la protection des renseignements personnels sont une priorité pour les assemblées législatives du monde entier. Les organisations doivent être prêtes à s'adapter aux nouvelles lois dans ce domaine adoptées par différents ordres de gouvernement dans les délais serrés prévus par ces textes, au risque d'être condamnées à de lourdes amendes en cas de non-conformité.

Évaluations des facteurs relatifs à la vie privée : Qu'il s'agisse de protection de la vie privée, de transfert ou d'algorithmes, la tendance à imposer une évaluation des facteurs relatifs à la vie privée dans des contextes de plus en plus diversifiés est appelée à se maintenir. Contrairement à la LPRPDE qui n'impose aucune exigence de la sorte, le projet de loi n° 64 prévoit l'exécution d'une évaluation des facteurs relatifs à la vie privée au moment du transfert de renseignements personnels à l'extérieur du Québec et de l'acquisition, de la mise au point ou du remaniement d'un système d'information ou de prestation électronique de services prévoyant le traitement de renseignements personnels. La LPVPC introduirait une variation sur le même thème en exigeant la mise en œuvre d'un programme de gestion de la protection des renseignements personnels. Le RGPD impose également une analyse d'impact relative à la protection des données lorsqu'il existe un risque élevé pour les droits et libertés des personnes physiques, notamment lors du recours à de nouvelles technologies ou à la prise de décisions fondées sur le traitement automatisé des renseignements personnels.

Comment se préparer : Veillez à ce que votre organisation dispose de modèles d'évaluation des facteurs relatifs à la vie privée adaptés à vos besoins, en plus des procédures d'exploitation normalisées (PON) qui signalent dans quelles circonstances il faut procéder à une évaluation des facteurs relatifs à la vie privée, obligatoire ou recommandée, aux termes des lois applicables. Soyez conscient du fait que les exigences quant au moment et aux modalités de la réalisation de ces évaluations varient d'un territoire à l'autre.

Anonymisation et minimisation : Aux termes de la LPRPDE et du RGPD, les renseignements dépersonnalisés ne sont pas des « renseignements personnels », parce que ce ne sont pas des renseignements concernant un individu identifiable. Malgré une certaine ambiguïté dans la LPVPC, les modifications proposées touchant la « dépersonnalisation » semblent considérer que tous les renseignements dépersonnalisés sont assujettis à ses dispositions. Cela pourrait mettre en péril l'harmonisation des lois au Canada et nuire à la compétitivité de notre pays. Pour de plus amples renseignements, veuillez consulter notre article : CPPA: Identifying the Inscrutable Meaning and Policy Behind the De-Identifying Provisions.

Comment se préparer : Les approches novatrices de l'anonymisation des données comme la suppression, le brouillage et la généralisation, réduisent le besoin de stocker les renseignements personnels sans nuire à la qualité du traitement analytique. Pour une analyse détaillée, veuillez-vous reporter à la section Utilisations stratégiques de l'anonymisation des données et de la minimisation des données dans le traitement analytique des données ci-dessous.

Connaissez vos données : Le repérage et la localisation des renseignements personnels avant l'automatisation de ce processus seront essentiels pour s'assurer de la conformité aux lois actuelles et futures.

Comment se préparer : Pour connaître ses données, il faut au préalable mettre en œuvre une stratégie de gouvernance de l'information pour repérer les renseignements personnels, élaborer des politiques et des procédures claires de gestion du cycle de vie des données, créer une cartographie des données pour retrouver l'endroit où elles sont stockées, tirer parti des outils technologiques pour mettre en œuvre les politiques et former les employés à la gestion des renseignements personnels.

Cybersécurité et protection des données en milieu de travail

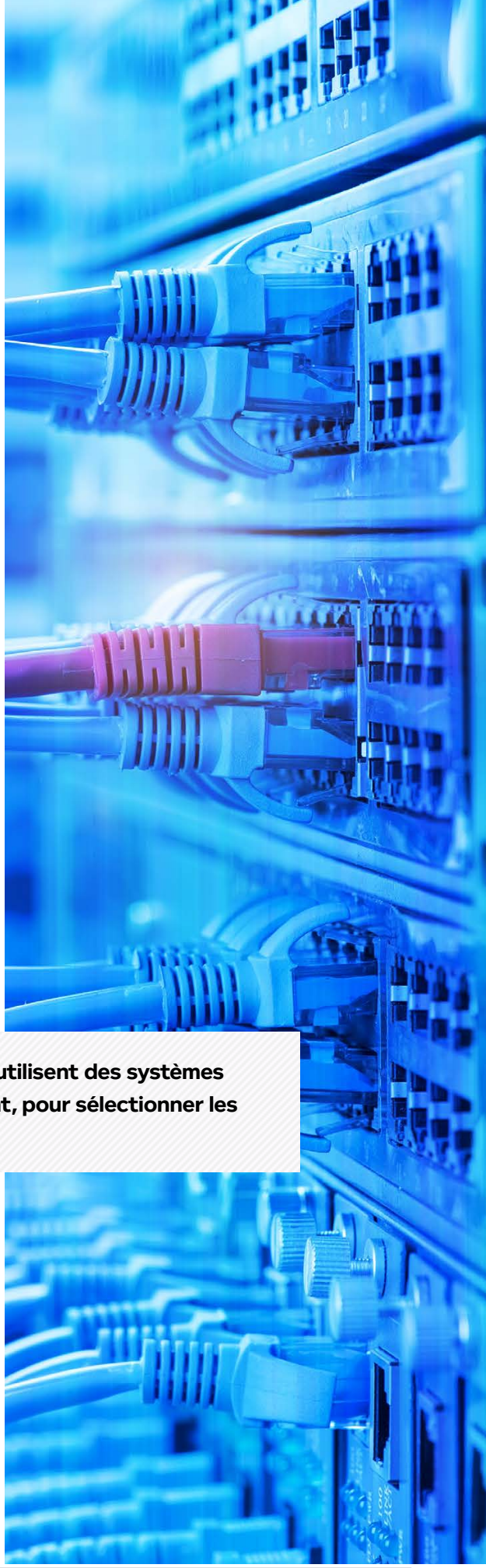
Éthique du recours à l'intelligence artificielle pour le recrutement et la gestion des talents

L'adoption de l'intelligence artificielle (« IA ») par les employeurs et les agences de recrutement a des répercussions d'ordre éthique dont il faut tenir compte.

L'IA est la science qui consiste à améliorer l'intelligence de machines, souvent dans le but d'automatiser des tâches ou de simplifier le processus décisionnel. Bon nombre de grands employeurs et d'agences de recrutement utilisent des systèmes de suivi des candidats automatisés faisant appel à l'IA, ou s'y fient, pour sélectionner les candidats dans le cadre du processus de recrutement. Certains peuvent avoir recours à des outils d'IA pour faire passer des tests aux candidats ou évaluer leurs réponses lors des entrevues.

Outre le recrutement, les employeurs se tournent également vers l'IA pour effectuer des analyses de la satisfaction de leurs employés aux fins de la gestion des talents. Les résultats des sondages et les courriels des employés sont analysés pour en évaluer le ton et l'humeur, dans le but de déterminer ce qu'ils pensent de l'organisation et de leur rôle au sein de celle-ci.

Dans l'ensemble, la gestion de la réputation d'un employeur et l'atténuation des risques juridiques passent nécessairement non seulement par l'examen des possibilités, mais aussi des pièges potentiels d'un recours à l'IA de l'une des façons susmentionnées.

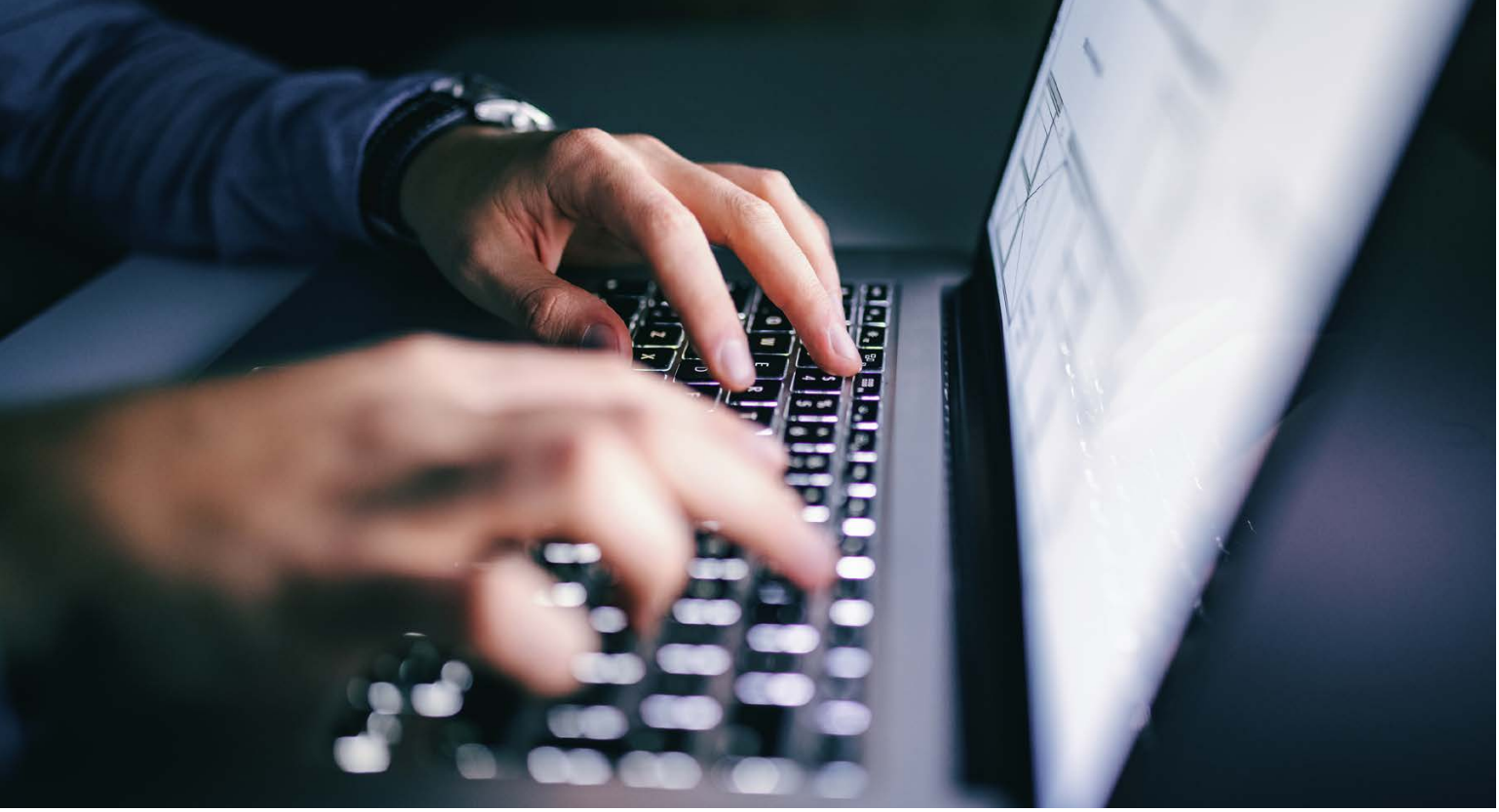


> **Bon nombre de grands employeurs et d'agences de recrutement utilisent des systèmes de suivi des candidats automatisés faisant appel à l'IA, ou s'y fient, pour sélectionner les candidats dans le cadre du processus de recrutement.**

RISQUES JURIDIQUES POTENTIELS ASSOCIÉS AU RECOURS À L'IA

Le plus souvent, la fiabilité des résultats produits par les outils analytiques d'IA est limitée par la fiabilité des données et des paramètres qui ont été Dans les phases de conception et d'apprentissage de ces outils. Qui plus est, l'utilisation de tels systèmes peut dans certains cas servir à renforcer les biais qui existaient dans les ensembles de données utilisés pour l'apprentissage des systèmes d'IA.

L'ensemble des provinces et des territoires du Canada ont des lois sur les droits de la personne qui protègent les individus contre toute discrimination en matière d'emploi fondée sur l'un ou l'autre des motifs



de distinction illicites énumérés, souvent appelés « caractéristiques protégées ». Ces protections en vertu des lois sur les droits de la personne s'étendent aux processus de recrutement. Les motifs énumérés peuvent varier d'un territoire à l'autre, mais comprennent en général, entre autres, la race, l'origine, les croyances, le sexe, la situation familiale et le handicap (physique ou mental).

Certains territoires et provinces ont également adopté des lois sur l'accessibilité prévoyant l'obligation d'offrir des mesures d'adaptation pour les personnes ayant un handicap dans le cadre du processus de recrutement et dans le cadre de l'emploi. Par exemple, la partie III, Normes pour l'emploi, des Normes d'accessibilité intégrées prises en application de la *Loi de 2005 sur l'accessibilité pour les personnes handicapées de l'Ontario*, énonce des exigences particulières pour le recrutement, dont celle d'offrir des mesures d'adaptation aux candidats dans le cadre des processus d'évaluation ou de sélection. Elle prévoit aussi l'obligation pour l'employeur de tenir compte des besoins en matière d'accessibilité de ses employés handicapés dans les processus de gestion du rendement.

Un rapport publié en 2018 pour le Conseil de l'Europe soulignait que chaque étape du processus de conception présente un risque que l'IA adopte une approche discriminatoire de l'analyse des données. Un biais peut s'introduire dans l'analyse faite par IA, même si le concepteur a les meilleures intentions. Cela peut se produire même en l'absence de collecte de données sur les caractéristiques protégées en raison de l'existence de « données indirectes », c'est-à-dire d'autres points de données recueillis qui présentent des corrélations avec des caractéristiques protégées. Par exemple, il existe des cas documentés de préjugés raciaux dans les applications d'IA utilisées pour la reconnaissance faciale, la détermination des peines, l'évaluation des risques pour la santé et l'évaluation de l'admissibilité à un prêt.

Le risque de biais dans l'analyse par IA s'étend également aux outils utilisés pour le recrutement et la gestion des talents. Pour définir les caractéristiques d'un « bon » employé, il faut établir la priorité de certains paramètres par rapport à d'autres dans la conception de IA. On peut ainsi introduire des biais dans l'analyse faite par IA qui peuvent être amplifiés lorsque l'IA utilise des données provenant d'Internet pour évaluer des candidats ou des employés. La sélection des caractéristiques et le processus servant à les évaluer pourraient défavoriser de façon déloyale les personnes handicapées. Par exemple, de nombreux candidats handicapés ont de la difficulté avec les entrevues vidéo asynchrones dans lesquelles l'IA est utilisée pour évaluer les réponses aux questions.

PRATIQUES EXEMPLAIRES DES EMPLOYEURS EN MATIÈRE D'UTILISATION DE L'IA

Les employeurs peuvent mettre en œuvre des politiques et des pratiques en vue de limiter le risque de biais dans le processus décisionnel lorsqu'on fait appel à des outils d'IA. Une surveillance humaine de l'analyse par IA peut éliminer les biais en chargeant une personne d'évaluer le résultat de

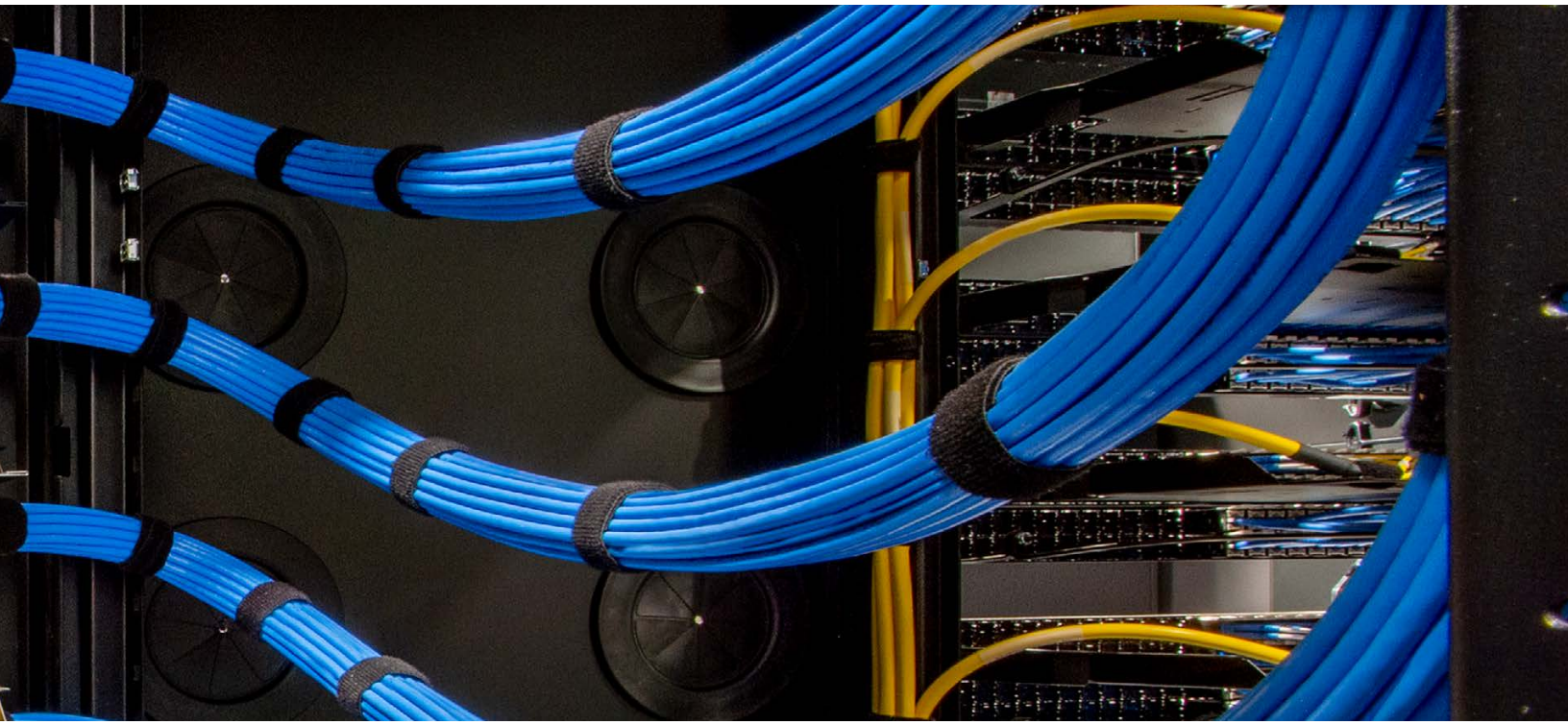
l'IA et de prendre une décision définitive. De plus, avant de faire l'acquisition d'un logiciel d'IA, les employeurs doivent envisager la réalisation d'évaluations des incidences de l'IA sur l'éthique. Les évaluations des incidences de l'IA sur l'éthique permettent d'apprécier l'imputabilité, l'équité, la transparence, l'explicabilité, l'exactitude et la fiabilité des systèmes d'IA et de leurs résultats. Un comité interne peut ensuite évaluer les résultats de ces évaluations et répondre aux préoccupations avant de prendre une décision d'achat.

Les employeurs ont un rôle important à jouer pour favoriser l'équité de l'IA en encourageant les développeurs à concevoir des systèmes d'IA responsables. Les entreprises qui sont des clients réguliers des développeurs de logiciels d'IA peuvent exprimer leurs préoccupations éthiques et demander à obtenir l'information requise pour évaluer les aspects éthiques de leur logiciel. De surcroît, les employeurs peuvent exercer des pressions pour que la diversité devienne une priorité dans les pratiques d'emploi des entreprises d'IA. Une des sources des biais constatés dans les outils d'IA pourrait être le manque de diversité dans les équipes de développeurs.

Les employeurs doivent mettre en œuvre des pratiques de stockage et de traitement des données qui protègent la vie privée des personnes dont les données sont recueillies. Bon nombre d'entreprises tiennent un registre des activités de traitement qui fait le suivi des paramètres clés de chaque activité de collecte et de traitement de données menée, y compris par un logiciel d'IA. Le registre des activités de traitement fait le suivi, pour chaque activité de traitement, des paramètres suivants : les responsables du traitement et les sous-traitants des données, les finalités du traitement, les catégories de personnes concernées, les données à caractère personnel, les destinataires des données en cause, la durée de conservation des données et les mesures de sécurité en place. Ce registre crée une piste de navigation pour le traitement des données qui peut être consulté à des fins internes ou être utilisé pour gérer les risques et limiter la responsabilité éventuelle des entreprises.

Les employeurs ont un rôle important à jouer pour favoriser l'équité de l'IA en encourageant les développeurs à concevoir des systèmes d'IA responsables.

De nombreuses options s'offrent aux employeurs pour prévenir les risques associés à l'utilisation de l'IA. On s'attend à ce que les technologies faisant appel à l'IA soient adoptées dans pratiquement tous les secteurs d'activité. Les employeurs qui ont une longueur d'avance en matière de gestion des risques de l'IA optimiseront leurs processus de recrutement et de gestion du rendement tout en protégeant leur réputation et en gérant leur exposition à une responsabilité éventuelle.



Protection de la vie privée pendant les enquêtes en milieu de travail

Ces dernières années, l'obligation juridique de mener des enquêtes en milieu de travail, par exemple en cas d'allégations de violence ou de harcèlement au travail en vertu de la *Loi sur la santé et la sécurité au travail*, a entraîné une augmentation du nombre d'enquêtes en milieu de travail. Des enquêtes en milieu de travail sont également réalisées pour évaluer les allégations d'inconduite, les signalements effectués par des dénonciateurs et les plaintes pour discrimination. Les éléments devant faire l'objet d'une attention particulière dans le cadre d'une procédure d'enquête en milieu de travail sont la confidentialité, le respect de la vie privée et la protection des renseignements recueillis à cette occasion. Ces éléments sont devenus encore plus importants du fait que bon nombre de ces enquêtes sont à présent réalisées en mode virtuel ou par conférence téléphonique en raison de la pandémie de COVID-19.

MISE EN PLACE DE MESURES APPROPRIÉES POUR PROTÉGER LES RENSEIGNEMENTS PERSONNELS

En cas d'enquête en milieu de travail, la première mesure à prendre est de nommer un enquêteur approprié. L'enquêteur, interne ou externe, doit avoir mis en place des mesures appropriées pour garantir la confidentialité et la protection des renseignements personnels qu'il reçoit dans le cadre de l'enquête. En général, l'approche fondée sur les pratiques exemplaires consiste à préserver la confidentialité des renseignements personnels relatifs à l'enquête, sauf dans la mesure où leur divulgation est requise par la loi ou est nécessaire aux fins de l'enquête et ce seulement aux personnes ayant besoin d'en avoir connaissance. Dans la mesure où une politique applicable au milieu de travail contient des exigences en matière de confidentialité, de protection, de stockage et de conservation de l'information, l'enquêteur doit s'y conformer.

> **L'enquêteur, interne ou externe, doit avoir mis en place des mesures appropriées pour garantir la confidentialité et la protection des renseignements personnels qu'il reçoit dans le cadre de l'enquête.**

Autrement dit, il doit veiller à ce que les copies électroniques et imprimées des courriels, des fichiers et des dossiers relatifs à l'enquête ne puissent pas être consultées par d'autres personnes. Les documents imprimés doivent être conservés de façon à ce que d'autres personnes ne puissent pas y accéder, et les documents électroniques doivent être protégés par un mot de passe. Les destinataires de tout renseignement sur l'enquête ou de ses conclusions doivent être choisis avec soin afin de contrôler la circulation de l'information. Si un enquêteur examine des documents

ou rédige un rapport dans un espace de travail partagé, il doit prendre les mesures nécessaires pour que personne ne puisse voir son écran.

Lorsque l'enquêteur rencontre pour la première fois une personne qu'il doit interroger dans le cadre d'une enquête, il doit informer cette personne de l'obligation de confidentialité et des conséquences possibles d'une infraction à cette règle et lui confirmer les fins auxquelles les renseignements personnels qu'il fournit seront utilisés. L'enquêteur doit se garder de faire des promesses sur la confidentialité, dans l'éventualité où il faut communiquer des renseignements personnels au cours de l'enquête ou les transmettre à l'employeur afin de lui permettre de prendre des mesures correctives.

SURVEILLANCE DES EMPLOYÉS

L'enquêteur doit être conscient des répercussions de ces lois sur la protection de la vie privée pouvant résulter de l'enquête. Une attention particulière doit être accordée lorsque l'enquête comprend la surveillance d'employés. En général, l'employeur peut faire surveiller des employés si la surveillance est raisonnable pour ce qui est (i) de l'objectif de la surveillance par l'employeur et (ii) de la manière dont l'employeur effectue la surveillance. L'employeur doit en général donner un préavis de la surveillance aux employés et, dans certaines provinces, obtenir leur consentement. Dans la plupart des cas, il est raisonnable pour l'employeur d'afficher un avis à un endroit susceptible d'être vu par les employés concernés pour les aviser que des activités de vidéosurveillance ou de surveillance sont en cours.

Un préavis n'est, en règle générale, pas nécessaire si la surveillance est raisonnable aux fins d'une enquête sur un manquement à des modalités expresses ou implicites d'un contrat d'emploi, ou si l'employeur a des motifs raisonnables de croire qu'un manquement a été ou sera commis.

APPAREILS EN DÉPÔT

Les appareils en dépôt sont des appareils électroniques dont l'employé a la garde, mais dont l'employeur est le propriétaire (par exemple, un téléphone cellulaire ou un ordinateur portable). L'attente raisonnable de respect de la vie privée et les autres droits de l'employé à l'égard des appareils dont l'employeur est le propriétaire sont susceptibles d'avoir un degré d'importance sensiblement inférieur aux droits qu'aurait l'employé à l'égard d'un appareil qu'il posséderait lui-même.

Un employeur peut réduire les attentes de respect de la vie privée d'un employé à l'égard de tels appareils en exigeant de l'employé qu'il signe une politique stipulant que l'employeur se réserve le droit de surveiller ces appareils et d'y accéder et qu'il conserve la propriété de leur contenu, et qu'il suive une formation sur cette politique. Il n'est en général pas interdit à l'employeur d'accéder aux communications qui sont stockées dans son propre réseau

électronique (par exemple, le serveur de courriels de l'employeur) si un tel accès est autorisé par ses propres politiques. Lorsque la police effectue une enquête criminelle dans le milieu de travail, le juge peut exclure toute preuve obtenue sans mandat en bonne et due forme (*R. c. Cole*).

UNE COLLECTE D'ÉLÉMENTS DE PREUVE INAPPROPRIÉE PEUT NUIRE À L'ENQUÊTE

Un employeur peut ne pas pouvoir s'appuyer sur les conclusions de son enquête pour justifier la prise de mesures correctives (par exemple, la suspension ou le congédiement pour un motif valable) si la preuve a été recueillie de manière inappropriée.

Dans le cadre d'une enquête sur un employé non syndiqué, le recours à des modalités inappropriées de surveillance ou de collecte de la preuve peut avoir plusieurs conséquences préjudiciables telles que : des dommages au titre du délit civil d'atteinte à la vie privée, des dommages au titre du délit en common law d'atteinte à la vie privée et des réclamations pour congédiement déguisé, dommages moraux et dommages punitifs (*Colwell v. Cornerstone Properties Inc.*).

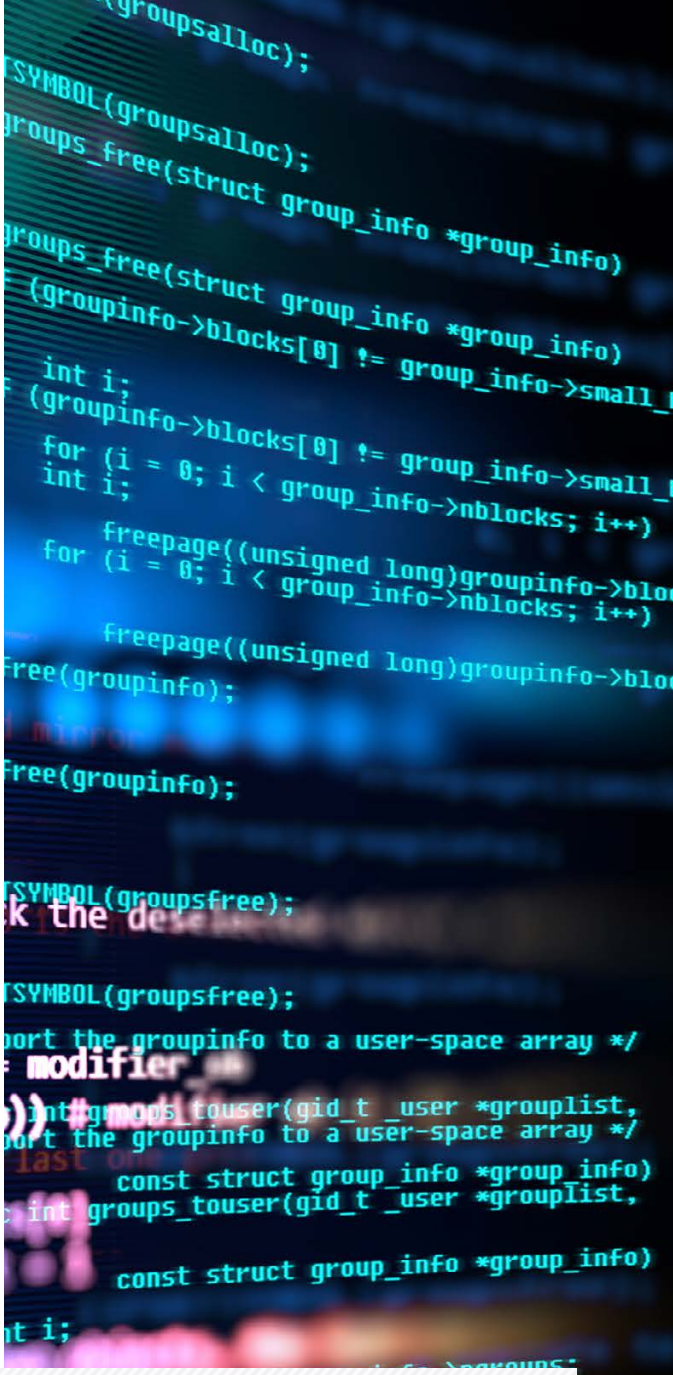
Dans le cadre d'une enquête sur un employé syndiqué, en l'absence de clause dans la convention collective traitant expressément de la surveillance des employés, il reviendra à l'arbitre de déterminer si la preuve recueillie au moyen de la surveillance est admissible. Si l'arbitre détermine que l'employé a été surveillé de façon inappropriée, il peut ordonner l'exclusion de la preuve ainsi recueillie.
Pour déterminer si la preuve est admissible, l'arbitre doit trouver le juste équilibre entre le droit de l'employé au respect de sa vie privée et le droit de l'employeur de faire enquête. En général, pour parvenir à une décision, l'arbitre évalue si la surveillance était raisonnablement nécessaire à la lumière des circonstances, si l'employeur a mené l'enquête de façon raisonnable et s'il existait des solutions de rechange à la surveillance (*Doman Forest Products Ltd. v. I.W.A.*).

De nombreux éléments doivent être pris en considération dans le cadre d'une enquête en milieu de travail. Les exigences régissant la collecte, l'utilisation et le stockage des renseignements pendant une enquête sont un élément clé de toute procédure d'enquête et contribuent de façon significative à assurer le respect par l'employeur des lois applicables en matière de protection de la vie privée et l'intégrité des résultats de l'enquête.

Utilisations stratégiques de l'anonymisation des données et de la minimisation des données dans le traitement analytique des données

Le traitement analytique des données se trouve actuellement à un moment charnière à l'échelle internationale qui aura probablement des répercussions sur les normes communes de l'industrie. Au Québec, bien sûr, le projet de loi no 64, assorti de ses pénalités draconiennes, entrera en vigueur, pour l'essentiel, en septembre 2023, ce qui comprend le premier traitement prévu par la loi au Canada des technologies qui permettent, relativement à une personne, « de l'identifier, de la localiser ou d'effectuer un profilage de celle-ci ». L'Europe va encore plus loin : le 23 novembre 2021, la commission du marché intérieur et de la protection du consommateur du Parlement européen a à l'unanimité appuyé le projet de loi sur les marchés numériques, qui interdit l'utilisation de combinaisons de renseignements personnels par les principales plateformes publicitaires pour produire de la publicité ciblée.

Les fournisseurs de données pour la publicité ciblée et de perspectives tirées des données ressentent également la pression exercée par les législateurs concernant le suivi par des tiers qui prend souvent la forme de témoins (*cookies*) tiers insérés dans les navigateurs qui suivent l'utilisateur pour recueillir de l'information sur ses habitudes et ses intérêts. L'industrie connaît actuellement de grands bouleversements : Firefox et Safari ont totalement bloqué les témoins tiers de leurs navigateurs, Apple a mis en place des paramètres de confidentialité sur ses appareils mobiles par l'intermédiaire d'iOS 14.5 rendant obligatoire le consentement au suivi par des tiers sur les applications mobiles, et Google s'est engagé à éliminer graduellement son système de témoins tiers d'ici 2023.



> **Les entreprises peuvent à la fois souhaiter anonymiser les renseignements personnels afin de simplifier leurs obligations réglementaires et réduire les risques liés à une contravention, tout en conservant suffisamment de renseignements personnels critiques pour que les données demeurent utiles.**

Le traitement analytique des données est une bataille incessante entre l'utilité et l'anonymat de l'ensemble de données sous-jacent. Les entreprises peuvent à la fois souhaiter anonymiser les renseignements personnels afin de simplifier leurs obligations réglementaires et réduire les risques liés à une contravention, tout en conservant suffisamment de renseignements personnels critiques pour que les données demeurent utiles. Cette situation soulève une question essentielle : comment les entreprises peuvent-elles tirer le maximum d'informations sur les comportements d'un groupe tout en limitant l'information sur chacun des individus qui composent ce groupe?

Soumises à un resserrement du contrôle réglementaire, les entreprises ont élaboré des solutions uniques afin de conserver certains renseignements personnels critiques tout en réduisant les risques d'atteinte à la vie privée qui y sont associés grâce à l'anonymisation. L'application stratégique de techniques d'anonymisation permet aux entreprises de maximiser la valeur analytique des renseignements personnels tout en réduisant au minimum les risques associés à leur conservation. Ces techniques permettent de réduire les risques de préjudice associé aux atteintes à la vie privée, les enquêtes réglementaires et les obligations de divulgation puisque les renseignements personnels détenus par l'entreprise ne permettent plus d'identifier un individu ou diminuent considérablement les préjudices possibles pour ces individus. Nous examinons ces solutions ci-dessous.

TECHNIQUES COURANTES D'ANONYMISATION ET DE MINIMISATION

Les organismes de réglementation en matière de protection de la vie privée encouragent de plus en plus le recours aux techniques d'anonymisation en vue de réduire les risques associés au traitement et à la conservation des renseignements personnels par les entreprises. À titre de guide, la Commission européenne a recensé trois critères permettant d'évaluer la fiabilité d'une technique d'anonymisation : i) est-il toujours possible d'isoler un individu?; ii) est-il toujours possible de relier entre eux les enregistrements relatifs à un individu?; et iii) peut-on déduire des informations concernant un individu?

Dans la pratique, une anonymisation parfaite des données rendrait celles-ci pratiquement inutilisables du point de vue de l'entreprise. Toutefois, les entreprises peuvent mettre en œuvre un large éventail de techniques d'anonymisation et de minimisation permettant de préserver l'utilité analytique des données afin d'en tirer des renseignements commerciaux tout en protégeant les renseignements personnels contre une diffusion à grande échelle. Comme ces techniques permettent la réidentification des données à des fins d'analyses, elles sont désignées sous le terme de « pseudonymisation ». En combinant diverses méthodes de pseudonymisation des renseignements personnels, les entreprises ont trouvé différents moyens créatifs de maximiser l'utilité analytique tout en réduisant le risque juridique associé au traitement des données.

Suppression

La suppression de données consiste à éliminer certaines catégories de données qui ne sont pas pertinentes pour un exercice analytique donné. À titre d'exemple, si le nom complet d'un individu n'est pas pertinent pour le traitement analytique, mais a été recueilli dans le cadre du processus de saisie des informations de paiement, il sera retiré de toute demande de données formulée par l'analyste. Idéalement, la suppression devrait être utilisée lorsqu'une catégorie de renseignements personnels est non pertinente, ou ne peut être convenablement anonymisée par une autre technique, car il n'est plus possible de récupérer les données par la suite.

Masquage

Le masquage est une méthode d'anonymisation des données semblable à la suppression, mais elle est de nature moins permanente. Cette technique consiste à remplacer des caractères des renseignements personnels par des caractères fictifs afin de réduire la possibilité d'un accès non autorisé aux données sensibles. Le recours à des caractères uniformes pour prévenir leur enregistrement (le mot de passe devient • • • • • • • • lorsqu'il est saisi) est un exemple courant. La même pratique est utilisée pour masquer le numéro de carte de crédit, dont les chiffres sont remplacés par XXXX-XXXX-XXX-1234 pour empêcher toute utilisation

malveillante. Le masquage peut être utile pour accroître la sécurité en empêchant la diffusion à grande échelle de renseignements personnels sensibles au sein d'une organisation, mais ses effets ne sont pas permanents.

Mélange, brouillage ou brassage

Ce processus consiste à déplacer les lettres ou les chiffres à l'intérieur d'un renseignement personnel ou dans tout l'ensemble de données. En dissociant l'ordre logique dans lequel un ensemble de données est présenté, on réduit significativement la quantité de renseignements identificatoires pouvant être extraits par un acteur malveillant. De plus, le traitement des données par brouillage ou mélange rend plus difficile le repérage des renseignements personnels des autres personnes concernées en tentant de décoder le processus de mélange, car les colonnes ou ensembles de données faisant l'objet d'un tel mélange sont bien souvent choisis au hasard et changent à chaque accès. [1]

Généralisation

La généralisation consiste à réduire délibérément la précision d'un ensemble de données en élargissant sa définition. Les catégories de données qui tirent parti d'une généralisation sont souvent celles dont la valeur analytique est préservée même lorsqu'elles sont condensées jusqu'à un certain degré. Un exemple dans le domaine des offres de services est de remplacer un code postal par les trois premiers caractères de ce code, voire par un indicateur de voisinage encore plus large. Ou encore, le remplacement d'une date de naissance par le mois et l'année de naissance, ou par un âge donné (55) ou par une tranche d'âge (de 50 à 60 ans). La généralisation est particulièrement efficace lorsqu'elle est appliquée de façon sélective, car la mesure dans laquelle une valeur de donnée est généralisée a d'importantes répercussions sur la protection offerte aux individus visés par l'ensemble de données.

La généralisation est particulièrement efficace lorsqu'elle est appliquée de façon sélective, car la mesure dans laquelle une valeur de donnée est généralisée a d'importantes répercussions sur la protection offerte aux individus visés par l'ensemble de données.

Ajout de bruit

L'ajout de bruit permet de dissimuler les renseignements personnels recueillis en y ajoutant des quantités choisies de données factices. Le « bruit » est constitué de points de données ou de champs entiers de données qui ne sont corrélés à aucun individu. Le processus d'ajout de bruit varie considérablement selon les données recueillies, mais le principe général consiste à « dissimuler » des renseignements personnels réels parmi des données générées au hasard n'ayant aucune utilité réelle. Lorsqu'une organisation insère

1. Un exemple concret de brassage est présenté sur la page d'Imperva What Is Data Anonymization."

des données fictives parmi des données réelles, il devient beaucoup plus difficile pour les acteurs malveillants d'utiliser l'ensemble de données à des fins nuisibles ou d'analyser par rétro-ingénierie les techniques d'anonymisation susmentionnées à partir de l'intégralité de l'ensemble de données. Une méthode plus récente utilisée par les entreprises, appelée « confidentialité différentielle », décrite plus bas, applique le procédé d'ajout de bruit par des moyens particuliers pour accroître la sécurité des renseignements personnels détenus par une organisation.

Chiffrement

Le chiffrement est un moyen efficace de mettre en œuvre les techniques mentionnées ci-dessus. Ce procédé consiste à filtrer les données recueillies à travers un algorithme de chiffrement qui les rend inutilisables par un lecteur humain; les données peuvent ensuite être déchiffrées à l'aide d'un mot de passe privé. Une méthode courante et facile à utiliser est le chiffrement symétrique, dans lequel les données sont dissimulées par un algorithme au moment de la collecte et ne deviennent lisibles qu'après la saisie du mot de passe d'une clé privée. Le chiffrement existe sous différentes formes, allant du chiffrement simple par clé privée au chiffrement de bout en bout plus complexe, mais son but demeure le même : rendre illisible les renseignements personnels recueillis par l'entreprise pour des acteurs malveillants. Les techniques comme celle du « salage et hachage » rendent beaucoup plus ardue la tâche de percer le code. Toutefois, les analystes autorisés qui ont besoin d'accéder à l'ensemble de données peuvent profiter de l'intérêt analytique des données s'ils ont accès à la clé de déchiffrement.[2]

2. Il va de soi que les organisations doivent mettre en place des mesures de sécurité internes robustes pour éviter que des acteurs malveillants internes ou externes mettent la main sur ces clés.

NOUVELLES TECHNIQUES D'ANONYMISATION ET DE MINIMISATION

Apprentissage fédéré des cohortes (FLoC)

Le FLoC est une technique combinant la généralisation, la suppression et l'ajout de bruit qui consiste à recueillir des renseignements personnels et à les trier selon les facteurs identifiants pour en faire des cohortes anonymisées. Google a mis en œuvre cette technique en mars 2021 pour remplacer sa technologie de suivi par témoins tiers dans son navigateur Chrome. Les cohortes sont triées selon le type d'activité des utilisateurs sur Internet, ce qui sert de méthode de généralisation et de suppression en ne fournissant aux publicitaires que les catégories de données les plus pertinentes de façon abstraite. De plus, les cohortes contiennent des centaines, voire des milliers d'utilisateurs, ce qui rend le comportement d'un individu difficile à associer à une personne en particulier.

La technique FLoC a été déployée chez les utilisateurs de Chrome dans le cadre d'un projet pilote, ce qui a occasionné un changement radical de l'efficacité des témoins tiers. La boîte à sable de confidentialité de Google fournit le mécanisme qui sous-tend la technique FLoC à code source ouvert, ce qui permet aux entreprises d'examiner si elles peuvent l'utiliser à leurs propres fins. En principe, la technologie liée au FLoC pourrait tout aussi bien être appliquée aux entreprises qui souhaitent généraliser les renseignements personnels qu'elles détiennent afin de se protéger contre toute atteinte à la vie privée, et se retrouver avec uniquement des cohortes abstraites plutôt que des renseignements permettant d'identifier une personne.

Tokénisation

La tokénisation est une méthode de chiffrement et de masquage plus approfondie qui consiste à remplacer des renseignements personnels par une série de jetons numériques qui identifient des éléments précis des renseignements personnels. Ce principe est déjà largement utilisé dans le secteur du traitement des paiements, où les renseignements sur les paiements par carte de crédit sont tokénisés pour permettre les demandes de transfert entre les établissements bancaires acquéreurs, les réseaux de paiement et les établissements bancaires émetteurs sans révéler de renseignements personnels durant les transferts.

La tokénisation constitue une étape supplémentaire de masquage où les valeurs des renseignements personnels sont intégralement remplacées. Le processus prévoit l'utilisation d'un « coffre-fort de jetons » qui contient l'algorithme de base utilisé pour produire un large éventail de jetons. Les renseignements personnels qui sont transmis à l'entreprise sont stockés dans le coffre-fort de jetons, et le jeton est ensuite transféré pour servir à diverses fins. Ce n'est que lorsqu'une demande est faite au coffre-fort de jetons que le jeton peut être échangé contre les renseignements personnels qu'il représente. Comme le jeton lui-même ne possède aucune valeur intrinsèque, même si un acteur malveillant parvient à briser le code de chiffrement, le jeton ne révélera aucun renseignement personnel. Un autre avantage de ce système est que toute demande d'échange de jeton contre les renseignements personnels qu'il représente peut faire l'objet d'un suivi par l'entreprise, ce qui facilite l'enquête sur un incident de confidentialité. De plus, les jetons sont fréquemment randomisés chaque fois qu'ils sont entrés, même si le renseignement personnel sous-jacent demeure le même.

La tokénisation est rarement mise en œuvre comme mesure de sécurité indépendante, elle est souvent assortie à d'autres solutions.

La technologie qui sous-tend la tokénisation est un concept ayant largement fait ses preuves et qui a fait l'objet d'innovations constantes grâce à la popularisation de la technologie des chaînes de blocs. Toutefois, la tokénisation est rarement mise en œuvre comme mesure de sécurité indépendante, elle est souvent assortie à d'autres solutions afin d'offrir un système de protection de la vie privée dont la sécurisation est plus exhaustive. Selon le type de renseignement personnel traité et transigé, la tokénisation

peut être un moyen efficace de protéger le transfert de renseignements personnels.

Calcul multipartite sécurisé

Le calcul multipartite sécurisé (ou traitement fractionné) est une solution cryptographique qui permet le partage des résultats du traitement des données tout en gardant secrètes les données utilisées pour produire ces résultats. Auparavant, ce processus nécessitait une « source tierce de confiance » agissant à titre d'intermédiaire. Dans ce processus, deux parties fournissaient des données pertinentes à une tierce partie, qui renvoyait de façon confidentielle les résultats requis sans révéler à aucune des deux parties quelles étaient les valeurs utilisées.

Le calcul multipartite sécurisé rend inutile le recours à l'intermédiaire en émulant la tierce partie par un procédé cryptographique avancé. L'entreprise obtient ainsi des renseignements commerciaux précis sans jamais avoir accès aux renseignements personnels d'où ils sont tirés, en particulier pour ce qui est des ensembles de données plus volumineux. Utilisé de façon appropriée, le calcul multipartite sécurisé pourrait offrir aux entreprises un moyen sécurisé de tirer des données de l'information

exploitable même lorsque l'environnement opérationnel pose des risques sérieux d'atteinte à la vie privée. Citons par exemple le cas d'un exportateur de données qui souhaite faire traiter des renseignements personnels conjointement par deux prestataires de services situés dans des territoires où l'étendue de la protection juridique des renseignements personnels est limitée. L'exportateur de données peut mettre en œuvre un système de calcul multipartite sécurisé dans lequel les deux prestataires de services traitent simultanément les renseignements personnels sans jamais avoir accès aux ensembles de données en question.

Utilisé de façon appropriée, le calcul multipartite sécurisé pourrait offrir aux entreprises un moyen sécurisé de tirer des données de l'information exploitable même lorsque l'environnement opérationnel pose des risques sérieux d'atteinte à la vie privée.

Même si la méthode du calcul multipartite sécurisé existe déjà depuis un certain temps, son application récente aux stratégies de protection des données s'explique principalement par la reconnaissance par les organismes de réglementation à l'échelle internationale de son efficacité comme mesure de protection de la vie privée. Le Comité européen de la protection des données mentionne le calcul multipartite sécurisé comme une mesure supplémentaire efficace pour protéger les données en dehors de l'UE et souligne son potentiel d'utilisation comme technologie applicable aux systèmes adhérant à des normes par défaut en matière de protection de la vie privée. L'International Association of Privacy Professionals rapporte qu'aux États-Unis, les institutions publiques mettent en œuvre le calcul multipartite sécurisé pour protéger les bases de données fédérales et que la *Promoting Digital Privacy Technologies Act* mentionne le calcul multipartite sécurisé comme une technique cryptographique qui mérite d'être étudiée.

Confidentialité différentielle

La confidentialité différentielle est une technique qui simplifie le processus d'ajout de bruit à un ensemble de données même pour les utilisateurs autorisés. Dans ce modèle, l'analyste est tenu à l'écart de la base de données et il ne peut pas voir les renseignements personnels recueillis par l'entreprise. Lorsqu'un analyste souhaite tirer des conclusions de certaines valeurs de données, il soumet une demande à un logiciel intermédiaire appelé « gardien de la confidentialité ». Le gardien de la confidentialité évalue le risque d'atteinte à la vie privée associé à chaque demande et ajoute un bruit aléatoire pour compenser ce risque avant de fournir une valeur de donnée.

Le résultat est que la valeur envoyée à l'analyste est suffisamment proche de la valeur réelle pour être utile, mais elle contient en même temps assez de bruit pour empêcher tout type de rétro-ingénierie qui exposerait les renseignements personnels d'un individu. Certaines entreprises, dont Microsoft, Apple et Google, ont mis en œuvre la technique de confidentialité différentielle avec un certain succès. En ajoutant une quantité de bruit aléatoire proportionnelle au risque pour la vie privée, la technique de confidentialité différentielle peut constituer une solution exhaustive permettant de conserver l'utilité analytique en masquant la valeur réelle des données tout en fournissant une image globale exacte des tendances à l'intérieur d'un ensemble de données.

Données synthétiques

Les données synthétiques sont un complément à la technique d'ajout de bruit susmentionnée. La pratique générale consiste à utiliser un algorithme qui simule les connexions effectuées par l'analyse des renseignements personnels et faire une rétro-ingénierie des conclusions pour générer des ensembles de données fictives. Le MIT a publié le Synthetic Data Vault pour aider les développeurs à cet égard. Lors d'un test de l'utilité des résultats tirés de l'utilisation de données synthétiques comparativement aux ensembles de données réels, les chercheurs ont été en mesure de tirer des conclusions exactes 70 % du temps, même en utilisant des ensembles de données synthétiques.

En principe, les méthodes faisant appel aux données synthétiques pourraient permettre de se passer totalement des renseignements personnels. Les entreprises pourraient tirer des résultats et des analyses utiles d'une simulation du comportement des clients, au lieu de s'exposer à des risques d'atteinte à la vie privée posés par la collecte de données auprès d'individus. Cependant, les solutions faisant appel aux données synthétiques en sont encore aux premiers stades de mise en œuvre. Selon le type de traitement analytique que l'entreprise souhaite reproduire, les données synthétiques pourraient constituer un moyen coûteux d'anonymiser les données comparativement aux autres méthodes mentionnées dans le présent document.

Identifiant universel

La technologie de l'identifiant universel est une application à la fois du chiffrement et de la suppression qui sert à identifier chaque utilisateur individuel par un nom d'utilisateur générique, au lieu de recueillir un large éventail de renseignements personnels pour les utilisateurs en ligne. La version la plus connue de cette technologie est la plateforme Unified ID 2.0 à code source ouvert, mise au point par TradeDesk et adoptée par Buzzfeed, AMC Networks, Foursquare, Salon et le *LA Times*. Universal ID propose un nom d'utilisateur à code source ouvert, crypté et unique pour les individus qui visitent les sites Web partenaires. Les utilisateurs qui créent un profil voient leur adresse courriel cryptée et tokénisée (voir les explications plus haut), et le jeton de l'identifiant universel est échangé entre les prestataires de services et les publicitaires afin de permettre à ces derniers d'offrir de la publicité ciblée aux individus sans connaître bon nombre d'attributs non nécessaires sur l'individu pouvant l'exposer aux acteurs malveillants.

Les systèmes à identifiant universel ne sont pas utilisés exclusivement par le secteur privé, car cette technologie a été appliquée avec succès dans le secteur public. Tel est le cas par exemple du programme ID Austria, dont la phase pilote a pris fin à l'automne 2021. Ce système utilise la même méthodologie de tokénisation pour chiffrer les renseignements personnels des citoyens autrichiens, qui peuvent utiliser l'identifiant numérique comme moyen d'accès aux services publics. Si les systèmes d'identifiants universels sont souvent mentionnés dans le contexte de l'applicabilité interentreprise, ils pourraient également être avantageux pour les sociétés ayant une société mère ou des filiales offrant de multiples services. Un exemple concret est l'offre d'identifiant universel de SAP, qui regroupe les offres de services au sein d'un seul et même système.

CONCLUSION

Le traitement analytique des données et des renseignements personnels est un volet incontournable des projections financières pour bon nombre d'entreprises à l'échelle mondiale. Alors que les organismes de réglementation continuent à prendre des mesures sévères et à imposer des normes rigoureuses au traitement des renseignements personnels, pendant que les sanctions pécuniaires atteignent un pourcentage élevé des recettes, l'anonymisation stratégique peut offrir certains avantages pratiques tout en préservant l'utilité des renseignements personnels. Les entreprises devraient prendre en considération les avantages pratiques de la mise en œuvre d'une ou de plusieurs des techniques abordées plus haut afin d'assurer une conformité d'une façon plus efficace sans nuire à l'efficience des pratiques commerciales.

Les gardiens (numériques) de l'application de la loi : le Bureau de la concurrence s'attaque aux géants de la technologie

Le changement de régime aux États-Unis a marqué le début d'une nouvelle ère d'activisme antitrust. Le président Biden a annoncé que l'application de la loi à l'égard des FAANG (Facebook, Amazon, Apple, Netflix, Google et entreprises apparentées) constituera une priorité pour son administration au cours des prochaines années et a confié à des critiques bien connus des géants des technologies de l'information, comme Lina Khan et Jonathan Kanter, le mandat de diriger la politique en matière de concurrence et de voir à son application. Compte tenu des liens économiques étroits entre les deux pays et de la sphère d'influence des États-Unis sur les économies occidentales, la stratégie du Canada en matière de concurrence sera nécessairement influencée par celle de son voisin du sud, et le Bureau de la concurrence du Canada (le « Bureau ») semble se préparer à durcir sa position en matière d'application de la loi dans le domaine du numérique.

Si ce phénomène n'est pas totalement nouveau, ces dernières années, les examens approfondis du Bureau dans le secteur des technologies et des données ont pris de l'ampleur, comme l'attestent plusieurs études de marché publiées, énoncés de position rendus publics et enquêtes dans l'espace numérique. Par exemple, en mai 2020, le Bureau a conclu un règlement avec Facebook concernant les indications trompeuses quant à la confidentialité. Par suite d'une enquête sur les pratiques en matière de protection des renseignements personnels du géant des médias sociaux, le Bureau a établi que Facebook donnait à ses utilisateurs la fausse impression qu'ils pouvaient contrôler l'accès à leurs renseignements personnels sur la plateforme, alors que Facebook partageait les données des utilisateurs avec des développeurs tiers, une pratique incompatible avec ses énoncés relatifs à la confidentialité. Par conséquent, Facebook a convenu de verser une pénalité de neuf millions de dollars et d'assumer les frais de l'enquête.

Les examens approfondis du Bureau dans le secteur des technologies et des données ont pris de l'ampleur, comme l'attestent plusieurs études de marché publiées, énoncés de position rendus publics et enquêtes dans l'espace numérique.

Plus tard la même année, le Bureau a annoncé qu'il menait une enquête sur le comportement d'Amazon afin de déterminer si l'entreprise se livrait à des pratiques restrictives du commerce dans son secteur du marché canadien et si de telles pratiques constituent un abus de position dominante. En particulier, le Bureau s'intéresse à toute politique d'Amazon susceptible de porter atteinte à la capacité des vendeurs tiers d'offrir leurs produits sur d'autres canaux de vente, à la capacité des vendeurs tiers de réussir dans le secteur de marché d'Amazon sans utiliser son service « Expédié par

Amazon » ou la publicité sur cette place de marché et à tout effort d'Amazon pour inciter les consommateurs à acheter ses produits plutôt que ceux offerts par des vendeurs tiers. Il semble que cette enquête soit toujours en cours, mais aucune nouvelle mise à jour n'a été publiée.

Le Bureau s'est également intéressé à l'application de la loi dans l'espace numérique par les acteurs autres que les grandes sociétés technologiques. Dans la foulée de la pandémie, les services de santé numériques demeurent une priorité du Bureau, celui-ci ayant lancé une consultation publique en 2020 afin d'évaluer les obstacles à l'accès, à la concurrence et à l'innovation dans ce secteur. Les commentaires initiaux des intervenants clés, comme les réseaux de soins de santé, les organismes de réglementation, les ordres professionnels et les fournisseurs de soins de santé numériques, ont été publiés en 2021. Les intervenants ont signalé le manque d'interopérabilité entre les fournisseurs (soulevant des préoccupations quant à la confidentialité), les défis relatifs à la rémunération et les problèmes liés aux processus d'approvisionnement et de commercialisation des technologies du domaine de la santé au Canada.

Certains événements survenus cet automne indiquent que la stratégie du Bureau en matière d'application de la loi dans le domaine du numérique va s'intensifier. Le 22 octobre 2021, le Bureau a obtenu une ordonnance d'un tribunal pour faire avancer son enquête civile sur la conduite de Google relativement à ses activités de publicité en ligne. La Cour fédérale du Canada a accordé la demande du Bureau de contraindre Google à produire des documents et des renseignements écrits sur ses activités d'affichage publicitaire au Canada. Même si peu d'information a été rendue publique, il semble que le Bureau tente d'évaluer si les pratiques de Google ont entravé la réussite des activités d'affichage publicitaire en ligne de ses concurrents et, ce faisant, ont entraîné une augmentation des prix et une réduction des choix et freiné l'innovation dans le secteur des services de technologies publicitaires et, en fin de compte, causé un préjudice aux annonceurs, aux éditeurs et aux consommateurs. L'enquête du Bureau suit son cours.

Ce même mois, dans le discours qu'il a prononcé lors de la conférence sur le droit de la concurrence organisée par l'Association du Barreau canadien, le commissaire de la concurrence, Matthew Boswell, a présenté les plans du Bureau pour s'attaquer à la concentration et à la conduite anticoncurrentielle dans l'économie numérique. Intitulé à juste titre « Le Canada a besoin de plus de concurrence », le discours du commissaire Boswell soulignait l'urgence pour le Canada de renforcer les mesures d'application de la *Loi sur la concurrence* du Canada afin de soutenir la reprise économique postpandémique et de rester en phase avec la transition observée à l'échelle internationale vers une application plus musclée des lois antitrust. Parmi les principales mesures annoncées figurait le renforcement de l'application numérique de la loi et la promotion de la conformité dans le marché numérique, où contrevenir aux lois sur la concurrence est simplement devenu la rançon des affaires.

Les objectifs du commissaire en matière d'application de la loi vont de pair avec une augmentation du budget du Bureau. Cela inclut des fonds pour la création d'une nouvelle Direction générale du renseignement et de l'exécution de la loi, qui sera dirigée par la sous-commissaire, Leila Wright. Cette direction générale est destinée à devenir le centre canadien d'expertise sur les questions liées aux technologies et aux données et servira de système d'avertissement précoce à l'égard d'enjeux potentiels liés à la concurrence dans les économies traditionnelles et numériques. Cette entité ne tranchera pas ses propres cas, mais fournira son expertise et son soutien en matière de renseignements aux directions générales qui prennent en charge des litiges, en plus de collaborer étroitement avec les activités de défense et de promotion de la concurrence du Bureau.

Si les répercussions de ses stratégies d'application de la loi dans l'espace numérique restent à voir, il semble que le Bureau, comme ses homologues internationaux, soit décidé à discipliner les marchés numériques, comme les géants de la technologie, au cours des prochaines années.

Contrôle préalable des pratiques de protection de la vie privée pour les fusions et acquisitions

Alors qu'il était auparavant rare, et probablement inutile, de demander à consulter une documentation exhaustive sur les pratiques de cybersécurité de la cible dans le cadre d'une vérification diligente, l'exposition au risque d'incidents de sécurité et les sanctions pécuniaires pouvant être imposées en cas de violation de la législation sur le respect de la vie privée ont amené certains changements dans les anciennes pratiques. L'évaluation de la conformité d'une entreprise cible aux lois pertinentes en matière de protection de la vie privée et de sa posture de sécurité fait à présent partie intégrante du processus standard de vérification diligente dans le cadre de toute opération de fusion et acquisition, et cette pratique est maintenant bien établie.

Les entreprises cibles doivent se préparer à répondre à des demandes exhaustives concernant leurs pratiques et politiques en matière de données. Les acheteurs doivent poser les questions appropriées et demander les documents pertinents.

ÉLÉMENTS FONDAMENTAUX

Toute entreprise cible est exposée dans une certaine mesure à un risque de cybersécurité et les acheteurs doivent en connaître les détails afin d'être en mesure de comprendre, d'atténuer et de répartir ce risque. Le risque peut être aussi évident qu'une atteinte à la protection des données connue du public, ou se dissimuler subrepticement dans toutes les activités de l'entreprise sous la forme de pratiques médiocres en matière de sécurité, d'un manque d'attention à l'égard du respect de la vie privée, ou d'une valeur excessive des indemnisations et des responsabilités dans les ententes commerciales. Les acheteurs ont également besoin de savoir que l'entreprise cible dispose des droits nécessaires pour utiliser les renseignements personnels comme elle le fait et, s'il y a lieu, pour mettre à exécution les nouveaux plans des acheteurs pour ces renseignements personnels.

> **Toute entreprise cible est exposée dans une certaine mesure à un risque de cybersécurité et les acheteurs doivent en connaître les détails afin d'être en mesure de comprendre, d'atténuer et de répartir ce risque.**

Risques d'action collective ou de litige : Les acheteurs doivent prendre connaissance des documents portant sur les réclamations, différends, litiges et autres procédures en cours intentées par ou contre l'entreprise cible concernant la vie privée, les données, les logiciels, les technologies ou les renseignements confidentiels. Les documents à l'appui expliquant le contexte de telles affaires sont cruciaux afin d'évaluer adéquatement les risques associés qu'elles peuvent présenter. Il existe un risque élevé de

poursuites en action collective à la suite d'une atteinte à la sécurité des données ou d'une utilisation inappropriée de renseignements personnels.

Amendes réglementaires : Alors que les amendes réglementaires étaient auparavant rares dans le modèle canadien de l'ombudsman de la réglementation sur la vie privée, la nouvelle loi du Québec (projet de loi no 64) en matière de protection des renseignements personnels prévoit des sanctions réglementaires inspirées du RGPD pouvant aller jusqu'à 10 millions de dollars ou 2 % du chiffre d'affaires mondial, selon le plus élevé de ces montants, et des sanctions pénales pouvant atteindre 25 millions de dollars ou 4 % du chiffre d'affaires mondial. Le montant des amendes peut doubler en cas de récidive. Le gouvernement fédéral canadien a lui aussi proposé une nouvelle loi sur la protection des renseignements personnels et, si ce projet de loi est actuellement en suspens, il n'en prévoit pas moins des pénalités dont le montant maximal est de 10 millions de dollars ou de 3 % des recettes globales brutes de l'organisation, selon le plus élevé de ces montants, et une amende maximale de 25 millions de dollars ou de 5 % des recettes globales brutes de l'organisation, selon le plus élevé de ces montants. Par ailleurs, comme l'Ontario, l'Alberta et la Colombie-Britannique en sont tous à l'étape d'envisager des modifications à leur loi sur la vie privée, l'apparition d'amendes additionnelles et redondantes est probable.

Licéité du traitement : Les acheteurs doivent savoir quels renseignements personnels sont traités par l'entreprise cible et sur quels fondements juridiques elle s'appuie pour que le traitement puisse se poursuivre dans l'avenir. Les acheteurs peuvent aussi avoir prévu de nouvelles façons de traiter les renseignements personnels. Comme la législation canadienne relative à la protection des renseignements personnels reste fondée sur le consentement, tout traitement actuel ou futur doit être conforme au consentement donné par les individus concernés.

Depuis l'adoption du projet de loi n° 64, au Québec, le consentement doit être manifeste, libre, éclairé et être donné à des fins spécifiques.

EXAMEN DES POLITIQUES ET DES PON

Utilisation du cycle de vie des données recueillies par une organisation pour orienter votre liste de vérification diligente.

Liste de contrôle des politiques de protection de la vie privée et de sécurité des données	
☐	Politiques et avis de protection de la vie privée (y compris les politiques internes)
☐	Plans d'intervention en cas d'incident
☐	Journaux et formulaires de déclaration des incidents de données internes
☐	Politiques de sécurité de l'information et politiques subordonnées
☐	Politiques de conservation des données
☐	Politiques de destruction des données
☐	Politiques relatives aux droits et aux demandes d'accès des personnes concernées
☐	Politiques de cyberassurance
☐	Contrats ayant des conséquences sur la responsabilité en matière de cyberrisques et d'atteinte à la vie privée
☐	Plans de poursuite des activités
☐	Plans de reprise après sinistre
☐	Ententes requises par la loi, telles que le « Data Processing Addenda » (Addenda relatif au traitement des données) et le « Business Associate Agreement » (accord de partenariat).

ATTÉNUATION DES INCIDENTS DE SÉCURITÉ ET DE DONNÉES

Procédures et dossiers relatifs aux atteintes à la sécurité des données : Comme l'exigent les lois canadiennes sur la protection des renseignements personnels, les entreprises doivent établir des procédures de notification des personnes touchées et des organismes de réglementation et tenir des dossiers sur les incidents de sécurité. Il faut repérer tout incident de sécurité ou atteinte à la sécurité des données mettant en cause l'infrastructure des technologies de l'information de l'entreprise cible ou la collecte, l'utilisation, le stockage et la transmission de renseignements personnels ou confidentiels par celle-ci.

Certificats : La documentation liée aux certificats de conformité aux normes de l'industrie comme ISO 27001 et NIST, ainsi que les certificats propres aux technologies de l'information, comme la norme PCI-DSS pour les informations des cartes de paiement si nécessaire, sont des indicateurs préliminaires utiles attestant que l'entreprise cible a mis en œuvre des mesures de sécurité pour assurer des contrôles d'ordre physique, technologique et organisationnel conformes aux normes de l'industrie, comme l'exige la législation canadienne. Sans égard aux certificats obtenus, un contrôle préalable opérationnel complet de la posture en matière de sécurité de l'entreprise cible pourrait être nécessaire, selon le type d'opération.

Audits : Qu'ils soient effectués à l'interne ou à l'externe, les audits peuvent aider à préciser le niveau de risque que l'acheteur acquiert, une information qui peut revêtir une grande importance pour l'opération ou servir à orienter la stratégie technologique de l'acheteur après la conclusion de la vente. Les résultats d'exercices en table ronde et d'essais de pénétration récents peuvent également être utiles pour évaluer la posture en matière de sécurité de l'entreprise cible.

Police de cyberassurance : Il est maintenant pratique courante pour les entreprises de souscrire une assurance responsabilité à l'égard des cyberrisques, mais les acheteurs doivent avoir une idée exacte de la couverture réelle et des réclamations présentées à ce jour par l'entreprise cible au titre de cette police.

TRANSFERTS DE DONNÉES À DES TIERS

Clauses relatives au transfert de données et à la protection des renseignements personnels dans les contrats avec des fournisseurs et des clients : L'entreprise cible dispose-t-elle de clauses contractuelles qui protègent les renseignements personnels qu'elle recueille et transfère à des tiers pour leur traitement? Quels sont les engagements pris par l'entreprise cible en ce qui concerne la protection des données qui lui sont fournies? Tous les contrats importants conclus avec des consommateurs et des fournisseurs qui prévoient le transfert de renseignements personnels doivent être analysés avec ces questions à l'esprit.

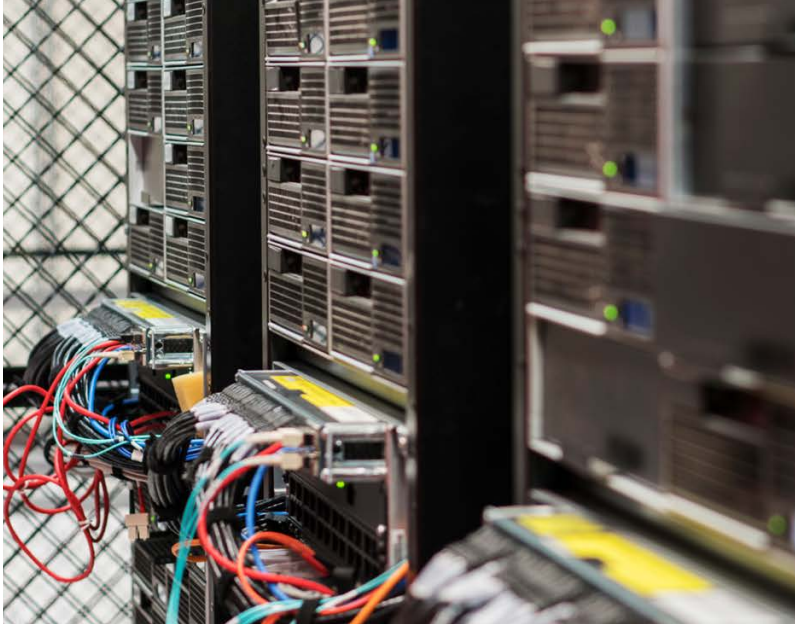
Dans les accords commerciaux, une variabilité importante subsiste en ce qui concerne les indemnités, les déclarations et les garanties dans les secteurs de la cybersécurité et de la protection des renseignements personnels.

Dans les accords commerciaux, une variabilité importante subsiste en ce qui concerne les indemnités, les déclarations et les garanties dans les secteurs de la cybersécurité et de la protection des renseignements personnels. Une entreprise cible qui traite des renseignements personnels au nom de ses clients peut être exposée à un risque considérable si elle a accordé des indemnités trop larges ou n'a pas limité sa responsabilité.

ÉLÉMENTS À CONSIDÉRER POUR LES TRANSFERTS TRANSFRONTALIERS

Transferts transfrontaliers de données : Il faut déterminer si l'opération pourrait être touchée par l'adoption récente d'une législation provinciale sur la protection des renseignements personnels ou par la jurisprudence de l'UE sur les transferts transfrontaliers de renseignements personnels.

- **Projet de loi nº 64 :** Avant de transférer des renseignements personnels à l'extérieur du Québec, il faut réaliser une évaluation des facteurs reliés à la vie privée tenant compte de la sensibilité du renseignement personnel, de l'usage auquel ils sont destinés, des mesures de protection et du régime juridique applicable dans le territoire de destination.



- **Schrems II :** L'arrêt Schrems II rendu par la Cour de justice de l'Union européenne a invalidé le bouclier de protection des données UE-États-Unis. À présent, les entreprises souhaitant transférer des renseignements personnels de l'UE aux États-Unis doivent effectuer une évaluation de l'impact du transfert. Soyez à l'affût de tout contrat avec un client ou un fournisseur qui prévoit le transfert de renseignements personnels de l'UE aux États-Unis.

Attention à la LCAP : Les investisseurs internationaux sont souvent surpris de constater qu'une violation de la Loi canadienne anti-pourriel (LCAP) donne lieu à des amendes dont le montant peut atteindre 10 millions de dollars. Ce dont vous aurez besoin :

- Un exemplaire de la politique de l'entreprise cible en matière de conformité à la LCAP;
- Une description de la façon dont l'entreprise cible se conforme à la LCAP, en particulier en ce qui concerne les conditions d'envoi des « messages électroniques commerciaux » (« MEC »), les destinataires des MEC et les mécanismes de désabonnement;
- Des exemples de MEC;
- Toutes les plaintes et les avis du gouvernement liés à la LCAP.

Vous pouvez commencer le volet du contrôle préalable concernant la LCAP avant d'avoir reçu ces documents. Par exemple, si les utilisateurs du site Web d'une entreprise sont invités à remplir un formulaire afin de s'inscrire à une liste d'envoi, il s'agit d'une bonne indication initiale que l'entreprise sollicite un consentement exprès comme l'exige la LCAP. Par contre, une entreprise dont la page « Pour nous joindre » accessible au public contient une case de consentement déjà cochée pour s'abonner à l'infolettre de l'entreprise contrevient à l'obligation prévue dans la LCAP d'obtenir un consentement exprès distinct avant d'envoyer des MEC (sauf exception applicable).

Actions collectives et litiges en matière d'atteinte à la protection des données au Canada

LE NOUVEAU RÉGIME APPLICABLE AUX ACTIONS COLLECTIVES REND L'ONTARIO MOINS INTÉRESSANT POUR LES DEMANDEURS

En octobre 2020, les modifications apportées à la Loi de 1992 sur *les recours collectifs* de l'Ontario sont entrées en vigueur, mettant en œuvre plusieurs changements quant à la procédure et au fond qui rendent plus difficile la tâche d'intenter un recours collectif fondé sur une atteinte à la protection des données dans cette province.

Le changement de fond le plus important apporté au texte de loi est le durcissement des conditions devant être réunies à l'étape de la certification. Influencée par le modèle en vigueur aux États-Unis, l'analyse du meilleur moyen exige maintenant des demandeurs d'établir que les questions communes prédominent sur les questions individuelles, et qu'un recours collectif est supérieur à tous les autres moyens raisonnablement disponibles pour établir le droit des membres du groupe à une mesure de redressement ou examiner la conduite reprochée au défendeur. Ces exigences contrastent fortement avec les anciens critères (et avec ceux qui demeurent en vigueur dans bon nombre d'autres provinces) aux termes desquels il suffisait d'établir qu'il existait certaines questions communes dont la résolution ferait progresser le règlement du litige. Les modifications imposent également des changements d'ordre procédural susceptibles de compliquer la tâche des demandeurs qui veulent faire valoir leurs réclamations en Ontario, notamment une nouvelle présomption selon laquelle toute motion présentée par le défendeur en vue de régler l'instance doit être entendue et réglée avant la motion en certification des demandeurs.

> **Les plaignants réclament souvent des dommages-intérêts pour l'anxiété, les inconvénients et le risque de l'utilisation abusive future de leurs informations résultant d'une violation de données, telle que le vol d'identité. Cependant, de plus en plus, de telles affirmations peuvent sembler opportunistes et infondées**

Dans l'ensemble, ces modifications font de l'Ontario un endroit moins intéressant pour les demandeurs qui souhaitent y intenter un recours collectif fondé sur une atteinte à la protection des données. Comme le prédisaient bon nombre d'observateurs, l'année suivant l'entrée en vigueur de ces modifications en Ontario a été marquée par une augmentation notable du nombre de demandes de recours collectifs déposées dans les autres provinces de common law, notamment la Colombie-Britannique et l'Alberta.

LES TRIBUNAUX SONT DE PLUS EN PLUS SCEPTIQUES À L'ÉGARD DES ACTIONS COLLECTIVES FONDÉES SUR UNE ATTEINTE À LA PROTECTION DES DONNÉES; NÉCESSITÉ DE RENFORCER L'IMPORTANCE DE L'ATTÉNUATION DES INCIDENTS APRÈS L'ATTEINTE

Pendant que les demandeurs continuent d'intenter des actions — qui sont souvent des actions collectives — à la suite d'une atteinte à la sécurité des données, la vraie question est de savoir si la communication réelle ou potentielle des renseignements personnels a bel et bien causé un préjudice aux individus visés. Au cours de la dernière année, les tribunaux ont commencé à porter un regard plus critique sur les allégations de dommages minimes ou hypothétiques.

Les demandeurs réclament réparation en alléguant des dommages comme l'anxiété, les désagréments et le risque d'une utilisation future inappropriée de leurs renseignements personnels découlant de l'atteinte à la protection des données, par exemple le vol d'identité. Toutefois, de plus en plus souvent, de telles réclamations peuvent apparaître comme opportunistes et non fondées. Les cyberattaques et les pertes de données qu'elles peuvent entraîner sont à présent généralement considérées comme des événements courants, et non pas exceptionnels. De plus, bon nombre d'entreprises répondent aux atteintes à la sécurité des données en offrant des services comme la surveillance du crédit pour réduire le risque de préjudice futur. Une fois qu'un recours collectif a franchi toutes les étapes jusqu'au tribunal, il est rare que les pertes subies alléguées par les personnes inscrites au recours collectif proposé soient corroborées par une preuve quelconque.

Les tribunaux canadiens ont scruté à la loupe les recours fondés sur une atteinte à la protection des données et, dans de nombreux cas, les ont rejetés ou ont refusé de les certifier au motif de l'inexistence d'une preuve établissant que les personnes inscrites au recours collectif avaient réellement subi un dommage indemnisable.

En 2021, les tribunaux canadiens ont scruté à la loupe les recours fondés sur une atteinte à la protection des données et, dans de nombreux cas, les ont rejetés ou ont refusé de les certifier au motif de l'inexistence d'une preuve établissant que les personnes inscrites au recours collectif avaient réellement subi un dommage indemnisable. Par exemple :

- Dans l'affaire *Lamoureux c. Organisme canadien de réglementation du commerce des valeurs mobilières (OCRCVM)*, la Cour supérieure du Québec a rejeté sur le fond une action collective autorisée au motif que le demandeur n'avait pas établi qu'il avait subi un préjudice dépassant le seuil des désagréments et des anxiétés de la vie courante, lesquels ne sont pas indemnisables.
- Dans l'affaire *Setoguchi c. Uber B.V.*, la Cour du Banc de la Reine de l'Alberta a tenu compte de son rôle de

gardien et de la tendance récente à ne plus certifier les actions reposant sur des conséquences de peu d'importance et a refusé d'autoriser une action découlant d'une atteinte à la sécurité des données. Aucun élément de preuve n'établissait que les personnes inscrites au recours collectif avaient subi des pertes ou des préjudices — au contraire, une preuve positive indiquait qu'aucune personne n'en avait subi. Et même si certaines personnes inscrites au recours collectif avaient subi une perte, il aurait fallu tenir une multitude d'auditions individuelles pour établir le lien de causalité et les dommages, ce qui faisait de l'action collective un moyen inapproprié en l'espèce.

- Dans les affaires *Simpson c. Facebook* et *Kish c. Facebook*, les tribunaux de l'Ontario et de la Saskatchewan ont refusé d'autoriser une action collective pour atteinte à la protection des données par Cambridge Analytica au motif qu'aucun élément de preuve n'indiquait que les renseignements personnels des utilisateurs canadiens de Facebook aient été partagés de façon inappropriée et que, par conséquent, il n'y avait pas de question commune en lien avec l'atteinte à la vie privée qui pouvait être autorisée.
- Dans l'affaire *Kaplan c. Casino Rama Services Inc*, la Cour supérieure de justice de l'Ontario a refusé de certifier un recours collectif au motif qu'aucune preuve n'établissait qu'un des membres du groupe avait subi quelque préjudice que ce soit, notamment parce que le défendeur avait réagi à l'incident de façon exemplaire. Il avait [Traduction] « communiqué avec toutes les autorités compétentes, pris des mesures pour fermer les deux sites Web qui contenaient les renseignements volés, avisé les milliers de clients, d'employés et de fournisseurs susceptibles d'être touchés par l'atteinte à la protection des données, et offert à bon nombre d'entre eux des services gratuits de surveillance du crédit ».

Dans l'avenir, les défendeurs qui sont victimes d'une cyberattaque peuvent s'attendre, en défense d'une action collective, à insister davantage sur l'absence de préjudice subi par les personnes inscrites à l'action collective et sur la robustesse de leur réaction à l'incident et des mesures prises pour réduire les risques de préjudice pour les demandeurs potentiels.

RENSEIGNEMENTS PRIVILÉGIÉS? LE DÉBAT SUR LES RAPPORTS D'ENQUÊTE D'EXPERTS EN CRIMINALISTIQUE NUMÉRIQUE

Les avocats qui conseillent des entreprises ayant subi une atteinte à la protection des données retiennent généralement les services d'experts en criminalistique numérique pour faire enquête sur l'incident et produire un rapport qui sera utilisé par les conseillers juridiques. Ces rapports jouent un rôle essentiel, car ils permettent à l'avocat de donner à ses clients un avis juridique honnête sur l'atteinte à la sécurité des données et le litige connexe et sont censés avoir un caractère privilégié et confidentiel. Toutefois, les demandeurs et les organisations peuvent tenter de forcer la production de ce rapport dans le cadre du litige ou d'une enquête réglementaire.

Les avocats qui conseillent des entreprises ayant subi une atteinte à la protection des données retiennent généralement les services d'experts en criminalistique numérique pour faire enquête sur l'incident et produire un rapport qui sera utilisé par les conseillers juridiques.

Plusieurs décisions récentes rendues aux États-Unis portent sur cette question et démontrent que dans certaines circonstances, les rapports d'enquête d'experts en criminalistique numérique peuvent être vulnérables à la contestation de leur caractère privilégié si les mesures protectrices appropriées ne sont pas prises. Par exemple, dans l'affaire *In re Capital One Customer Data Security*

Breach Litigation, un tribunal de l'État de Virginie a statué qu'un rapport d'enquête d'un expert en criminalistique numérique n'avait pas un caractère privilégié parce qu'il n'avait pas été élaboré aux fins du litige : les services de l'enquêteur expert en criminalistique numérique qui l'avait préparé avaient été au préalable retenus par l'entreprise dans le cadre d'un engagement non couvert par le privilège du secret professionnel et, même si les avocats de l'entreprise avaient signé une nouvelle lettre d'engagement de l'enquêteur à la suite de l'incident, la portée du travail était demeurée la même. La Cour a de plus conclu que, même si le rapport avait été couvert par le privilège du secret professionnel, l'entreprise y avait renoncé en communiquant son contenu à son vérificateur, aux organismes de réglementation et à certains de ses employés. De même, dans l'affaire *In re Rutter's Data Security Breach Litigation*, un tribunal de l'État de Pennsylvanie a statué qu'un rapport d'enquête n'était pas couvert par le privilège du secret professionnel parce que le rapport avait été établi pour déterminer si une atteinte à la protection des données avait eu lieu — et non pas pour étayer la défense de l'entreprise dans le cadre du litige.

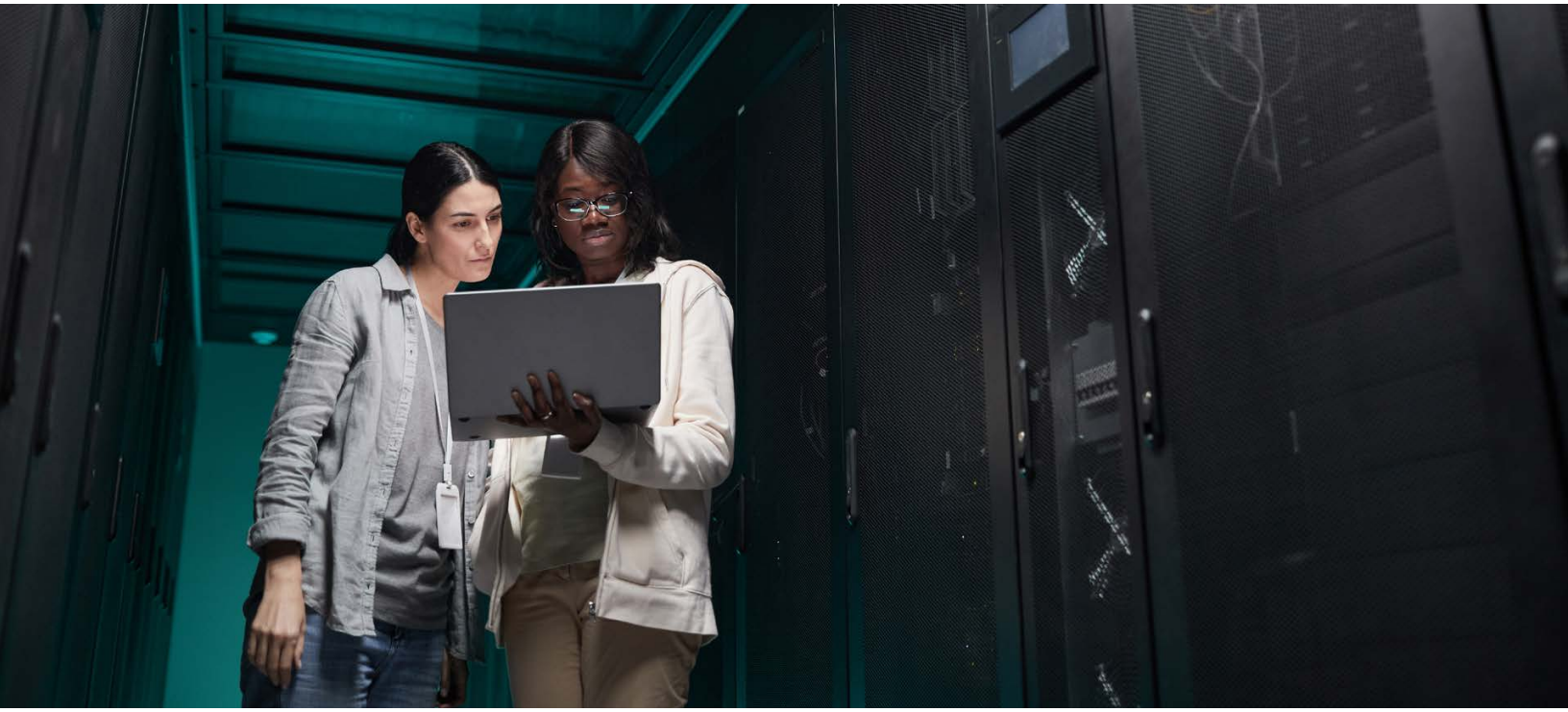
Les décisions rendues par les tribunaux américains, même si elles reposent sur le droit américain sur les privilèges, sont annonciatrices d'enjeux dont seront vraisemblablement saisies de plus en plus souvent les cours canadiennes. Par exemple, dans l'affaire *Kaplan c. Casino Rama Services Inc.*, la Cour supérieure de justice de l'Ontario a conclu que l'entreprise avait renoncé à un privilège sur certaines sections des rapports d'enquête de criminalistique numérique préparés à la suite d'une atteinte à la sécurité des données en divulguant le nombre de personnes touchées par cet incident.

À l'avenir, les organisations devront envisager la possibilité que les organismes de réglementation ou les avocats de la partie demanderesse demandent la divulgation des rapports d'enquête et contestent tout privilège allégué à leur égard. Les entreprises doivent agir en conséquence pour protéger ce privilège. Elles devront notamment élaborer, en concertation avec leurs conseillers juridiques, un plan d'intervention en cas d'incident et une stratégie de préservation du privilège, tant pour les rapports d'enquêtes de criminalistique numérique que de façon plus générale. Selon toute vraisemblance, il va devenir de plus en plus important de s'assurer de mettre à contribution les conseillers juridiques et de structurer les mandats des experts de façon appropriée pour prévenir la perte du privilège qui y est rattaché.

TENDANCES DANS LE SECTEUR DE LA CYBERASSURANCE

Les assureurs réduisent la couverture des cyberrisques

La souscription d'une assurance couvrant les coûts des litiges et des interventions en cas d'incident advenant une atteinte à la protection des données continue d'être



un moyen important de gestion du risque. Toutefois, le passage au télétravail pendant la pandémie de COVID-19 et l'avalanche de cyberattaques qui s'en est suivie ont rendu les polices de cyberassurance fort coûteuses pour les assureurs. Sans surprise, au cours des 12 derniers mois, les assureurs ont rapidement ajusté leurs approches et leurs offres dans ce domaine.

Tout d'abord, il devient de plus en plus courant pour les assureurs d'offrir des polices expressément pour les cyberrisques et de refuser la couverture des cyberincidents au titre d'une assurance de responsabilité civile commerciale ou d'une police autre qu'une cyberassurance. Bon nombre d'assureurs, dans le but d'exclure la couverture soi-disant « silencieuse » des cyberrisques, ont inséré des clauses d'exclusion des « données » dans leurs polices de cyberassurance. Dans l'affaire *Family and Children's Services of Lanark, Leeds and Grenville c. Co-operators General Insurance Company*, la Cour d'appel de l'Ontario a donné une interprétation large à l'une de ces clauses d'exclusion des « données » dans une assurance de responsabilité civile commerciale et a statué que celle-ci excluait bel et bien la couverture des litiges liés à une atteinte à la protection des données.

Il sera de plus en plus hasardeux pour les entreprises de s'appuyer sur des polices autres qu'une cyberassurance pour couvrir des cyberattaques et des atteintes à la protection des données. La décision rendue dans l'affaire Co-operators est le signe d'un tournant dans l'interprétation que font les tribunaux des polices autres que les cyberassurances en faveur de l'exclusion de la couverture des atteintes à la protection des données. Si certaines polices d'assurance responsabilité civile générale, d'assurance responsabilité civile des dirigeants et des administrateurs et d'autres polices peuvent continuer à offrir une couverture des données selon leur libellé, la meilleure pratique est, et continuera d'être, de disposer d'une police adéquate propre aux cyberrisques.

Les assureurs paient plus près attention à la sécurité informatique aux questionnaires que les assurés doivent à remplir lors de la demande ou renouvellement de la cyber-assurance.

Ensuite, les assureurs prêtent davantage attention aux questionnaires sur la sécurité des TI que doivent remplir les titulaires de polices au moment de souscrire ou de renouveler une police de cyberassurance. Désormais, les entreprises peuvent s'attendre à ce que les assureurs leur imposent de répondre à des questionnaires plus détaillés et exhaustifs, voire de mettre en œuvre certaines mesures de sécurité des données avant de leur accorder une quelconque couverture. Ces questionnaires sont importants; les assureurs peuvent s'appuyer sur toute réponse erronée ou incomplète pour refuser ou limiter la couverture après un incident. Les entreprises devraient investir le temps nécessaire pour fournir des réponses exactes et complètes au questionnaire de l'assureur pour éviter de compromettre leur couverture.

Conserver la liberté de choix des prestataires de services

Avec l'essor des polices d'assurance couvrant expressément les cyberrisques, les assureurs sont de plus en plus susceptibles d'exiger des détenteurs de police qu'ils obtiennent une approbation pour tout tiers prestataire de services qui est embauché pour intervenir en cas d'atteinte à la protection des données, voire qu'ils choisissent ce prestataire de services à partir d'une liste de fournisseurs présélectionnés par l'assureur. Or, les tiers prestataires de services comme les conseillers juridiques externes et les experts en criminalistique numérique font partie intégrante de la réponse de l'entreprise à une atteinte à la protection des données. La faculté de choisir les prestataires de services avec lesquels l'entreprise souhaite travailler et de les faire intervenir immédiatement peut être un élément essentiel d'un plan d'intervention en cas d'incident. Les détenteurs de police doivent comprendre qu'il deviendra de plus en plus important de vérifier si leur police d'assurance impose des restrictions ou des exigences d'approbation préalable quant au choix des prestataires de services et de négocier l'approbation du prestataire de leur choix au moment de souscrire ou de faire renouveler une police (et non pas à la suite d'une atteinte à la sécurité des données).

Attaques par rançongiciel : stratégies de préparation et d'atténuation

La dépendance des entreprises envers les infrastructures connectées en raison de la pandémie de COVID-19 (et leurs investissements dans ce domaine), conjuguée à la disponibilité des cryptomonnaies, a créé un contexte propice à l'augmentation, en fréquence comme en ingéniosité, des attaques par rançongiciel. Pendant que le monde du travail poursuit sa transformation à long terme, les modalités de travail flexibles et l'accès à distance aux données des entreprises devraient continuer à fournir aux acteurs malveillants une quantité amplement suffisante de cibles potentielles. À l'instar d'autres entreprises criminelles, la cybercriminalité continue à gagner en sophistication et à calquer ses pratiques sur le milieu des affaires.

Au cours de la dernière année, l'évolution des attaques par rançongiciel – parallèlement à certaines atteintes à la sécurité des données très médiatisées dans les secteurs public et privé – a suscité des préoccupations à l'échelle internationale au sujet de la cybercriminalité et risque d'entraîner une mobilisation de la volonté politique et l'élaboration de stratégies concertées pour lutter contre cette menace dans un proche avenir. Les responsables politiques et les acteurs du milieu des affaires canadiens, y compris la Chambre de commerce du Canada, partagent également ces préoccupations. Ces événements rendent la réponse à une attaque excessivement complexe et hautement dépendante du facteur temps, car les sanctions des gouvernements étrangers ou nationaux visant les groupes de rançonneurs et les opérations de change des monnaies virtuelles peuvent faire dérailler des négociations en cours de route.

Les stratégies permettant de lutter contre la cybercriminalité, de réglementer les cryptomonnaies et de venir à bout du problème à l'échelle mondiale malgré les frontières traditionnelles entre les territoires n'en sont encore qu'à leurs débuts. Les entreprises doivent savoir que les cadres juridiques dans ce domaine sont loin d'être fixés et que leur évolution se poursuivra de façon assez régulière, allant parfois jusqu'à perturber le processus de reprise des activités après une attaque de rançonnage.

Les stratégies permettant de lutter contre la cybercriminalité, de réglementer les cryptomonnaies et de venir à bout du problème à l'échelle mondiale malgré les frontières traditionnelles entre les territoires n'en sont encore qu'à leurs débuts.

DÉFINITION DU RANÇONGICIEL

Un rançongiciel est un logiciel malveillant, ou « maliciel » qui empêche l'accès aux données et les retient en otage jusqu'à ce que l'utilisateur ciblé paie une rançon. Le plus souvent, les rançons sont payées en

cryptomonnaie, par exemple en Bitcoin.

Il existe deux formes principales de rançongiciel : (i) le rançongiciel à chiffrement, qui chiffre les données de l'utilisateur et lui remet une clé lui permettant de déverrouiller le chiffrement une fois la rançon payée, et (ii) le rançongiciel à verrouillage d'écran, qui empêche l'utilisateur d'accéder à son ordinateur ou à son appareil en ligne jusqu'au paiement de la rançon.

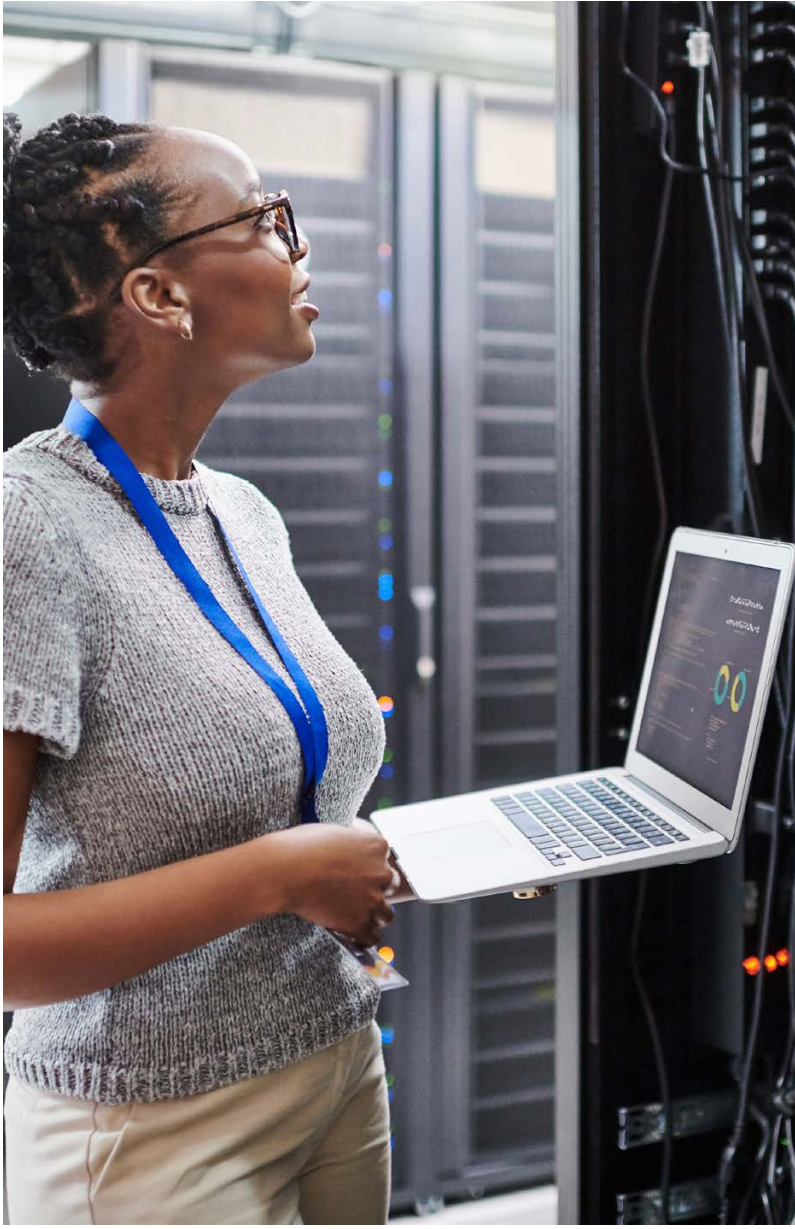
Ces méthodes sont souvent utilisées de concert avec d'autres stratégies afin de procéder à une double ou une triple extorsion, notamment le recours à des menaces de divulguer des données sensibles exfiltrées dans une attaque par rançongiciel ou de cibler directement des individus ou des clients dont les données ont été volées et de poser des gestes nuisibles à leur égard. Ces menaces additionnelles permettent aux criminels de soutirer à la victime une somme supérieure à ce qu'ils auraient reçu en échange d'un simple débrouillage des données chiffrées.

Il est également possible qu'une fois la rançon initiale payée, des niveaux additionnels de chiffrement ou de verrouillage d'écran imposent le paiement de rançons supplémentaires. Toutefois, les criminels qui se cachent derrière les principaux groupes de rançonneurs sont, en général, conscients du fait qu'ils profitent d'une « prime de marque » tant qu'ils préservent leur réputation de tenir parole. Une partie qui promet de déchiffrer les données, mais qui ne le fait pas pourra difficilement gagner la confiance des prestataires de services spécialisés qui viennent en aide aux entreprises dans de telles circonstances.

TENDANCES ACTUELLES EN MATIÈRE DE RANÇONGICIELS

L'évolution du rançongiciel est un exemple fascinant d'innovation dans le monde souterrain de la criminalité : tout comme les autres entreprises, les cybercriminels se diversifient. Ils sont influencés par l'évolution des technologies et des demandes du marché et évaluent en continu l'efficacité et l'efficience de leurs produits en s'inspirant de leurs concurrents.

L'*industrie* du rançongiciel est une forme extrême de changement technologique perturbateur de type entrepreneurial, qui présente plusieurs points communs avec la façon dont Napster et Pirate Bay ont perturbé les industries de la création en violant les droits d'auteur à une échelle sans précédent. Ce n'est pas une coïncidence si les acteurs du rançonnage numérique ont recours à Megaupload/Mega, un service réputé pour faciliter la



violation massive du droit d'auteur, pour dissimuler les fichiers volés de l'entreprise, ou si des systèmes de pair-à-pair sont utilisés pour diffuser les maliciels et infecter les utilisateurs à leur insu.

Ainsi, ces dernières années, nous avons vu des cybercriminels abandonner leurs stratégies initiales, axées sur des volumes élevés d'attaques, au profit d'une approche beaucoup plus sélective qui consiste à cibler les plus grandes entreprises dans le but d'exiger le paiement de sommes plus importantes. En règle générale, les cybercriminels commencent par obtenir l'accès aux données de la cible (comme leurs états financiers) et effectuer une reconnaissance *depuis* ces données avant de déclencher l'attaque réelle afin d'adapter leur demande de rançon à la situation et de tenter de chiffrer de façon plus efficace les systèmes de copie de sauvegarde. Par ailleurs, les cybercriminels ciblent de plus en plus les municipalités et les organisations de soins de santé de moindre importance, s'appuyant sur la perception voulant

qu'elles disposent de contrôles de sécurité moins robustes et qu'elles soient plus susceptibles de payer des rançons pour rétablir des services publics essentiels, en particulier en ces temps de pandémie de COVID-19.

En parallèle, l'essor du rançongiciel offert en tant que service (« RaaS ») a entraîné de profonds changements dans le paysage du rançonnage numérique, devenant le moyen d'attaque le plus utilisé (Rapport Sophos 2022 sur les menaces). Les criminels peuvent acheter sur le Web caché (ou Dark Web) des abonnements mensuels leur donnant accès à des trousses de rançongiciels conviviales, souvent assorties d'un service de soutien technique. Au lieu d'acheter des abonnements mensuels, certains utilisent plutôt un modèle de participation aux bénéfices en partageant les rançons obtenues avec le fournisseur du RaaS. Certains « fournisseurs » ont investi dans des présentations graphiques haut de gamme pour leur portail de service à la clientèle et d'édition.

Trois enseignements clés doivent être retenus de ces évolutions récentes : (i) les cybercriminels réagissent très rapidement aux nuances des événements en cours et ciblent les vulnérabilités dès qu'elles apparaissent; (ii) la diversification signifie que tout le monde, du simple individu à l'entreprise de taille moyenne ou à la grande société peut être victime d'une telle attaque au Canada; et (iii) le rançongiciel est en constante évolution, ce qui signifie que les stratégies utilisées pour les empêcher d'agir ou pour réagir après leur attaque exigent une maintenance diligente.

COMMENT SE PRÉPARER À UNE ATTAQUE PAR RANÇONGICIEL OU EN ATTÉNUER LES CONSÉQUENCES

La grande diversité des cibles et les coûts potentiels exorbitants des attaques par rançongiciel mettent en lumière l'importance pour l'entreprise d'investir dans les mesures préventives. Ces mesures consistent notamment à mettre en œuvre des systèmes et des procédures de sécurité robustes, à colmater rapidement les vulnérabilités, à effectuer des tests de pénétration, à expliquer aux employés comment les courriels d'hameçonnage et les autres rançongiciels peuvent être introduits dans un système, à réduire les surfaces d'attaque, à isoler les copies de sauvegarde des données, à superposer plusieurs couches d'accès au stockage des données en ligne et à utiliser l'authentification multifactorielle. Plus la navigation dans le système et l'accès aux données sensibles sont difficiles, moins il est probable qu'une attaque de cybercriminels puisse réussir.

Les facteurs de vulnérabilité particuliers qui doivent être examinés dans les mesures préventives sont le stockage des copies de sauvegarde, le stockage en nuage et les points d'accès à distance. Un examen fréquent des mesures préventives est également essentiel; au fil du temps, les outils qui étaient réputés être particulièrement bien protégés finissent par être victimes de l'ingéniosité des cybercriminels. Par exemple, les monnaies numériques utilisant les chaînes de blocs et les applications connexes

font de plus en plus l'objet de piratages et d'arnaques et le stockage infonuagique n'est pas non plus invulnérable. Pour en savoir plus, veuillez lire notre article intitulé Blockchain vulnerabilities – crypto hacks, blockchain forensics and legal challenges (en anglais seulement).

Même avec la mise en place de mesures préventives robustes, il n'en demeure pas moins important pour une entreprise de disposer d'un plan d'intervention en cas d'incident décrivant la marche à suivre pour réagir à une attaque de rançongiciel. Les fenêtres contextuelles du rançongiciel (comme celle dans l'image ci-dessous) sont déconcertantes, et le plan d'intervention en cas d'incident aide à prendre des décisions mesurées et efficaces, y compris en ce qui concerne le moment et la façon de faire appel à un conseiller juridique et à une expertise externe. De plus, le fait de disposer dans le plan d'intervention en cas d'incident d'instructions clairement formulées pour la restauration des données à partir des copies de sauvegarde contribuera à réduire la portée de toute atteinte à la réputation susceptible de découler du rançonnage. Pour en savoir plus, veuillez consulter notre article intitulé Ransomware : avoidance and response (en anglais seulement).

Figure 1 (Source: More Ransomware-as-a-Service Operations Seek Affiliates (bankinfosecurity.com))

Lorsqu'elle élabore un plan d'intervention en cas d'incident, l'entreprise doit également examiner les facteurs clés à prendre en considération pour déterminer si elle paie ou non la rançon. L'entreprise doit être consciente du fait que le paiement de la rançon, s'il peut être le seul moyen de récupérer les données, peut aussi en faire une cible privilégiée pour des attaques futures. Un tel paiement pourrait également constituer une violation de sanctions imposées, notamment par les États-Unis. De plus, les assureurs peuvent ne pas couvrir les coûts du paiement

3. Voir par exemple US charges two men over ransomware attacks, seizes $6M | nypost.com, U.S. charges Ukrainian and Russian in major ransomware spree, seizes $6 mln | Reuters, and Department of Justice Seizes $2.3 Million in Cryptocurrency Paid to the Ransomware Extortionists Darkside | OPA | Department of Justice

d'une rançon ou d'autres coûts liés aux attaques par rançongiciel, et les données peuvent demeurer compromises ou altérées même une fois la rançon payée.

TENDANCES FUTURES EN MATIÈRE DE RANÇONGICIELS

À brève échéance, on doit s'attendre à un accroissement des efforts de réglementation, de coopération internationale et d'application de la loi dans des secteurs d'activité voisins du rançonnage numérique comme les cryptomonnaies, les bourses de cryptomonnaies et le blanchiment d'argent. Il existe déjà quelques exemples de cas où des mesures d'application de la loi à l'endroit de cybercriminels ont été couronnées de succès et ont permis de saisir les profits tirés du rançonnage[3] , sans oublier des procès au civil où la cible d'une attaque a pu récupérer les sommes volées en cryptomonnaie. Dans les prochaines années, les cabinets d'avocats pourraient être en mesure d'aller plus loin que leur rôle principal actuel de conseillers spécialisés en intrusion et d'interface avec les autorités de réglementation et de recouvrer les fonds extorqués grâce à des procédures judiciaires spécialisées innovantes faisant appel à des ordonnances de type *Norwich Pharmacal ou Bankers Trust* ou à des injonctions de type *Mareva*, qui ont été élaborées par les tribunaux dans le cadre d'affaires récentes pour retracer et geler les gains obtenus frauduleusement. Pour en savoir plus, veuillez lire notre article intitulé Blockchain vulnerabilities – crypto hacks, blockchain forensics and legal challenges (en anglais seulement).

Les entreprises doivent toutefois être conscientes du fait que les cybercriminels continueront de modifier leurs armes pour se soustraire à l'application de la loi et à cibler les vulnérabilités. Elles devront donc continuer à surveiller les évolutions en matière de rançongiciels et à mettre à l'essai leurs mesures préventives et leur plan d'intervention d'urgence en conséquence.

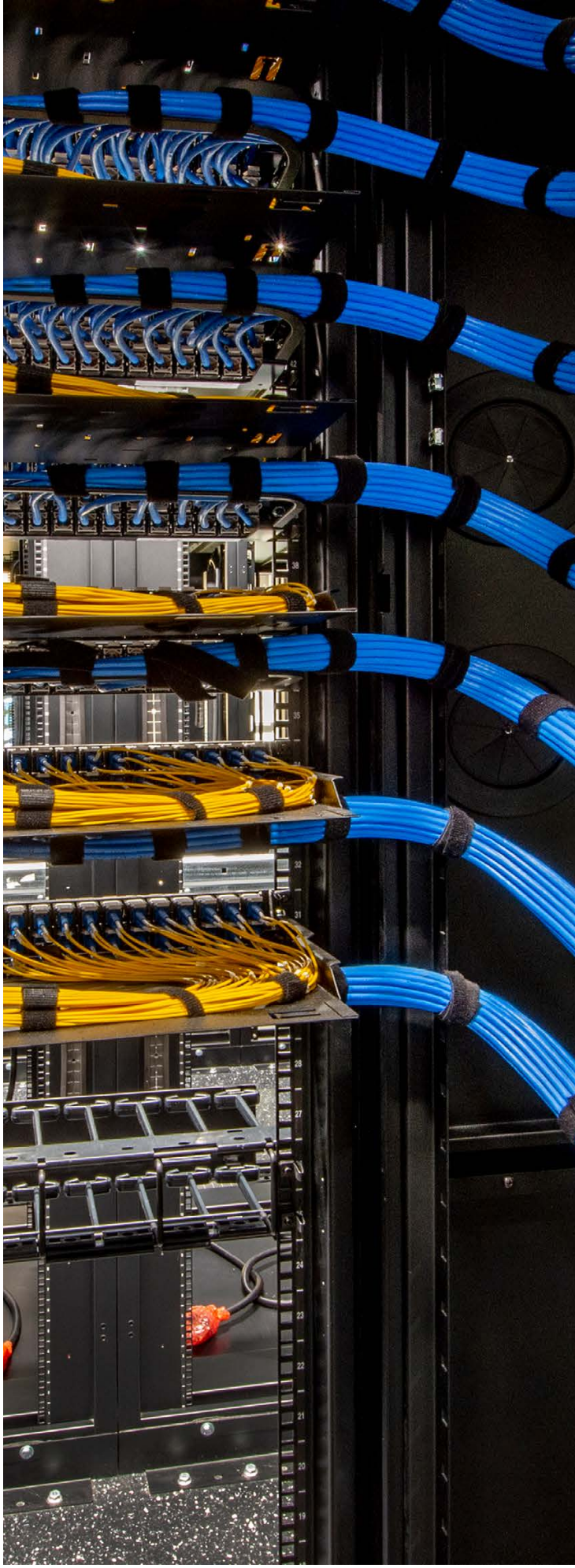
Comprendre l'intérêt de la cyberassurance

LA MONTÉE DE LA CYBERCRIMINALITÉ CIBLANT LES ORGANISATIONS

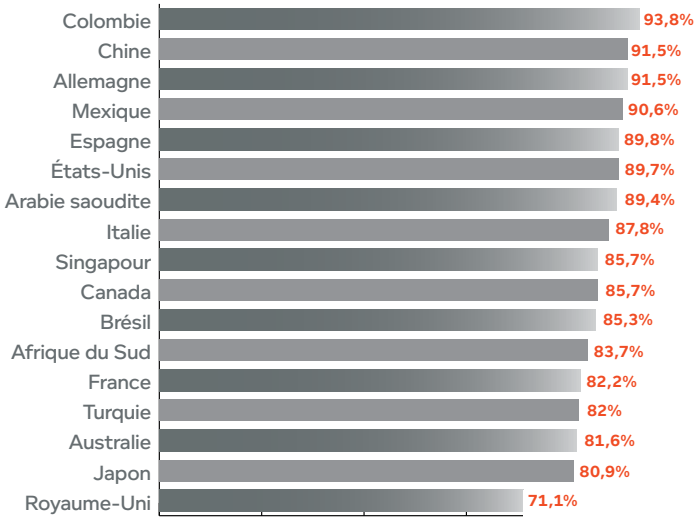
Alors que le virage numérique se poursuit à l'échelle mondiale, l'assurance est de plus en plus utilisée pour gérer les risques connexes. La pandémie de COVID-19 a accéléré le passage au numérique dans de nombreuses industries. Cette transformation s'est accompagnée d'une augmentation des cybervulnérabilités alors que les employeurs s'adaptaient aux nouvelles modalités de travail en mode hybride ou à distance. Les auteurs du Rapport Hiscox 2021 sur la gestion des cyberrisques (« rapport Hiscox 2021 ») portant sur plus de 6 000 organisations aux États-Unis et dans sept pays européens ont constaté que 43 % des répondants avaient rapporté au moins une cyberattaque en 2021. Alors que les grandes entreprises comptant plus de 1 000 employés ont renforcé leur résilience en augmentant leur budget de dépenses en cybersécurité, elles ont également été la cible de davantage d'attaques que leurs homologues de plus petite taille.

En particulier, un changement majeur au cours de la dernière année a été l'augmentation des surfaces d'attaque collectives avec l'adoption des politiques sur le télétravail et l'utilisation au travail de l'appareil mobile personnel du salarié. Le rapport Hiscox 2021 indique que plus de la moitié des employés sont en télétravail au moins à temps partiel, ce qui oblige les équipes responsables de la sécurité des TI à prioriser la sécurité des employés dispersés, et que les appareils mobiles se sont avérés être parmi les technologies les plus difficiles à protéger pour les rendre conformes à ces politiques.

Les cyberincidents sont difficiles à prévoir et à budgétiser, comme le montrent les statistiques du rapport Hiscox 2021. Le coût moyen des cyberincidents pour les grandes organisations a été plus élevé que pour celles de taille moyenne ou petite. Les coûts des cyberattaques varient en fonction de leur impact, ce qui rend impossible leur inclusion dans la planification financière. Une entreprise ciblée sur dix a dû s'acquitter d'une amende conséquente qui a nui considérablement à la santé financière de l'entreprise. Une entreprise sur six a été victime d'une attaque par rançongiciel, et plus de la moitié de ces entreprises ont versé une rançon, soit pour récupérer des données, soit pour empêcher la publication d'informations sensibles. Le magazine Canadian underwriters reconnaît que la portée et le niveau de sophistication des cybermenaces ne cessent de croître grâce au recours à l'automatisation.



Les organisations canadiennes n'ont pas été épargnées. Coalition Canada, un cyberassureur, affirme que le montant moyen de la rançon demandée à ses détenteurs de police canadiens a presque triplé depuis le début de 2020. Le rançongiciel est devenu l'une des principales causes du durcissement du marché de la cyberassurance canadien. Quelque 61 % des organisations canadiennes ont été victimes d'une attaque par rançongiciel au cours des 12 derniers mois (2021 Cyberthreat Defense Report). Les coûts moyens de remise en état pour les organisations canadiennes victimes d'une attaque par hameçonnage, y compris le montant de la rançon versée, s'élevaient à 1,92 million de dollars américains (Rapport de Sophos : L'état des ransomwares 2021). Les cybercriminels justifient les montants plus élevés des demandes en prenant en otage les cyberopérations des organisations jusqu'à leur paiement.



Pourcentage d'entreprises dont les données ont été compromises par au moins une attaque ayant réussi au cours des 12 derniers mois, par pays.

Source: 2021 Cyberthreat Defense Report, CyberEdge Group, LLC.

LE DURCISSEMENT DU MARCHÉ DE LA CYBERASSURANCE

L'évolution du climat en matière de cybermenaces a entraîné une augmentation en flèche de la demande pour les couvertures de cyberassurance. Parallèlement à la croissance de la demande, les primes de cyberassurance ont également augmenté de façon appréciable, une tendance qui devrait se poursuivre. Selon S&P Global Ratings, la croissance du montant des primes pourrait atteindre 100 % d'ici 2023. Le Bureau du surintendant des institutions financières du Canada a récemment fait état des activités de cyberassurance au cours du deuxième trimestre de 2021 des sociétés d'assurances multirisques qu'il réglemente. Le rapport a révélé un indice de perte de près de 113 % pour les assureurs en ce qui concerne la cyberresponsabilité; autrement dit, les primes et les modalités des polices actuellement en vigueur font perdre de l'argent à bon nombre d'assureurs.

Les polices portant exclusivement sur la cybercriminalité permettent aux assureurs de définir précisément la couverture et le travail à effectuer aux côtés des clients afin qu'ils soient mieux préparés aux attaques informatiques. Bon nombre de cyberassureurs ont ajusté leurs polices pour y inclure des sous-limites et des clauses de coassurance. Les assureurs sont également en train de revoir les facteurs standard en fonction desquels était jusqu'ici effectué le calcul des primes de cyberassurance. Au Canada comme à l'étranger, bon nombre d'assureurs commencent à pénaliser les entreprises qui ne parviennent pas à démontrer qu'elles ont mis en place des mesures de cybersécurité résilientes (Howden Cyber Insurance: A Hard Reset).

LA CYBERASSURANCE EST-ELLE IMPLICITEMENT INCLUSE DANS UNE ASSURANCE IARD?

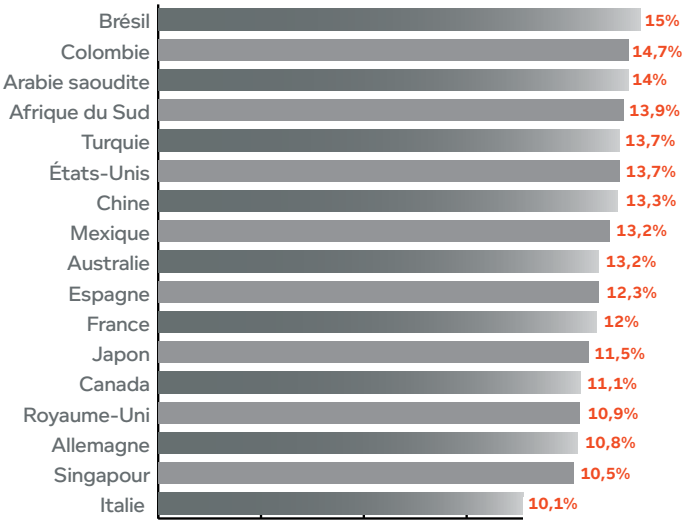
Ce qu'on appelle « cyberrisque silencieux » (ou « nonaffirmative cybercoverage ») renvoie à la couverture implicite des cyberrisques dans les polices d'assurance biens et responsabilité civile générale. Il s'agit d'une source d'incertitude majeure pour les assureurs. Tout en mettant en œuvre des polices autonomes couvrant expressément les cyberrisques, les compagnies d'assurance doivent également se défendre contre des réclamations invoquant la couverture silencieuse des cyberrisques dans des polices qui ne prévoient pas expressément une telle couverture.

Dans l'affaire *Family and Children's Services of Lanark, Leeds and Grenville v. Co-operators General Insurance Company*, la Cour d'appel de l'Ontario s'est penchée sur un litige sur la couverture silencieuse des cyberrisques par les polices d'assurance. Une cyberattaque d'un portail géré par un organisme de services aux familles et aux enfants avait entraîné le vol et la diffusion publique sur Facebook de rapports confidentiels concernant 285 personnes. L'assureur a décliné toute obligation de défendre l'organisme et son fournisseur de services de communication dans le cadre d'une action collective de 75 millions de dollars découlant de la fuite de données. Il a fondé sa position sur la clause d'exclusion des données figurant dans la police d'assurance aux termes de laquelle était exclue toute réclamation liée aux « données ». La

Cour a statué à l'unanimité que la clause d'exclusion visait de manière non ambiguë l'atteinte à la sécurité des données et la fuite dont il était question en l'espèce, ce qui excluait de fait toutes les réclamations liées aux cyberrisques. Cette décision représente un tournant dans l'interprétation par les tribunaux canadiens de telles clauses d'exclusion. Par conséquent, il est fortement recommandé aux organisations canadiennes de souscrire une police d'assurance couvrant expressément les cyberrisques. Cependant, un obstacle à l'admissibilité à une cyberassurance abordable est l'absence d'infrastructure de cybersécurité dans l'organisation.

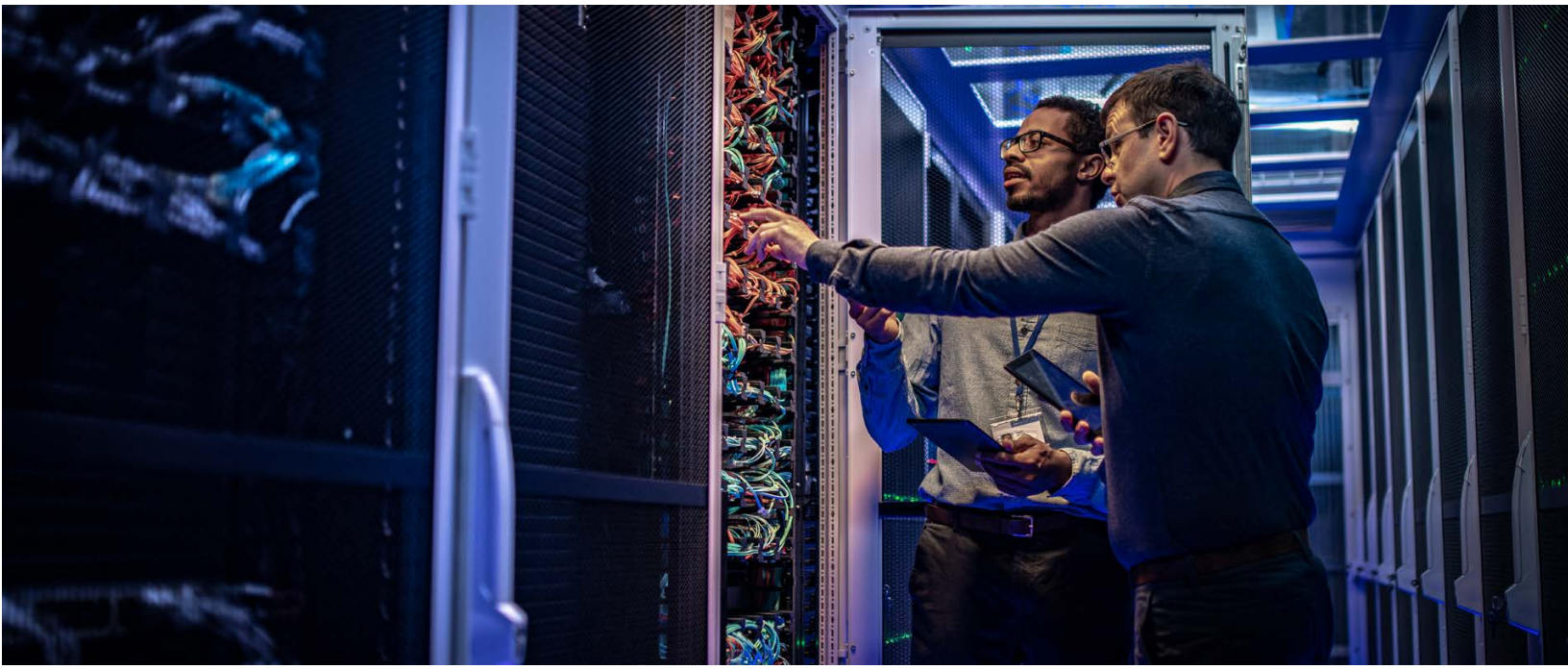
Un obstacle à l'admissibilité à une cyberassurance abordable est l'absence d'infrastructure de cybersécurité dans l'organisation.

La cybersécurité de nombreuses entreprises canadiennes est inadéquate. Dans de tels cas, il n'est pas rare que les assureurs leur imposent des primes plus élevées ou leur refusent tout simplement une cyberassurance. Le Canada figure parmi les pays industrialisés où les entreprises consacrent le plus faible pourcentage de leur budget d'exploitation à la cybersécurité. D'après le rapport 2021 Cyberthreat Defense Report, les dépenses au titre de la cybersécurité des organisations canadiennes correspondaient à 11,1 % de leur budget des TI. Ce pourcentage est bien inférieur à la moyenne mondiale, qui se situe à 12,7 %. Malgré une augmentation constante année après année de la part du budget affectée à la cybersécurité, les entreprises canadiennes doivent se montrer plus proactives à cet égard pour éviter de prendre du retard.



Pourcentage du budget des TI consacré à la sécurité, par pays.

Source: 2021 Cyberthreat Defense Report, CyberEdge Group, LLC.



Même si la pandémie a contraint de nombreuses petites entreprises à prendre ne serait-ce qu'en partie un virage numérique, les statistiques pour cette catégorie d'organisation sont encore plus préoccupantes. Les petites entreprises ne sont que 24 % à souscrire une forme quelconque de cyberassurance et 15 % seulement à disposer d'une police indépendante couvrant exclusivement les cyberrisques. Plus de la moitié des petites entreprises n'ont aucune intention de souscrire une cyberassurance au cours de la prochaine année. Les petites entreprises qui affectent des fonds à la cybersécurité y consacrent en moyenne 21 % de leur budget annuel. Par contre, elles étaient 47 % à ne prévoir aucune dépense en cybersécurité en 2021. Ce nombre est en hausse, comparativement à 33 % en 2019, ce qui indique que les petites entreprises font preuve d'une complaisance croissante malgré une intensification de la numérisation. Compte tenu des préoccupations légitimes des cyberassureurs, la première étape pour ces organisations sera de mettre en œuvre des politiques et des pratiques en matière de cybersécurité.

Les organisations canadiennes à la recherche d'une cyberassurance doivent accorder une attention particulière à plusieurs facteurs. D'abord et avant tout, elles doivent s'assurer, en scrutant à la loupe les clauses et la portée des exclusions, que la police leur offre la couverture dont elles ont besoin. Une fois le choix de la police arrêté, l'admissibilité à celle-ci et la conformité à ses clauses dépendent principalement de l'entreprise. Les assureurs évalueront le montant des primes en fonction du degré de préparation aux cyberrisques indiqué par les réponses au questionnaire. Par conséquent, les organisations ont tout intérêt à répondre à ces questions attentivement et minutieusement et à actualiser régulièrement leur situation auprès de l'assureur. Si elles privilégient le recours à certains tiers prestataires de services, elles doivent au préalable les faire approuver par l'assureur. Elles éviteront ainsi d'être contraintes de recourir à l'un des prestataires présélectionnés par l'assureur pour remplir les conditions de la police. Une fois la police en vigueur, elles doivent éviter son renouvellement automatique sans s'informer des éventuels changements ou améliorations apportés à la couverture. Pour en savoir plus, veuillez lire notre article intitulé Getting Cyber Insurance Right: 5 Practical Tips (en anglais seulement).

COMMUNIQUEZ AVEC NOUS :

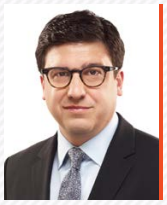
Dan Glover
coleader, groupe
Cyber/Données, associé
dglover@mccarthy.ca
416-601-806
TORONTO

Charles Morgan
coleader, groupe
Cyber/Données, associé
cmorgan@mccarthy.ca
514-397-4230
MONTREAL

Michael Scherman
technologie, associé
mscherman@mccarthy.ca
416-601-8861
TORONTO

Gillian Kerr
litiges/actions collectives,
associée
gkerr@mccarthy.ca
416-601-8226
TORONTO

Hovsep Afarian
assurance, associé
hafarian@mccarthy.ca
416-601-7615
TORONTO

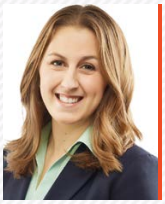


Nikiforos Iatrou
droit de la concurrence,
associé
niatrou@mccarthy.ca
416-601-7642
TORONTO

Isabelle Vendette
litiges/actions collectives,
protection des
renseignements personnels
ivendette@mccarthy.ca
514-397-5634
MONTREAL

Jade Buchanan
préparation et intervention,
protection des
renseignements personnels
jbuchanan@mccarthy.ca
604-643-7947
VANCOUVER

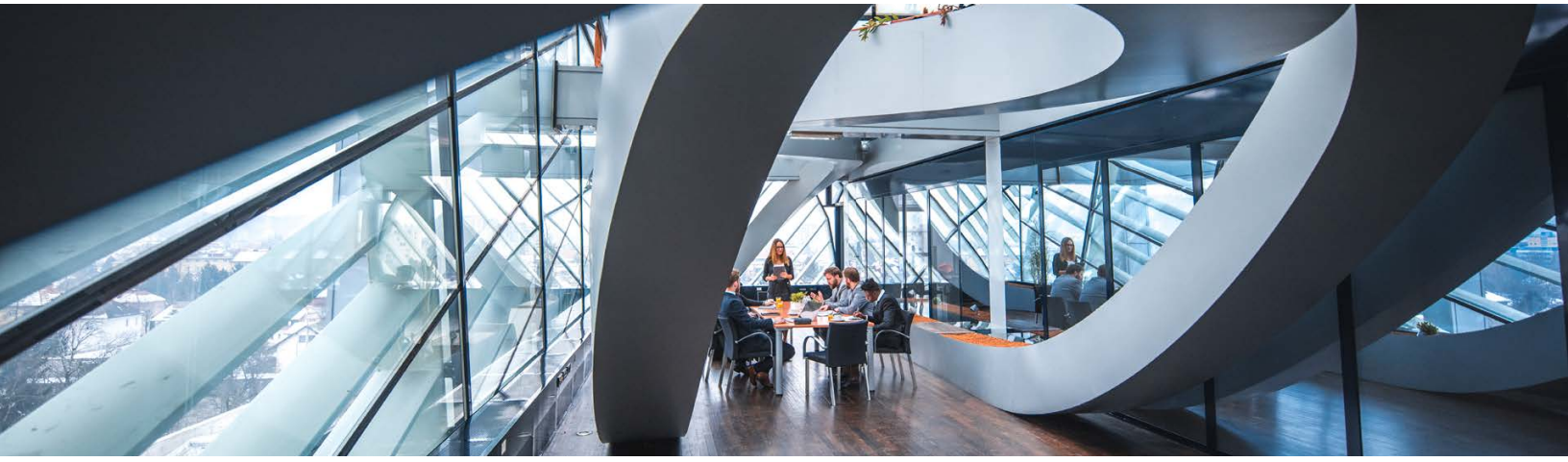
Katherine Booth
préparation et intervention
litiges/actions collectives,
associée
kbooth@mccarthy.ca
604-643-7198
VANCOUVER



Justine Lindner
du droit du travail
et de l'emploi, associé
jlinder@mccarthy.ca
416-601-8214
TORONTO

UN MERCI TOUT SPÉCIAL À

Marissa Caldwell, Ellen Chen, Jon Jacob Adessky, Erin Keogh, Cassidy Bishop, Kelsey Franks, Ella Hantho, Philippe April, Madison Howell, Todd Pribanic White, Loic Turner, Heather Mallabone, Rachael Carlson, Daniel Moholia



Contactez-nous

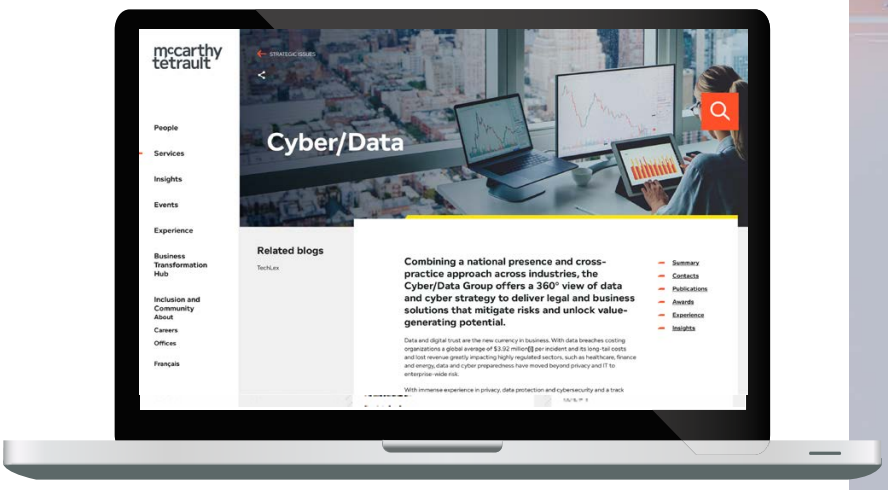
Combinant une présence nationale et une approche collaborative des groupes de pratiques dans tous les secteurs industriels, le groupe Cyber/Données offre une vue à 360° des données et de la cyberstratégie pour fournir des solutions juridiques et commerciales qui atténuent les risques et libèrent le potentiel de création de valeur. Notre équipe nationale intégrée offre également des conseils juridiques dans le cadre de mandats transfrontaliers et a conseillé des sociétés internationales lors des plus grands incidents de cybersécurité et d'enquêtes réglementaires de l'histoire du Canada, en plus d'influencer le droit canadien en matière de protection des renseignements personnels, de données et de cybersécurité comme aucun autre cabinet.

À propos de McCarthy Tétrault

McCarthy Tétrault offre une vaste gamme de services juridiques et fournit des conseils stratégiques spécialisés par secteur d'activité et des solutions dans le cadre de mandats concernant des intérêts canadiens et internationaux. Le cabinet jouit d'une forte présence dans les principaux centres d'affaires du Canada, ainsi qu'à New York et à Londres, au Royaume-Uni.

Fort d'une approche intégrée de l'exercice du droit et de la prestation de services innovants, le cabinet est en mesure de capitaliser sur ses compétences juridiques, ses connaissances sectorielles et sa vaste expérience pour aider ses clients à atteindre les résultats qui comptent pour eux.

POUR OBTENIR DE PLUS AMPLES RENSEIGNEMENTS, VEUILLEZ COMMUNIQUER AVEC LE GROUPE DE CYBER/DONNÉES ÉTRANGER DE MCCARTHY TÉTRAULT



mccarthy tétrault

VANCOUVER
Suite 2400, 745 Thurlow Street
Vancouver (Colombie-Britannique) V6E 0C5

CALGARY
Suite 4000, 421 7th Avenue SW
Calgary (Alberta) T2P 4K9

TORONTO
Suite 5300, TD Bank Tower
Box 48, 66 Wellington Street West
Toronto (Ontario) M5K 1E6

MONTRÉAL
Bureau 2500
1000, rue De La Gauchetière Ouest
Montréal (Québec) H3B 0A2

QUÉBEC
500, Grande Allée Est, 9e étage
Québec (Québec) G1R 2J7

NEW YORK
55 West 46th Street, Suite 2804
New York, New York 10036
États-Unis

LONDRES
1 Angel Court, 18th Floor
London EC2R 7HJ
Royaume-Uni