Les pandémies et la confidentialité : principales considérations sur la protection de la vie privée et la sécurité de l'information

par David Elder

Avril 2020

Parmi les nombreux défis et incertitudes liés à la pandémie de COVID-19 auxquels elles font face, bon nombre d'entreprises doivent également composer avec l'application des lois sur la protection des renseignements personnels et l'obligation corrélative de veiller à la sécurité de l'information dans le cadre de la poursuite de leur exploitation, tout en minimisant le potentiel de propagation du virus.

La réaction éventuelle d'une entreprise à la pandémie peut entraîner la collecte d'une série de renseignements personnels (ceux des employés, fournisseurs, clients et autres visiteurs de l'organisation), ainsi que l'utilisation et la communication de ces données à des fins et dans des contextes qui sortent de l'ordinaire. De plus, les plans de continuité des activités prévoient souvent des façons radicalement différentes de faire des affaires, par exemple le recours au travail à distance pour la totalité ou la majorité des employés. Ces mesures peuvent présenter des défis importants pour le maintien et la surveillance (i) des procédures de conformité aux obligations de protection des renseignements personnels en vigueur et (ii) des cadres de gestion de la sécurité de l'information existants.

Une plus grande marge de manœuvre est accordée par les lois sur la protection des renseignements personnels pendant les crises de santé publique

La bonne nouvelle pour les entreprises qui doivent composer avec les répercussions de cette crise sanitaire en évolution, c'est qu'en situation d'urgence, les lois sur la protection des renseignements personnels dans le secteur privé du Canada peuvent permettre la collecte, l'utilisation et la communication de renseignements personnels à des fins et dans des circonstances qui ne seraient pas autrement permises, notamment leur traitement sans le consentement des particuliers concernés. En outre, comme plusieurs commissaires à la protection de la vie privée canadiens ont pris la peine de le préciser, les lois sur la protection des renseignements personnels ne doivent pas faire obstacle à une communication de renseignements appropriée.

En particulier, toutes les lois sur la protection des renseignements personnels dans le secteur privé permettent le traitement des renseignements personnels sans consentement, si la loi l'exige, comme lorsqu'une autorité de santé publique a le pouvoir légal d'obliger l'organisation à recueillir ou communiquer certains renseignements (par exemple les divers états d'urgence et états d'urgence sanitaires déclarés par les provinces et les municipalités du pays lui en donnent le pouvoir). En outre, les lois sur la protection des renseignements personnels confèrent une certaine latitude, notamment sous forme d'exceptions légales formelles, qui peut permettre la collecte, l'utilisation et la communication de renseignements personnels par les entreprises sans consentement, si nécessaire dans une situation d'urgence.

La moins bonne nouvelle est que la nature et la portée de la marge de manœuvre accordée en vertu des quatre lois sur la protection des renseignements personnels dans le secteur privé du Canada varient d'un territoire à l'autre. À cet égard, les lois sur la protection des renseignements personnels dans le secteur privé

édictées par les provinces de l'Alberta, de la Colombie-Britannique et du Québec s'appliquent aux activités exercées dans ces provinces et une loi fédérale, la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE) s'applique au traitement des renseignements personnels dans le cadre d'activités commerciales exercées dans les autres provinces. La LPRPDE s'applique aussi à toutes les entreprises fédérales, sans égard aux provinces dans lesquelles elles peuvent exercer leurs activités.

Par conséquent, les organisations qui examinent les réactions à la pandémie sous l'angle des renseignements personnels doivent évaluer attentivement les exceptions et les obligations que contiennent les lois auxquelles elles sont assujetties. L'évaluation peut poser un défi en soi parce qu'il y a peu de jurisprudence canadienne sur l'application des lois sur la protection des renseignements personnels dans une situation d'urgence sanitaire de portée et de gravité semblables à la COVID-19. Par conséquent, l'incertitude plane dans une certaine mesure sur l'interprétation et l'application de ces lois par les commissaires à la protection de la vie privée pendant la pandémie.

Les lois sur la protection des renseignements personnels continuent toutefois de s'appliquer

Même si la marge de manœuvre que les lois sur la protection des renseignements personnels procurent aux organisations varie dans les situations d'urgence, les entreprises n'ont pas carte blanche : toutes les activités et initiatives qui concernent les renseignements personnels ne seront pas conformes simplement parce qu'elles ont été prises en réaction à la pandémie. Lorsqu'elles appliquent de nouvelles mesures liées à une pandémie qui nécessitent le traitement de renseignements personnels, les entreprises ne doivent pas perdre de vue l'application continue des obligations et principes fondamentaux des lois sur la protection des renseignements personnels dans le secteur privé, notamment les suivants :

1. **Consentement**

   Avant tout, les lois sur la protection des renseignements personnels dans le secteur privé requièrent généralement le consentement du particulier pour la collecte, l'utilisation et la communication de ses renseignements personnels, sous réserve de certaines exceptions légales strictes. Par conséquent, dans la mesure du possible, les initiatives liées à la pandémie qui nécessitent le traitement de renseignements personnels ne devraient généralement être lancées qu'avec le consentement des particuliers concernés, sauf si une exception s'applique.

   Même s'il est expressément envisagé dans la LPRPDE et dans les lois de l'Alberta et de la Colombie-Britannique que le consentement tacite (c.-à-d. le consentement découlant de la conduite adoptée) suffit à satisfaire l'obligation de consentement dans certaines circonstances, le consentement exprès ou formel est généralement nécessaire en lien avec la collecte et le traitement de renseignements personnels sensibles. Comme les données liées à la santé sont généralement considérées sensibles, il est probable qu'en contexte de réaction d'une organisation à la COVID-19, un consentement formel sera généralement exigé en application des lois sur la protection des renseignements personnels.

2. **Caractère acceptable**

   Même si le consentement exigé est obtenu dans la forme souhaitée, les lois sur la protection des renseignements personnels dans le secteur privé comprennent l'obligation générale voulant que le traitement des renseignements personnels doive être acceptable et légitime dans les circonstances. Afin d'établir si le traitement du renseignement personnel est acceptable, les commissaires à la protection de la vie privée ont généralement tenu compte des facteurs suivants, qui ne sont pas exhaustifs :

   a. ***Le caractère sensible du renseignement personnel en cause***. Il faut trouver un équilibre entre le droit à la vie privée du particulier et les besoins commerciaux afin d'établir le caractère acceptable; toutefois, une norme de caractère acceptable plus rigoureuse s'applique au traitement de renseignements personnels sensibles, relativement auxquels la balance penche davantage du côté des droits individuels. Comme il a été mentionné précédemment, les renseignements liés à la santé sont généralement considérés comme sensibles.

b. ***La légitimité de l'objectif de l'initiative***. La légitimité peut découler d'un intérêt commercial valable ou de l'intérêt public plus large; toutefois, lorsque des renseignements sensibles sont en jeu, le commissaire à la protection de la vie privée se demandera également si l'initiative en cause répond à une nécessité immédiate ou impérative. En règle générale, les objectifs liés à l'« aplanissement de la courbe » ou à l'atténuation de la propagation du virus dans l'entreprise seront probablement considérés comme légitimes et impératifs, même si d'autres objectifs, comme la gestion de la réputation de l'entreprise, ne seront pas considérés comme légitimes ou impératifs, lorsqu'ils reposent sur la collecte ou l'utilisation de renseignements personnels supplémentaires et, particulièrement, de renseignements personnels sur la santé.

c. ***L'efficacité de la mesure***. Dans le cadre de son analyse, le commissaire évaluera si la mesure en cause atteint ou est susceptible d'atteindre son objectif. Par exemple, les initiatives visant à réduire la propagation de la COVID sur un lieu de travail seront examinées en fonction de la probabilité qu'il existe un lien rationnel entre ces initiatives et l'objectif à atteindre. Par conséquent, si l'objectif consiste à réduire la transmission dans la communauté, il faut se demander si l'initiative aura vraisemblablement une incidence importante sur la transmission du virus, compte tenu d'un éventail de facteurs, notamment les données scientifiques et les directives des organismes de santé publique disponibles.

d. ***L'existence de solutions moins intrusives***. Afin d'établir le caractère acceptable d'une initiative de riposte à la pandémie qui nécessite le traitement de renseignements personnels supplémentaires, le commissaire se demandera également s'il existe un moyen moins intrusif d'atteindre la même fin à des coûts et avantages comparables. Dans ce contexte, il faut observer les méthodes des organisations comparables.

e. ***Proportionnalité***. Enfin, le commissaire à la protection de la vie privée se demandera si, compte tenu de tous les facteurs pertinents, l'intrusion dans la vie privée découlant d'une initiative précise est proportionnelle aux avantages perçus de l'initiative.

3. Minimisation

La minimisation des données est un principe fondamental sous-jacent aux lois sur la protection des renseignements personnels. Ce principe oblige les organisations à recueillir seulement les renseignements personnels dont elles ont raisonnablement besoin, à ne les utiliser qu'à des fins raisonnables et à les conserver uniquement le temps nécessaire à l'atteinte des objectifs précisés. Le principe comprend aussi l'obligation de communiquer les renseignements personnels de manière sélective aux employés de l'organisation, c.-à-d. lorsqu'ils en ont raisonnablement besoin pour s'acquitter de leurs fonctions. De même, lorsqu'une organisation retient les services d'un tiers qui fournit un service en son nom, le tiers devrait obtenir seulement les renseignements personnels nécessaires à la prestation du service pour lequel il a été retenu et ses propres employés ne devraient obtenir qu'un accès sélectif aux renseignements personnels. Le principe de minimisation est particulièrement important lorsqu'on traite de renseignements sensibles comme les données liées à la santé.

4. Confidentialité et sécurité

Même si, en situation d'urgence, la législation sur la protection des renseignements personnels pourrait autoriser la collecte, l'utilisation ou la communication de renseignements personnels supplémentaires sans consentement, l'obligation légale de conformité à la confidentialité et à la sécurité qui incombe à l'organisation est maintenue et s'applique à tous les renseignements personnels conservés et utilisés par l'organisation et pas seulement aux renseignements recueillis dans le cadre de sa réaction à la COVID-19. Malheureusement, la transition soudaine vers un modèle de travail à distance peut présenter des défis considérables en lien avec le respect de ces obligations.

Les lois sur la protection des renseignements personnels obligent les organisations à maintenir la confidentialité de tous les renseignements personnels sous leur contrôle et à empêcher la consultation des données par des parties non autorisées. Les organisations sont en outre tenues de protéger tous les renseignements personnels sous leur contrôle en prenant les mesures de sécurité matérielles, organisationnelles et technologiques qui conviennent au degré de sensibilité des renseignements. Le

passage rapide d'un modèle d'activités exercées au sein d'une installation de l'entreprise qui est contrôlée et sécurisée à un modèle de travail à distance peut présenter de nombreux défis de conformité continue à ces obligations.

Certaines organisations ont déjà mis en place des solutions d'accès à distance sécurisées pour leurs employés qui travaillent à distance, alors que d'autres vont devoir mettre rapidement à niveau les solutions existantes ou repartent à zéro, mais elles doivent toutes soigneusement veiller à la confidentialité et à la sécurité continues des renseignements personnels dans un environnement de travail où les ressources sont dispersées et travaillent à distance. Les entreprises qui n'ont pas de solutions d'accès à distance et opèrent la transition vers le travail à distance de manière pratiquement instantanée sont particulièrement exposées. Les nombreux enjeux de conformité potentiels en lien avec l'accès à distance sont notamment les suivants :

- **Environnement physique non sécurisé**. En fonction de leur mode de vie, les lieux à partir desquels les employés peuvent consulter ou stocker des renseignements confidentiels pourraient ne pas être physiquement sûrs, ce qui augmente le risque d'accès et d'utilisation non autorisés. En outre, même sur un lieu de vie, des colocataires, des membres de la famille et d'autres personnes non autorisées pourraient avoir libre accès aux systèmes ou aux documents papiers de l'organisation ou surprendre des conversations dans lesquelles il est question des renseignements personnels d'un client ou d'un employé. Il faut rappeler aux nouveaux télétravailleurs leurs obligations de confidentialité et de sécurité et leur donner de la formation sur la manière de travailler à distance de façon sécurisée.

- **Appareils de traitement et de communication non sécurisés**. Dans certains cas, les employés peuvent se servir de leurs ordinateurs, tablettes, téléphones intelligents et autres appareils domestiques ou personnels afin de travailler dans des documents qui contiennent des renseignements personnels. Les mots de passe, pare-feux ou protections contre les logiciels malveillants de ces appareils pourraient être insuffisants et les appareils pourraient être déjà infectés par des logiciels malveillants ou avoir des vulnérabilités connues. Toutes les tâches liées à l'emploi doivent idéalement être accomplies sur des appareils fournis par l'employeur ou au moins sur des appareils de l'employé dont l'employeur a assuré la sécurité.

- **Moyens de communication non sécurisés**. Les employés peuvent utiliser leurs comptes de courriels et leurs comptes de médias sociaux personnels pour communiquer avec leurs collègues, clients et fournisseurs. Le niveau de sécurité de ces moyens de communication pourrait être insuffisant. Les employés peuvent également utiliser des connexions Wi-Fi domestiques non sécurisées ou accéder au réseau de l'employeur sans subir de contrôles d'authentification suffisants. Il faudrait fournir aux employés des moyens de transmission cryptés sécurisés, par lesquels ils peuvent communiquer à des fins professionnelles et accéder aux systèmes de l'employeur; ces accès aux systèmes devraient être sécurisés par des solutions d'authentification à facteurs multiples.

- **Stockage des données non sécurisé**. Les employés pourraient stocker des renseignements personnels sur leurs appareils portables personnels ou dans des comptes « en nuage » gratuits et, dans les deux cas, la sécurité serait insuffisante. Les moyens d'archivage électroniques devraient être cryptés. Les employés pourraient laisser les documents sensibles sur support papier au vu et au su des autres membres de leur foyer ou n'avoir aucun moyen matériel de les conserver en toute sécurité. Il faut limiter la manipulation de documents sur support papier et, lorsqu'un employé en télétravail demande à consulter un dossier sur support papier qui contient des renseignements personnels, il faut lui fournir un classeur qui peut être verrouillé.

- **Risque plus élevé d'arnaques et de menaces provenant de logiciels malveillants**. Dans les situations inconnues et très stressantes, les employés sont particulièrement à risque d'être les victimes de tentatives d'hameçonnage ou d'installation de logiciels malveillants au moyen d'une pièce jointe à un courriel ou autrement. Un certain nombre de menaces actuelles ont été repérées. Il faut rappeler aux employés les protocoles et les astuces qui permettent de reconnaître les tentatives d'arnaque et d'installation de logiciels malveillants.

Certains commissaires à la protection de la vie privée, comme le Commissaire à l'information et à la protection de la vie privée de la Colombie-Britannique, ont également publié des astuces et des directives destinées aux organisations qui installent des espaces de travail à distance.

5. Employés

Les lois sur la protection des renseignements personnels dans le secteur privé traitent généralement les renseignements personnels des employés différemment des autres types de renseignements personnels, mais le traitement qui leur réservé varie d'un bout à l'autre du pays.

La LPRPDE et les lois applicables au secteur privé de l'Alberta et de la Colombie-Britannique prévoient expressément des exceptions larges qui permettent à une organisation de recueillir, utiliser et communiquer les renseignements personnels de ses employés sans consentement, lorsque ce traitement est nécessaire pour établir ou gérer la relation d'emploi ou pour y mettre fin; un avis portant sur les fins auxquelles leurs données seront traitées est fourni aux employés. L'interprétation qu'il faut donner à l'expression « gérer la relation d'emploi » et sa portée ne sont pas établies avec certitude, mais il est vraisemblable qu'elle comprend la collecte et l'utilisation des renseignements personnels de l'employé en vue de suivre les directives d'une autorité de santé publique et de limiter la propagation de la COVID sur les lieux de travail ou parmi les employés et les clients.

Notons que la LPRPDE s'applique au traitement des renseignements personnels dans le cadre d'une activité commerciale dans les provinces autres que l'Alberta, la Colombie-Britannique et le Québec, mais ne s'applique pas aux renseignements personnels d'un employé des autres provinces, sauf si l'employeur en cause est une entreprise fédérale.

La législation du Québec ne comprend pas d'exception précise pour les renseignements personnels de l'employé, auxquels s'appliquent des obligations légales et normes de consentement identiques à celles qui s'appliquent aux renseignements personnels du consommateur.

Bien sûr, en plus des préoccupations en matière de protection de la vie privée, la collecte et l'utilisation des renseignements personnels de l'employé et des réponses se rapportant à la pandémie peuvent aussi soulever d'importantes questions en vertu de la législation en matière d'emploi. À cet effet, les entreprises pourraient aussi consulter la page COVID-19 : Ressources en matière d'emploi du cabinet.

6. Transparence

Comme les lois sur la protection des renseignements personnels dans le secteur privé sont essentiellement fondées sur le consentement, il est important que les entreprises fassent des déclarations exactes et continues aux particuliers précisant les fins de la collecte, de l'utilisation et de la communication de leurs renseignements personnels. Même lorsque des exceptions s'appliquent aux renseignements personnels d'un employé, il faut lui fournir un avis qui précise les fins auxquelles ses renseignements serviront. Plus concrètement, le fait d'être transparent en ce qui concerne la manière dont les renseignements personnels seront utilisés par l'entreprise pendant la pandémie actuelle contribue à éviter les malentendus, l'absence de collaboration, le ressentiment et les plaintes.

7. Responsabilité

Finalement, selon un principe essentiel des lois sur la protection des renseignements personnels, les organisations sont légalement responsables du traitement convenable de tous les renseignements personnels qui sont sous leur contrôle, y compris lorsqu'ils sont entre les mains de tiers. Ce principe comprend l'obligation légale de mise en œuvre des mesures nécessaires, notamment des restrictions contractuelles, afin de veiller à ce que les tiers utilisent et protègent les renseignements personnels auxquels ils pourraient avoir accès.

Par conséquent, pendant la crise de la COVID, les organisations doivent non seulement veiller à la conformité de leurs propres cadres de télétravail aux obligations qui leur incombent aux termes des lois sur la protection des renseignements personnels, mais aussi à la conformité des fournisseurs qui traitent les renseignements pour leur compte. Dans la mesure où les entreprises cherchent à mettre en œuvre

leurs plans de continuité des activités en collaboration avec des tiers, par exemple au moyen d'une licence d'exploitation de nouvelles solutions réseau à distance, les fournisseurs en cause, leurs produits et les conditions contractuelles d'utilisation de ces produits doivent être soigneusement évalués.

Conclusion

Comme il a été résumé par le commissaire à la protection de la vie privée du Canada, toutes les organisations doivent continuer de mener leurs activités conformément à la loi et faire preuve de bon jugement pendant l'épidémie de COVID-19. Les entreprises vont devoir évaluer soigneusement la manière dont leur réaction à la pandémie pourrait influer sur leurs obligations légales liées au traitement des renseignements personnels et s'assurer que les nouvelles collectes ou utilisations de renseignements personnels sont « acceptables » et que tous les renseignements personnels continuent d'être convenablement utilisés et protégés en contexte de télétravail.

À propos de Stikeman Elliott

Stikeman Elliott est un chef de file mondial en droit des affaires canadien et la référence des entreprises canadiennes et des sociétés étrangères exploitant leurs activités au Canada. Nos bureaux sont situés à Montréal, Toronto, Ottawa, Calgary, Vancouver, New York, Londres et Sydney. Nous offrons des conseils hautement stratégiques et innovateurs à nos clients et leur proposons des solutions concrètes. Le cabinet possède un bilan exceptionnel aux États-Unis et à l'échelle internationale en matière d'opérations multiterritoriales d'envergure et est une entreprise de taille dans ses principaux domaines de pratique, notamment les fusions et acquisitions, les valeurs mobilières, le litige commercial, le droit bancaire et financier, la concurrence et les investissements étrangers, la fiscalité, la restructuration, l'énergie, le droit immobilier, le développement de projets, le droit de l'emploi et du travail et les régimes de retraite. Pour obtenir de plus amples renseignements sur Stikeman Elliott, consultez notre site Web (www.stikeman.com).

Pour obtenir de plus amples renseignements, veuillez communiquer avec votre représentant de Stikeman Elliott ou l'auteur :

David Elder
delder@stikeman.com

Abonnez-vous aux publications portant sur des sujets juridiques clés.
Visitez la section Notre savoir de Stikeman Elliott au stikeman.com/fr-ca/savoir