COMPRENDRE LES LIMITES DU PRIVILÈGE JURIDIQUE À LA SUITE D'UNE CYBERATTAQUE : ENSEIGNEMENTS TIRÉS DE LA VIOLATION DES DONNÉES DE LIFELABS

Publié le 10 mai, 2024

Catégories: Perspectives, Publications

Lorsqu'elles ont été victimes d'une cyberattaque, les organisations ont tendance à exercer une surveillance étroite sur les renseignements relatifs à l'incident. Il y a de bonnes raisons à cela. Premièrement, les renseignements relatifs à une cyberattaque pourraient révéler des vulnérabilités susceptibles d'être exploitées par d'autres cybercriminels. Deuxièmement, la divulgation de détails sensibles sur l'incident peut pousser à examiner de plus près les décisions prises par l'organisation avant ou après l'incident, ce qui pourrait porter atteinte à sa réputation ou même entraîner une responsabilité civile et réglementaire.

C'est ainsi que les organisations peuvent tenter de protéger les renseignements sensibles liés à l'incident en invoquant un certain privilège juridique. Toutefois, les récents développements juridiques ont mis en lumière la portée limitée du privilège juridique en ce qui concerne les dossiers produits dans le cadre de l'enquête sur l'incident et du processus d'intervention.

Dans *LifeLabs LP v. Information and Privacy Commr (Ontario)*[1], une formation de la Cour divisionnaire de la Cour supérieure de justice de l'Ontario a confirmé une décision réglementaire selon laquelle les privilèges juridiques invoqués par LifeLabs ne s'appliquaient pas, entre autres, à l'analyse interne des données touchées par la violation, aux communications avec les auteurs de l'attaque et au rapport d'expertise judiciaire préparé par un tiers consultant en cybersécurité.

Cette décision souligne l'importance de sensibiliser l'équipe d'intervention aux limites du privilège juridique et d'élaborer une stratégie efficace pour gérer les préoccupations en matière de confidentialité concernant les renseignements sensibles sur les incidents.

Contexte

LifeLabs LP (« **LifeLabs** ») fournit des services de laboratoire partout au Canada et, dans le cadre de cette activité, traite des renseignements personnels sensibles sur la santé de ses clients[2]. En 2019, LifeLabs a été victime d'une attaque par rançongiciel qui a entraîné un accès non autorisé aux renseignements personnels

sur la santé de millions de Canadiens[3]. Le commissaire à l'information et à la protection de la vie privée de l'Ontario et le bureau du commissaire à l'information et à la protection de la vie privée de la Colombie-Britannique (collectivement, les « **Commissaires** ») ont mené une enquête conjointe sur l'incident[4].

Dans le cadre de leur enquête, les Commissaires ont demandé à consulter plusieurs documents relatifs à la cyberattaque que LifeLabs avait obtenus de ses consultants[5]. Il s'agissait notamment des documents ci-après :

1. un rapport d'enquête d'un cabinet d'expertise en cybersécurité décrivant la cyberattaque;
2. les courriels échangés entre un cabinet de cyberenseignement et les pirates après la découverte de l'attaque;
3. l'analyse des données internes de LifeLabs décrivant les personnes touchées par la violation des données;
4. d'autres communications entre LifeLabs et les Commissaires[6].

LifeLabs avait refusé de fournir les documents en question, alléguant que ces renseignements étaient protégés par le privilège du secret professionnel de l'avocat et/ou du secret des renseignements préparatoires au procès (privilège relatif au litige)[7]. Les Commissaires ont estimé conjointement que les revendications de privilège devaient être rejetées, au motif que LifeLabs ne leur a pas fourni de preuves suffisantes pour démontrer que les documents étaient effectivement soumis aux privilèges juridiques invoqués[8].

Le privilège ne protège pas les faits sous-jacents relatifs à l'incident

La Cour divisionnaire a confirmé la décision du Commissaire selon laquelle ni le secret professionnel de l'avocat ni le secret des renseignements préparatoires au procès ne s'appliquaient aux documents visés.

Le secret professionnel de l'avocat protège les communications confidentielles entre un avocat et son client tenues dans le cadre de la demande, de la prestation et de la réception de conseils juridiques. Le secret des renseignements préparatoires au procès protège les communications faites et les documents créés principalement dans l'intention d'être utilisés dans le cadre d'un litige en cours, prévu ou envisagé.

Ces deux privilèges sont souvent invoqués dans le contexte d'un incident de cybersécurité.

Tout en reconnaissant le sacro-saint principe du privilège juridique, la Cour divisionnaire a néanmoins conclu qu'une partie ne saurait étendre ce privilège à des faits défavorables à son égard concernant une cyberattaque, en fournissant une copie des faits à son avocat ou en les incluant dans un rapport préparé, en partie, en gardant à l'esprit l'éventualité d'un litige[9].

Par exemple, la Cour a conclu que les lignes de code utilisées par les pirates ne pouvaient pas être privilégiées simplement parce qu'elles avaient été copiées et collées dans un rapport d'expertise judiciaire, et que les

mesures prises pour se protéger contre les failles de sécurité ne pouvaient pas non plus être privilégiées simplement parce que ces renseignements avaient été recueillis par un avocat.

Attention aux limites du privilège de l'intérêt commun!

Bien que la décision dans l'affaire *LifeLabs* ne traite pas expressément de la question, il convient de garder à l'esprit les implications importantes d'un recours éventuel au privilège d'intérêt commun. Les organisations victimes d'une cyberattaque sont souvent tenues de communiquer les rapports d'expertise judiciaires ou d'autres renseignements liés à cet incident aux compagnies d'assurance qui couvrent les coûts liés aux interventions en cas de violations de données, ou à d'autres tiers qui ont un intérêt commun dans l'affaire. Il est essentiel que les parties à de tels arrangements réfléchissent aux limites susmentionnées.

Le privilège d'intérêt commun permet aux parties ayant un intérêt juridique commun de se transmettre des informations confidentielles sans renoncer aux privilèges qui les couvrent. Fait important, le privilège d'intérêt commun ne constitue pas une catégorie distincte de privilège; il ne s'applique que lorsqu'un autre privilège existe déjà et n'a pour seul but que de protéger le privilège existant contre la renonciation[10]. Par exemple, les tribunaux ont refusé de lever le privilège relatif au secret des renseignements préparatoires au procès visant un document partagé entre une organisation et son assureur lorsque le document est principalement destiné à être utilisé dans un litige envisagé ou en instance (c'est-à-dire lorsque le privilège relatif au secret des renseignements préparatoires au procès s'applique déjà)[11].

Les parties ayant un intérêt commun dans un incident particulier devraient examiner attentivement la pertinence des revendications de privilèges sous-jacentes, évaluer les implications potentielles de la communication d'informations entre elles, puis élaborer une stratégie pour faciliter la transmission d'informations nécessaires, de sorte que cela puisse préserver leur intérêt commun.

À retenir

La gestion des questions de privilège est une étape préliminaire essentielle du processus d'intervention en cas d'incident.

Bien que le privilège juridique soit sans aucun doute un outil précieux pour faciliter la circulation de renseignements en toute franchise dans le cadre de la recherche de conseils juridiques ou de la préparation à un litige, l'arrêt dans l'affaire *LifeLabs* démontre l'importance de sensibiliser l'équipe d'intervention en cas d'incident aux limites du privilège. Ensuite, en gardant les yeux grands ouverts, il convient d'élaborer une stratégie efficace d'enquête, de correction et de communication en tenant compte des risques importants liés au litige et à la réglementation.

L'équipe de protection de la vie privée et des données de McMillan est disposée à fournir des conseils

stratégiques afin d'aider les organisations à intervenir en cas de cyberattaques et de violations de données mettant en cause des renseignements personnels et confidentiels sensibles, notamment en élaborant une approche efficace de gestion de questions de privilège.

[1] *LifeLabs LP v. Information and Privacy Commr. (Ontario)*, 2024 ONSC 2194 [LifeLabs] (en anglais).
[2] *LifeLabs* au paragraphe 2.
[3] *LifeLabs* au paragraphe 1.
[4] *LifeLabs* au paragraphe 5.
[5] *LifeLabs* au paragraphe 6.
[6] *LifeLabs* au paragraphe 62.
[7] *LifeLabs* au paragraphe 6.
[8] *LifeLabs* au paragraphe 7; LifeLabs LP (Re), 2020 CanLII 24923 (CIPVP ON), aux paragraphes 56 et 68 (en anglais).
[9] *LifeLabs* aux paragraphes 78 et 81.
[10] Trillium Motor World c. General Motors, 2014 ONSC 4894 au paragraphe 14 (en anglais).
[11] Panetta v. Retrocom, 2013 ONSC 2386, aux paragraphes 61 et 62 (en anglais).

Par Mitch Koczerginski, Robbie Grant et Ada Ang (stagiaire en droit)

Mise en garde