



Alerte de Deloitte Legal

Trouver le juste équilibre : la reprise des activités sans revenir en arrière en matière de respect de la vie privée

Le 9 juin 2020

Alors que s’amorce la réouverture des lieux de travail à travers le Canada, les employeurs sont en train de mettre en œuvre des plans de retour au travail visant à protéger la santé et la sécurité de leurs employés et de leurs clients.

Ces plans comprennent une évaluation des risques en milieu de travail, ainsi que l’identification et la mise en œuvre de diverses solutions permettant de contrôler ou d’atténuer les risques, notamment des outils de vérification de l’état de santé des employés et (ou) le traçage des contacts (pour obtenir plus de renseignements au sujet de la planification en matière de santé et de sécurité au travail, consultez notre [bulletin](#) précédent).

Personnes-ressources :

Olivier Fournier
Associé, Leader national
Deloitte Legal Canada
S.E.N.C.R.L./s.r.l.
Tél. : 514-393-8362

Hélène Deschamps Marquis
Associée, Confidentialité des
données et cybersécurité
Tél.: 514-393-8300

Charif El-Khoury
Associé, Droit de l’emploi et du
travail
Tél.: 514-393-5581

Or, étant donné que de multiples solutions envisagées nécessitent la collecte, l'utilisation et la divulgation à des tiers de renseignements personnels sur les employés et les clients, notamment sur leur état de santé, les entreprises doivent tenir compte des lois applicables en matière de protection des renseignements personnels et de la vie privée, en ce qui a trait au choix, à la conception et à la mise en œuvre de toute solution technologique.

D'ailleurs, suivant la déclaration de pandémie mondiale émise par l'Organisation mondiale de la santé, les commissaires fédéral, provinciaux et territoriaux à la protection de la vie privée ont rappelé que les lois sur la protection des renseignements personnels sont toujours en vigueur malgré la pandémie, en insistant sur le fait que les gouvernements comme les organisations devraient respecter le cadre établi¹, principalement en ce qui concerne la technologie de traçage des contacts².

En guise de contexte, quatre (4) lois régissent actuellement la protection de la vie privée au Canada. La *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE) s'applique à toute organisation à l'égard des renseignements personnels qu'elle recueille, utilise ou communique dans le cadre d'activités commerciales. En outre, les entreprises du secteur privé sous réglementation provinciale au Québec, en Colombie-Britannique et en Alberta sont également assujetties aux lois provinciales en matière de protection des renseignements personnels³.

Ces quatre lois canadiennes présentent des différences de forme, mais reposent sur les mêmes principes de base. Par contre, en ce qui concerne les employés, la LRPDE ne s'applique qu'aux renseignements personnels d'employés d'entreprises de compétence fédérale. Dans les autres provinces n'ayant pas de lois sur la protection de la vie privée, comme l'Ontario, les tribunaux ont recours au droit de la responsabilité civile et à la common law applicable pour protéger les renseignements personnels des employés.

Aperçu de certaines technologies en matière de santé et de sécurité

Selon la nature des lieux de travail, les entreprises peuvent prévoir des solutions technologiques à leurs plans de retour au travail.

Il existe deux grandes catégories de solutions technologiques pouvant être envisagées par les entreprises pour promouvoir la sécurité au travail :

- **Solutions de dépistage** – processus en vertu duquel l'employé (au moyen d'une autoévaluation) ou l'employeur évalue le risque d'infection d'une personne;
- **Traçage des contacts** – processus en vertu duquel une entité (généralement une autorité de santé publique) est en mesure de retracer les personnes avec lesquelles un individu infecté par le virus a été en contact.

Dépistage

Le dépistage vise à évaluer les facteurs de risque associés à la COVID-19. Il peut être effectué par l'employé ou par le client eux-mêmes (autoévaluation)

¹ https://priv.gc.ca/fr/sujets-lies-a-la-protection-de-la-vie-privee/renseignements-sur-la-sante-renseignements-genetiques-et-autres-renseignements-sur-le-corps/urgences-sanitaires/fw_covid/

² https://www.priv.gc.ca/fr/nouvelles-du-commissariat/allocutions/2020/s-d_20200507/

³ *Loi sur la protection des renseignements personnels dans le secteur privé* (Québec), *Personal Information Protection Act* (Alberta) et *Personal Information Protection Act* (Colombie-Britannique).

Jessica Kearsey

Associée, Droit de l'emploi et du travail
Tél. : 416-775-2302

Québec

Philippe Ross

Avocat, Droit de l'emploi et du travail
Tél. : 514-393-9704

Nasim Ghasemi

Avocate, Confidentialité des données et cybersécurité
Tél. : 514-369-9730

Nareg Froundjian

Avocat, Confidentialité des données et cybersécurité
Tél. : 514-393-6506

Ontario

Alexis Lemajic

Avocate, Droit de l'emploi et du travail
Tél. : 416-874-3436

Liens connexes :

Deloitte Legal Canada
S.E.N.C.R.L./s.r.l.

ou par un employeur ou une entreprise. Le dépistage fait généralement appel à une combinaison : (i) de questionnaires de dépistage et (ii) d'une forme quelconque de vérification des symptômes, telle la prise de température, afin d'identifier les personnes qui pourraient présenter des symptômes.

Questionnaires de dépistage – remplis par l'employé ou par l'employeur

Pour déterminer si un *employé présente un risque d'infection*, un questionnaire peut demander à l'employé : (i) s'il a voyagé récemment à l'étranger et n'a pas encore terminé sa période de quarantaine obligatoire, (ii) s'il a été en contact étroit avec une personne ayant contracté la COVID-19 ou ayant récemment voyagé à l'étranger et qui a été en contact avec l'employé dans les 14 jours suivant son retour au Canada, ou (iii) s'il présente lui-même des symptômes. De même, bon nombre d'entreprises partiellement ouvertes apposent, à l'extérieur de leur établissement, des affiches comportant quelques-unes de ces questions, encourageant ainsi les visiteurs à procéder à une autoévaluation et demandant à toute personne ayant répondu « oui » à l'une des questions de s'abstenir d'entrer sur les lieux.

D'autre part, pour déterminer si *l'infection pose un plus grand risque pour l'employé*, le questionnaire d'autoévaluation peut comporter des questions au sujet des problèmes de santé sous-jacents d'un employé (p. ex., système immunitaire affaibli ou problèmes respiratoires), le cas échéant, ou de tout autre facteur qui, de l'avis des autorités de santé publique, pourrait engendrer un risque accru pour l'individu qui contracte la COVID-19 (p. ex., l'usage du tabac).

Lorsqu'ils recueillent des renseignements à propos de l'état de santé d'un employé, les employeurs devraient éviter de recueillir plus de renseignements que nécessaire (p. ex., en demandant si l'employé a des problèmes de santé sous-jacents pouvant aggraver le risque d'infection, plutôt que d'exiger l'énumération de toutes ses conditions médicales) et indiquer clairement aux employés la raison pour laquelle ces renseignements sont recueillis. Les employeurs devraient également protéger la confidentialité de tous les renseignements concernant la santé de leurs employés et veiller à ce que ces renseignements soient communiqués uniquement en cas de nécessité, ne soient pas stockés dans les dossiers d'employé ou associés à ceux-ci et soient détruits une fois l'objectif atteint et conformément aux lois et politiques applicables.

Vérification des symptômes – questionnaire rempli par l'employé ou par l'employeur

Parmi les symptômes les plus connus de la COVID-19 sont la fièvre et une diminution du taux d'oxygène dans le sang. Dans le cadre d'une autoévaluation et vérification des symptômes à la maison, l'employeur pourrait potentiellement demander aux employés de prendre leur température et de vérifier leur taux d'oxygène dans le sang avant de se présenter au travail.

Dans le premier cas, il suffit d'utiliser un thermomètre en vente libre et, dans le deuxième cas, on utilise un oxymètre de pouls, soit un petit dispositif abordable et non intrusif qui permet, grâce à une impulsion de lumière dans le doigt, de déterminer la concentration d'oxygène dans le sang.

Une fois que les trousse de détection des anticorps contre le SARS-CoV-2 (ou COVID-19) seront plus répandues, il se pourrait que les entreprises soient tentées de demander à leurs employés de s'en servir. Par contre, nous ne pensons pas que cette autovérification des symptômes s'appliquera aux clients et à la population en général.

De plus, les entreprises pourraient adopter d'autres solutions de dépistage sur place en ce qui concerne leurs employés et leurs clients. Les solutions retenues pourraient être peu intrusives (p. ex., l'utilisation d'un thermomètre à infrarouge pour vérifier si une personne fait de la fièvre) ou plus intrusives (p. ex., l'utilisation d'un thermomètre à mercure et d'un oxymètre de pouls). Plusieurs directives ont été émises à ce sujet par les organismes de réglementation et de surveillance en matière de la protection du droit à la vie privée.

Traçage des contacts

Le traçage des contacts est un processus utilisé par les autorités de santé publique pour identifier, sensibiliser et surveiller les personnes ayant été en contact étroit avec une personne infectée. Il s'agit d'un aspect essentiel des mesures de lutte contre la propagation et d'éradication de la pandémie.

Pour recueillir les données nécessaires au traçage des contacts, les applications technologiques actuelles de façon générale (i) font appel à la technologie Bluetooth d'un téléphone intelligent pour déterminer à quel moment deux personnes ont été en contact étroit, ii) permettent à une personne infectée de procéder volontairement à une mise à jour de son état de santé et iii) avisent toute personne ayant été en contact avec la personne infectée.

Possiblement afin d'éviter de permettre à un employeur d'avoir accès aux téléphones intelligents de ses employés, ou pour faire en sorte que la technologie soit plus répandue (et, par le fait même, plus efficace), une entreprise est en train de concevoir un bracelet faisant appel à la technologie Bluetooth afin de créer un système de traçage des contacts géré par l'employeur.

Les entreprises pourraient être tentées de demander l'accès aux données d'une application de traçage des contacts et envisager la possibilité d'exiger que tous leurs employés et visiteurs installent une application quelconque pour accéder à leur lieu de travail. Nous sommes cependant d'avis que de telles mesures violeraient potentiellement les lois en vigueur en matière de protection de la vie privée (voir ci-après).

La plupart des moutures actuelles d'applications de traçage des contacts ne semblent pas permettre de recueillir des données de géolocalisation. D'ailleurs, Apple et Google ont exprimé des réticences quant à la possibilité de permettre que leur interface de programmation d'application (API) recueille de telles données. Par contre, les appareils fournis et (ou) gérés par l'employeur peuvent transmettre des données de géolocalisation (à partir de l'application GPS d'un téléphone intelligent). Il se peut que certains employeurs choisissent d'utiliser les données de géolocalisation qu'ils recueillent déjà (notamment pour assurer un suivi de leur flotte) à de nouvelles fins, notamment le traçage des contacts ou l'évaluation des risques d'infection d'une personne. Or, l'utilisation de renseignements personnels concernant les employés à des fins autres que celles pour lesquelles ces renseignements ont été recueillis soulève des préoccupations relatives au respect de la vie privée (voir ci-après).

Les applications de traçage des contacts s'appuient généralement sur le principe du consentement de l'utilisateur. En fait, Google et Apple ont fait savoir qu'elles désactiveraient l'accès à leur API dans tout territoire où l'utilisation d'une application de traçage devenait obligatoire. Certains pays sont même en train de mettre en place des mesures législatives de protection de l'exigence fondamentale du consentement de l'utilisateur. Ainsi, un projet de loi de l'Australie érigerait en infraction le fait de rendre l'accès à un lieu, un service

et, à plus forte raison, son milieu de travail conditionnel à l'utilisation d'une application de traçage des contacts.

Principes applicables en matière de protection de la vie privée

Les entreprises souhaitant mettre en œuvre l'une des solutions décrites ci-dessus afin de protéger leurs employés ou leurs clients doivent (i) avoir des fins commerciales légitimes de le faire et (ii) utiliser des solutions raisonnables eu égard à ces fins.

Le caractère raisonnable est évalué en termes de nécessité et de proportionnalité de la solution. L'analyse sera par ailleurs tributaire des faits et du contexte, selon le lieu de travail, le secteur d'activité et d'autres caractéristiques du milieu de travail.

Compte tenu de ce qui précède, une entreprise doit envisager l'adoption d'une approche à trois volets pour déterminer la solution appropriée, le cas échéant, pour gérer les risques pour la sécurité au travail associés à la COVID-19.

1. Identifier un objectif légitime

La **première étape** consiste à définir l'objectif pour lequel une solution exigeant la collecte de renseignements personnels est envisagée. Citons, à titre d'exemples d'objectifs légitimes, la protection de la sécurité des travailleurs et, dans certains lieux de travail, la santé et la sécurité des clients, des consommateurs ou des patients.

Cette analyse est faite au cas par cas et dépend des conditions du milieu de travail, ainsi que de la disponibilité d'autres solutions pour protéger la sécurité des travailleurs, notamment la distanciation sociale, le contrôle des infections et l'équipement de protection individuelle (EPI).

L'objectif de toute solution doit être établi clairement puisqu'il aura une incidence directe sur l'évaluation de sa légalité.

2. Identifier des mesures raisonnables eu égard l'objectif

La **deuxième étape** consiste à évaluer si une solution envisagée est raisonnable par rapport à l'objectif poursuivi, compte tenu des principes de **nécessité** et de **proportionnalité**. L'analyse se décline en trois étapes :

- i) Est-ce que la solution impliquant la collecte de renseignements personnels est **nécessaire et efficace** pour atteindre l'objectif poursuivi?

Une solution est **nécessaire** s'il existe un lien rationnel entre la solution et la raison pour laquelle elle a été conçue. Ainsi, une application de traçage des contacts gérée par des intérêts privés pourrait être jugée inutile et inefficace, surtout si les autorités publiques ont déjà mis en place un tel système. De même, le suivi continu des signes vitaux des employés n'est peut-être pas nécessaire.

Une solution est **efficace** si elle est fonctionnelle et si elle est fondée sur des données probantes. L'exactitude, l'efficacité et l'efficience d'une solution doivent toujours être évaluées en fonction des directives de sources externes comme les autorités de santé publique, au besoin. Par exemple, la prise de la température au moyen d'un thermomètre à infrarouge ou d'un thermomètre à mercure, combinée à un questionnaire de dépistage, pourrait accroître

l'exactitude des résultats et l'efficacité de la solution. En revanche, un système axé sur la collecte de renseignements personnels, mais donnant lieu à une évaluation inexacte des risques (ce qui a pour effet de refuser l'accès à des personnes en santé ou de permettre l'accès à des personnes infectées) n'est pas une solution efficace. Aucune solution n'est parfaitement exacte, mais le degré de précision y étant associé, incluant les faux positifs et les faux négatifs, aura une incidence sur l'analyse de l'efficacité d'une solution donnée.

- ii) Est-ce que la solution impliquant la collecte de renseignements personnels est **proportionnée** eu égard à l'objectif poursuivi?

Le principe de proportionnalité exige que les avantages d'une solution surpassent ses effets négatifs quant au droit à la vie privée. Ainsi, un système de traçage des contacts faisant appel à un dispositif portable doté de la technologie Bluetooth, qui ne permet pas d'emmagasiner des renseignements personnels à propos d'une personne, respecte probablement plus le principe de proportionnalité qu'un système exigeant l'accès à de nombreux renseignements n'ayant aucune pertinence qui sont emmagasinés dans un téléphone intelligent. De même, il pourrait être suffisant de vérifier les symptômes ou les facteurs de risque de vive voix, ou au moyen d'une alerte temporaire concernant les personnes pertinentes, sans pour autant recueillir des renseignements personnels ou créer un dossier temporaire ou permanent.

- iii) Est-ce que la solution impliquant la collecte de renseignements personnels occasionne une **atteinte minimale à la vie privée** eu égard à l'objectif poursuivi?

Une solution constitue une **atteinte minimale à la vie privée** si elle respecte les principes de nécessité, d'efficacité et de proportionnalité, et si elle porte *le moins* atteinte à la vie privée comparativement à d'autres solutions. Ainsi, il est peut-être suffisant qu'un employé indique que son taux d'oxygène dans le sang est peu élevé au lieu d'exiger le taux exact, puisqu'une telle exigence risquerait de révéler d'autres détails inutiles à propos de son état de santé. Enfin, les entreprises devront également justifier la vérification des symptômes sur place, plutôt que de se fier à l'autoévaluation des employés ou des visiteurs, la collecte d'information étant faite de manière moins intrusive dans l'intimité et le confort de leurs foyers.

3. Principes de protection des renseignements personnels dès la conception

La **troisième étape** de l'analyse d'une solution donnée par l'entreprise consiste à envisager et à appliquer des **principes de protection des renseignements personnels** dans la conception et le déploiement de celle-ci. Même si une solution est jugée raisonnable, l'entreprise doit respecter diverses considérations relatives à la protection des renseignements personnels dans le cadre de la mise en œuvre de la solution, notamment :

- i) Les entreprises doivent obtenir le **consentement** de leurs employés ou de leurs clients pour la collecte, l'utilisation et la communication de renseignements personnels à leur sujet. Il est entendu que cette exigence de consentement ne doit pas être confondue avec le droit d'une entreprise, dans certaines circonstances, d'interdire l'accès au milieu de travail à des personnes qui refusent de donner leur consentement à la collecte de données nécessaires à la solution mise en place.
- ii) Sous réserve de certaines exceptions, les entreprises peuvent utiliser ou communiquer les renseignements requis uniquement **aux fins** pour

lesquelles elles ont obtenu le consentement d'un employé ou d'un client.

- iii) Si possible, les entreprises devraient **assurer l'anonymat de la personne visée et dépersonnaliser** les données recueillies, de façon à atteindre l'objectif poursuivi sans pour autant identifier l'employé ou le client. Elles devraient également éliminer tous les dossiers contenant des renseignements personnels qui ne sont plus nécessaires à l'atteinte de l'objectif poursuivi, dans la mesure permise par les exigences législatives en matière de conservation de documents.
- iv) Les entreprises doivent mettre en œuvre des **mesures de sécurité** raisonnables afin de protéger les renseignements recueillis. L'accès aux renseignements personnels devrait se limiter aux personnes au sein de l'organisation qui ont « besoin d'en connaître la teneur » en vue d'atteindre l'objectif poursuivi (p. ex., un gestionnaire des RH, un spécialiste de la santé et de la sécurité au travail, un spécialiste de l'évaluation des risques, etc.).
- v) Les entreprises devraient évaluer et réévaluer régulièrement l'efficacité d'une solution donnée (degré de précision, faux positifs et faux négatifs) et adapter leurs processus, si cela s'avère nécessaire, afin d'atteindre l'objectif poursuivi. Elles devraient envisager des contrôles internes et externes permettant de procéder à une vérification et une évaluation de la solution mise en place.
- vi) Les employés et les clients ont le **droit de savoir** de quelle façon leurs renseignements personnels seront utilisés, qui aura accès à ces renseignements, à quel endroit ils seront entreposés, de quelle façon ils seront protégés et à quel moment ils seront détruits. Ils ont également le **droit de consulter ces renseignements** et d'en contester l'exactitude, le cas échéant. Les entreprises devraient s'attendre à des questions à ce sujet et désigner un responsable qui sera en mesure d'y répondre.
- vii) Les entreprises restent en tout temps responsables envers les employés et les clients de tous les renseignements recueillis, y compris lorsqu'elles transmettent ces renseignements personnels à de tierces parties (p. ex., des sous-traitants et des fournisseurs de services) qui utilisent, hébergent ou divulguent ces renseignements. Un certain nombre de juridictions canadiennes ont des exigences particulières en ce qui concerne les renseignements personnels des employés qui sont hébergés à l'extérieur du Canada ou de la province ou du territoire.

Enfin, pour ce qui est des employés, les employeurs devraient tenir compte des enjeux liés au moral de leur effectif et s'assurer d'avoir un plan de communication clair et efficace avant le déploiement de la solution envisagée. Pour ce qui est des clients, les entreprises ne doivent pas oublier que la confiance est la pierre angulaire de la reprise du cours normal des activités et qu'ils doivent travailler de façon proactive avec les clients afin de créer un milieu sain et sécuritaire pour toutes les parties concernées.

Si vous avez des questions au sujet de la réouverture de votre entreprise dans le respect de la protection des renseignements personnels de ceux qui franchissent vos portes, n'hésitez pas à communiquer avec l'un des membres de notre équipe du Droit relatif au respect de la vie privée ou de notre équipe du Droit de l'emploi et du travail.

Deloitte Legal Canada S.E.N.C.R.L./s.r.l.
La Tour Deloitte
1190, avenue des Canadiens-de-Montréal, bureau 500
Montréal (Québec) H3B 0M7
Canada

Ce document est publié par Deloitte Legal Canada S.E.N.C.R.L./s.r.l. à l'intention des clients et amis du Cabinet et ne doit pas remplacer les conseils judiciaires d'un professionnel. Aucune mesure ne devrait être prise sans avoir consulté préalablement un spécialiste. Vous utilisez le présent document à vos propres risques.

Deloitte Legal Canada S.E.N.C.R.L./s.r.l. est un cabinet juridique national indépendant ayant des bureaux partout au Canada et affilié à Deloitte S.E.N.C.R.L./s.r.l., une société à responsabilité limitée canadienne membre de Deloitte Touche Tohmatsu Limited (DTTL), une société fermée à responsabilité limitée par garanties du Royaume-Uni. Deloitte Legal Canada S.E.N.C.R.L./s.r.l., Deloitte S.E.N.C.R.L./s.r.l., DTTL et chacun des cabinets membres de DTTL constituent des entités juridiques distinctes et indépendantes.

Deloitte désigne une ou plusieurs entités parmi Deloitte Touche Tohmatsu Limited (DTTL), société fermée à responsabilité limitée par garanties du Royaume-Uni, ainsi que son réseau de cabinets membres dont chacun constitue une entité juridique distincte et indépendante. Veuillez consulter À propos de Deloitte afin d'en apprendre davantage sur notre réseau mondial de cabinets membres.

Deloitte souhaite offrir sur demande ses publications dans des formats accessibles et des aides à la communication.

© Deloitte Legal Canada S.E.N.C.R.L./s.r.l.