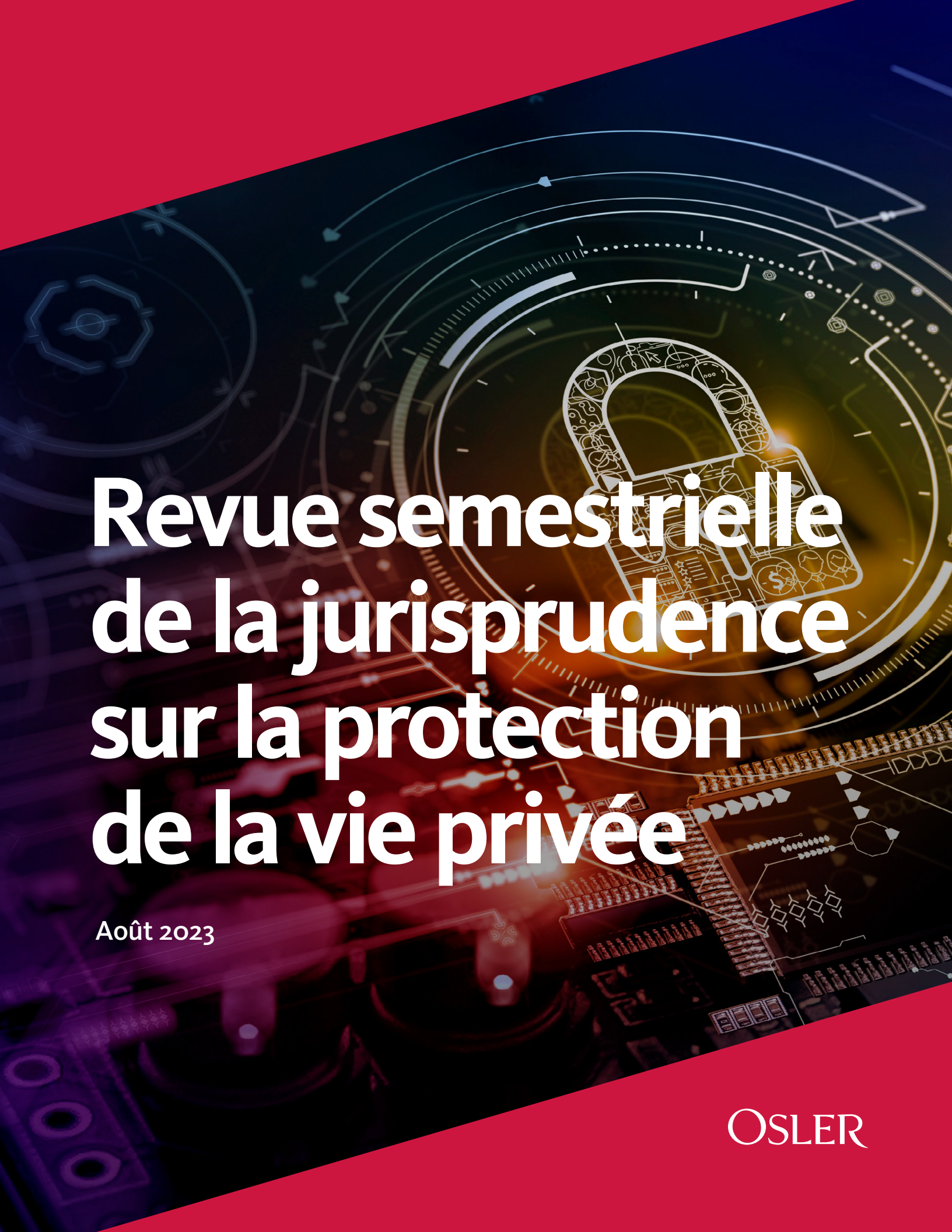


Revue semestrielle de la jurisprudence sur la protection de la vie privée

Août 2023

OSLER

Note de la rédaction

La *Revue semestrielle de la jurisprudence sur la protection de la vie privée* s'adresse aux avocats-conseils internes, aux chefs de la protection des renseignements personnels et aux professionnels de la conformité dont l'agenda est bien chargé. Elle vise à les aider à s'y retrouver dans les décisions récentes rendues par les tribunaux canadiens, à comprendre de manière approfondie l'évolution du droit en matière de protection des renseignements personnels au Canada et à se préparer aux changements à venir pour leur organisation.

La Revue de la jurisprudence sur la protection de la vie privée se compose de résumés de décisions accompagnés de commentaires d'experts qui aideront les lecteurs à déterminer et à comprendre les tendances émergentes tout en leur permettant de mieux comprendre les possibles répercussions concrètes de ces tendances pour leur organisation dans un contexte stratégique plus vaste d'évolution du droit en matière de protection des renseignements personnels.

Comme il peut parfois s'avérer difficile de suivre le rythme des évolutions juridiques, cette *Revue de la jurisprudence sur la protection de la vie privée* se veut une ressource facile d'accès, efficace et pratique pour aider les lecteurs à se tenir au courant de ces évolutions, tout en gagnant du temps.

Nous remercions particulièrement tous les collaborateurs d'Osler qui ont participé à la rédaction des résumés des décisions, pour leur précieuse contribution.

Contributeurs et contributrices

Kristian Brabander
Associé, Litige
kbrabander@osler.com
514 904-8107

Robert Carson
Associé, Litige
rcarson@osler.com
416 862-4235

Tommy Gelbman
Associé, Litige
tgelbman@osler.com
403 260-7073
604 692-2794

Jessica Harding
Associée, Litige
jharding@osler.com
514 904-8128

Craig Lockwood
Associé, Litige
clockwood@osler.com
416 862-5988

Julien Morissette
Associé, Litige et Insolvabilité et restructuration
jmorissette@osler.com
514 904-5818

Table des matières

VIE PRIVÉE ET EMPLOI

PROTECTION DES RENSEIGNEMENTS PERSONNELS DANS LE PROCESSUS DE RÈGLEMENT DES DIFFÉRENDS

INTÉRÊTS LIÉS À LA PROTECTION DES RENSEIGNEMENTS PERSONNELS DES PARTICULIERS

Actions collectives en matière de protection des renseignements personnels : atteintes à la protection des données

Dans le cadre d'une trilogie d'appels en certification de recours collectifs en matière de protection des renseignements personnels, la Cour d'appel de l'Ontario (CAO) a refusé de certifier trois recours collectifs fondés sur le délit d'intrusion dans l'intimité reconnu pour la première fois dans l'affaire *Jones c. Tsige*. En juin 2022, la Cour a entendu les trois appels de manière consécutive et a rendu ses décisions conjointement en novembre 2022. La Cour a conclu que les défendeurs qui recueillent et conservent des renseignements personnels (les Défendeurs exploitant des bases de données) ne peuvent être tenus responsables d'un délit intentionnel d'intrusion dans l'intimité dans le cas d'une atteinte à la protection des données commise par un pirate informatique tiers.

Dans chacune de ces affaires, les demandeurs ont cherché à faire certifier des recours collectifs contre les Défendeurs exploitant des bases de données ayant été victimes d'une atteinte à la protection des données commise par des auteurs de menaces ayant piraté les réseaux informatiques des défendeurs et compromis leurs données, y compris les renseignements personnels des membres proposés du recours collectif. En plus des

allégations de négligence et de rupture de contrat, les demandeurs ont allégué que les Défendeurs exploitant des bases de données étaient également responsables d'une intrusion dans l'intimité des demandeurs.

En ce qui concerne les réclamations avancées, la CAO a conclu que les Défendeurs exploitant des bases des données n'avaient commis aucune action susceptible de constituer une intrusion dans la vie privée des demandeurs ou une atteinte à la vie privée de ces derniers. Les intrusions présumées ont été commises par des pirates informatiques tiers non identifiés, agissant indépendamment des Défendeurs exploitant des bases de données et au détriment des intérêts de ceux-ci. Aucun des faits allégués ne pouvait, en droit, constituer un fondement au titre duquel les actes des pirates informatiques auraient pu être attribués aux Défendeurs exploitant des bases de données. De plus, aucun des faits importants allégués n'indiquait que les Défendeurs exploitant des bases de données avaient agi de concert avec les pirates informatiques ou étaient responsables du fait d'autrui au titre de leurs agissements.

Au cours des dernières années, plusieurs demandeurs ont tenté d'étendre l'application du délit intentionnel d'intrusion dans l'intimité à la cybersécurité et cherché à faire certifier des recours collectifs sur ce fondement. Ces trois décisions en matière de protection de la vie privée rendues par la CAO clarifient la portée du délit et indiquent clairement que la responsabilité ne peut être attribuée qu'à une partie qui cherche activement à accéder de manière abusive à des renseignements personnels d'une autre personne. Bien que la Cour d'appel ait effectivement restreint la portée des futurs recours collectifs en matière de protection des renseignements personnels contre les Défendeurs exploitant des bases de données, la protection imprudente des renseignements ou l'ignorance volontaire de mesures de cybersécurité inadéquates pourraient entraîner la responsabilité des sociétés au titre d'autres délits, comme la négligence.

Owsianik c. Equifax Canada Co., 2022 ONCA 813

Lire les détails de l'affaire

Faits

L'affaire *Owsianik* a été la première à être entendue par les tribunaux de première instance. La demanderesse représentant les autres membres du recours soutenait que les pratiques de gestion des données « imprudentes » d'Equifax constituaient une intrusion extrêmement offensante pour une personne raisonnable. Des pirates informatiques avaient commis une atteinte à la protection des données en accédant de manière non autorisée aux renseignements personnels conservés par Equifax, y compris les numéros d'assurance sociale, les noms, les dates de naissance, les adresses, les numéros de permis de conduire, les numéros de carte de crédit, les adresses de courriel et les mots de passe des personnes.

Décision

En première instance, le tribunal a certifié la plainte pour délit d'intrusion dans l'intimité en concluant qu'il n'était pas évident que les demandeurs n'obtiennent pas gain de cause relativement au délit. Cette décision a toutefois été infirmée à la majorité par la Cour divisionnaire, qui a conclu qu'il n'y avait aucune possibilité de constituer le délit si les Défendeurs exploitant des bases de données n'étaient pas accusés d'avoir commis l'intrusion eux-mêmes.

Point principal à retenir

En rejetant l'appel de cette décision, la CAO a examiné les trois éléments caractérisant un délit d'intrusion dans l'intimité : (1 la conduite ; (2 l'état d'esprit ; et (3 la conséquence. La CAO a déterminé que la revendication des demandeurs n'avait pas satisfait à l'exigence de la « conduite » lors de l'analyse. La CAO a conclu que les défendeurs n'étaient coupables d'aucune conduite ayant mené à une intrusion dans l'intimité des demandeurs. La faute imputable aux défendeurs, le cas échéant, était de ne pas avoir empêché les pirates informatiques de commettre un délit d'intrusion dans l'intimité. La Cour a estimé que pour intenter une action en responsabilité, il aurait été approprié de le faire au titre du délit de négligence, d'une rupture de contrat ou d'une autre obligation prévue par la loi. Puisque ni Equifax, ni aucune personne agissant au nom d'Equifax, ni conjointement avec elle, n'avait accédé illégalement à des renseignements, faire porter à Equifax la responsabilité de la conduite délictueuse de pirates informatiques non identifiés créerait un nouveau fondement potentiellement très large pour conclure à une responsabilité au titre de délits intentionnels.

Obodo c. Trans Union of Canada, Inc., 2022 ONCA 814

Lire les détails de l'affaire

Faits

Comme Equifax, Trans Union a recueilli et conservé les renseignements personnels de ses clients dans sa base de données afin de proposer des services liés au crédit. Comme dans l'affaire *Owsianik*, des pirates informatiques non identifiés se sont introduits dans la base de données. En première instance, le juge saisi de la requête a certifié le recours collectif proposé relativement aux allégations de négligence, ainsi qu'à certaines revendications au titre de la loi, mais a rejeté la certification des allégations d'intrusion dans l'intimité en se fondant sur le raisonnement de la Cour divisionnaire dans l'affaire *Owsianik*.

Décision

Le demandeur a directement fait appel auprès de la Cour d'appel au sujet de ce dernier aspect de la décision. Finalement, la CAO a confirmé le rejet de la certification proposée des allégations d'intrusion dans l'intimité au motif que le délit n'était pas imputable à un Défendeur exploitant des bases de données (avec renvoi aux motifs fournis dans l'appel de l'affaire *Owsianik*). Dans les motifs de l'affaire *Obodo*, la CAO a également tenu compte des arguments supplémentaires du demandeur concernant la responsabilité du fait d'autrui et a conclu que TransUnion n'était pas responsable du fait d'autrui pour les agissements des pirates informatiques, car cette responsabilité repose principalement sur des considérations de principe qui sont, quant à elles, conditionnées à l'existence d'une relation employeur-employé et d'un lien entre cette relation et la conduite délictuelle de l'employé.

Point principal à retenir

Cette relation est une condition préalable à l'attribution de la responsabilité du fait d'autrui et, si cette relation n'existe pas, la demande doit être rejetée.

Winder c. Marriott International, Inc., 2022 ONCA 815

Lire les détails de l'affaire

Faits

Dans l'affaire *Winder*, des pirates informatiques tiers avaient accédé à la base de données de réservation de Marriott qui contenait les renseignements personnels des clients, comme leurs numéros de passeport et leurs informations de paiement. Contrairement aux allégations avancées dans les affaires *Owsianik* et *Obodo*, cette demande alléguait que la société Marriott avait porté atteinte à la vie privée de ses clients, car elle avait recueilli et conservé leurs renseignements personnels d'une manière qui (i) n'était pas conforme aux déclarations que Marriott leur avait faites et (ii) ne respectait pas les obligations juridiques de Marriott concernant la préservation de la sécurité des renseignements. Les demandeurs soutenaient que ces obligations juridiques comprenaient des obligations contractuelles et légales, ainsi que des obligations imposées par les normes et les pratiques de l'industrie. Les demandeurs tentaient de faire valoir que le fait d'obtenir les renseignements personnels des clients de façon trompeuse, sur la base de fausses prémisses, rendait la société coupable d'une intrusion « imprudente », qu'un tiers ait ou non réellement eu accès aux renseignements des clients conservés dans la base de données.

Décision

La CAO a conclu qu'il n'existait aucune allégation selon laquelle Marriott avait recueilli, conservé ou utilisé les renseignements personnels fournis par ses clients à des fins autres que celles pouvant être raisonnablement envisagées par les clients. La faute commise par Marriott n'était pas le non-respect des droits de ses clients en matière de protection des renseignements personnels, mais plutôt le manquement à son devoir de protection de ces droits contre l'intrusion de tiers. Le seul moment où les clients n'avaient pas pu contrôler l'accès à leurs renseignements personnels et l'utilisation de ces derniers avait eu lieu lorsque des pirates informatiques tiers non identifiés s'étaient introduits dans la base de données de Marriott. Avant les agissements des pirates informatiques, aucune atteinte aux droits des clients en matière de protection des renseignements personnels ni aucune intrusion n'avait eu lieu.

Point principal à retenir

Dans ces trois affaires, les demandeurs ont demandé l'autorisation d'interjeter appel devant la Cour suprême du Canada. Ces demandes ont été rejetées en juillet 2023.

Danny Lamoureux c. Organisme canadien de réglementation du commerce des valeurs mobilières (OCRCVM), 2023 CanLII 24495 (CSC)

Lire les détails de l'affaire

Faits

L'action collective de l'appelant concernait la perte d'un ordinateur portable oublié par erreur dans un train par un inspecteur de l'OCRCVM. L'ordinateur n'a jamais été retrouvé. L'information figurant sur l'ordinateur était protégée par mot de passe, mais, malgré les politiques internes mises en place par intimé pour assurer une meilleure protection des données, il n'était pas protégé par chiffrement. L'ordinateur contenait les renseignements personnels de milliers d'investisseurs canadiens. Les membres de l'action collective alléguaient que le fait que l'intimé n'ait pas mis en place de mesures de sécurité pour protéger leurs renseignements personnels constituait une atteinte à leur droit au respect de la vie privée, droit protégé par l'article 5 de la *Charte des droits et libertés de la personne du Québec*.

Décision

La Cour suprême du Canada a rejeté la demande d'autorisation d'appel d'un arrêt de la Cour d'appel du Québec ayant rejeté l'appel d'un arrêt de la Cour supérieure. La juridiction inférieure avait rejeté l'action collective après un procès portant entièrement sur le fond. La Cour suprême n'a pas justifié son rejet de la demande d'autorisation. Toutefois, les décisions de la Cour supérieure et de la Cour d'appel ont été maintenues.

Les juridictions inférieures avaient conclu que la peur et le malaise ressentis par les membres de l'action collective en raison de la perte de leurs renseignements personnels ne constituaient pas un préjudice indemnisable. Ces sentiments sont plutôt des désagréments normaux que toute personne qui vit en société ressent et doit accepter. Les preuves n'étayaient pas l'hypothèse selon laquelle l'ordinateur ou les renseignements des membres de l'action collective étaient tombés entre les mains d'une personne malveillante, et aucun lien convaincant n'avait été établi entre la perte de l'ordinateur et les utilisations illicites alléguées par les membres de l'action collective. Le défendeur (puis intimé) avait réagi avec diligence, selon les normes attendues dans de telles circonstances.

Point principal à retenir

En l'absence d'un préjudice indemnisable démontré, une société peut se défendre avec succès contre des réclamations faites à la suite d'un incident lié aux données en réagissant avec diligence à l'incident.

Sciscente c. Audi Canada Inc., 2022 QCCS 2911

Lire les détails de l'affaire

Faits

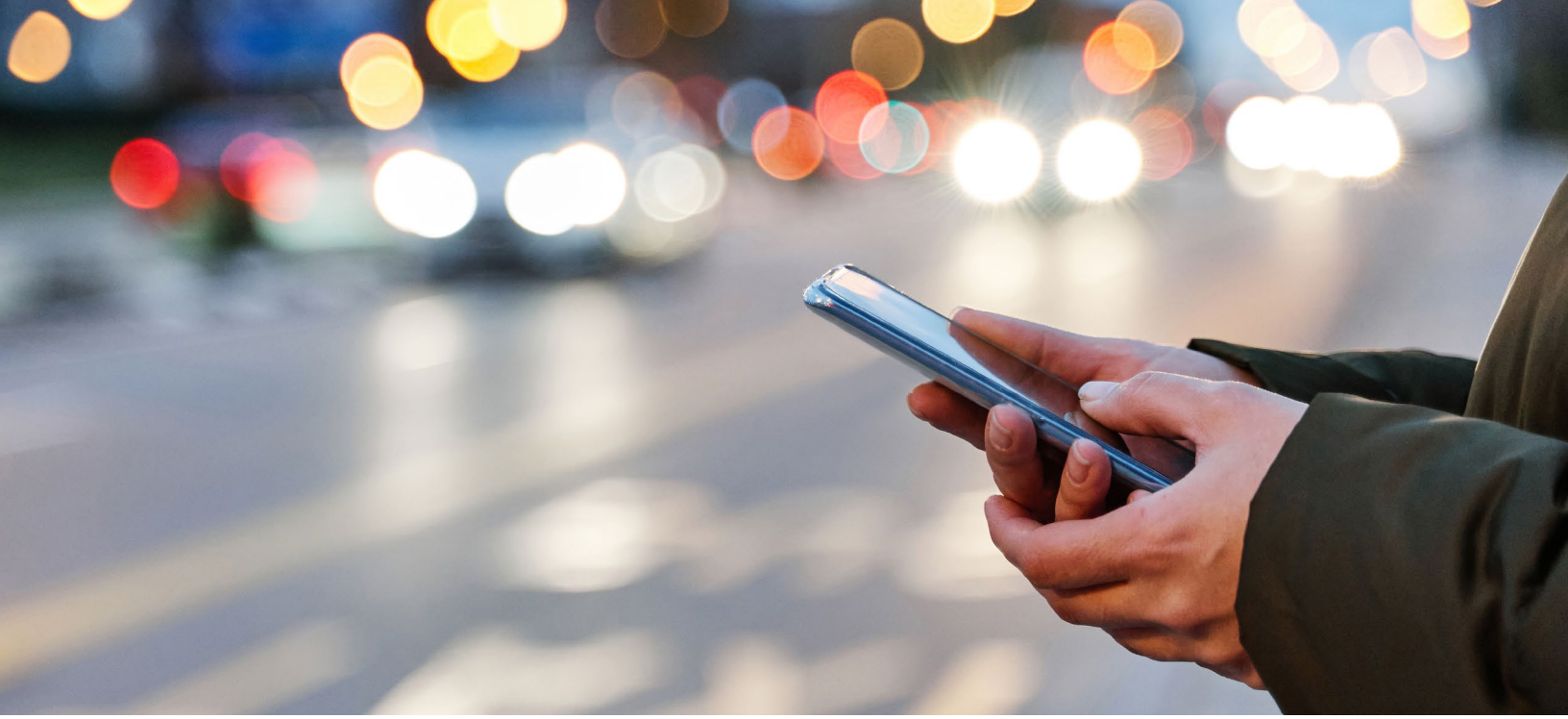
La demanderesse recherchait l'autorisation d'intenter une action collective pancanadienne au nom des personnes au Canada dont les renseignements personnels détenus par les défenderesses Audi Canada Inc. et Volkswagen Group Canada Inc. avaient été compromis à la suite d'une atteinte à la protection des données survenue en mars 2021. L'atteinte à la protection des données avait compromis les renseignements personnels de 3,3 millions de clients en Amérique du Nord.

Décision

La Cour supérieure a autorisé l'action collective contre Audi seulement, et seulement pour les résidents du Québec. Aucun des faits allégués ne pouvait appuyer une conclusion selon laquelle l'atteinte touchait les clients de VW au Canada, puisque la preuve fournie ne concernait que des clients situés aux États-Unis. La Cour a conclu que les preuves d'une possible faute de la part d'Audi étaient suffisantes, notamment en raison du temps écoulé avant que l'atteinte ne soit constatée et du fait que les clients ont été avertis tardivement.

Point principal à retenir

Les tribunaux du Québec exigent des éléments de preuve démontrant que des clients québécois ou canadiens ont été concernés par un incident lié aux données. Le demandeur ne peut s'appuyer uniquement sur la preuve que des clients américains ont été concernés.



Confidentialité et utilisation abusive de renseignements personnels

Option Consommateurs c. Flo Health Inc., 2022 QCCS 4442

Lire les détails de l'affaire

Faits

En 2016, la défenderesse a lancé une application appelée « Flo » permettant aux femmes de suivre leur cycle menstruel et leurs périodes d'ovulation. Un rapport d'enquête a révélé que des renseignements intimes, non chiffrés et permettant d'identifier des personnes avaient été transmis par la défenderesse à Facebook. À la suite de la publication de ce rapport, la défenderesse a modifié sa politique de confidentialité, indiquant qu'elle ne partagerait aucune donnée personnelle avec des tiers. La demanderesse a demandé l'autorisation d'intenter une action collective contre la défenderesse au nom de personnes résidant au Québec ayant utilisé l'application Flo entre le 1er juin 2016 et le 23 février 2019. La demanderesse alléguait que la défenderesse avait manqué à ses obligations contractuelles et légales concernant la préservation de la confidentialité des renseignements personnels des membres de l'action collective. La demanderesse demandait des dommages-intérêts compensatoires (pour préjudice

matériel, relativement à la violation du droit à l'image) et punitifs (en vertu de la *Charte des droits et libertés de la personne* et de la *Loi sur la protection du consommateur* du Québec).

Décision

La Cour supérieure a autorisé l'action collective. La défenderesse avait admis avoir transféré certains renseignements qu'elle avait recueillis, y compris un « unique device identifier » (identifiant unique à l'appareil des membres). La Cour a donc conclu qu'il n'était ni hypothétique ni spéculatif d'affirmer que des renseignements personnels, de nature très délicate, avaient été transférés à des tiers qui les avaient utilisés ou pouvaient les utiliser à des fins autres que le fonctionnement technique de l'application Flo. La mesure dans laquelle l'effet combiné de la divulgation de renseignements et de l'identifiant unique à l'appareil des membres permet l'identification personnelle de l'utilisatrice a été considérée comme une question à examiner sur le fond dans le cadre de l'action collective.

Point principal à retenir

Les tribunaux peuvent, dans certaines circonstances, autoriser une action collective même s'il existe une certaine incertitude quant au fait que les renseignements divulgués permettent d'identifier des personnes.

Canada (Commissaire à la protection de la vie privée) c. Facebook, Inc., 2023 FC 533

Lire les détails de l'affaire

Faits

Le commissaire à la protection de la vie privée du Canada (CPVP) a examiné une plainte selon laquelle une application tierce obtenait les données personnelles des utilisateurs de Facebook par le biais de la plateforme Facebook et les divulguait à un autre tiers, Cambridge Analytica. Le CPVP a publié un rapport concluant que Facebook avait enfreint la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE) en partageant les renseignements personnels des utilisateurs de Facebook avec des applications tierces sans le consentement des utilisateurs et en ne protégeant pas adéquatement les renseignements des utilisateurs. Le CPVP a ensuite présenté une demande à la Cour fédérale en vertu de l'alinéa 15a) de la LPRPDE pour intenter un recours contre Facebook, alléguant que Facebook avait enfreint ladite loi.

Décision

La Cour a rejeté la demande, concluant que le CPVP ne s'était pas acquitté de son obligation d'établir que Facebook avait enfreint la LPRPDE en n'obtenant pas un consentement valable. Le CPVP n'avait présenté aucun témoignage d'expert précisant ce que Facebook aurait vraisemblablement pu faire différemment, ni aucune preuve subjective rédigée par des utilisateurs de Facebook indiquant leurs attentes en matière de protection des renseignements personnels ou leur compréhension des enjeux liés à la protection de ces renseignements personnels lorsqu'ils utilisent Facebook. La Cour a déclaré que, même si ces éléments de preuve n'étaient pas strictement nécessaires, (traduction libre) « ils auraient certainement permis à la Cour de mieux évaluer le caractère raisonnable du consentement valable dans un domaine où la norme en matière de caractère raisonnable et d'attentes des utilisateurs peut sensiblement varier selon le contexte et évolue constamment ». Par conséquent, la Cour a été contrainte d'effectuer des déductions qui n'étaient pas étayées par le dossier de preuve.

La Cour a également déterminé qu'une fois les renseignements divulgués à une application tierce, les obligations en matière de protection des données de Facebook en vertu de la LPRPDE prenaient fin. La Cour a également souligné que, même si les obligations de préservation de la confidentialité s'appliquaient à Facebook après la divulgation de renseignements à des applications tierces, il n'y avait pas suffisamment d'éléments de preuve pour déterminer si les ententes contractuelles et les politiques de mise en application des règles de Facebook constituaient des mesures de protection adéquates.

Principaux points à retenir

Dans le cadre d'une audience *de novo* tenue en vertu de l'alinéa 15a) de la LPRPDE, il n'est pas possible de conclure qu'il y a eu infraction à la loi en cas d'« absence totale de preuves ». Il incombe au CPVP de présenter des éléments de preuve convaincants pour établir une infraction. De plus, cette décision appuie le principe selon lequel, une fois qu'une organisation est autorisée par un utilisateur à divulguer des renseignements à une application tierce, les obligations en matière de protection des données incombant à l'organisation en vertu de la LPRPDE prennent fin.

Facebook, Inc. c. Canada (Commissaire à la protection de la vie privée), 2023 FC 534

Lire les détails de l'affaire

Faits

Les faits sous-jacents sont fondamentalement les mêmes que ceux du résumé précédent : le CPVP a examiné une plainte selon laquelle une application tierce obtenait les données personnelles des utilisateurs de Facebook par le biais de la plateforme Facebook, et les divulguait à Cambridge Analytica. Le CPVP a publié un rapport concluant que Facebook avait enfreint la LPRPDE en partageant les renseignements personnels des utilisateurs de Facebook avec des applications tierces sans le consentement des utilisateurs et en ne protégeant pas adéquatement leurs renseignements. Toutefois, cette décision concerne une demande déposée par Facebook devant la Cour fédérale, sollicitant la révision judiciaire « des décisions [du CPVP] d'enquêter et de poursuivre son enquête, du processus d'enquête et du Rapport de conclusions qui en a résulté ».

Décision

La Cour a rejeté cette demande de révision judiciaire au motif qu'elle n'avait pas été présentée à temps et qu'une prorogation de l'échéance n'était pas justifiée. Néanmoins, la Cour a ensuite abordé le fond des allégations, dans l'éventualité où la décision sur le fondement de base serait erronée. La Cour n'a pas accepté les arguments de Facebook selon lesquels les plaignants n'avaient pas qualité pour agir, l'enquête du CPVP ne présentait pas de lien réel et important avec le Canada et selon lesquels l'enquête avait entraîné un manquement à l'équité procédurale.

Vie privée et données biométriques/IA

Enquête concernant le Centre de services scolaire du Val-des-Cerfs (anciennement Commission scolaire du Val-des-Cerfs), 2022-11-09, 1020040-S

Lire les détails de l'affaire

Faits

Cette décision émane de la section de surveillance de la Commission d'accès à l'information (CAI). La CAI a lancé une enquête sur le conseil scolaire du Val-des-Cerfs, qui avait mis au point un algorithme, en partenariat avec un cabinet d'experts-conseils, pour cibler les élèves de sixième année qui risquaient fortement de décrocher. Le conseil scolaire avait mis au point une méthodologie d'apprentissage automatique capable d'analyser plus de 300 types de données brutes issues d'une base de données contenant les renseignements personnels des élèves et de générer un ensemble d'indicateurs

prédictifs du risque de décrochage (l'« Outil »). La décision de la CAI, à la suite de l'enquête, a statué sur la question de savoir si l'organisation avait respecté ses obligations en vertu de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (la « Loi sur l'accès ») lors de la collecte et de l'utilisation des renseignements personnels au cours de la phase d'élaboration du projet.

Décision

Premièrement, la CAI a déterminé que, bien que les renseignements personnels aient été dépersonnalisés pour empêcher l'identification directe des élèves et de leurs parents, ils n'avaient pas été anonymisés puisqu'ils n'avaient pas été dépersonnalisés de façon irréversible, ce qui permettait quand même d'identifier les élèves.

Deuxièmement, la CAI a conclu que, lors de la phase d'élaboration de l'Outil, le conseil scolaire avait utilisé les renseignements personnels à une nouvelle fin, en contravention avec l'article 65.1 de la Loi sur l'accès. Lorsque les renseignements avaient été recueillis pour la première fois, les élèves et leurs parents n'avaient pas été informés que les renseignements seraient utilisés pour générer des indicateurs prédictifs du risque de décrochage et n'avaient donc pas consenti à cette utilisation. Toutefois, la CAI a déterminé que la raison pour laquelle les renseignements avaient été utilisés était compatible avec les objectifs du conseil scolaire, à savoir d'assurer la réussite scolaire.

Troisièmement, la CAI a conclu que l'Outil relevait de l'intelligence artificielle, s'agissant « d'un système dont l'objectif est d'enrichir un travail réalisé par des humains, capable de produire des analyses prédictives grâce à un système technologique faisant appel à des algorithmes ». De surcroît, à la suite des analyses effectuées, l'Outil produisait de nouveaux renseignements personnels, à savoir des indicateurs prédictifs du risque de décrochage, ce qui, selon la CAI, constituait une *collecte* de renseignements personnels au sens de la Loi sur l'accès.

Comme il a été déterminé que le conseil scolaire avait recueilli des renseignements personnels lors de la phase d'élaboration de l'Outil, la CAI a conclu que le conseil scolaire avait manqué à son obligation d'informer les parents des élèves des façons dont les données étaient utilisées. La CAI a demandé au conseil scolaire d'adopter des mesures de sécurité pour assurer la protection des renseignements personnels recueillis, y compris des procédures de destruction des renseignements personnels et des résultats existants de l'Outil. Elle a également demandé au conseil scolaire de procéder à une évaluation de l'incidence de l'Outil sur la protection de la vie privée avant son déploiement.

Point principal à retenir

Cette décision de la section de surveillance de la CAI est la première au Québec à donner des indications sur l'interprétation faite par la CAI de plusieurs questions entourant l'intelligence artificielle. Plus précisément, la définition de l'intelligence artificielle donnée par la CAI et le fait que cette dernière ait déterminé que la production d'indicateurs prédictifs constituait une « collecte » de renseignements personnels sont inédits. En particulier, cette détermination pourrait assujettir les organisations qui utilisent l'intelligence artificielle pour générer des statistiques aux dispositions des lois relatives au respect de la vie privée applicables à la collecte (et non à l'utilisation) de renseignements personnels, notamment relativement à l'obtention du consentement des personnes concernées. Dans certaines circonstances, il pourrait être nécessaire de prendre en compte cette décision dans l'interprétation du nouveau paragraphe 65.2 de la Loi sur l'accès, ainsi que de son équivalent pour le secteur privé, le paragraphe 12.1 de la *Loi sur la protection des renseignements personnels dans le secteur privé,* qui entrera en vigueur en septembre 2023 et établira de nouvelles règles de transparence pour la prise de décisions automatisée.

Situmorang c. Google LLC, 2022 BCSC 2052

Lire les détails de l'affaire

Faits

Le demandeur a demandé la certification d'un recours collectif contre Google LLC concernant l'utilisation par Google de la technologie de regroupement de visages. Le demandeur a allégué que Google n'avait pas obtenu le consentement éclairé des membres du recours collectif pour l'utilisation de la technologie de regroupement de visages et qu'elle avait utilisé les données biométriques faciales des membres du recours pour son propre avantage concurrentiel. Le demandeur a formulé ses revendications en vertu de la loi sur la protection des renseignements personnels de la Colombie-Britannique (*Privacy Act*) (la Revendication en droit) et du délit d'intrusion dans l'intimité reconnu en common law (la Revendication en common law).

Décision

La Cour suprême de la Colombie-Britannique a refusé de certifier le recours, concluant qu'il était clair et évident que le demandeur n'obtiendrait pas gain de cause, ni pour la Revendication en droit, ni pour la Revendication en common law.

La Cour a conclu qu'il était clair et évident que la Revendication en droit ne pouvait pas aboutir, car il n'avait pas été possible d'établir que la conduite de Google constituait une violation délibérée de la vie privée ou que Google n'avait pas le droit de procéder au regroupement de visages.

Pour évaluer la Revendication en common law, la Cour devait déterminer si Google s'était ingérée dans les « affaires ou intérêts privés » du demandeur. La Cour a conclu que la revendication posait une question ouverte : un ensemble de données biométriques faciales conservé peut-il constituer de l'information relevant des « affaires et intérêts privés » d'une personne? Malgré ce questionnement, la Cour a conclu qu'il était clair et évident que la Revendication en common law n'aboutirait pas, le demandeur n'ayant pas pu établir qu'une intrusion découlant de l'utilisation par Google de la technologie de regroupement de visages serait considérée comme hautement offensante par une personne raisonnable.

Principaux points à retenir

La question posée, à savoir « un ensemble de données biométriques faciales conservé peut-il constituer de l'information relevant des "affaires et intérêts privés" d'une personne? », reste ouverte. Les organisations qui recueillent et conservent des données biométriques faciales peuvent donc être vulnérables aux allégations d'intrusion dans l'intimité fondées sur la common law.

Accès à l'information

Dutremble c. Hydro-Québec, 2023 QCCAI 3

Lire les détails de l'affaire

Faits

La demanderesse a demandé à Hydro-Québec de lui donner accès aux documents concernant le barrage de la Chute-Bell. L'organisme a soutenu que ces renseignements étaient toujours en litige et que leur divulgation aurait pour effet de réduire l'efficacité d'un programme destiné à la protection de biens ou de personnes, en l'occurrence le Programme de sécurité 2019-2023, visant à protéger ses barrages, et porterait atteinte à la sécurité de l'État.

Décision

La demande de révision du refus d'Hydro-Québec de divulguer les documents a été rejetée. Hydro-Québec avait fondé son refus sur l'article 29 de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels.* Les éléments de preuve ont démontré que les renseignements concernés étaient de nature délicate et que la divulgation de ces renseignements aurait pour effet de réduire l'efficacité de son programme de sécurité. De plus, les renseignements étaient suffisamment précis pour qu'une personne soit en mesure de les exploiter. Leur divulgation pourrait permettre à des personnes malveillantes de commettre des actes susceptibles de mettre

l'infrastructure en péril, ce qui aurait des conséquences prévisibles, telles que la rupture du barrage, qui auraient une incidence directe sur la sécurité des personnes ainsi que sur les infrastructures routières, y compris les ponts des autoroutes 148 et 50.

Point principal à retenir

L'exception relative à la sécurité invoquée pour refuser l'accès est rarement utilisée, mais il se peut qu'elle soit invoquée de plus en plus fréquemment en raison des préoccupations grandissantes au sujet de la sécurité des infrastructures essentielles. Dans certains cas, cette exception pourra s'appliquer à une demande d'accès à de l'information posant des préoccupations de sécurité, même si la portée de ces préoccupations variera en fonction de déterminations hautement factuelles.

Ville de Laval c. Savard, 2022 QCCQ 8465

Lire les détails de l'affaire

Faits

La CAI avait ordonné à la partie appelante, la Ville de Laval, de fournir à l'intimé, M. Savard, des extraits d'un avis juridique au sens de l'article 31 de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*. L'avis juridique avait été rédigé par un avocat dans le contexte de la détermination de l'admissibilité d'une plainte pour harcèlement psychologique déposée par M. Savard contre la Ville de Laval.

Décision

La Ville de Laval a soutenu qu'une fois qu'un document est considéré comme un avis juridique au sens de l'article 31 de la Loi, l'avis juridique dans son ensemble devient indivisible, car il est protégé par le secret professionnel de l'avocat, et aucun extrait ne peut donc être communiqué. La Cour du Québec a accueilli en partie l'appel de la décision de la CAI. La Cour a d'abord déterminé que des extraits d'un document protégé par le secret professionnel de l'avocat peuvent être communiqués à une partie qui dépose une demande d'accès. Le fait qu'un document soit protégé par le secret professionnel de l'avocat ne le rend pas indivisible. Cela dit, en l'espèce, les extraits de l'avis juridique auxquels la CAI avait accordé l'accès étaient en grande partie protégés par le secret

professionnel de l'avocat et la CAI avait commis une erreur de droit en ordonnant à la Ville de Laval de les divulguer, à l'exception d'un extrait relatif à la description des parties.

Point principal à retenir

Bien que la CAI et la Cour du Québec soient sensibles aux revendications relatives à la protection du secret professionnel de l'avocat, il n'existe pas de règle absolue selon laquelle un document protégé par le secret professionnel de l'avocat est indivisible. Dans certains cas, des extraits peuvent être communiqués à un tiers. La partie qui s'oppose à la divulgation devra établir que les renseignements pertinents sont à tel point intégrés à des conseils juridiques protégés par le secret professionnel de l'avocat et qu'ils ne peuvent être extraits sans que le secret professionnel soit levé.

Saskatchewan (ministère des Relations et de la Sécurité en milieu de travail), Re, 2023 Carswell Sask 99

Lire les détails de l'affaire

Faits

Le ministère des Relations de travail et de la Sécurité en milieu de travail a reçu une demande d'accès à l'information en vertu de la loi intitulée *Freedom of Information and Protection of Privacy Act, SS 1990-91* (FOIP) de la part de l'employeur d'un travailleur blessé. La demande portait sur des documents liés à une blessure au travail. Le ministère a divulgué certains documents, mais pas tous. Le ministère a refusé de communiquer des documents en vertu des paragraphes 22(b), 22(c), 29(1), 15(1)(c), 15(1)(e), 19(1)(b) et 13(1)(a) de la FOIP et du paragraphe 27(1) de la loi sur la protection des renseignements sur la santé de la Saskatchewan *(Health Information Protection Act, SS 1999 (HIPA)*. Le Commissariat à l'information et à la protection de la vie privée de la Saskatchewan a reçu une demande d'examen de la part de la partie demanderesse. Après le dépôt de cette demande, le ministère a rendu une deuxième décision, modifiant la première en retirant son affirmation selon laquelle les paragraphes 13(1)(a) et 22(b) de la FOIP s'appliquaient.

Décision

Le Commissariat a examiné chaque paragraphe individuellement. En ce qui concerne le paragraphe 27(1) de la HIPA, le commissaire a conclu que le travailleur blessé n'avait pas consenti à la divulgation de ces documents et que, par conséquent, le ministère avait eu raison d'invoquer ce paragraphe pour refuser l'accès à la majorité des documents. Le Commissariat s'est prononcé en faveur de la divulgation d'un seul document, car celui-ci avait été fourni par le demandeur et qu'il aurait été « absurde » que le ministère

lui refuse l'accès à ce document. En ce qui concerne le paragraphe 15(1)(c) de la FOIP, le Commissariat a de nouveau souligné qu'il était « absurde » que le ministère refuse de divulguer les documents au demandeur étant donné que ce dernier avait participé à leur création (il s'agissait notamment de contrats que le demandeur avait signés ou de courriels où il était copié). En ce qui concerne le paragraphe 29(1) de la FOIP, le Commissariat a conclu que le ministère avait refusé à tort l'accès à certains documents, car des informations accessibles au public et des signatures de personnes apposées dans un contexte de travail ne constituaient pas des renseignements personnels. Les noms des témoins de l'évènement ayant causé la blessure n'ont pas non plus été considérés comme des renseignements personnels. Le Commissariat a conclu que certains documents, y compris des adresses que le demandeur ne connaissait pas, étaient protégés en vertu du paragraphe 29(1) de la FOIP.

Principaux points à retenir

En vertu du principe d'« absurdité », si la réflexion du Commissariat mène à une conséquence absurde, telle que l'interdiction de communiquer des renseignements à un demandeur qui y a accès, cette conséquence doit être évitée.

Brightwater Senior Living, Re, 2022 CarswellSask 535

Lire les détails de l'affaire

Faits

Le 5 octobre 2021, la partie demanderesse a présenté une demande d'accès à l'information à Brightwater Senior Living pour obtenir les dossiers médicaux de sa mère décédée. Brightwater a répondu à la demande de la partie demanderesse le 14 décembre 2021. La partie demanderesse a estimé que Brightwater avait mis trop de temps à répondre à sa demande. Le 3 février 2022, le Commissariat à l'information et à la protection de la vie privée de la Saskatchewan a informé la partie demanderesse et Brightwater qu'il allait entreprendre un examen.

Décision

Le Commissariat a conclu que Brightwater n'avait pas répondu à la demande de la partie demanderesse dans les délais prescrits en vertu des paragraphes 36(1)(a) de la loi sur la protection des renseignements sur la santé de la Saskatchewan (*Health Information Protection Act*). Brightwater a soutenu qu'au départ, elle n'avait pas répondu à la demande, car la partie demanderesse n'était pas inscrite comme mandataire ou personne-ressource

de la résidente. Le Commissariat a conclu que Brightwater était tenue de répondre à la demande dans les délais prescrits par la loi, en énonçant les raisons pour lesquelles elle refusait l'accès.

Principaux points à retenir

Lorsqu'un curateur estime qu'une personne qui demande l'accès à l'information n'a pas le droit d'accéder à l'information demandée, il doit répondre à la demande dans les délais prescrits par la loi, en précisant les raisons pour lesquelles il lui refuse l'accès.

Cain c. Canada (Santé), 2023 FC 55

Lire les détails de l'affaire

Faits

La Cour fédérale a examiné une demande présentée en vertu de la *Loi sur l'accès à l'information* concernant la divulgation des codes postaux et des villes des titulaires d'une licence permettant de cultiver de la marijuana à des fins médicales. Santé Canada a accepté de divulguer seulement le premier caractère des codes postaux, alors que le demandeur souhaitait accéder aux trois premiers caractères (la région de tri d'acheminement), car il existait une « forte possibilité » que les deuxième et troisième caractères des codes postaux puissent être recoupés avec d'autres renseignements afin d'identifier des personnes en particulier.

Décision

La Cour fédérale a rejeté la demande. La Cour a estimé que, dans certaines zones, un nombre relativement faible de personnes vivent dans une même région de tri d'acheminement, et qu'il existe donc un risque que les trois premiers caractères soient combinés à d'autres renseignements accessibles au public pour identifier un titulaire de licence en particulier. La Cour a conclu que les droits en matière de protection des renseignements personnels devaient prévaloir. Des éléments de preuve ont démontré une forte possibilité que la divulgation des données demandées permette de révéler des renseignements très sensibles concernant des personnes. Cet argument justifiait le refus de Santé Canada de divulguer les deuxième et troisième caractères des codes

postaux. La Cour fédérale a également conclu que Santé Canada n'était pas tenue de recourir à d'autres « techniques de dépersonnalisation » pour divulguer davantage de renseignements.

Principaux points à retenir

La Cour fédérale s'est appuyée sur la jurisprudence de la Cour suprême du Canada et sur l'intention du Parlement pour conclure que la protection des renseignements personnels devait prévaloir en cas de conflit entre le droit d'accès à l'information et le droit à la protection des renseignements personnels. Compte tenu des faits de cette affaire, la Cour fédérale était convaincue que les risques pour la vie privée étaient « tout simplement trop importants ».

Vie privée et emploi

Hébert c. Syndicat de professionnelles et professionnels du Gouvernement du Québec, 2022 QCCAI 300

Lire les détails de l'affaire

Faits

La demanderesse, une employée du ministère de l'Agriculture, des Pêcheries et de l'Alimentation (MAPAQ), a affirmé avoir été victime de harcèlement psychologique de la part de ses gestionnaires et de ses collègues. Elle a formulé une plainte pour harcèlement psychologique ainsi qu'un grief envers son employeur. Le Syndicat de professionnelles et professionnels du gouvernement du Québec (SPGQ) a représenté la demanderesse dans le cadre de son grief. Une enquêtrice a été désignée pour enquêter sur la plainte et préparer un rapport. La demanderesse a déposé une demande auprès du SPGQ pour obtenir l'accès à ce rapport ainsi qu'aux éventuels autres rapports ou documents liés à son grief. L'accès à 10 documents lui a été refusé. La demanderesse a également souhaité rester anonyme afin que son identité n'apparaisse pas dans cette décision, étant donné la nature délicate des renseignements contenus dans celle-ci.

Décision

La CAI a annulé en partie la décision du MAPAQ. L'article 13 de la *Loi sur la protection des renseignements personnels dans le secteur privé* stipule que les renseignements personnels ne peuvent être communiqués à des tiers que dans la mesure où la personne concernée consent à cette divulgation. Certains documents déposés dans le cadre de l'analyse du grief de la demanderesse contenaient des communications échangées entre plusieurs employés du MAPAQ. Le nom de la demanderesse ne figurait dans aucune de ces communications et la demanderesse n'avait pas été mise en copie des messages. Les documents contenaient des faits, des opinions ou des perceptions de tiers à l'égard de certains évènements ou de certains sujets dans le cadre de leur travail, qui, selon la CAI, constituaient des renseignements personnels sur des tiers. En l'absence du consentement des tiers concernés, les renseignements personnels ne pouvaient pas être divulgués.

Point principal à retenir

Les opinions exprimées par une personne au sujet d'une autre sur ses compétences, ses opinions, ses choix ou ses pratiques de travail constituent des renseignements personnels tant pour la personne qui les exprime que pour celle qui en fait l'objet. Ces renseignements ne peuvent donc être divulgués qu'avec le consentement du tiers concerné. Pour les organisations qui détiennent ce type d'information, il peut être souhaitable de déterminer quelles évaluations sont de nature subjective et les séparer des compilations factuelles ou des dossiers strictement objectifs de renseignements personnels.

Advanced Upstream Ltd., Re, 2023 CarswellAlta 630

Lire les détails de l'affaire

Faits

Le plaignant est un ancien employé d'Advanced Upstream Ltd. Son contrat de travail comprenait une clause de non-sollicitation dont les effets se prolongeaient 12 mois après la résiliation de son contrat de travail. Advanced Upstream a appris que le plaignant avait fourni des services à un concurrent et a envoyé une lettre à ce concurrent par l'entremise d'avocats. La lettre informait le concurrent de la possibilité que le plaignant ne respecte pas ses clauses restrictives. Après avoir reçu la lettre, le concurrent a informé Advanced Upstream qu'il avait entamé des discussions avec le plaignant, mais qu'il avait décidé de ne pas l'embaucher. Le plaignant a découvert que la lettre avait été envoyée et a déposé une plainte alléguant qu'Advanced Upstream avait divulgué ses renseignements

personnels. Advanced Upstream a par la suite reconnu une violation de la PIPA, mais a continué de contester le fait que la divulgation violait les droits du plaignant en matière de protection des renseignements personnels.

Décision

La Commission a d'abord conclu que la lettre contenait des renseignements personnels, à savoir le nom du plaignant, le fait qu'il était employé par Advanced Upstream à un poste spécifique, son adresse, sa signature et une lettre de divulgation qui énumérait ses activités caritatives et sans but lucratif, d'autres activités commerciales, ses intérêts dans d'autres entités et sa situation de famille, ainsi que le prénom de sa compagne. La Commission a ensuite conclu que le plaignant avait consenti à la divulgation de ses renseignements personnels dans un article de son contrat de travail qui autorisait la divulgation des renseignements personnels de l'employé pour les activités courantes de la société. Enfin, la Commission s'est attachée à déterminer si la divulgation était raisonnable, comme l'exige l'article 19 de la PIPA, et a conclu que l'objet de la divulgation était raisonnable puisque la société cherchait à éviter un manquement à un contrat de travail, mais que la portée de la divulgation ne l'était pas, en particulier en ce qui concerne la divulgation de l'adresse du plaignant, de sa situation de famille, du nom de sa conjointe, de sa signature et des conflits d'intérêts.

Principaux points à retenir

Les organisations qui traitent des renseignements personnels peuvent communiquer avec leurs concurrents pour protéger leurs intérêts au titre de la non-sollicitation et de la non-concurrence, mais, ce faisant, elles doivent veiller à ce que les renseignements personnels figurant dans ces documents qui ne sont pas nécessaires pour protéger ces intérêts soient caviardés ou ne soient pas, divulgués d'une autre manière.

Direct Energy Regulated Services, Re, 2023 CarswellAlta 629

Lire les détails de l'affaire

Faits

En vertu d'une entente sur les locaux vacants (Premise Vacancy Agreement), le propriétaire d'un bien (le plaignant) devait fournir ses coordonnées à une entreprise de services énergétiques (l'organisation). Seize ans après la vente du bien, l'organisation a communiqué avec le plaignant. Le plaignant a avancé que l'organisation n'avait pas respecté l'article 35 de la loi sur la protection des renseignements personnels de l'Alberta (*Personal Information Protection Act*, « PIPA ») (relatif à la conservation et à la destruction d'information).

Décision

L'organisation a respecté la PIPA, cette dernière ne s'appliquant pas aux renseignements en question en vertu du paragraphe 4(3)(d) de cette même loi. Comme le paragraphe 4(3)(d) a pour effet d'exempter du respect de ladite loi, la collecte, l'utilisation et la communication de renseignements personnels, ce paragraphe doit, au moins dans une certaine mesure, avoir le même effet relativement à la conservation de ces renseignements. Dans le cadre de l'obtention de services énergétiques au sens large de la part de l'organisation, les responsabilités commerciales du plaignant relativement à l'organisation ont pris fin au moment de la vente du bien, mais l'exigence pour le plaignant de communiquer avec l'organisation pour résilier l'entente sur les locaux vacants a persisté.

Principaux points à retenir

Le paragraphe 4(3)(d) de la PIPA exempte les organisations du respect de ladite loi pour la conservation de coordonnées d'entreprises, dans la mesure où ces renseignements sont conservés aux seules fins énoncées dans cet article, à savoir pour permettre à une personne d'être contactée dans le cadre de ses responsabilités commerciales.

Autorité de la santé de la Saskatchewan, Re, 2023 CarswellSask 44

Lire les détails de l'affaire

Faits

Un employé a formulé un grief à l'encontre de son employeur, l'Autorité de la santé de la Saskatchewan, qui avait affiché un avis sur un tableau blanc indiquant que l'employé était en congé de maladie. L'employé a soutenu que cette divulgation de ses renseignements personnels de santé violait ses droits en matière de protection des renseignements personnels.

Décision

Le Commissariat à l'information et à la protection de la vie privée de la Saskatchewan a donné raison à l'employé et a conclu que l'employeur avait manqué à son obligation de protéger les renseignements personnels de santé de l'employé. Il a constaté que des atteintes à la protection des renseignements personnels avaient eu lieu, notamment lorsque le gestionnaire avait communiqué les renseignements personnels de santé de l'employé au personnel administratif du bureau, lorsque le personnel administratif du

bureau avait affiché ces renseignements personnels sur le tableau blanc des présences et lorsque le personnel avait pu consulter ces renseignements personnels sur le tableau blanc.

Principaux points à retenir

Cette affaire met en évidence l'importance de préserver la confidentialité des renseignements médicaux, ainsi que la nécessité pour les employeurs de mettre en place des politiques et des procédures claires pour assurer la protection de ces renseignements. Elle souligne également l'importance des droits en matière de protection de la vie privée et l'importance pour les employeurs de prendre des mesures adéquates pour protéger les renseignements personnels de santé sur le lieu de travail.

Livingston c. Commission des droits de la personne de la Saskatchewan, 2022 SKCA 127

Lire les détails de l'affaire

Faits

L'appelant a interjeté appel d'une décision en cabinet annulant son action pour défaut de compétence et abus de procédure. La déclaration initiale portait sur une atteinte à la protection des renseignements personnels dans une affaire de droits de la personne en matière d'emploi. L'appelant et son syndicat ont allégué que la Commission des droits de la personne de la Saskatchewan, où travaillait l'appelant, avait violé le droit à la vie privée de l'appelant et n'avait pas respecté son obligation d'équité procédurale lorsqu'elle s'était renseignée sur son problème d'emploi, l'ayant également divulgué à ses collègues.

Décision

La Cour d'appel a rejeté l'appel et a conclu que le juge en son cabinet n'avait pas commis d'erreur en concluant que la question principale était liée à l'emploi et qu'elle relevait donc de la compétence d'un arbitre, comme stipulé par la convention collective applicable. Plus précisément, la nature même de la demande de l'appelant pour atteinte à la vie privée découlait de son emploi. La Cour a déclaré que ces questions de droits de la personne sont abordées et incorporées dans les conventions collectives. La Cour a également cité les jugements de la Cour suprême du Canada dans les affaires *Weber c. Ontario Hydro* et *Office régional de la santé du Nord c. Horrocks*, qui ont établi que les

juridictions de compétence inhérente ne peuvent pas examiner des questions liées à une convention collective, sous réserve de la compétence discrétionnaire résiduelle.

Principaux points à retenir

Les questions de protection des renseignements personnels qui découlent de préoccupations liées à l'emploi sont assujetties aux limites de compétence précisées dans les conventions collectives.

Protection des renseignements personnels dans le processus de règlement des différends

Rousseau c. Conseil de l'industrie forestière du Québec, 2022 QCCAI 332

Lire les détails de l'affaire

Faits

Une entreprise avait mis fin à l'emploi du demandeur, ce qui a amené ce dernier à déposer une plainte auprès de la Commission des normes, de l'équité, de la santé et de la sécurité au travail (CNESST). Le demandeur a ensuite demandé à l'entreprise de lui fournir une copie de son dossier d'employé, y compris son contrat d'emploi, et sa lettre de confirmation d'emploi, ainsi que toutes les politiques concernant l'utilisation des courriels et les vacances. Cependant, certains des documents pertinents dans le cadre de son licenciement ne lui ont pas été envoyés. Par conséquent, le demandeur a déposé une demande auprès de la CAI. Deux jours plus tard, le demandeur a signé une entente de départ, qui ne mentionnait pas explicitement les procédures devant la CNESST. L'entreprise a allégué que la plainte devait être rejetée.

Décision

La CAI a confirmé le refus de l'entreprise de fournir les documents. Une entreprise peut refuser, en vertu du paragraphe 39(2) de la *Loi sur la protection des renseignements personnels dans le secteur privé* (la « Loi »), de communiquer des renseignements personnels si ces derniers peuvent avoir une incidence sur une procédure judiciaire. De plus, cette décision doit être prise au regard des procédures en cours à la date de la cessation d'emploi. Même si les procédures se terminent plus tard, la décision sera maintenue si l'exception a été appliquée au moment pertinent. En l'espèce, un lien direct existait entre les documents sollicités par le demandeur et la procédure judiciaire ; au moment où la société a envoyé sa réponse à la demande d'accès du demandeur, les plaintes déposées auprès de la CNESST étaient en instance.

Point principal à retenir

La CAI a interprété au sens large le droit de refuser la communication de renseignements personnels à la personne concernée si la divulgation de ces renseignements peut avoir une incidence sur une procédure judiciaire dans laquelle l'une ou l'autre des parties a un intérêt. Il est également intéressant de remarquer que la CAI a établi que les termes généraux de libération des obligations d'une entente de règlement n'entraînent pas la libération des obligations liées à une plainte déposée auprès de la CAI.

Centre universitaire de santé McGill c. Lemay, 2022 QCCA 1394

Lire les détails de l'affaire

Faits

En septembre 2012, l'Unité permanente anticorruption (UPAC) du Québec a exécuté un mandat de perquisition dans les bureaux de l'appelant, le Centre universitaire de santé McGill, à la suite d'allégations de collusion et de corruption dans l'attribution de contrats de construction. L'appelant a alors retenu les services d'un avocat pour obtenir des conseils sur les recours et les mesures à prendre à la lumière de ces allégations. L'avocat a fait appel aux services d'un cabinet d'expertise comptable judiciaire qui a rédigé un rapport préliminaire. Ce rapport a ensuite été volontairement communiqué à l'UPAC. La principale question soulevée par l'appel était de savoir si la divulgation volontaire du rapport protégé par le secret professionnel de l'avocat à l'UPAC, dans le contexte d'une enquête criminelle, avait levé la protection du document au titre du secret professionnel de l'avocat et sa confidentialité à l'égard d'autres tiers.

Décision

La Cour d'appel a conclu que la CAI et la Cour du Québec avaient eu raison de déterminer que le secret professionnel de l'avocat et la confidentialité à l'égard des tiers n'avaient pas été levés lorsque les renseignements avaient été communiqués aux services de police. La CAI et la Cour du Québec se sont fondées, à juste titre, sur une décision ayant établi que la communication de renseignements protégés par le secret professionnel de l'avocat à la police est une obligation morale, qui ne relève pas d'une intention claire et sans équivoque de renoncer au secret professionnel de l'avocat.

Point principal à retenir

La divulgation de renseignements protégés par le secret professionnel de l'avocat aux autorités chargées de l'application de la loi, dans le but de contribuer à une enquête criminelle, n'entraîne pas automatiquement la levée du secret ou de la confidentialité du document à l'égard d'autres tiers.

Nintendo du Canada Ltée c. Tilmant-Rousseau, 2022 QCCQ 5610

Lire les détails de l'affaire

Faits

Cette affaire est un appel d'une décision de la CAI ayant infirmé une décision de l'Office québécois de la langue française (OQLF). En septembre 2007, l'appelante, l'Association canadienne du logiciel de divertissement (ACLD), a conclu un protocole d'entente avec l'OQLF sur les conditions relatives à la distribution de jeux vidéo au Québec et sur divers aspects de leur commercialisation. En 2017, l'OQLF a refusé de fournir à l'intimée Laurence Tilmant-Rousseau une copie du protocole d'entente, invoquant le caractère confidentiel du document. Cette décision a été contestée devant la CAI. L'ACLD et Nintendo du Canada Ltée sont intervenues pour s'opposer à la demande en révision, au motif que le protocole d'entente était protégé par le privilège relatif aux règlements des litiges. En août 2019, la CAI a ordonné à l'OQLF de divulguer le protocole d'entente à l'intimée.

Décision

La Cour du Québec a conclu que la CAI avait commis une erreur en refusant d'appliquer le privilège relatif aux règlements des litiges dans le contexte d'une demande d'accès à l'information. La CAI avait fondé sa décision sur la nature quasi constitutionnelle de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* qui protège le droit des citoyens à l'information. La Cour du Québec a conclu que, lorsque le privilège relatif aux règlements des litiges s'applique, il y a présomption *prima facie* d'inaccessibilité des tiers aux communications faites en vue de

régler le litige, y compris l'accord de règlement. Cette présomption s'applique à tout litige porté devant les tribunaux, les tribunaux administratifs, les arbitres et les médiateurs, même en l'absence de dispositions législatives ou de clauses contractuelles en matière de confidentialité. Il ne s'agit pas simplement d'une règle de preuve, mais d'une règle de fond. Dans cette affaire, la Cour a conclu que le protocole d'entente était protégé par le privilège relatif aux règlements des litiges.

Point principal à retenir

Conformément à la jurisprudence récente, la Cour du Québec a réaffirmé que le privilège relatif aux règlements des litiges était un principe générique ayant préséance sur la règle générale d'accès aux documents des organismes publics. Il s'agit d'une interprétation relativement large du privilège relatif aux règlements des litiges, qui va au-delà des droits des parties au règlement et ne fixe pas de délai à son application.

Acuren Group Inc., Re, 2023 CarswellAlta 217

Lire les détails de l'affaire

Faits

Le demandeur était un employé de l'intimée, Acuren Group Inc. Le demandeur a allégué avoir été licencié sans motif valable et a avancé qu'une plainte déposée à son sujet par un autre employé avait joué un rôle dans son licenciement. En vertu de la loi sur la protection des renseignements personnels de l'Alberta (*Personal Information Protection Act*) (« PIPA »), le demandeur a demandé à l'intimée de lui communiquer des renseignements concernant les plaintes portées contre lui, son dossier personnel ainsi que toutes les communications et tous les dossiers concernant son licenciement. L'intimée a fait valoir qu'une grande partie des renseignements demandés n'étaient pas des renseignements personnels du demandeur et que, par conséquent, elle retenait certains des renseignements en vertu des paragraphes 24(3)(b) et 24(3)(c) de la PIPA. L'intimée n'a pas non plus communiqué les autres documents en vertu du paragraphe 24(2)(a) de la PIPA, car ils sont protégés par le privilège relatif au litige ou le secret professionnel de l'avocat.

Décision

La Cour a conclu que l'intimée avait eu raison de ne pas communiquer les renseignements en vertu des paragraphes 24(3)(b) et 24(3)(c) de la PIPA, car la divulgation de ces renseignements aurait eu pour effet de révéler des opinions exprimées à l'intention de l'intimée à titre confidentiel, ainsi que des renseignements personnels au sujet d'une autre personne. En examinant les renseignements non communiqués au titre du privilège relatif au litige, la Cour a conclu qu'il n'existait pas de privilège relatif au litige puisque le demandeur avait signé un abandon général des poursuites à l'égard de l'intimée et qu'aucun litige n'était donc raisonnablement à craindre pour cette dernière. De plus, la

Cour a conclu que même si certains renseignements contenaient des conseils juridiques, ils n'étaient pas protégés par le secret professionnel de l'avocat, les renseignements n'étant pas confidentiels puisqu'ils avaient été communiqués en dehors d'une relation entre un avocat et son client.

Principaux points à retenir

Une organisation peut refuser l'accès aux renseignements personnels d'un employé si cet accès entraîne la révélation des renseignements personnels d'une autre personne ou des opinions ayant été exprimées à titre confidentiel. De même, pour que le secret professionnel de l'avocat soit applicable, les renseignements doivent être communiqués entre l'avocat et son client, doivent contenir des conseils juridiques et doivent demeurer confidentiels.

Intérêts liés à la protection des renseignements personnels des particuliers

Charest c. Procureur général du Québec, 2023 QCCS 1050

Lire les détails de l'affaire

Faits

En avril 2017, une entreprise de presse a publié des documents concernant le demandeur, Jean Charest, ancien premier ministre du Québec, obtenus auprès de l'Unité permanente anticorruption (UPAC) du Québec ou créés par celle-ci. Les documents ont filtré dans la presse alors qu'une enquête sur le financement sectoriel du Parti libéral du Québec, à l'époque où il était au pouvoir, était en cours. Cette affaire qui a été très médiatisée à l'époque, l'est encore aujourd'hui.

Décision

La Cour supérieure du Québec s'est prononcée en faveur du demandeur, lui accordant 35 000 $ en dommages-intérêts compensatoires et 350 000 $ en dommages-intérêts punitifs. La Cour a conclu que l'UPAC n'avait pas protégé les renseignements personnels

de M. Charest, contrairement aux dispositions de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*. En vertu de cette Loi, la divulgation de renseignements personnels aux médias, à l'insu de la personne concernée, est interdite. Le procureur général soutenait que le demandeur, en tant que politicien, ne pouvait pas avoir des attentes élevées en matière de protection de la vie privée. La Cour a rejeté cet argument.

Point principal à retenir

Bien que cette affaire concerne un organisme public ayant divulgué des renseignements personnels à la presse, la décision de la Cour montre que la protection des renseignements personnels est prise très au sérieux, même dans le cas de personnalités publiques qui ont également droit à la protection de leurs renseignements personnels et qui sont en droit d'avoir des attentes en matière de respect de leur vie privée malgré leurs apparitions publiques.

Bellevue West Building Management Ltd., Re, 2022 BCIPC 74

Lire les détails de l'affaire

Faits

La plaignante est propriétaire d'un appartement dans un immeuble dont l'ensemble des propriétaires ont constitué la société Bellevue West Building Management Ltd. En vue de coordonner l'utilisation et la jouissance de cet immeuble. La société Bellevue est dirigée par un comité de gestion qui a installé un système de vidéosurveillance pour lutter contre les tentatives d'effraction et les dommages matériels mineurs. La plaignante a déposé une plainte auprès du Commissariat à l'information et à la protection de la vie privée de la Colombie-Britannique, faisant valoir que la société Bellevue avait recueilli et utilisé ses renseignements personnels sous la forme d'images capturées par la surveillance.

Décision

Le Commissariat a d'abord cherché à déterminer si la plaignante avait consenti à la collecte de ses renseignements personnels et a conclu que, même si les panneaux mis en place constituaient un avis suffisant, l'utilisation par la plaignante des espaces publics sous surveillance ne valait pas consentement, comme le soutenait Bellevue, le consentement étant par nature un choix, alors que la plaignante était obligée de passer par la buanderie et le hall d'entrée pour accéder à son appartement. La société Bellevue a invoqué les paragraphes 12(1)(c), 12(1)(h) et 12(1)(j)(i) de la loi sur la protection des renseignements personnels de la Colombie-Britannique (*Personal Information Protection Act*, (« PIPA ») pour expliquer pourquoi elle n'avait pas demandé le consentement de la plaignante,

mais le Commissariat a conclu qu'aucun de ces paragraphes ne s'appliquait. Si la société Bellevue n'était initialement pas autorisée à recueillir des renseignements personnels, le Commissariat a également conclu qu'elle n'était pas autorisée à les utiliser en vertu des paragraphes 6(1) et 6(2) de la PIPA.

Principaux points à retenir

Pour obtenir le consentement à l'utilisation ou à la collecte de renseignements personnels d'une personne, celle-ci doit avoir la possibilité légitime de refuser.

Métis Addictions Council of Saskatchewan Inc., Re, 2023 CarswellSask 124

Lire les détails de l'affaire

Faits

Des renseignements personnels de nature délicate concernant des patients du Métis Addictions Council of Saskatchewan Inc. (MACSI) ont été trouvés dans un bac de recyclage par un membre du public, qui les a ensuite communiqués aux médias. Ces dossiers contenant des renseignements confidentiels portant sur les dépendances et les problèmes de santé mentale des patients, n'avaient pas été correctement détruits par le MACSI. Un membre des médias a informé le Commissariat à l'information et à la protection de la vie privée de la Saskatchewan que ces dossiers avaient été trouvés.

Décision

Une enquête menée par le Commissariat à l'information et à la protection de la vie privée de la Saskatchewan a révélé que les dossiers contenaient des renseignements personnels de nature délicate, y compris des détails portant sur les dépendances et les problèmes de santé mentale des patients, et que ces documents n'avaient pas été détruits de façon appropriée. Il a été déterminé que le MACSI n'avait pas respecté la loi sur la protection des renseignements sur la santé de la Saskatchewan (*Health Information Protection Act*), n'avait pas pris toutes les mesures nécessaires pour limiter cette infraction et n'avait pas fait suffisamment d'efforts pour aviser les personnes concernées. Le MACSI a été sommé de payer une amende et de prendre des mesures pour empêcher que des infractions semblables se produisent à l'avenir.

Principaux points à retenir

L'affaire met en évidence l'importance de traiter et de détruire les renseignements personnels de nature délicate de manière appropriée, particulièrement dans le contexte des soins de santé et dans les autres secteurs qui traitent de ces renseignements. Elle rappelle également aux organisations leurs obligations en vertu des lois en matière de protection des renseignements personnels et les conséquences possibles en cas de non-respect de ces obligations.

James c. Amazon.com.ca, Inc., 2023 FC 166

Lire les détails de l'affaire

Faits

La demanderesse, Tamara James, affirmait avoir créé un compte auprès d'Amazon.com.ca, Inc., mais avoir oublié son mot de passe. Elle a cherché à obtenir des renseignements sur son compte client, y compris des reçus liés au compte et des enregistrements audio de ses communications avec le service à la clientèle d'Amazon. Amazon a tenté d'aider Mme James à réinitialiser son mot de passe, mais Mme James a refusé cette aide.

Mme James a déposé une plainte auprès de la commissaire à la protection de la vie privée et a correspondu avec l'agent de protection de la vie privée d'Amazon, les employés-cadres du service de relations avec la clientèle d'Amazon et les avocats d'Amazon pour tenter de résoudre le problème. Amazon a conclu qu'elle ne pouvait pas authentifier Mme James en tant qu'auteure de la demande, car (i) Mme James ne voulait pas suivre les étapes fournies pour réinitialiser son mot de passe, et (ii) l'information fournie par Mme James ne correspondait pas à l'information figurant sur le serveur d'Amazon.

Le rapport de la commissaire a conclu qu'« Amazon avait fourni à Mme James une réponse juste et raisonnable à sa demande d'accès à l'information puisque la société n'était pas parvenue à vérifier son identité ». Mme James a ensuite porté le litige devant la Cour fédérale en vertu de l'article 14 de la LPRPDE.

Décision

La Cour a rejeté la demande. Mme James ne s'était pas acquittée de son obligation d'établir qu'il y avait eu infraction à la LPRPDE. Amazon avait l'obligation de protéger les renseignements sur le compte (selon le septième principe de la LPRPDE). La Cour a d'ailleurs déclaré : « c'est l'objet même de la LPRPDE ». Par conséquent, la Cour a conclu qu'Amazon « avait eu raison de refuser de donner accès à des renseignements personnels sans pouvoir vérifier l'identité de l'auteure de la demande dans les circonstances de cette affaire ».

La Cour a rejeté plusieurs autres questions soulevées par Mme James, y compris des arguments selon lesquels Amazon aurait enfreint le sixième principe (au motif qu'une information prétendument inexacte en la possession d'Amazon aurait empêché la vérification de l'identité de l'auteure de la demande) et qu'Amazon aurait enfreint l'exigence relative au délai de réponse en vertu de l'article 8 de la LPRPDE.

Principaux points à retenir

Les organisations peuvent légitimement refuser l'accès aux renseignements personnels si l'identité de l'auteur de la demande ne peut être vérifiée de façon appropriée. Amazon a proposé une aide raisonnable pour vérifier l'identité de Mme James. Comme la Cour a conclu : « De l'aide était disponible. La demanderesse a choisi de ne pas l'utiliser. »

Barrett c. Banque Royale du Canada, 2022 FC 1534

Lire les détails de l'affaire

Faits

Maureen Barrett avait démissionné de son poste à la Compagnie d'assurance vie RBC et avait commencé son nouveau poste de conseillère financière à la Financière Sun Life (« la Sun Life »). Au moment de sa démission de la Compagnie d'assurance vie RBC, l'entreprise enquêtait sur Mme Barrett pour un présumé comportement frauduleux impliquant son compte bancaire personnel. La Sun Life a également mené sa propre enquête indépendante sur la conduite de Mme Barrett en tant qu'employée de la Sun Life. Après que la Sun Life a mis fin au contrat de travail de Mme Barrett, cette dernière a allégué que cette décision avait été prise en raison de la divulgation, par la Compagnie d'assurance vie RBC à la Sun Life, de ses renseignements bancaires personnels sans son consentement, enfreignant de ce fait la LPRPDE. Mme Barrett a présenté une demande en vertu de l'article 14 de la LPRPDE. Elle demandait une déclaration selon laquelle la divulgation de ses renseignements personnels à la Sun Life par la Compagnie d'assurance vie RBC contrevenait à la LPRPDE, ainsi que des dommages-intérêts et le remboursement des frais.

Décision

La Cour a rejeté la demande de Mme Barrett, concluant que la divulgation de renseignements personnels avait été faite conformément au paragraphe 7(3)(d.1) de la LPRPDE, qui permet la divulgation de renseignements personnels à l'insu de la personne ou sans son consentement afin de poursuivre une enquête. La Cour a conclu que la Compagnie d'assurance vie RBC avait divulgué les renseignements bancaires personnels

de Mme Barrett de manière raisonnable dans le cadre de l'enquête de la Sun Life sur la conduite de Mme Barrett. La Cour a déclaré que les renseignements étaient pertinents pour l'enquête de la Sun Life et qu'il était raisonnable pour la Compagnie d'assurance vie RBC de ne pas en informer Mme Barrett ni de lui demander son consentement avant la divulgation, car cela aurait pu compromettre l'enquête.

La Cour a expliqué qu'elle n'aurait pas conclu que la divulgation était autorisée si la Compagnie d'assurance vie RBC était la seule à mener une enquête, car la divulgation des renseignements personnels à la Sun Life n'aurait pas contribué à faire avancer l'enquête de la Compagnie d'assurance vie RBC ni à empêcher une fraude, puisque l'activité frauduleuse présumée avec le compte bancaire de Mme Barrett avait déjà eu lieu.

Enfin, la Cour a déclaré que, même si Mme Barrett était en mesure de démontrer une infraction à la LPRPDE, l'octroi de dommages-intérêts ne serait pas approprié, car l'infraction de la part de la Compagnie d'assurance vie RBC ne serait pas flagrante, et son contrat de travail n'avait pas été résilié en raison de la divulgation très limitée de ses renseignements personnels par la Compagnie d'assurance vie RBC.

Principaux points à retenir

Cette décision clarifie les circonstances dans lesquelles les paragraphes 7(3)(d.1) et (d.2) de la LPRPDE permettent la divulgation de renseignements personnels d'une personne à son insu ou sans son consentement afin de faire avancer une enquête, et de réprimer ou d'empêcher une fraude. Dans ce cas particulier, la divulgation était raisonnable pour faire avancer une enquête, même si elle n'aurait pas été considérée raisonnable pour réprimer ou empêcher la fraude.

Al-Husseini c. Altaif Inc., 2022 FC 1497

Lire les détails de l'affaire

Faits

Le demandeur, Sadeq Al-Husseini, a présenté une demande en vertu de l'article 14 de la LPRPDE contre Altaif Inc. pour avoir divulgué des renseignements financiers qui auraient dépassé la portée d'une ordonnance de communication liée à la procédure de divorce de M. Al-Husseini devant la Cour supérieure de justice de l'Ontario (l'« Ordonnance de communication »).

Décision

La Cour fédérale a rejeté la demande, concluant qu'Altaif n'avait pas enfreint les droits de M. Al-Husseini en matière de protection des renseignements personnels, car les transferts de devises qu'Altaif avait divulgués respectaient la portée de l'Ordonnance de communication. La Cour a également accepté les arguments d'Altaif selon lesquels cette dernière estimait raisonnablement que les renseignements devaient être divulgués en vertu de l'Ordonnance de communication.

Compte tenu de cette conclusion, il n'était pas nécessaire d'aborder la question des dommages-intérêts. Toutefois, la Cour a expliqué que même si l'interprétation de la Cour à l'égard de la portée de l'Ordonnance de communication était erronée, M. Al-Husseini n'avait pas établi qu'il avait subi des dommages-intérêts en raison de la divulgation. La Cour a ajouté que, bien que la LPRPDE donne à la Cour fédérale le pouvoir discrétionnaire d'accorder des réparations en cas d'atteinte à la vie privée, l'octroi de dommages-intérêts au titre du droit relatif au respect de la vie privée ne doit avoir lieu que dans les « circonstances les plus extrêmes ».

Principaux points à retenir

Cette décision met en lumière certaines des difficultés qui surviennent lorsqu'il est demandé à un tribunal d'interpréter la portée d'une ordonnance rendue par un autre tribunal aux fins de l'évaluation d'une infraction présumée à la LPRPDE. La Cour fédérale a finalement pu rendre ses conclusions sur la portée et l'objet de l'Ordonnance de communication dans cette affaire, mais les motifs reflètent les limites de cet exercice.

À propos d'Osler, Hoskin & Harcourt S.E.N.C.R.L./s.r.l.

Osler est un cabinet d'avocats de premier plan ayant une seule priorité : vos affaires. Que ce soit de Montréal, Toronto, Calgary, Ottawa, Vancouver ou New York, notre équipe fournit des conseils à ses clients canadiens, américains et internationaux pour un large éventail de questions juridiques nationales et transfrontalières. Notre approche intégrée nous permet d'offrir un accès direct à l'un de nos 500 avocats afin de fournir des solutions juridiques efficaces, proactives et pratiques dictées par vos besoins. Depuis plus de 150 ans, nous avons bâti notre réputation en fournissant les réponses dont vous avez besoin, quand vous en avez besoin.

C'est le droit à l'oeuvre.

Osler, Hoskin & Harcourt S.E.N.C.R.L./s.r.l.
Montréal Toronto Calgary Ottawa Vancouver New York | **osler.com**

OSLER