ACQUISITIONS DE SOCIÉTÉS DE TECHNOLOGIE : PALLIER LES RISQUES EN MATIÈRE DE PROTECTION DE LA VIE PRIVÉE, DE TECHNOLOGIES ET DE CYBERSÉCURITÉ

Publié le 6 décembre, 2022

Catégories: Perspectives, Publications

Sauf rares exceptions, les logiciels et les systèmes liés aux technologies de l'information (collectivement, les « **TI** ») font aujourd'hui partie intégrante des activités des entreprises. En conséquence, de plus en plus d'acquisitions concernent des sociétés de technologie, qu'il s'agisse de grands fournisseurs de TI, de jeunes pousses qui ont capté l'attention d'acheteurs ou d'investisseurs, ou même de sociétés qui vendaient traditionnellement des produits physiques, mais qui utilisent désormais les TI pour tirer des revenus de la collecte, de l'analyse ou de la monétisation de données.

Au Canada, la généralisation de la collecte, de l'utilisation, de l'échange et d'autres formes de traitement des données dans les entreprises s'accompagne pour celles-ci du risque lourd de conséquences que leur responsabilité soit engagée dans les domaines de la protection de la vie privée, des technologies et de la cybersécurité. Par exemple :

- la *Loi sur la concurrence* prévoit des sanctions administratives pécuniaires allant jusqu'à 10 millions de dollars en cas d'indications fausses ou trompeuses relatives à la protection de la vie privée[1];
- dès septembre 2023, la *Loi sur la protection des renseignements personnels dans le secteur privé* du Québec (la « **loi du Québec** ») prévoira pour les organisations contrevenantes des sanctions administratives pécuniaires pouvant atteindre 10 millions de dollars ou 2 % de leur chiffre d'affaires mondial de l'exercice précédent, selon le plus élevé des deux, et, pour certaines infractions, des amendes pouvant atteindre 25 millions de dollars ou 4 % du chiffre d'affaires mondial;
- le gouvernement fédéral a déposé récemment un projet de loi sur la protection de la vie privée des consommateurs qui, s'il est adopté, remplacera de nombreuses dispositions de l'actuelle *Loi sur la protection des renseignements personnels et les documents électroniques* (la « **LPRPDE** ») et instaurera des sanctions administratives pécuniaires pouvant atteindre 10 millions ou 3 % du chiffre d'affaires mondial de l'exercice précédent, selon le plus élevé des deux, et, pour certaines infractions, des amendes pouvant atteindre 25 millions de dollars ou 5 % du chiffre d'affaires mondial;

- les atteintes à la protection des données donnent régulièrement lieu à des actions collectives coûteuses, sans compter qu'elles ternissent la réputation des organisations en minant la confiance des clients ou des partenaires d'affaires et suscitent une couverture médiatique défavorable.

D'où l'importance, pour les acquéreurs potentiels de sociétés de technologie, d'évaluer rigoureusement la conformité de la société cible en matière de protection de la vie privée, de technologies et de cybersécurité à l'étape de la vérification diligente et, pour chacune des parties, de veiller à ce que les risques et les responsabilités soient adéquatement répartis dans la convention d'acquisition.

Vérification diligente

Les organisations envisageant d'acquérir une société de technologie ont tout intérêt à scruter minutieusement ses pratiques et procédures antérieures et courantes en ce qui concerne la protection de la vie privée, les technologies et la cybersécurité. Si la société cible a de piètres pratiques de traitement des renseignements personnels, emploie des TI désuètes ou qui ne sont plus prises en charge par leurs fournisseurs ou a des contrôles inadéquats en matière de sécurité de l'information, l'acquéreur pourrait devoir investir massivement pour rendre ces éléments conformes à la loi, et il pourrait s'exposer aux risques financiers et réputationnels mentionnés précédemment.

Les documents et les informations à demander dans le cadre de la vérification diligente varieront selon les circonstances. Souvent, le personnel technique de l'acquéreur ou un consultant externe peut procéder à la vérification concernant les technologies en même temps qu'est menée la vérification d'ordre juridique. Voici des exemples de choses qui peuvent être demandées relativement à la protection de la vie privée, aux technologies et à la cybersécurité :

- une liste de toutes les TI que la société cible possède ou utilise sous licence (indiquant lesquelles sont exclusives et lesquelles appartiennent à des tiers) et des exemplaires des contrats de licence et autres conventions relatives à l'utilisation de TI de tiers;
- une description des renseignements personnels que la société cible recueille, détient ou traite autrement dans le cadre de ses activités;
- des exemplaires des politiques et procédures relatives à la protection de la vie privée, à la sécurité des données et aux TI, notamment les plans d'intervention en cas d'atteinte et les plans de reprise après sinistre, les procédures de sélection et de gestion des fournisseurs et des prestataires de services ainsi que les procédures de gouvernance et de gestion des risques en matière de cybersécurité;
- des informations sur les audits menés sur la protection de la vie privée et la cybersécurité, y compris leur fréquence, des exemplaires des rapports récents et les mesures prises pour corriger toute lacune relevée;
- des informations concernant ou mesurant l'efficacité, la sécurité, la disponibilité ou l'intégrité des TI de la

société cible;

- des informations sur les moyens qu'emploie la société cible pour obtenir les consentements, les consigner et y donner effet (ainsi que pour consigner les retraits de consentement et y donner effet), y compris des exemplaires des avis relatifs à la protection de la vie privée et des formulaires de consentement;
- des informations sur les mesures que prend la société cible pour protéger les TI et les renseignements personnels;
- des informations sur la formation que reçoit le personnel sur la conformité en matière de protection de la vie privée et de cybersécurité, et des exemplaires des conventions que doivent signer les employés sur ces sujets;
- des informations sur toute atteinte importante ou récente à la protection de la vie privée ou à la cybersécurité (les « **atteintes** »);
- des informations sur toute réclamation, toute plainte, tout litige ou toute mesure d'application de la réglementation, réel ou menacé, lié à la protection de la vie privée ou à la sécurité des données;
- des exemplaires de tous les contrats contenant des clauses de protection de la vie privée et de protection des données (p. ex., des accords d'échange de données ou des dispositions pertinentes d'accords de services);
- un exemplaire de toute police d'assurance relative à la cybersécurité.

En somme, l'objectif poursuivi dans le cadre d'une vérification diligente est de comprendre : 1) la manière dont la société cible procède pour recueillir, utiliser, stocker, protéger et communiquer les renseignements personnels et d'autres informations sensibles; et 2) les niveaux de performance, l'adéquation, la convenance et l'évolutivité des TI de la société cible, compte tenu de ses activités et de ses plans d'affaires. Ainsi éclairé, l'acquéreur sera en mesure d'évaluer la conformité à la loi et de cerner les risques, dont ceux qui pourraient engager sa responsabilité.

Communication de renseignements personnels

S'il peut être nécessaire qu'une société cible communique certains renseignements personnels à un acquéreur dans le cadre d'une vérification diligente, les organisations doivent aussi savoir où leurs obligations s'arrêtent.

Par exemple, selon la LPRPDE, dans le contexte d'une éventuelle transaction commerciale, des renseignements personnels peuvent être communiqués sans le consentement des personnes concernées uniquement s'ils sont nécessaires pour décider si la transaction aura lieu et, le cas échéant, pour l'effectuer[2]. Des restrictions analogues sont prévues dans les lois de l'Alberta[3], de la Colombie-Britannique[4] et du Québec[5] qui encadrent la protection de la vie privée dans le secteur privé (les « **lois provinciales** »).

En d'autres termes, les lois canadiennes sur la protection de la vie privée interdisent les demandes générales et non balisées de communication de renseignements personnels dans le cadre des exercices de vérification diligente. Les parties doivent plutôt échanger la plus petite quantité de renseignements nécessaire dans les circonstances. Par exemple, dans le cas où des statistiques globales fourniraient suffisamment d'information à l'acquéreur, une partie ne devrait pas communiquer d'informations permettant d'identifier des personnes.

La LPRPDE et les lois provinciales[6] obligent aussi les parties à conclure un accord si des renseignements personnels doivent être communiqués dans le cadre de la vérification diligente. Par exemple, selon la LPRPDE[7], les parties à une éventuelle transaction commerciale peuvent utiliser et communiquer des renseignements personnels à l'insu de l'intéressé ou sans son consentement si elles ont conclu un accord aux termes duquel l'organisation recevant des renseignements s'est engagée : i) à ne les utiliser et à ne les communiquer qu'à des fins liées à la transaction, ii) à les protéger au moyen de mesures de sécurité correspondant à leur degré de sensibilité et, iii) si la transaction n'a pas lieu, à les remettre à l'organisation qui les lui a communiqués ou à les détruire, dans un délai raisonnable. Dans la pratique, ces clauses peuvent être intégrées à un accord général de non-divulgation ou de confidentialité que les parties signent au début de la vérification diligente.

Convention d'acquisition

Diverses questions relatives à la protection de la vie privée, aux technologies et à la cybersécurité peuvent devoir être couvertes dans la convention d'acquisition entre les parties. L'acquéreur, par exemple, peut souhaiter y inclure des déclarations et garanties couvrant les éléments suivants :

- la conformité aux lois applicables et aux politiques et procédures de la société cible concernant la protection de la vie privée, les technologies et la cybersécurité, et la confirmation que ces politiques, procédures et pratiques respectent ou dépassent les normes du secteur;
- le respect des exigences concernant la protection de la vie privée, la protection des données et la cybersécurité contenues dans des contrats avec des tiers;
- le caractère suffisant des TI de la société cible, qui lui appartiennent ou qu'elle utilise sous licence, pour répondre à ses besoins de traitement de données et à d'autres besoins informatiques;
- la formation des employés sur la protection de la vie privée et la sécurité des données, et le fait que les employés sont tenus à des obligations contractuelles appropriées;
- l'exactitude des politiques, avis et déclarations de la société cible qui concernent ses rapports avec le public, en matière de protection de la vie privée;
- le caractère suffisant des contrôles liés à la sécurité des données, y compris le fait que la société cible ait mis en place des mesures de sécurité organisationnelle, technologique et physique raisonnables compte

tenu de la sensibilité des renseignements personnels qu'elle traite;
- la déclaration de toute atteinte ainsi que des dysfonctionnements, défectuosités, problèmes techniques et défaillances liés aux TI que la société cible possède ou utilise sous licence, et la confirmation qu'on y a remédié.

Du point de vue de la société cible, il peut être nécessaire de limiter ou d'assortir de conditions certaines déclarations et garanties, en établissant des seuils d'importance relative ou des critères limitant l'application de certaines clauses à ce que la société sait. La société cible doit déterminer avec soin les déclarations et garanties qu'elle peut donner de façon réaliste sans risquer d'engager gravement sa responsabilité dans l'éventualité où une atteinte préalable à la conclusion serait découverte une fois la transaction conclue. Elle s'assurera aussi de bien connaître les exigences de la loi et toutes les TI qu'elle possède ou utilise sous licence avant de faire certaines déclarations et garanties.

D'autres aspects peuvent devoir être pris en compte en ce qui a trait à la convention d'acquisition, dont les suivants :

1. ***Rajustement du prix d'achat et retenue*** – Une clause de rajustement du prix d'achat et/ou de retenue peut être nécessaire dans le cas où la vérification diligente relève des risques ou des vulnérabilités considérables qui pourraient réduire la valeur de la société cible et où : a) des ressources substantielles seront nécessaires pour rendre la société cible conforme aux lois applicables ou pour corriger ou remplacer des TI désuètes ou compromises; ou b) la société cible a subi une atteinte qui n'a pas encore entraîné de procédures judiciaires, mais les délais de prescription applicables n'ont pas encore expiré.
2. ***Indemnisation*** – Bien qu'elles soient souvent couvertes par les clauses générales d'indemnisation, des clauses d'indemnisation portant spécifiquement sur la protection de la vie privée et la cybersécurité peuvent être requises dans certains cas. Par exemple, des clauses individuelles peuvent être nécessaires si la vérification diligente a relevé des risques précis ou si : a) la durée d'application des clauses générales est trop courte pour couvrir les délais habituels de découverte d'atteintes; ou b) les clauses générales fixent des plafonds d'indemnisation trop bas pour couvrir adéquatement le risque d'une atteinte majeure.

Pour réduire les risques de litiges liés aux clauses de retenue ou d'indemnisation de la convention d'acquisition, il est prudent de prévoir des mécanismes permettant à l'acquéreur de faire une réclamation à leur égard, notamment des dispositions déterminant la manière dont les dommages-intérêts seraient calculés et qui les calculerait.

Après la conclusion

Une fois la transaction conclue, l'acquéreur pourra souhaiter évaluer si les TI existantes seront suffisantes pour lui permettre de réaliser les ambitions qu'il nourrit pour son acquisition. En ce sens, il aura intérêt à corriger rapidement toute lacune des TI découverte pendant la vérification diligente.

La loi prescrit aussi la manière dont doivent être traités, une fois la transaction conclue, les renseignements personnels recueillis avant la conclusion. Par exemple, selon la LPRPDE, les parties peuvent utiliser et communiquer des renseignements personnels qui ont été communiqués, en lien avec la transaction, sans le consentement des personnes concernées si[8] :

- les renseignements sont nécessaires à la poursuite de l'entreprise ou des activités faisant l'objet de la transaction; et dans un délai raisonnable après que la transaction a été effectuée, l'une des parties avise l'intéressé du fait que la transaction a été effectuée et que ses renseignements personnels ont été communiqués.

Les lois provinciales fixent des exigences analogues[9]. L'acquéreur ne doit donc pas utiliser de renseignements personnels obtenus de la société cible avant la transaction à des fins autres que celles autorisées par les lois applicables et couvertes par des consentements préalables, s'il y a lieu. En outre, comme il est mentionné précédemment, la LPRPDE exige qu'il soit expressément établi dans un accord entre les parties que celles-ci donneront effet à tout retrait de consentement que demanderont des personnes après avoir été avisées que des renseignements personnels les concernant ont été communiqués en lien avec la transaction.

Conclusion

Le cadre juridique régissant la protection de la vie privée, la protection des données, les technologies et la cybersécurité est complexe, et la common law sur ces questions évolue rapidement. Il n'en demeure pas moins que de piètres pratiques de traitement des renseignements personnels et une mauvaise gestion des TI peuvent avoir de graves répercussions pour une entreprise, sur les plans financier et judiciaire, notamment. Les parties à des transactions concernant des sociétés de technologie ont donc tout intérêt à accorder à ces questions toute l'attention qu'elles méritent, aussi bien avant la transaction qu'au moment de sa conclusion et une fois qu'elle est effectuée.

[1] Voir cette décision faisant autorité rendue en 2020.
[2] LPRPDE, alinéa 7.2(1)b). Note : Le paragraphe 7.2(1) de la LPRPDE ne s'applique pas à l'égard de la transaction commerciale dont l'objectif premier ou le résultat principal est l'achat, la vente ou toute autre forme d'acquisition ou de disposition de renseignements personnels, ou leur location
[3] *Personal Information Protection Act* (Alberta), sous-alinéa 22(3)a)ii). Note : L'article 22 de cette loi ne s'applique pas à l'égard de la transaction commerciale dont l'objectif ou le résultat principal est l'achat, la

vente, la location, le transfert, la cession ou la communication de renseignements personnels.
[4] *Personal Information Protection Act* (Colombie-Britannique), alinéa 20(2)a). Note : L'article 20 de cette loi n'autorise pas une organisation à communiquer des renseignements personnels à une partie ou à une partie prospective pour les fins d'une transaction commerciale si la transaction ne concerne pas des actifs substantiels de l'organisation autres que lesdits renseignements personnels.
[5] Dès septembre 2023, l'article 18.4 de la loi du Québec prévoira ce qui suit : « Lorsque la communication d'un renseignement personnel est nécessaire aux fins de la conclusion d'une transaction commerciale à laquelle elle entend être partie, une personne qui exploite une entreprise peut communiquer un tel renseignement, sans le consentement de la personne concernée, à l'autre partie à la transaction » (soulignement ajouté).
[6] *Personal Information Protection Act* (Alberta), sous-alinéa 22(3)a)i); *Personal Information Protection Act* (Colombie-Britannique), alinéa 20(1)b). Dès septembre 2023, l'article 18.4 de la loi du Québec exigera que l'entente conclue stipule notamment que la partie à laquelle sont communiqués les renseignements personnels s'engage : « 1) à n'utiliser le renseignement qu'aux seules fins de la conclusion de la transaction commerciale; 2) à ne pas communiquer le renseignement sans le consentement de la personne concernée, à moins d'y être autorisée par la présente loi; 3) à prendre les mesures nécessaires pour assurer la protection du caractère confidentiel du renseignement; et 4) à détruire le renseignement si la transaction commerciale n'est pas conclue ou si l'utilisation de celui-ci n'est plus nécessaire aux fins de la conclusion de la transaction commerciale. »
[7] LPRPDE, alinéa 7.2(1)a). Note : Le paragraphe 7.2(2) de la LPRPDE ne s'applique pas à l'égard de la transaction commerciale dont l'objectif premier ou le résultat principal est l'achat, la vente ou toute autre forme d'acquisition ou de disposition de renseignements personnels, ou leur location
[8] LPRPDE, par. 7.2(2).
[9] *Personal Information Protection Act* (Alberta), alinéa 22(3)b); *Personal Information Protection Act* (Colombie-Britannique), par. 20(3). Dès septembre 2023, l'art. 18.4 de la loi du Québec prévoira ce qui suit : « [l]orsque la transaction commerciale est conclue et que l'autre partie souhaite continuer d'utiliser le renseignement ou le communiquer, cette partie ne peut l'utiliser ou le communiquer que conformément à la présente loi. Dans un délai raisonnable après la conclusion de la transaction commerciale, elle doit aviser la personne concernée qu'elle détient maintenant un renseignement personnel la concernant en raison de la transaction. »

par Lyndsay Wasser, Robert Piasentin, Kristen Pennington et Yue Fei

Mise en garde

une décision, mais devrait plutôt obtenir des conseils juridiques précis.