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

Automne 2024

OSLER

Table des matières

Note de la rédaction

En cette ère numérique où les données personnelles circulent à une vitesse et dans des proportions sans précédent, les responsables de la protection des renseignements personnels, les avocats-conseils internes et les professionnels de la conformité ont un mandat qui est à la fois vital et stimulant. La présente revue se veut une publication incontournable pour ceux et celles qui souhaitent bénéficier d'un aperçu de la jurisprudence récente en matière de protection de la vie privée au Canada, de même que d'un regard critique sur les décisions judiciaires et les tendances qui définissent les contours des droits des personnes physiques et des responsabilités des personnes morales en ce qui a trait à la protection de la vie privée. En recensant les principales décisions judiciaires, et au moyen de commentaires d'experts, nous souhaitons armer les responsables de la protection des renseignements personnels avec la prévoyance et les connaissances requises pour toujours respecter les lois et gérer de manière proactive l'interaction entre l'évolution des normes juridiques, les technologies émergentes et les impératifs commerciaux.

L'équipe spécialisée dans les litiges relatifs au respect de la vie privée et le groupe de pratique national du droit relatif au respect de la vie privée et à la gestion de l'information d'Osler contribuent régulièrement aux initiatives de leadership éclairé présentées sur la plateforme AccessPrivacy d'Osler. La plateforme AccessPrivacy permet de tirer parti de l'expertise des deux groupes pour présenter des informations globales sur les questions de protection de la vie privée et de litiges relatifs aux données. En complément à la *Revue de la jurisprudence sur la protection de la vie privée*, la plateforme propose notamment des tables rondes très suivies portant sur les litiges relatifs aux données à l'occasion de l'appel mensuel AccessPrivacy, ainsi que des ateliers et des tables rondes sur les tendances émergentes en matière d'intelligence artificielle et de gouvernance.

Les auteurs souhaitent remercier Andrea Korajlija, Tamara Kljakic, Josy-Ann Therrien, Brodie Noga et Marie-Laure Saliah-Linteau pour leur précieuse collaboration.

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
Associé, 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

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

Option Consommateurs c. Home Depot of Canada Inc., 2024 QCCS 1305

Lire les détails de l'affaire

Faits

La demanderesse a demandé l'autorisation d'exercer une action collective à l'encontre de Home Depot. Selon la demanderesse, Home Depot a manqué à ses obligations légales et statutaires en partageant avec des tiers, y compris Facebook, des renseignements personnels des membres du groupe sans leur consentement, portant ainsi atteinte à leur droit fondamental à la vie privée. Le partage de renseignements a fait l'objet d'une enquête du Commissariat à la protection de la vie privée du Canada (le CPVP), qui a conclu que la défenderesse avait omis d'obtenir un consentement valable et valide pour la communication de renseignements personnels.

Décision

Le tribunal a accueilli en partie la demande pour autorisation d'exercer une action collective à l'encontre de Home Depot, et permis à la demanderesse de demander le recouvrement de 10 000 000 $ en dommages-intérêts punitifs, mais a rejeté les prétentions fondées sur la responsabilité extracontractuelle et les fausses représentations. Le tribunal a également modifié la description du groupe, afin de le restreindre aux membres qui sont détenteurs d'un compte Facebook.

Selon le tribunal, les allégations considérées véridiques suggèrent que Home Depot aurait partagé les renseignements personnels de ses membres sans leur consentement implicite ou explicite, en violation des articles 35 et 37 du *Code civil du Québec* (le CcQ) ainsi que de l'article 13 de la *Loi sur la protection des renseignements personnels dans le secteur privé* et des articles 5 et 6.1 de la *Loi sur la protection des renseignements personnels et les documents électroniques*. Il était donc possible de soutenir que Home Depot avait commis une faute en vertu de l'article 1457 du CcQ.

Toutefois, le tribunal a estimé que la demanderesse n'avait pas démontré l'existence d'un préjudice. Le simple fait que des renseignements personnels soient en possession non autorisée d'un tiers ne constitue pas un préjudice et, par conséquent, ne donne pas lieu à des dommages compensatoires. Pour ces raisons, le tribunal a considéré que la demanderesse n'avait pas démontré l'existence d'une cause défendable fondée sur la responsabilité extracontractuelle.

Le tribunal a également rejeté les arguments de la demanderesse fondés sur les fausses prétentions, car il a estimé que les articles pertinents de la *Loi sur la protection des consommateurs* ne s'appliquaient pas.

En ce qui concerne les dommages-intérêts punitifs pour atteinte illicite et intentionnelle du droit à la vie privée, le tribunal a estimé que les allégations permettaient de déduire que la défenderesse devait connaître les conséquences du comportement fautif allégué.

Point principal à retenir

Le tribunal rappelle l'importance d'obtenir du consommateur son consentement exprès à l'utilisation de ses renseignements personnels. Le simple fait que des renseignements personnels soient en possession non autorisée d'un tiers ne constitue pas, en soi, un préjudice. Cette affaire rappelle que la réclamation de dommages-intérêts punitifs peut, à elle seule, donner lieu à l'autorisation d'exercer une action collective.

Del Giudice v. Thompson, 2024 ONCA 70, autorisation d'appel devant la CSC rejetée 2024 CanLII 88330

Lire les détails de l'affaire

Faits

Cet appel fait suite à une décision rejetant la requête en certification d'une action collective projetée fondée sur une atteinte à la protection des données concernant des renseignements personnels et confidentiels recueillis auprès de demandeurs de cartes de crédit. Les causes d'action distinctes invoquées ont été classées en deux catégories : (1) les prétentions d'utilisation abusive de données et (2) les prétentions d'atteinte à la protection des données. Le juge saisi de la requête a estimé que les actes de procédure n'étayaient aucune cause d'action valable et qu'ils étaient « exagérés » (*egregious*) et contrevenaient aux règles les régissant. Les appelants ont soutenu que le juge saisi de la requête avait commis une erreur (1) en déterminant qu'aucune des causes d'action invoquées n'était viable, (2) en s'appuyant sur des documents non assermentés, et (3) en supprimant des parties de l'exposé de la demande sans accorder l'autorisation de le modifier.

Décision

La Cour d'appel de l'Ontario a rejeté l'appel, estimant que les actes de procédure étaient invalides, car les prétentions plaidées n'avaient aucune chance de succès. La Cour a également estimé que le juge saisi de la requête avait le droit de s'appuyer sur des documents non assermentés pour parvenir à cette conclusion, en vertu du principe bien établi selon lequel un acte de procédure est réputé inclure tout document auquel il se réfère. En l'espèce, les documents en question (notamment la politique de confidentialité du défendeur, la demande de crédit du demandeur et un contrat de carte de crédit) étaient tous expressément mentionnés dans l'exposé de la demande. La Cour a donc conclu que le juge saisi de la requête était en droit de s'appuyer sur ces documents pour rejeter la prétention selon laquelle les défendeurs avaient utilisé les renseignements des demandeurs à des fins non autorisées. La Cour s'en est également remise à la décision du juge saisi de la requête de ne pas accorder l'autorisation de modifier l'exposé de la demande, reconnaissant que les appelants avaient eu de multiples occasions de le faire, mais qu'ils ne l'avaient pas fait.

Point principal à retenir

Cette affaire confirme que la certification continue d'être un puissant outil de filtrage des demandes sans fondement et illustre également comment les défendeurs peuvent contester les actes de procédure à un stade précoce. Il s'agit également d'un rappel utile de la portée des actes de procédure, qui sont réputés inclure tout document auquel ils font référence.

Ari v. Insurance Corporation of British Columbia, 2024 BCSC 964

Lire les détails de l'affaire (disponible en anglais seulement)

Faits

La Cour suprême de la Colombie-Britannique a accordé des dommages-intérêts à l'échelle du groupe pour une atteinte à la vie privée commise par un employé de l'Insurance Corporation of British Columbia (ICBC) qui avait accédé de manière inappropriée aux renseignements personnels de certains clients de l'ICBC et les a vendues. Certains de ces renseignements ont servi à déclencher des incendies criminels et des fusillades visant des maisons et des véhicules appartenant à certains de ces clients.

Décision

À un stade antérieur de l'instance, l'ICBC a été jugée responsable du fait d'autrui pour la violation par son employé de la loi de la Colombie-Britannique intitulée *Privacy Act*. Le groupe comprenait toutes les personnes résidant dans une maison touchée par l'atteinte à la vie privée.

La Cour a accordé à chaque membre du groupe des dommages-intérêts symboliques de 15 000 $, indépendamment du préjudice réel subi par les membres du groupe. Elle a estimé que ce montant entrait dans la catégorie des dommages-intérêts modestes ou symboliques, compte tenu de la gravité de la violation, de l'objectif public de la loi et de la nécessité de rendre des comptes. La Cour a rejeté la proposition de l'ICBC d'accorder des dommages-intérêts de 500 $ au motif qu'elle banaliserait le droit à la vie privée qui a été violé et rendrait la cause d'action prévue à la loi en question effectivement dénuée de sens. Les dommages-intérêts individuels seront évalués ultérieurement.

Point principal à retenir

Des dommages-intérêts symboliques peuvent être accordés en cas de violation des lois sur la protection des renseignements personnels, et leur montant peut, dans certaines circonstances, atteindre un montant non négligeable afin d'assurer la protection des renseignements vulnérables et de clarifier les conséquences de tout manquement à cet égard. Les motivations du défendeur à atteindre à la vie privée d'une personne, y compris le gain financier personnel, et le partage délibéré des renseignements avec des criminels augmentent la gravité de l'incident et les sanctions encourues.

G.D. v. South Coast British Columbia Transportation Authority, 2024 BCCA 252

Lire les détails de l'affaire (disponible en anglais seulement)

Faits

La Cour d'appel de la Colombie-Britannique a apporté des éclaircissements sur la responsabilité des dépositaires de données en cas d'atteinte à la protection des données. Cette affaire concernait une atteinte à la protection des données par des pirates informatiques tiers malveillants qui ont accédé aux renseignements personnels sensibles des employés, y compris leurs numéros d'assurance sociale, leurs renseignements bancaires, leurs dates de naissance et leurs adresses. L'action collective projetée a été déposée au nom des personnes touchées à l'encontre de TransLink, le dépositaire de la base de données, alléguant qu'il avait agi de manière imprudente en ne faisant rien pour empêcher l'atteinte à la protection des données.

Décision

La loi de la Colombie-Britannique intitulée *Privacy Act* crée une cause d'action pour les atteintes délibérées à la vie privée. Lors de la certification, le juge en chambre a rejeté les prétentions du demandeur au titre de cette loi au motif que le défendeur, même s'il était insouciant, n'avait pas délibérément atteint à la vie privée des membres du groupe en n'empêchant pas un tiers d'accéder à leurs renseignements sans autorisation. La Cour d'appel de la Colombie-Britannique a infirmé cette décision, estimant qu'il est au moins possible de soutenir qu'un dépositaire de données qui ne protège pas adéquatement les renseignements personnels peut être tenu responsable d'une atteinte délibérée à la vie privée.

Le juge en chambre a également rejeté la prétention de négligence du demandeur au motif que celle-ci était fondée sur une violation de la loi de la Colombie-Britannique intitulée *Freedom of Information and Protection of Privacy Act* (BCFIPPA), car cette loi ne crée pas de cause d'action. La Cour a estimé que la prétention de négligence n'était pas vouée à l'échec, estimant que les violations alléguées de la BCFIPPA constituaient un contexte pertinent et n'empêchaient pas TransLink d'avoir en common law une obligation de diligence envers ses employés et ses clients en ce qui concerne la protection de leurs renseignements personnels.

La Cour d'appel a renvoyé la question de la certification de l'action au juge en chambre.

Point principal à retenir

Les dépositaires de bases de données peuvent être tenus responsables, en vertu des lois sur la protection des renseignements personnels, d'avoir omis par négligence d'empêcher l'accès non autorisé à des renseignements personnels sensibles, même s'ils n'ont pas eu l'intention de commettre l'atteinte sous-jacente ou s'ils n'y ont pas participé. Cela contraste avec le délit d'intrusion dans l'intimité en common law, lequel, selon les tribunaux de l'Ontario, ne s'applique pas aux dépositaires de bases de données.

L'affaire précise également que les violations des lois sur la protection des renseignements personnels qui ne prévoient pas elles-mêmes une cause d'action autonome peuvent néanmoins servir à déterminer si l'omission d'un défendeur à empêcher une atteinte à la protection des données constituait un comportement « délibéré » aux fins des prétentions invoquées en vertu des lois sur la protection des renseignements personnels applicables.

Campbell v. Capital One Financial Corporation, 2024 BCCA 253

Lire les détails de l'affaire (disponible en anglais seulement)

Faits

La Cour d'appel de la Colombie-Britannique a récemment fourni des orientations concernant les prétentions d'abus de confiance et de négligence dans le cadre d'une action collective découlant d'une atteinte à la protection des données touchant des personnes ayant demandé ou détenu des cartes de crédit émises par Capital One.

Décision

La décision porte sur les causes d'action viables dans le contexte d'une action collective pour atteinte à la protection des données. Le demandeur a fait appel de la décision du juge de la requête en certification de biffer ses prétentions d'abus de confiance et de délit d'intrusion dans l'intimité en common law. Les défendeurs ont interjeté appel de la certification des prétentions de violation des lois provinciales sur la protection des renseignements personnels, de négligence, de rupture de contrat et de violation des lois sur la protection du consommateur.

Le demandeur avait allégué que le pirate informatique était responsable du délit d'intrusion dans l'intimité et de violation des lois provinciales sur la protection des renseignements personnels, et que Capital One était conjointement responsable de tout dommage moral causé par le pirate informatique en vertu de la loi de la Colombie-Britannique intitulée *Negligence Act*. La Cour d'appel n'a pas été de cet avis, estimant que cette loi ne pouvait être invoquée pour rendre une partie négligente conjointement responsable de dommages dont elle n'aurait jamais pu être responsable si elle avait agi seule. Étant donné que les dommages moraux recouvrables en cas de délit d'intrusion dans l'intimité en common law ou de violation des lois sur la protection des renseignements personnels sont d'une nature différente de ceux qui le sont en cas de négligence, Capital One ne pouvait être tenue conjointement responsable des dommages moraux causés par le pirate informatique. La Cour d'appel a refusé de répondre à la question de savoir si le délit d'intrusion dans l'intimité est reconnu en Colombie-Britannique.

La Cour d'appel a également rejeté la prétention d'abus de confiance du demandeur au motif que le défendeur avait conservé à tort des renseignements sur les clients. Pour le délit d'abus de confiance, le demandeur doit établir qu'il a subi un préjudice par suite de la violation de l'obligation de confiance. Or, il n'a allégué avoir subi un préjudice que par suite des actes du pirate informatique, et non d'une utilisation abusive des renseignements par Capital One. Une telle allégation ne suffisait pas à justifier une prétention d'abus de confiance.

La Cour d'appel a toutefois confirmé les autres causes d'action, y compris les prétentions de violation des lois provinciales sur la protection des renseignements personnels, de négligence, de rupture de contrat et de violation des lois sur la protection du consommateur.

Point principal à retenir

Un demandeur ne peut pas invoquer la loi de la Colombie-Britannique intitulée *Negligence Act* pour obtenir des dommages moraux qu'un pirate informatique pourrait être tenu de payer en vertu des lois provinciales sur la protection des renseignements personnels ou du délit d'intrusion dans l'intimité d'un défendeur dépositaire de bases de données qui, par négligence, n'a pas empêché la même atteinte à la protection des données.

Une prétention d'abus de confiance à l'encontre d'un défendeur dépositaire de bases de données au motif que celui-ci a conservé à tort certains renseignements peut être rejetée s'il n'est pas fait état d'un préjudice distinct par suite de l'utilisation abusive alléguée.

L'affaire met également en lumière l'incertitude qui subsiste quant à la viabilité des prétentions statutaires formulées à l'encontre d'un défendeur dépositaire de bases de données dans le contexte d'une atteinte causée par l'intrusion d'un tiers. À tout le moins, ces prétentions sont susceptibles d'être maintenues à l'étape des contestations préliminaires.

Droit au respect de la vie privée des particuliers

Canada (Privacy Commissioner) v. Facebook, Inc. 2024 FCA 140

Lire les détails de l'affaire (disponible en anglais seulement)

Faits

En 2020, le commissaire à la protection de la vie privée du Canada (le commissaire) a intenté une action contre Facebook devant la Cour fédérale, après avoir conclu, dans le cadre d'une enquête, que Facebook n'avait pas réussi à protéger les renseignements des utilisateurs ou à obtenir de leur part un consentement valide en vue de communiquer des données à des applications tierces hébergées sur sa plateforme. L'action faisait suite à l'enquête du commissaire sur le moissonnage des données des utilisateurs de Facebook par l'application « thisisyourdigitallife ». En première instance, la Cour fédérale a rejeté la demande du commissaire, estimant que ce dernier n'avait pas démontré que Facebook avait omis d'obtenir des utilisateurs un consentement valable pour la communication de leurs données, ni que Facebook n'avait pas réussi à protéger de manière adéquate les données des utilisateurs. La Cour a également estimé qu'elle ne disposait pas de preuves subjectives concernant les attentes et la compréhension des utilisateurs de Facebook en matière de protection des renseignements personnels. La Cour a donc conclu qu'elle était en situation d'« absence de preuves » (*evidentiary vacuum*).

Décision

La Cour d'appel fédérale a accueilli l'appel, estimant que le tribunal de première instance avait commis une erreur dans son analyse des principes de consentement valable et de sécurité prévus par la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE). Plus précisément, elle a conclu que la Cour fédérale avait commis une erreur en fondant sa conclusion exclusivement ou en grande partie sur l'absence de preuves expertes et subjectives. En outre, la Cour d'appel fédérale a estimé que le tribunal de première instance avait omis de vérifier l'existence ou la validité du consentement donné, non seulement par les utilisateurs qui avaient téléchargé les applications tierces, mais aussi par leurs *amis* de façon indépendante. La Cour d'appel fédérale a estimé que les *amis* n'avaient pas eu la possibilité d'examiner les politiques d'utilisation des données des applications tierces, application par application, avant la communication de leurs données, et qu'ils n'avaient pas pu comprendre à quelles fins leurs données seraient utilisées par les applications. Bien que la politique d'utilisation des données de Facebook – à laquelle tous les utilisateurs ont adhéré – contienne des clauses expliquant comment et quand les applications tierces peuvent accéder à leurs données, la Cour d'appel fédérale a estimé que la formulation était trop générale pour constituer un consentement valable, car, à la lecture des clauses, un utilisateur ne pouvait pas « [traduction libre] s'informer de manière adéquate des innombrables façons dont une application pouvait utiliser ses données, et ne pouvait donc pas consentir de manière valable à de futures communications à des applications tierces inconnues téléchargées par ses *amis* ».

Point principal à retenir

Cette affaire comprend une analyse approfondie des principes de consentement valable et de sécurité prévus par la LPRPDE.

Parker v. Ontario Medical Association, 2024 FC 667

Lire les détails de l'affaire (disponible en anglais seulement)

Faits

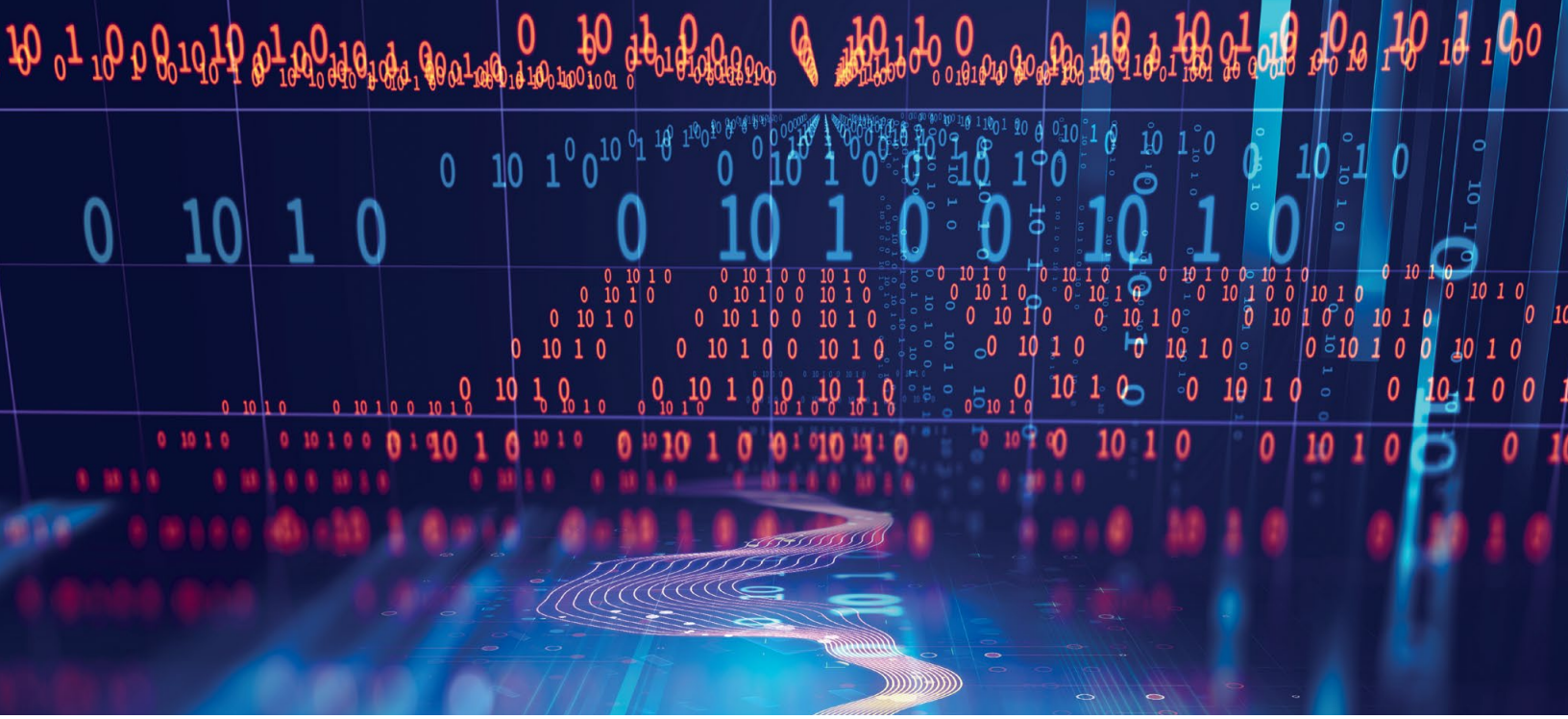
Les requérants, trois médecins, ont demandé un contrôle judiciaire en vertu de l'article 14 de la LPRPDE concernant une étude commandée par l'intimée, l'Ontario Medical Association (OMA), concernant les frais généraux des médecins. Dans le cadre de cette étude, l'OMA devait communiquer à Statistique Canada le prénom, le nom, la date de naissance, le sexe, l'adresse principale et la spécialité des médecins. Les requérants étaient membres de l'Ontario Specialists Association (OSA). L'OSA a déposé une plainte auprès du Commissariat à la protection de la vie privée du Canada (CPVP), alléguant que l'étude proposée par l'OMA contreviendrait à l'article 6.1 et au principe 4.3 de la LPRPDE. Le CPVP a rejeté la plainte au motif que l'étude ne constituait pas une « activité commerciale » au sens de la LPRPDE et qu'elle n'entrait donc pas dans le champ d'application de la loi. En outre, le CPVP a estimé qu'il n'avait pas compétence pour enquêter sur la plainte. Les médecins ont saisi la Cour fédérale d'une demande de contrôle judiciaire de la décision du CPVP.

Décision

La Cour a rejeté la demande de contrôle judiciaire, estimant que l'étude proposée ne constituait pas une « activité commerciale » au sens de la LPRPDE. Par conséquent, la LPRPDE ne s'appliquait pas. La juge Fothergill a conclu que les renseignements que l'OMA souhaitait communiquer à Statistique Canada constituaient des « renseignements personnels » au sens de la LPRPDE, car ils étaient destinés à permettre l'identification des individus. Toutefois, la Cour a estimé que la communication des renseignements personnels des médecins à Statistique Canada ne constituait pas une « activité commerciale » parce qu'elle ne comportait pas « [traduction libre] l'échange, le commerce, l'achat et la vente » de quoi que ce soit. L'étude proposée visait à soutenir les négociations avec le gouvernement en vue d'un accord sur les services médicaux (ASM), qui fixe les taux de facturation des services de santé en Ontario. L'OMA ne tirerait aucun profit ou avantage financier de l'étude proposée ou de la négociation de l'ASM. En outre, l'OMA n'agit pas au nom du gouvernement lorsqu'elle reçoit ou paie les factures des médecins, et n'oriente pas les patients vers des médecins pour qu'ils reçoivent un traitement. L'objectif de l'étude était de fournir des renseignements sur les frais généraux des médecins et de promouvoir une plus grande « relativité des revenus » (*income relativity*) dans le prochain ASM.

Point principal à retenir

Cette analyse fait la lumière sur ce qui constitue – ou non – une « activité commerciale » au sens de la LPRPDE. Par exemple, l'échange de renseignements personnels peut ne pas constituer une « activité commerciale » si l'organisation qui communique les renseignements ne tire pas de profit ou d'avantage financier ou autre de la communication.



Cyberattaques et atteintes à la protection des données : rapports

Conclusions en vertu de la LPRPDE n° 2024-002, Re, Commissariat à la protection de la vie privée du Canada

Lire les détails de l'affaire

Faits

Un client de la société de télésurveillance Brinks Home (Brinks) a déposé une plainte auprès du Commissariat à la protection de la vie privée du Canada (CPVP) après avoir consulté par inadvertance les renseignements personnels d'autres clients sur le portail en ligne de Brinks. Peu après, Brinks a modifié les paramètres du portail en ligne pour empêcher l'affichage de ces renseignements. Le CPVP a mené une enquête pour déterminer si Brinks avait mis en place des mesures de sécurité adéquates et si elle s'était conformée aux exigences de la LPRPDE en matière de signalement des atteintes à la vie privée.

Décision

Le CPVP a établi que Brinks n'avait pas su protéger adéquatement les renseignements personnels de ses clients contre des accès non autorisés, mais qu'elle avait par la suite mis en place des mesures techniques et des règles de procédure pour éviter que de tels incidents se reproduisent. Enfin, Brinks a vendu l'ensemble des comptes de ses clients. Pour ces raisons, le CPVP a estimé que l'élément de la plainte relatif à la protection des données était fondé et résolu. Pour déterminer si Brinks s'est conformée aux exigences en matière de signalement des atteintes à la vie privée, le CPVP a conclu que les renseignements personnels en cause pouvaient être considérés comme sensibles, mais que la probabilité d'une mauvaise utilisation était faible. Le CPVP a établi que l'atteinte ne posait pas un risque réel de préjudice grave et que Brinks n'était pas tenue d'en aviser les individus touchés ou de la signaler au CPVP.

Point principal à retenir

Cette affaire souligne l'importance de protéger adéquatement les renseignements personnels et de prendre des mesures actives permettant d'atténuer tout préjudice potentiel en cas d'atteinte à la vie privée.

A Medical Imaging Clinic, Re, Commissaire à l'information et à la protection de la vie privée de l'Ontario

Lire les détails de l'affaire (disponible en anglais seulement)

Faits

Une clinique d'imagerie médicale a informé le Commissaire à l'information et à la protection de la vie privée de l'Ontario (CIPVP) qu'elle avait été victime d'une attaque par rançongiciel. La clinique a payé la rançon en échange d'une clé de chiffrement qui lui a permis de récupérer tous les fichiers touchés. Le CIPVP a mené une enquête pour déterminer si la clinique avait pris des mesures raisonnables pour protéger les renseignements personnels sur la santé et si un examen était justifié en vertu de la *Loi de 2004 sur la protection des renseignements personnels sur la santé*.

Décision

Le CIPVP a établi que la clinique avait déployé des efforts suffisants pour déterminer l'ampleur de la violation, qui comprenait des renseignements sur les patients et les employés, ainsi que des codes de facturation. Le CIPVP a également établi que, en affichant un avis dans l'entrée de la clinique et au bureau d'information, de même qu'un avis « surgissant » (« pop-up ») sur son site Web, la clinique avait fourni un avis approprié. En outre, la clinique a envoyé des avis à plus de 14 000 médecins traitants, ainsi qu'à ses employés et à ses partenaires de santé. En outre, pour réduire au minimum les risques qu'une telle violation se reproduise, la clinique a pris un certain nombre de mesures, notamment les suivantes : elle a revu sa politique en matière de mots de passe, elle s'est dotée d'une politique de repérage et de suppression des comptes d'utilisateurs dormants, et elle a modifié son approche en matière de sauvegardes afin de s'assurer de toujours conserver hors ligne une sauvegarde impossible à compromettre en cas de violation ultérieure. Sur la base de ces constatations, le CIPVP a estimé qu'un examen n'était pas justifié.

Point principal à retenir

L'affaire démontre que les victimes d'attaques de rançongiciel qui fournissent un avis approprié et qui prennent des mesures correctives adéquates permettant de réduire au minimum les risques de violation future peuvent éviter ou réduire les examens du CIPVP.

Vankoughtnett, Re, Commissaire à l'information et à la protection de la vie privée de la Saskatchewan

Lire les détails de l'affaire (disponible en anglais seulement)

Faits

Quatre dentistes exploitaient une clinique de dentisterie générale en tant qu'entreprise individuelle aux termes d'un accord de partage des coûts. L'un des quatre dentistes s'est retiré de l'accord, tout en emportant avec lui une copie de l'ensemble de la base de données des patients de la clinique. Les dentistes restants ont contacté le commissaire à l'information et à la protection de la vie privée (CIPVP) de la Saskatchewan pour lui faire part de leurs inquiétudes. Le CIPVP, jugeant qu'il était compétent pour enquêter sur l'affaire, a examiné s'il y avait eu des atteintes à la vie privée et si les dentistes restants y avaient réagi de manière adéquate.

Décision

Le CIPVP a établi que, en vertu de la loi de la Saskatchewan intitulée *The Health Information Protection Act* (HIPA), la collecte par le dentiste sortant de l'ensemble de la base de données des patients n'était pas autorisée et constituait une atteinte à la vie privée. Le CIPVP a constaté que la cause première de l'atteinte à la vie privée était l'absence de mesures techniques de protection des renseignements personnels, car le dentiste sortant n'aurait pas dû être en mesure d'accéder aux renseignements des patients des dentistes restants. Pour ces raisons, le CIPVP a estimé que les dentistes restants avaient manqué à leur obligation de protéger les renseignements personnels sur la santé des patients en vertu de la HIPA. Il a constaté par ailleurs que les dentistes restants avaient pris des mesures raisonnables pour limiter cette atteinte en la signalant au CIPVP et en veillant à ce que le dentiste sortant ne puisse plus accéder à la base de données, mais qu'ils n'avaient pas pris les mesures nécessaires pour aviser les individus touchés. Le CIPVP a aussi jugé que la version actualisée de la politique de confidentialité adoptée par les dentistes restants dans l'accord de partage des coûts était inadéquate, car elle confondait les exigences de la LPRPDE avec celles de la HIPA.

Point principal à retenir

Cette affaire montre à quel point les autorités de réglementation attendent des professionnels de la santé qu'ils veillent à protéger de manière adéquate les renseignements personnels sur la santé des patients et à empêcher tout accès non autorisé.

Actions collectives en matière de protection des renseignements personnels : données biométriques

Homsy c. Google, 2024 QCCS 1324

Lire les détails de l'affaire

Faits

Le demandeur, un individu dont les données personnelles avaient été collectées, a demandé au tribunal l'autorisation d'exercer une action collective contre la défenderesse, Google. Le demandeur reprochait à la défenderesse d'avoir procédé, par l'intermédiaire de l'application Google Photos, à l'extraction, à la collecte, à la conservation et à l'utilisation des données biométriques faciales des résidents du Québec, sans fournir de préavis suffisant, sans obtenir un consentement éclairé et sans publier de politiques de conservation des données biométriques.

Le demandeur réclamait des dommages compensatoires en vertu de la *Loi sur la protection des renseignements personnels dans le secteur privé* (LPRPSP) et du CcQ. Le demandeur réclamait également des dommages punitifs en vertu de l'article 272 de la *Loi sur la protection du consommateur* (LPC) et de l'article 49 de la *Charte des droits et libertés de la personne* (Charte québécoise).

Décision

Le tribunal a autorisé l'exercice de l'action collective contre Google.

Le tribunal a estimé que les données biométriques faciales constituaient des renseignements personnels au sens de l'article 2 de la LPRPSP. Par conséquent, la pratique de Google consistant à extraire, à collecter, à conserver et à utiliser les données biométriques faciales des résidents du Québec et à communiquer ces données à des tiers sans leur consentement pourrait être considérée comme une violation des articles 8, 10, 13, 14 et 17 de la LPRPSP, ainsi que des articles 35 et 37 du CcQ.

Selon le tribunal, la pratique de Google pouvait être considérée comme une faute civile au sens de l'article 1457 du CcQ. Le tribunal a également autorisé la question commune de déterminer si Google a volontairement violé l'article 5 de la Charte québécoise, qui prévoit le droit à la vie privée. Le demandeur a donc été autorisé à demander des dommages punitifs en vertu de l'article 49 de la Charte québécoise, en plus des dommages compensatoires.

Enfin, la lecture des conditions d'utilisation (*Terms of Services*) de Google a démontré qu'il n'y avait aucune mention de l'extraction, de la collecte, de la conservation et de l'utilisation des données biométriques faciales des membres. En faisant cette omission, la défenderesse pourrait avoir passé sous silence un fait important dans ses représentations aux consommateurs.

Point principal à retenir

Étant donné le faible fardeau du demandeur à l'étape de l'autorisation d'exercer une action collective au Québec, les allégations d'utilisation de renseignements biométriques sans le consentement d'une personne peuvent être suffisantes pour permettre l'autorisation d'exercer une action collective alléguant une violation du droit à la vie privée. Lorsqu'une telle violation est délibérée, elle peut donner lieu à des dommages punitifs, en plus des dommages compensatoires.

Lam v. Flo Health Inc, 2024 BCSC 391

Lire les détails de l'affaire (disponible en anglais seulement)

Faits

La Cour suprême de la Colombie-Britannique a certifié une action collective contre Flo Health Inc. (Flo), une société qui fabrique une application permettant de suivre la santé reproductive des femmes. Le demandeur allègue que Flo a atteint à la vie privée des utilisatrices en divulguant des renseignements personnels sensibles à des tiers sans leur consentement. Le groupe proposé comprend toutes les utilisatrices du Canada hors Québec.

Décision

La Cour a certifié les questions communes relatives à la violation des lois sur la protection des renseignements personnels, à l'intrusion dans l'intimité (sauf pour les membres du groupe résidant en Colombie-Britannique et en Alberta), à l'abus de confiance et à la violation de la *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE). La Cour a toutefois rejeté les prétentions de négligence, d'enrichissement injustifié, de violation des lois provinciales sur la protection du consommateur, de conversion et, pour les résidents de la Colombie-Britannique et de l'Alberta, d'intrusion dans l'intimité.

La Cour a rejeté les arguments de Flo selon lesquels les prétentions du demandeur étaient interdites par les clauses d'exclusion de responsabilité et de renonciation aux actions collectives figurant dans ses conditions d'utilisation, au motif que ces clauses étaient iniques et contraires à l'intérêt public.

Point principal à retenir

La décision confirme que les clauses de renonciation aux actions collectives dans les contrats de consommation sont généralement inapplicables en Colombie-Britannique.

La violation de l'obligation de confiance renvoie à la vaste notion de préjudice et n'exige pas du demandeur qu'il invoque une perte économique ou un trouble psychologique grave et prolongé.

Bien qu'une violation de la LPRPDE ne crée pas en soi une cause d'action, de telles violations peuvent constituer un contexte pertinent pour d'autres causes d'action.

Attente au respect de la vie privée

R. c. Bykovets, 2024 CSC 6

Lire les détails de l'affaire

Faits

L'appelant, Bykovets, a été déclaré coupable de fraude par carte de crédit. Au cours de leur enquête, les services de police ont obtenu de Moneris, une société tierce de traitement des paiements, les adresses IP utilisées pour les opérations de l'appelant. Ils ont fait cette démarche sans autorisation judiciaire préalable.

L'appelant a allégué que la demande faite par la police à Moneris avait violé son droit à la protection contre les fouilles, les perquisitions et les saisies abusives garanti par l'article 8 de la *Charte canadienne des droits et libertés*, partie I de la *Loi constitutionnelle de 1982*, Annexe B de la *Loi de 1982 sur le Canada* (Royaume-Uni), 1982, c. 11 (Charte canadienne). La question soumise à la Cour suprême était celle de savoir si un individu avait une attente raisonnable au respect de sa vie privée à l'égard de son adresse IP.

Décision

La Cour suprême a accueilli l'appel à la majorité et ordonné un nouveau procès, estimant que l'adresse IP d'un individu est protégée par l'article 8 de la Charte canadienne. Les services de police sont donc tenus d'obtenir une autorisation judiciaire avant de se procurer une adresse IP auprès d'un tiers.

La Cour a interprété l'article 8 de la Charte canadienne de manière large et téléologique. Définir une « attente raisonnable au respect de la vie privée » est une opération de mise en balance. En l'espèce, la balance penche en faveur de l'extension de l'attente raisonnable au respect de la vie privée aux adresses IP. Le caractère éminemment privé des renseignements que peut révéler une adresse IP suggère fortement que le droit du public de ne pas être importuné devrait l'emporter sur le droit du gouvernement de réaliser ses objectifs d'application de la loi.

Internet a fait augmenter de manière exponentielle tant la qualité que la quantité de renseignements stockés à propos des internautes. Il a permis à des sociétés privées de suivre les utilisateurs et d'établir des profils contenant des renseignements que les utilisateurs ne savent pas qu'ils dévoilent. En concentrant cette masse de renseignements entre les mains de tiers du secteur privé, Internet a modifié la topographie de la vie privée sous le régime de la Charte canadienne. Il a ajouté un tiers à l'écosystème constitutionnel, et a fait de la relation horizontale entre l'individu et l'État une relation tripartite.

Bien que l'article 8 de la Charte canadienne ne s'applique pas aux tiers eux-mêmes, ceux-ci jouent le rôle de médiateur(s) dans une relation directement régie par cet article – celle entre le défendeur et la police. La surveillance judiciaire est donc le moyen approprié pour enlever aux sociétés privées le pouvoir de décider s'il convient de dévoiler des renseignements et, le cas échéant, en quelle quantité.

Les juges dissidents auraient rejeté l'appel, car, selon eux, l'appelant n'avait pas d'attente raisonnable au respect de sa vie privée à l'égard de son adresse IP. Par conséquent, la police n'aurait pas eu besoin d'une autorisation judiciaire.

Point principal à retenir

L'attente raisonnable au respect de la vie privée comprend la protection de l'adresse IP d'un individu et est donc protégée par l'article 8 de la Charte canadienne. Il faut donc se procurer une autorisation judiciaire préalable pour obtenir une adresse IP auprès d'un tiers.

Accès à l'information

Excavation National inc. c. Autorité des marchés publics, 2024 QCCS 2159

Lire les détails de l'affaire

Faits

La demanderesse, Excavation National, est une entreprise de construction faisant affaire au Québec. La défenderesse, l'Autorité des marchés publics (AMP), est un organisme public ayant comme rôle la surveillance des marchés publics et l'application des lois et des règlements encadrant les contrats publics au Québec.

Le 16 novembre 2023, l'AMP a rendu une décision aux termes de laquelle elle a refusé d'autoriser la conclusion d'un contrat entre Excavation National et un organisme public, ce qui a eu pour effet d'inscrire la demanderesse au registre des entreprises non admissibles aux contrats publics au Québec.

La demanderesse a déposé un pourvoi en contrôle judiciaire de la décision de l'AMP, dans lequel elle demandait la communication d'une grande partie des documents de l'AMP. Elle a fait valoir que la Cour avait besoin du dossier complet pour pouvoir se prononcer sur la légalité de la décision de l'AMP. La demanderesse a simultanément déposé une demande d'accès à l'information auprès de l'AMP. L'AMP a refusé de transmettre les documents demandés et a reporté la décision concernant la demande d'accès à l'information.

Décision

Le tribunal a rejeté les demandes de la demanderesse, au motif que la communication du dossier complet de l'AMP constituait une partie de pêche. En particulier, pour se prononcer sur la légalité de la décision, le tribunal n'avait pas besoin du dossier complet de l'AMP, notamment à la lumière des motifs détaillés fournis à Excavation National.

Point principal à retenir

Dans le cadre du contrôle judiciaire d'une décision administrative prise par un organisme public, il ne sera pas fait droit aux parties de pêche prenant la forme de demandes d'accès à l'information visant le dossier complet du décideur. Le tribunal n'ordonnera la communication de documents ou de preuves supplémentaires que lorsque cela est nécessaire pour évaluer le caractère raisonnable de la décision administrative.

Gravel c. Agence du revenu du Québec, 2024 QCCQ 1589

Lire les détails de l'affaire

Faits

L'appelant, Gravel, qui faisait l'objet d'une enquête de la part de l'Agence du revenu du Québec (ARQ), a déposé une demande d'accès à l'information auprès de l'ARQ, afin d'obtenir divers documents et renseignements, notamment la liste des employés de l'ARQ qui avaient accédé à son dossier fiscal. L'ARQ a refusé de lui fournir les documents demandés. La Commission d'accès à l'information (la Commission) a partiellement accueilli la demande de révision de la décision de l'ARQ introduite par l'appelant. L'ARQ a détruit certaines données visées par la demande de Gravel entre la date du refus de l'ARQ de fournir les documents demandés et celle de la décision de la Commission. La destruction des données a rendu impossible la production de la liste d'employés demandée.

La Commission a conclu que la destruction des données ne constituait pas une violation de l'article 52.1 de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (Loi sur l'accès), puisque ce qui a été détruit ne constituait pas un document, mais des données permettant de produire le document demandé. Gravel a fait appel de la décision de la Commission devant la Cour du Québec.

Décision

Le tribunal a accueilli l'appel et infirmé la décision de la Commission.

Le tribunal a conclu que la Commission avait erré en droit et était allée à l'encontre de la jurisprudence lorsqu'elle avait écrit que les données informatiques qui correspondaient à la demande d'accès détenues par l'ARQ n'étaient pas un document.

Interprétant l'article 1 de la Loi sur l'accès, le tribunal a déterminé que ce n'était pas parce qu'il fallait interroger le système de l'ARQ pour produire un document, qu'il fallait conclure que le document n'existait pas. Une seule exception existe à cette règle, si des calculs ou des comparaisons doivent être faits, alors là seulement, il s'agit de la création d'un nouveau document.

Par conséquent, le tribunal a déterminé que l'ARQ détenait le document demandé au sens de l'article 1 de la Loi sur l'accès au moment où la demande d'accès avait été déposée par Gravel. L'ARQ avait l'obligation de conserver le document le temps de permettre des recours conformément aux articles 52.1 et 102.1 de la Loi sur l'accès. En détruisant les données, l'ARQ a manqué à son obligation de conservation de documents prévue aux articles 52.1 et 102.1 de la Loi sur l'accès.

Point principal à retenir

Des données informatiques peuvent constituer un document dans le contexte d'une réponse à une demande d'accès à l'information. Une seule exception à cette règle existe, si des calculs ou des comparaisons doivent être faits, alors là seulement, il s'agit de la création d'un nouveau document. Les données informatiques qui sont visées par une demande d'accès à l'information et un appel ultérieur doivent être conservées.

Ontario (Procureur général) c. Ontario (Commissaire à l'information et à la protection de la vie privée), 2024 CSC 4

Lire les détails de l'affaire

Faits

Dans cette affaire, la Cour suprême du Canada a examiné la portée de la confidentialité du Cabinet dans le contexte d'une demande d'accès à l'information en vertu de la *Loi sur l'accès à l'information et la protection de la vie privée* (Ontario) (LAIPVP).

Un journaliste a demandé d'avoir accès à 23 « lettres de mandat » que le premier ministre de l'Ontario avait remises à chacun de ses ministres peu après avoir formé le gouvernement en 2018. Le Bureau du Cabinet a refusé la demande en prétendant que les lettres de mandat étaient soustraites de la divulgation en application du paragraphe 12(1) de la LAIPVP parce qu'il s'agissait de documents qui auraient pour effet de révéler l'objet des délibérations du Cabinet. Le Commissaire à l'information et à la protection de la vie privée de l'Ontario (CIPVP) a conclu que les lettres n'étaient pas exemptées et a ordonné leur divulgation. Lors de la révision judiciaire, la Cour divisionnaire de l'Ontario a infirmé la décision, estimant que les lettres étaient exemptes de divulgation, et la Cour d'appel de l'Ontario s'est dit du même avis.

Décision

La Cour suprême a jugé à l'unanimité que les lettres de mandat étaient exemptes de divulgation. Le juge Karakatsanis a rédigé l'opinion des juges majoritaires, tandis que la juge Côté a rédigé une opinion concordante qui est en accord avec le résultat de la majorité, mais qui n'est pas en accord avec son approche de la norme de contrôle de la décision du CIPVP.

Les juges majoritaires ont estimé que le CIPVP ne s'était pas penché adéquatement sur le contexte juridique et factuel général au moment d'interpréter le paragraphe 12(1) de la LAIPVP. En particulier, le CIPVP n'a pas apprécié les conventions et traditions constitutionnelles qui régissent la confidentialité et le processus de délibération du Cabinet. Dans une démocratie constitutionnelle, la confidentialité des délibérations du Cabinet est une condition préalable au gouvernement responsable. Elle s'impose pour que les ministres ne se censurent pas lors d'un débat sur une politique, et ensuite qu'ils puissent être solidaires en public, et soient tenus responsables collectivement, dès qu'une décision de politique générale est prise et annoncée.

Le défaut du CIPVP de tenir compte de ce contexte l'a amené à retenir une interprétation déraisonnablement étroite du paragraphe 12(1), et ainsi à ne pas protéger les « résultats » des délibérations du Cabinet, et à mal qualifier les lettres de mandat elles-mêmes comme un produit final des délibérations du Cabinet. Les juges majoritaires ont estimé que la confidentialité du Cabinet inclut la prérogative de choisir l'occasion et la manière d'annoncer ses décisions. Les lettres de mandat faisaient état de priorités stratégiques qui n'avaient pas encore été annoncées et qui, n'étant pas encore publiques, pouvaient faire l'objet d'un débat plus approfondi et donc être modifiées par les délibérations du Cabinet. Les lettres de mandat étaient donc soumises à la confidentialité du Cabinet et exemptes de divulgation en application du paragraphe 12(1) de la LAIPVP.

Les juges majoritaires ont examiné la décision du CIPVP selon la norme de la décision raisonnable, puisque c'était la norme invoquée par les parties. La juge Côté a écrit que la décision devait être examinée selon la norme de la décision correcte parce que le privilège du Cabinet est une question qui revêt une importance capitale pour le système juridique dans son ensemble.

Point principal à retenir

Les exemptions de divulgation prévues par les lois sur l'accès à l'information doivent être interprétées dans leur contexte juridique et factuel général, y compris les normes et conventions constitutionnelles pertinentes.

Le privilège du Cabinet est un principe constitutionnel fondamental, et les exemptions de divulgation destinées à le protéger doivent être interprétées de manière large.

Le privilège du Cabinet comprend la prérogative du gouvernement de décider de l'occasion et de la manière d'annoncer les décisions du Cabinet. Les décisions du Cabinet qui n'ont pas encore été annoncées peuvent donc être exemptes de divulgation en application des lois sur l'accès à l'information.

Miville de Chêne c. Québec (Ville), 2024 QCCAI 127

Lire les détails de l'affaire

Faits

Le demandeur a déposé une demande d'accès auprès de la Ville de Québec, la défenderesse, afin d'obtenir l'accès à divers documents relatifs à une convention de gestion datant de 2011 et à un bail commercial (les conventions) portant sur l'exploitation du Centre Vidéotron. De nombreux tiers prenaient part aux conventions.

En particulier, le demandeur a demandé l'accès aux états financiers de 2015 et des exercices subséquents. La Ville de Québec a refusé de les lui fournir, soutenant qu'elle n'en avait pas la détention juridique, car ces documents appartenaient à des tiers et que la Ville n'en avait pas la détention physique ni juridique.

Décision

La Commission a conclu que la Ville n'avait pas la détention juridique des états financiers. Même si, lors de visites semestrielles, les employés de la Ville de Québec y avaient eu accès, les états financiers ont été produits par des tiers pour leur propre usage et non pour celui de la Ville. En prenant sa décision, la Commission a tenu compte du fait que les états financiers avaient été fournis à la Ville aux fins de vérification seulement et que la Ville n'était pas dans une situation de contrôle sur les documents et qu'elle ne pouvait pas les requérir en tout temps. En outre, la Commission a confirmé que la Ville ne tentait pas de se soustraire à ses responsabilités en n'ayant pas la détention physique des documents.

Point principal à retenir

Les organisations n'ont pas la détention juridique de documents du simple fait d'y avoir accès aux fins de vérification, si elles ne sont pas dans une situation de contrôle sur les documents.

Respect de la vie privée et emploi

Conseil scolaire de district de la région de York c. Fédération des enseignantes et des enseignants de l'élémentaire de l'Ontario, 2024 CSC 22

Lire les détails de l'affaire

Faits

L'appelant, le Conseil scolaire de district de la région de York, représente une école publique de l'Ontario. L'intimée, la Fédération des enseignantes et des enseignants de l'élémentaire de l'Ontario, représente deux enseignantes employées par une école publique de l'Ontario.

Deux enseignantes ont consigné leurs communications privées relatives à des préoccupations quant à leur milieu de travail sur un journal électronique personnel partagé, protégé par un mot de passe, et sauvegardé sur une plateforme infonuagique. Le directeur de l'école est entré dans la salle de classe d'une des enseignantes et, en son absence, a fait défiler le document et pris des photos avec son téléphone cellulaire. Le conseil scolaire s'est ensuite basé sur ces communications pour formuler des réprimandes écrites. Le syndicat des enseignantes a déposé un grief pour contester cette mesure disciplinaire, alléguant que la fouille avait violé leur droit au respect de la vie privée au travail. Une arbitre du travail a conclu qu'il n'y avait pas eu atteinte à l'attente raisonnable des enseignantes au respect de la vie privée, compte tenu du droit du conseil scolaire de gérer le lieu de travail.

La Cour d'appel de l'Ontario a été saisie de la question de savoir si des employés avaient droit à la protection contre les fouilles, les perquisitions et les saisies abusives en milieu de travail en application de l'article 8 de la *Charte canadienne des droits et libertés*, partie I de la *Loi constitutionnelle de 1982*, Annexe B de la *Loi de 1982 sur le Canada* (Royaume-Uni), 1982, c. 11 (Charte canadienne). La Cour d'appel a estimé que la fouille était déraisonnable au regard de l'article 8 de la Charte canadienne. L'appelant a interjeté appel de cette décision, principalement au motif que la Charte canadienne ne s'appliquait pas aux conseils scolaires publics de l'Ontario.

Décision

La Cour suprême a rejeté le pourvoi.

Selon la majorité des juges de la Cour suprême, les enseignantes et les enseignants de l'Ontario sont protégés par l'article 8 de la Charte canadienne et ont donc droit à la protection contre les fouilles, perquisitions et saisies abusives en milieu de travail.

L'article 32 de la Charte canadienne précise son champ d'application. La Charte canadienne s'applique au gouvernement, mais peut également être étendue à d'autres entités. C'est le cas lorsqu'une entité peut – soit de par sa nature même, soit à cause du degré de contrôle exercé par le gouvernement sur elle – être à juste titre considérée comme faisant partie du « gouvernement » au sens de l'article 32 de la Charte canadienne.

La Cour suprême a conclu à la majorité que la Charte canadienne s'appliquait aux conseils scolaires publics de l'Ontario, car ceux-ci font partie du gouvernement de par leur nature même, au sens voulu par l'application de l'article 32. Il en est ainsi parce que l'enseignement public est une mission gouvernementale de par sa nature même et que les conseils scolaires publics de l'Ontario sont une émanation du gouvernement. Il s'ensuit que toutes les activités menées par les conseils scolaires publics de l'Ontario sont soumises à la Charte canadienne.

Les juges concordants ont reconnu l'applicabilité de la Charte canadienne aux conseils scolaires publics.

Point principal à retenir

La Cour suprême a confirmé que la Charte canadienne s'appliquait aux conseils scolaires publics de l'Ontario. Elle a toutefois laissé ouverte la question de l'applicabilité de la Charte canadienne aux écoles publiques d'autres provinces.

Pelletier c. Transvrac Montréal Laval inc., 2024 QCCAI 102

Lire les détails de l'affaire

Faits

Pelletier, la demanderesse, a présenté une demande d'accès à son ancien employeur, Transvrac Montréal Laval Inc., afin d'accéder à ses courriels et à ses contacts personnels stockés dans sa boîte courriel professionnelle. Avant son départ, une règle de transfert automatique avait été mise en place pour transférer ses courriels arrivant dans sa boîte personnelle vers sa boîte professionnelle.

Cela a conduit à un mélange de courriels personnels et de courriels professionnels dans sa boîte professionnelle. Après la fin d'emploi de la demanderesse, Transvrac a procédé à la migration de sa boîte courriel professionnelle vers la boîte Outlook du directeur général.

Transvrac s'est inquiétée de la lourdeur du traitement de la demande, qui nécessitait l'analyse de plus de 5 000 courriels. L'entreprise a également fait valoir que la liste de contacts contenait des renseignements sur des tiers qui devraient être protégés en vertu de la *Loi sur la protection des renseignements personnels dans le secteur privé*.

Transvrac a demandé à la Commission de ne pas tenir compte de la demande d'accès de la demanderesse au motif que celle-ci était abusive.

Décision

La Commission a conclu que Transvrac devait effectivement analyser tous les courriels qui se trouvaient dans l'ancienne boîte courriel professionnelle de la demanderesse, qui se trouvaient maintenant dans la boîte du directeur général.

Toutefois, la Commission a finalement accédé à la demande de Transvrac d'être exemptée du traitement de la demande d'accès. Elle a estimé que, bien qu'elle ait été faite de bonne foi, la demande de la demanderesse était abusive en raison du volume important de documents visés et de l'effort nécessaire pour départager les communications personnelles des communications professionnelles. La Commission a pris en considération les ressources limitées de l'entreprise, notant que le fait de demander au directeur général d'analyser manuellement plus de 5 000 courriels et 2 000 contacts n'était pas raisonnable compte tenu de la petite taille de l'entreprise et de ses effectifs.

Point principal à retenir

Lorsque des employés utilisent leur boîte courriel professionnelle pour des communications personnelles, cela peut compliquer les obligations de l'entreprise lorsqu'elle répond à des demandes d'accès à l'information. Pour déterminer les obligations de l'entreprise à cet égard, le tribunal peut prendre en considération le volume de documents visés, les efforts requis pour départager les courriels personnels des courriels professionnels, et les ressources de l'entreprise.

Martineau c. Telus, 2024 QCCAI 200

Lire les détails de l'affaire

Faits

Martineau, la demanderesse, a adressé une demande d'accès afin d'obtenir de son ancien employeur plusieurs documents, notamment ses fichiers de payes, ses feuilles de temps et le rapport final d'enquête de harcèlement psychologique. L'enquête avait été menée en vertu du *Code canadien du travail* et du *Règlement sur la prévention du harcèlement et de la violence dans le lieu de travail* (le Règlement). Le paragraphe 30(2) du Règlement, qui stipule que le rapport d'un enquêteur ne doit pas révéler, directement ou indirectement, l'identité des personnes impliquées dans une enquête ou dans le processus de règlement d'une enquête, revêt une importance particulière.

Telus a communiqué certains documents, mais en a retenu d'autres. En particulier, elle a caviardé des extraits du rapport final d'enquête de harcèlement psychologique, invoquant l'article 40 de la *Loi sur la protection des renseignements personnels dans le secteur privé* (LPRPSP), en faisant valoir que les renseignements caviardés contenaient des renseignements personnels concernant des tiers et que leur divulgation serait susceptible de nuire sérieusement à ces personnes.

Décision

La Commission d'accès à l'information (la Commission) a précisé que l'application de l'article 30 du Règlement ne relevait pas de sa juridiction.

En se fondant sur l'article 40 de la LPRPSP, la Commission a conclu que Telus avait raison de ne pas communiquer les extraits du rapport contenant des renseignements personnels concernant des tiers, car leur divulgation pourrait leur nuire sérieusement, notamment entacher leur réputation ou donner lieu à des représailles sur le lieu de travail. Toutefois, la Commission a ordonné à Telus de communiquer les extraits du rapport qui contenaient les renseignements personnels concernant Martineau, étant donné que ces extraits n'étaient pas visés par la protection offerte par l'article 40.

Point principal à retenir

Les organisations peuvent avoir raison de caviarder des renseignements personnels concernant des tiers en application de l'exception prévue à l'article 40 de la LPRPSP lorsque leur divulgation risque de nuire sérieusement à ces tiers, notamment si elle risque d'entacher leur réputation ou de donner lieu à des représailles sur le lieu de travail.

Compétence des autorités chargées de la protection des renseignements personnels

Forest c. Bell, 2024 QCCAI 202

Lire les détails de l'affaire

Faits

En novembre 2021, Forest, le demandeur, s'est abonné à différents services de Bell, l'intimée, y compris le service de téléphonie résidentielle. À ce moment-là, on l'a informé que seule la première lettre de son prénom et son nom de famille, « Forest, S. », accompagneraient son numéro de téléphone dans l'annuaire. Le sommaire de la transaction sous « Directory listing » l'indique bien.

Le 28 mars 2023, ayant constaté que son nom complet, son adresse et son numéro de téléphone étaient affichés et diffusés publiquement sur le site Canada411.ca, Forest a contacté le service à la clientèle de Bell, afin d'exposer son absence de consentement et d'exiger de faire cesser le partage de ses renseignements personnels avec des tiers, notamment Pages Jaunes. En outre, Forest a souligné qu'il existait un enjeu de sécurité en lien avec sa profession, notamment que la diffusion publique de ses données personnelles présentait un risque.

Comme il n'avait toujours pas reçu satisfaction quant à ses demandes, Forest a formulé, le 28 avril 2023, une demande d'examen de mésentente auprès de la Commission d'accès à l'information (la Commission). Parallèlement à son recours devant la Commission, Forest a également poursuivi l'entreprise devant la Cour du Québec, division des petites créances, et sollicité des conclusions injonctives similaires aux conclusions recherchées devant la Commission, en plus d'une réclamation de nature pécuniaire.

Décision

La Commission a déclaré avoir la compétence exclusive pour examiner la demande d'examen de mésentente présentée par Forest, malgré le recours parallèle exercé devant la Cour du Québec.

Citant l'article 134.2 de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (Loi sur l'accès), la Commission a souligné qu'elle avait compétence exclusive pour trancher les questions relatives aux différends en matière de renseignements personnels en vertu de la *Loi sur la protection des renseignements personnels dans le secteur privé* (LPRPSP).

La Commission a rejeté l'argument de litispendance de Bell, notant qu'elle conservait le pouvoir d'examiner et de résoudre la demande de Forest, indépendamment des procédures judiciaires en cours. La Commission a procédé à l'examen de la plainte de Forest et a conclu que Bell s'était conformée à sa demande initiale en s'assurant que seuls « Forest, S. » et son numéro de téléphone apparaîtraient dans l'annuaire.

Point principal à retenir

La Commission a compétence exclusive sur les différends concernant les renseignements personnels en vertu de la LPRPSP, même si des questions similaires sont traitées par d'autres tribunaux. Les prétentions de litispendance n'empêchent pas la Commission de statuer sur les questions qui relèvent de sa compétence.

Protection du droit au respect de la vie privée dans le cadre des procédures d'injonction

Boisvert Marine inc. c. Dumas, 2024 QCCS 3240

Lire les détails de l'affaire

Faits

La demanderesse, Boisvert Marine Inc. (BMI), exploite un commerce de gros d'articles de loisir et de sport qui se spécialise dans la vente et la réparation de bateaux. Le défendeur, Dumas, est le directeur général de BMI, ce qui lui permettait d'acheter des pièces et de payer des fournisseurs directement au nom de BMI, à même les fonds de BMI.

BMI a pris connaissance de l'existence de transactions louches impliquant Dumas. BMI a allégué que Dumas avait détourné pour son bénéfice personnel plus de 3 millions de dollars, notamment en modifiant le relevé d'opérations bancaires de BMI.

BMI a demandé au tribunal de rendre des ordonnances de type *Mareva* et *Norwich*, ainsi qu'une ordonnance de vérification d'une clé USB par un enquêteur judiciaire.

Décision

Le tribunal a prononcé les ordonnances de type *Mareva* et *Norwich*, ainsi que l'ordonnance de vérification de la clé USB par un expert en informatique.

L'ordonnance de type *Norwich* a obligé les institutions financières mises en cause de communiquer les documents en leur possession qui permettraient à BMI de retracer les fonds que Dumas avait détournés. Le tribunal a déterminé que BMI satisfaisait aux critères d'une ordonnance de type *Norwich* : (1) il existe à première vue quelque chose à reprocher à l'auteur inconnu du préjudice; (2) la personne devant faire l'objet d'un interrogatoire préalable doit avoir quelque chose à voir avec la question en litige – elle ne peut être un simple spectateur; (3) la personne devant faire l'objet de l'interrogatoire préalable doit être la seule source pratique de renseignements dont disposent les demandeurs; (4) la personne devant faire l'objet de l'interrogatoire préalable doit recevoir une compensation raisonnable pour les débours occasionnés par son respect de l'ordonnance portant sur l'interrogatoire préalable, en sus de ses frais de justice; et (5) l'intérêt public à la divulgation l'emporte sur l'attente légitime de respect de la vie privée.

En ce qui concerne le dernier critère, le droit au respect de la vie privée est prévu aux articles 3, 35, 36 et 37 du CcQ et à l'article 5 de la *Charte des droits et libertés de la personne*. Le tribunal a déterminé que, bien que l'attente légitime de respect de la vie privée mérite une attention particulière, elle ne fera pas obstacle à une ordonnance de type *Norwich*.

Point principal à retenir

Le droit à la vie privée ne constitue pas un obstacle à la délivrance d'une ordonnance de type *Norwich*.

De Trinidad c. Chambre de la sécurité financière, 2024 QCCAI 195

Lire les détails de l'affaire

Faits

Le demandeur, de Trinidad, conseiller en sécurité financière et membre accrédité par la Chambre de la sécurité financière (CSF) du Québec, a été visé par une enquête disciplinaire en 2016. Le 25 mai 2018, il a été interrogé dans les bureaux de la CSF et l'entretien a été enregistré. Les enregistrements ont été sauvegardés dans le système informatique de la CSF, et une copie DVD lui a été remise.

En 2019, en revoyant le DVD en prévision de l'audition de la plainte devant le comité de discipline, de Trinidad a constaté que certains passages de l'enregistrement – au cours desquels il aurait fait l'objet de menace de la part des enquêteurs – étaient manquants. Il a demandé à avoir accès aux enregistrements originaux, mais la CSF l'a informé que l'unité de stockage sur laquelle étaient conservés les fichiers originaux avait été endommagée lors d'une panne de courant survenue en 2018, et que son contenu avait été définitivement perdu. De Trinidad a estimé que la production de ces enregistrements originaux était essentielle afin d'établir que la CSF avait falsifié la preuve et a donc soumis une demande d'accès afin d'obtenir des documents concernant l'infrastructure technologique de la CSF et la panne de courant.

La CSF a refusé la demande sur la base des articles 14 et 29 de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels* (Loi sur l'accès). La CSF a fait valoir que les documents demandés contenaient des renseignements sensibles sur son infrastructure technologique, y compris les configurations et les vulnérabilités des systèmes, et que leur divulgation pourrait compromettre la sécurité de ses systèmes.

Décision

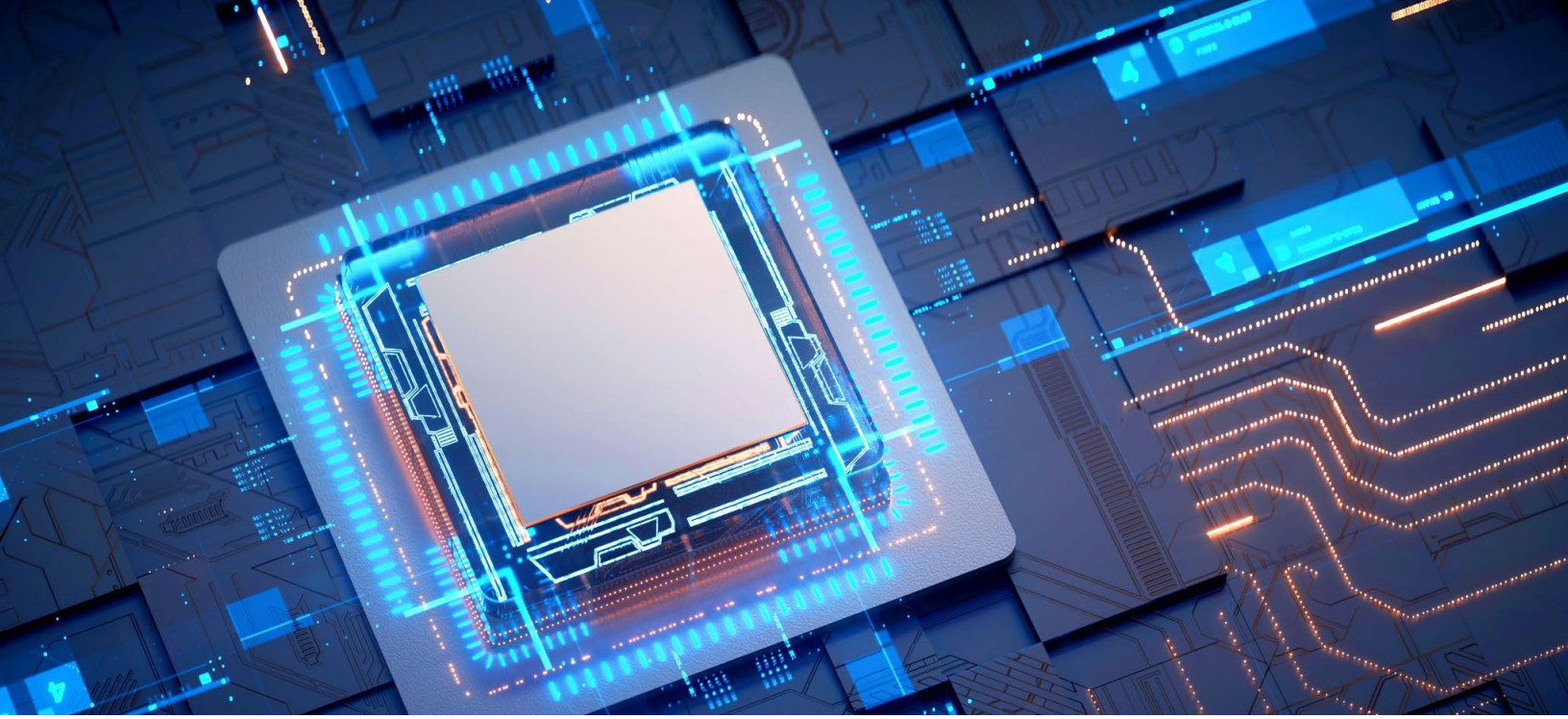
La Commission d'accès à l'information (la Commission) a donné gain de cause à la CSF, confirmant sa décision de retenir les documents demandés en vertu des articles 14 et 29 de la Loi sur l'accès.

La Commission a reconnu que les documents demandés contenaient des renseignements susceptibles d'exposer les systèmes de la CSF à des risques, tels que des cybermenaces ou des accès non autorisés, et que la divulgation de ces renseignements pouvait donc compromettre la sécurité des systèmes de la CSF.

La Commission a souligné que la révélation de ces renseignements posait un risque qui l'emportait sur tout objectif d'enquête que de Trinidad aurait pu avoir en y accédant.

Point principal à retenir

Les organisations peuvent légitimement refuser de communiquer des renseignements concernant leur infrastructure technologique si une telle communication pose un risque pour la sécurité, même lorsque ces renseignements sont demandés dans le cadre d'une enquête ou d'une action en justice.



IA et protection des renseignements personnels

McMaster University (Re), 2024 CanLII 17583 (ON IPC)

Lire les détails de l'affaire (disponible en anglais seulement)

Faits

L'affaire concerne l'utilisation par l'Université McMaster du logiciel Respondus Monitor, un logiciel de surveillance des examens en ligne propulsé par l'intelligence artificielle (IA), et du logiciel Respondus LockDown Browser, un logiciel qui limite ce à quoi les étudiants peuvent accéder sur leur ordinateur pendant un examen. L'Université McMaster a adopté cette technologie pendant la pandémie de COVID-19 afin de préserver l'intégrité académique dans un environnement de cours à distance.

Le Commissaire à l'information et à la protection de la vie privée de l'Ontario (CIPVP) a enquêté sur le respect par l'Université de la *Loi sur l'accès à l'information et la protection de la vie privée* (la Loi), en particulier en ce qui concerne la collecte, l'utilisation et la communication des renseignements personnels des étudiants par le logiciel Respondus Monitor.

Décision

Le CIPVP a constaté que le logiciel Respondus LockDown Browser recueillait peu de renseignements personnels et qu'il ne collectait et n'utilisait que ce dont il avait besoin pour fonctionner. En revanche, il a constaté que le logiciel Respondus Monitor recueillait des renseignements personnels plus sensibles, notamment des données biométriques, et utilisait l'IA, ce qui a accru les inquiétudes.

Bien que la collecte ait été autorisée en vertu du paragraphe 38(2) de la Loi, le CIPVP a constaté que l'Université n'avait pas fourni un avis adéquat pour sa collecte de renseignements personnels, comme l'exige le paragraphe 39(2) de la Loi, et a également constaté que l'utilisation des renseignements personnels des étudiants par l'entremise du logiciel Respondus Monitor n'était pas conforme au paragraphe 41(1).

En outre, le CIPVP a conclu que l'entente contractuelle entre l'Université et Respondus était contraire au paragraphe 41(1) de la Loi, car elle ne protégeait pas de manière adéquate tous les renseignements personnels recueillis et parce qu'elle permettait à Respondus d'utiliser les renseignements personnels des étudiants sans leur consentement, afin d'améliorer son système.

Le CIPVP a formulé plusieurs recommandations pour que l'Université soit dorénavant en conformité avec la Loi. Il lui a recommandé d'adopter des garde-fous supplémentaires dans le cadre de son utilisation du logiciel Respondus Monitor et d'intégrer des mesures de protection plus vigoureuses dans le cadre de son utilisation continue du logiciel ainsi que dans toute entente qu'elle pourrait conclure à l'avenir avec Respondus.

Point principal à retenir

Les institutions qui utilisent des logiciels tels que le logiciel Respondus Monitor doivent veiller à ce que les individus touchés soient dûment informés de la collecte de leurs renseignements. Elles doivent également veiller à ce que les ententes qu'elles concluent avec des tiers fournisseurs de services protègent de manière adéquate les renseignements personnels collectés et interdisent à ces tiers d'utiliser à quelque fin que ce soit les renseignements personnels collectés sans le consentement des individus concernés.

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 Vancouver Ottawa New York | **osler.com/fr**

OSLER