Revue de la jurisprudence sur la protection de la vie privée d'Osler

Quatrième édition – Été 2025

OSLER

Table des matières

Note de la rédaction

En cette ère numérique où les données personnelles circulent à une vitesse et dans des quantités sans précédent, le rôle des chefs de la protection des renseignements personnels, des avocats-conseils internes et des professionnels de la conformité n'a jamais été aussi crucial, ou aussi complexe. La présente revue a pour but de fournir une analyse des dernières évolutions en droit canadien de la protection de la vie privée. Elle offre des éclaircissements précieux sur les décisions judiciaires et les tendances juridiques qui façonnent les lois sur la protection des renseignements personnels au Canada. À travers l'examen des principaux cas de jurisprudence et des questions émergentes, nous souhaitons doter les chefs de la protection des renseignements personnels des compétences stratégiques et de l'expertise nécessaires pour leur permettre de s'y retrouver dans un environnement en constante évolution, où se croisent normes juridiques, innovations technologiques et priorités commerciales.

Grâce aux commentaires d'experts, nous explorons comment les organisations peuvent assurer leur conformité aux lois et relever de façon proactive les défis que pose l'évolution rapide des technologies et du cadre réglementaire.

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 collaborent régulièrement aux initiatives de leadership éclairé présentées sur la plateforme AccessPrivacy d'Osler. Cette dernière 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.

Alliant une expertise approfondie en litige et en droit de la protection de la vie privée à une approche avant-gardiste en matière de technologie et de gouvernance, Osler demeure un partenaire de confiance pour les organisations qui souhaitent garder une longueur d'avance dans le domaine en constante évolution de la protection de la vie privée.

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

Contributeurs et contributrices

Kristian Brabander

Associé, Litiges

kbrabander@osler.com
514.904.8107

Robert Carson

Associé, Litiges

rcarson@osler.com
416.862.4235

Tommy Gelbman

Associé, Litiges

tgelbman@osler.com
403.260.7073

Jessica Harding

Associée, Litiges

jharding@osler.com
514.904.8128

Craig Lockwood

Associé, Litiges

clockwood@osler.com
416.862.5988

Julien Morissette

Associé, Litiges
et Insolvabilité et
restructuration

jmorissette@osler.com
514.904.5818

Actions collectives en matière de protection de la vie privée : atteintes à la protection des données

Royer c. Capital One Bank (Canada Branch) et al., 2025 QCCA 217

Lire les détails de l'affaire

Faits

Une brèche de sécurité a permis à une ex-employée d'accéder illégalement aux données confidentielles de demandes de carte de crédit d'environ 100 millions d'Américains et 6 millions de Canadiens collectées par les défenderesses Capital One Bank et al. (Capital One) sur une période de 14 ans, et de les stocker sur des serveurs des défenderesses Amazon Web Services Inc. et al. (Amazon). Lorsqu'il a été informé de la brèche de sécurité, l'appelant, Michael Royer (M. Royer), a demandé l'autorisation d'intenter une action collective.

Le juge chargé de la demande d'autorisation (première instance) a conclu qu'il existait une preuve suffisante de faute contractuelle de la part de Capital One, notamment pour avoir omis de protéger adéquatement les renseignements personnels, pour avoir trop tardé à découvrir la fuite et à informer ses clients et pour avoir conservé les données de certaines personnes pendant une période déraisonnable, en particulier celles dont la demande de carte de crédit a été refusée.

Le juge de l'autorisation a également conclu qu'il existait une preuve suffisante de la responsabilité civile d'Amazon, notamment sur le fondement des articles 3 et 10 de la *Loi sur la protection des renseignements personnels dans le secteur privé*, RLRQ c. P-39.1.

Il a souligné l'absence d'allégations de vol d'identité et a rejeté la plupart des réclamations de dommages proposées relativement à la valeur des données ayant fait l'objet de la fuite et au préjudice causé par le retard à aviser les membres du groupe. Il a toutefois estimé que la surveillance du crédit requise à la suite de la violation constituait un préjudice indemnisable et que la suffisance de cette surveillance déjà offerte par Capital One (deux ans) devait faire l'objet d'une décision du juge de première instance. Le juge a également estimé que les allégations étaient suffisantes pour permettre une réclamation de dommages punitifs à l'encontre de Capital One, mais pas à l'encontre d'Amazon.

Toutes les parties ont fait appel. M. Royer a critiqué le juge d'autorisation pour avoir exclu d'autres réclamations de dommages de l'action collective (l'appel principal). Capital One et Amazon ont fait valoir que le juge d'autorisation n'aurait pas dû accueillir les réclamations de dommages pour des préjudices que le représentant du groupe n'avait pas lui-même subis (l'appel incident). Capital One a également contesté l'autorisation de la réclamation de dommages punitifs.

Décision

La Cour d'appel du Québec a accueilli l'appel principal et a rejeté l'appel incident.

La Cour a estimé que le cas personnel du représentant du groupe ne doit pas nécessairement être représentatif de celui de l'ensemble ou de la majorité des membres du groupe, mais doit plutôt démontrer qu'ils ont subi au moins un chef de dommages. L'autorisation ne doit pas être limitée et doit viser tout dommage ayant été potentiellement subi par au moins un membre du groupe.

De plus, la Cour a déclaré que les préjudices subis par les membres du groupe à la suite de la violation ne sont pas nécessairement de même nature. C'est ainsi que certains peuvent avoir payé des frais de surveillance alors que d'autres peuvent avoir fait d'autres démarches et engagé d'autres coûts pour assurer la même fin.

Enfin, la Cour a jugé qu'il ne convient pas de déterminer, à ce stade, l'existence de pertes non pécuniaires indemnisables. Tant qu'il existe des allégations qui établissent de manière suffisante la possibilité d'une atteinte fautive entraînant des conséquences indemnisables, il revient au juge du fond d'en décider. La Cour a donc autorisé l'action collective pour tous les chefs de dommages compensatoires.

Quant aux dommages punitifs, la Cour a jugé qu'il n'y avait aucun motif de révision en appel.

Point principal à retenir

Cette décision renforce le critère du seuil relativement peu élevé pour autoriser les actions collectives au Québec, en particulier dans les affaires portant sur des atteintes à la vie privée. Même si le représentant du groupe n'a pas subi tous les chefs de dommages, l'action collective peut inclure d'autres chefs potentiellement subis par au moins un membre du groupe. Malgré le fait que différents membres du groupe puissent avoir subi différents types de pertes, ces variations n'empêchent pas l'autorisation d'une action collective.

Cette décision souligne également le fait que la menace d'un préjudice financier découlant de certains types d'atteintes à la confidentialité des données peut parfois suffire à justifier une action collective au Québec, même lorsque la défenderesse offre une quelconque forme de surveillance de crédit.

InvestorCOM Inc. v. L'Anton, 2025 BCCA 40

Lire les détails de l'affaire

Faits

Cette action concerne une atteinte présumée à la protection des données stockées sur des serveurs exploités par InvestorCOM Inc. Une action collective a été intentée en Colombie-Britannique. Une action collective parallèle avait déjà été intentée en Ontario par différents demandeurs et leurs avocats, qui réclamaient la certification d'une action collective nationale portant sur le même sujet. L'action intentée en Ontario était en voie d'être entendue en audience de certification.

InvestorCOM et Mackenzie Financial Corporation ont demandé le rejet de l'action intentée en Colombie-Britannique pour abus de procédure, faisant valoir que l'existence de l'action intentée en Ontario rendait la procédure en Colombie-Britannique redondante et inutile. Le juge en chambre a rejeté la demande. InvestorCOM et Mackenzie ont interjeté appel.

Décision

La Cour d'appel a rejeté les appels, jugeant que la simple existence d'actions collectives similaires ou parallèles dans différentes provinces ne constitue pas, en soi, un abus de procédure. Pour autant, cela ne veut pas dire que l'action intentée en Colombie-Britannique sera autorisée à aller de l'avant. La Cour d'appel a souligné que les préoccupations relatives au dédoublement sont dûment prises en compte à l'étape de la certification aux termes de l'alinéa 4.1(1)(b) de la *Class Proceedings Act* de la Colombie-Britannique, qui prévoit la constitution d'un dossier complet aux fins de la certification. Cette disposition permet au tribunal de refuser la certification s'il est préférable que l'instance soit menée dans un autre territoire de compétence.

La Cour a distingué cette affaire des situations où une action provisoire est intentée uniquement à des fins tactiques. Elle a également reconnu que les différences entre les lois provinciales, le régime des dépens et le lieu de résidence du demandeur justifiaient que l'action soit intentée en Colombie-Britannique.

Point principal à retenir

Il est courant que des actions collectives soient intentées dans plusieurs provinces après une atteinte à la protection des données. En Colombie-Britannique, les tribunaux semblent préférer traiter les chevauchements dans le cadre de la requête en certification. En général, cela augmente le temps et les coûts nécessaires pour régler les chevauchements.

Hvitved v. Home Depot of Canada Inc., 2025 BCSC 18

Lire les détails de l'affaire

Faits

Dans sa demande de certification d'une action collective projetée, le demandeur alléguait que Home Depot avait porté atteinte au droit à la vie privée de ses clients en recueillant leurs adresses de courriel et les renseignements sur leurs achats — fournis dans le but de recevoir des reçus électroniques — et en divulguant ces renseignements à Meta Platforms.

Le demandeur a présenté des réclamations en vertu des lois provinciales sur la protection des renseignements personnels (Colombie-Britannique, Saskatchewan, Terre-Neuve-et-Labrador et Manitoba), ainsi que des réclamations pour intrusion dans l'intimité, rupture de contrat et enrichissement sans cause. Home Depot s'est opposée à la certification, soutenant que les réclamations étaient sans fondement et qu'une action collective n'était pas appropriée.

Décision

La Cour a certifié l'action collective uniquement en ce qui concerne les prétentions fondées sur des dispositions législatives et a rejeté les réclamations pour intrusion dans l'intimité, rupture de contrat et enrichissement sans cause.

Principales conclusions :

- **Violation des lois sur la protection des renseignements personnels :** La prétention fondée sur la loi était suffisante pour établir une cause d'action aux fins de la certification. La Cour a rejeté l'argument de Home Depot selon lequel on ne pouvait raisonnablement s'attendre à ce que les données partagées soient visées par les lois sur la protection des renseignements personnels, s'appuyant sur l'arrêt *Insurance Corporation of British Columbia v. Ari*, 2023 BCCA 331, pour souligner que la protection des renseignements personnels doit être évaluée en tenant compte du contexte et non de manière fragmentaire.

- **Intrusion dans l'intimité :** La Cour a jugé que les actes de procédure ne satisfaisaient pas au seuil plus élevé requis pour établir le délit d'intrusion dans l'intimité en common law, car les renseignements partagés étaient moins sensibles que ceux pris en compte dans des affaires analogues de l'Ontario et ne constituaient pas une intrusion très offensante. En appliquant le droit de l'Ontario, la Cour a déterminé que le délit d'intrusion dans l'intimité n'était pas établi dans les actes de procédure. La Cour a refusé de se prononcer sur la question de savoir si ce délit est applicable en Colombie-Britannique.

- **Rupture de contrat et enrichissement sans cause :** La Cour a jugé l'exposé de la demande incomplet, soulignant l'absence de faits pertinents concernant l'existence de clauses contractuelles expresses et l'insuffisance des allégations à l'appui d'une demande d'enrichissement sans cause, en particulier en ce qui concerne la perte de la possibilité de vendre des renseignements personnels.

Point principal à retenir

L'avocat du demandeur devait faire preuve de rigueur dans l'exposé de ses arguments en se concentrant sur les causes d'action liées aux atteintes présumées à la vie privée et en privilégiant manifestement les prétentions fondées sur des dispositions législatives, qui semblent plus susceptibles d'être accueillies dans le cadre des demandes de certification. La Cour a signalé — sans toutefois se prononcer — qu'elle doutait que le délit d'intrusion dans l'intimité puisse être invoqué en Colombie-Britannique, en raison de la réticence des tribunaux de cette province à se prononcer sur cette question depuis des années. Enfin, contrairement à de nombreuses autres décisions rendues en Colombie-Britannique, la Cour n'a pas autorisé le demandeur à modifier les actes de procédure qui avaient été radiés, imposant ainsi une fois de plus des règles strictes quant à la manière dont les actions collectives doivent être formulées.

Shriqui v. Blackbaud Canada Inc., et al., 2024 ONSC 6957

Lire les détails de l'affaire

Faits

La demanderesse a demandé la certification d'une action collective à la suite d'une attaque par rançongiciel qui a compromis les données personnelles de diverses organisations et personnes utilisant les services des défenderesses. L'attaque a eu lieu entre février et mai 2020, période durant laquelle des données ont été extraites de Blackbaud, exigeant de l'entreprise qu'elle paye une rançon. Malgré cette atteinte, ni la demanderesse ni aucune autre personne touchée n'ont signalé de conséquences négatives découlant de l'incident. Le groupe visé par l'action projetée comprenait des résidents canadiens dont les renseignements personnels ont été consultés.

Décision

La Cour a conclu que l'action satisfaisait aux critères de certification prévus par la *Loi de 1992 sur les recours collectifs*, notamment l'existence d'une question commune concernant le devoir de diligence des défenderesses. Toutefois, la Cour a conclu que la probabilité de succès de la procédure était faible, car aucun préjudice n'avait été démontré. Les parties ont conclu un règlement de 340 000 $, qui devait être distribué selon la doctrine du *cy-près* en common law à deux établissements d'enseignement spécialisés en politique Internet et en sécurité des données. La Cour a certifié l'action en vue d'un règlement et a approuvé un plan de notification limité, compte tenu de l'impossibilité pratique d'identifier les membres du groupe.

Point principal à retenir

Lorsqu'un demandeur ne peut démontrer un préjudice réel découlant des actes de la défenderesse, les chances d'obtenir gain de cause sur le fond peuvent être faibles. Un règlement selon la doctrine du *cy-près* peut être recommandé dans les affaires d'atteinte à la protection des données pour lesquelles il est impossible d'identifier les membres du groupe.

Donegani v. Facebook, Inc., 2024 ONSC 7153

Lire les détails de l'affaire

Faits

Les demandeurs alléguaient que Facebook avait utilisé leurs données de manière abusive en les mettant à la disposition de certaines applications tierces. Les demandeurs ont demandé la certification d'une action collective nationale, alléguant, entre autres, une intrusion dans l'intimité et une violation des lois provinciales sur la protection des renseignements personnels.

Décision

La juge Akbarali a rendu diverses conclusions concernant la cause d'action et les critères relatifs aux questions communes du critère de certification, mais n'a finalement pas statué sur la requête en certification. Voici certaines de ses conclusions :

- Les tribunaux de l'Ontario n'ont pas compétence pour entendre les réclamations en vertu des lois sur la protection des renseignements personnels de la Colombie-Britannique, du Manitoba et de Terre-Neuve-et-Labrador, ni pour statuer sur celles-ci.
- Les questions communes proposées relatives à l'intrusion dans l'intimité ne pouvaient pas faire l'objet d'une certification dans ces circonstances.
- Certaines des questions communes proposées relatives aux contrats entre Facebook et ses utilisateurs, ainsi qu'au consentement, pouvaient faire l'objet d'une certification. Toutefois, aucune des questions communes proposées relatives aux préjudices ne pouvait être certifiée.

La juge Akbarali n'a pas statué sur le critère de la procédure préférable. Elle a ordonné aux demandeurs de proposer une nouvelle définition du groupe et un nouveau plan de litige, à la suite de quoi les parties reviendraient pour présenter leurs arguments.

Point principal à retenir

La requête en certification reste en suspens.

Données biométriques

Cleaver v. The Cadillac Fairview Corporation Limited, 2025 BCSC 910

Lire les détails de l'affaire

Faits

En 2018, Cadillac Fairview Corporation Limited (Cadillac Fairview) a installé des caméras équipées de la technologie d'analyse vidéo anonyme (le logiciel) fournie par MappedIn Inc. (MappedIn) dans les bornes d'orientation numériques (les bornes d'orientation) de ses centres commerciaux situés dans plusieurs provinces du Canada (les centres commerciaux).

Cadillac Fairview a mené un projet pilote de huit semaines dans le but d'obtenir une estimation du nombre de visiteurs de chaque propriété et de leurs caractéristiques démographiques (âge et sexe) rudimentaires. Elle a désactivé le logiciel en réponse à des informations erronées circulant en ligne suggérant que le logiciel était une technologie de « reconnaissance faciale ». Les données obtenues dans le cadre du projet ont été conservées en toute sécurité par MappedIn sur un serveur hors service. Aucune des défenderesses n'a reçu ou utilisé les données, et les images prises n'ont pas été conservées.

Le Commissaire à la protection de la vie privée du Canada, le Commissaire à l'information et à la protection de la vie privée de l'Alberta et le Commissaire à l'information et à la protection de la vie privée de la Colombie-Britannique (collectivement, les commissaires) ont lancé une enquête conjointe afin de déterminer si Cadillac Fairview recueillait et utilisait les renseignements personnels des visiteurs de ses centres commerciaux.

Le 28 octobre 2020, ils ont publié leur rapport concluant que le logiciel créait une représentation numérique unique d'un visage particulier, constituant ainsi une collecte de renseignements biométriques. Étant donné que ces représentations numériques étaient créées à partir d'images captées par les caméras, les commissaires ont estimé que la création de renseignements biométriques à partir de ces images constituait une

collecte supplémentaire de données à caractère personnel. Ils ont également conclu que la plainte était résolue, étant donné que le logiciel avait été désactivé et que toutes les données avaient été supprimées.

Les demandeurs, Joshua Cleaver et Curtis Kieres (les demandeurs), ont présenté une demande de certification d'une action collective nationale en vertu de la *Class Proceedings Act*, R.S.B.C. 1996, c. 50 (CPA) au nom de toutes les « personnes qui ont consulté une borne d'orientation dans un ou plusieurs centres commerciaux pendant les périodes pertinentes et de toutes les personnes, y compris les mineurs, qui les accompagnaient ». Ils alléguaient que Cadillac Fairview avait secrètement exploité les données biométriques de visiteurs qui ne se doutaient de rien dans ses centres commerciaux et que les défenderesses avaient porté atteinte aux droits à la vie privée des membres du groupe proposé en recueillant leurs données personnelles, à savoir les images de leur visage, et en les convertissant en données numériques.

Décision

La Cour a rejeté la possibilité de certifier les demandes pour i) certaines violations alléguées de la loi; ii) intrusion dans l'intimité en Colombie-Britannique et en Alberta; iii) négligence; et iv) violations alléguées de la Charte québécoise.

Elle a conclu que les demandeurs satisfaisaient aux exigences de l'alinéa 4(1)(a) de la CPA en ce qui concerne certaines des causes d'action énoncées dans les actes de procédure, même si elle a conclu qu'il n'y avait aucun « fondement en fait » permettant de conclure que les défenderesses avaient saisi ou stocké des données biométriques ou personnelles.

Elle a toutefois conclu que les demandeurs n'avaient pas établi l'existence d'un groupe identifiable de deux personnes ou plus, condition requise pour certifier une action collective en vertu de l'alinéa 4(1)(b) de la CPA. En effet, il n'existait aucun fondement factuel permettant de démontrer que les membres du groupe pouvaient s'identifier eux-mêmes, ni aucun lien rationnel entre la définition du groupe proposée (qui avait été modifiée à trois reprises) et les questions communes fondamentales, à savoir que l'image du visage d'une personne avait été enregistrée et utilisée pour créer des renseignements biométriques et personnels à son sujet.

La Cour a également jugé que les demandes des membres du groupe ne soulevaient pas de questions communes, autre condition de certification prévue à l'alinéa 4(1)(c) de la CPA. Elle a notamment conclu qu'il n'existait aucun fondement factuel permettant de conclure que des images de visages avaient été enregistrées par les caméras installées dans les bornes d'orientation ou que des données biométriques et personnelles concernant les membres du groupe avaient été créées. Elle a également conclu qu'il n'existait aucun fondement factuel permettant de conclure que les données contenaient des renseignements personnels au sens des lois pertinentes, car aucune personne ne pouvait être identifiée à partir de ces données.

Enfin, la Cour n'était pas convaincue qu'une action collective constituait la procédure préférable pour régler de manière équitable et efficace les questions communes conformément à l'alinéa 4(1)(d) de la CPA. Il est important de noter que l'analyse de la Cour a tenu compte de l'absence de preuve d'un préjudice démontrable, de la conclusion du programme pilote et de la destruction des données.

Point principal à retenir

Le rejet de cette demande de certification souligne les difficultés auxquelles les demandeurs sont confrontés dans le cadre d'actions collectives liées à la protection des renseignements personnels. Cette décision démontre que les demandeurs ne peuvent pas se fonder uniquement sur des constatations et des conclusions réglementaires pour étayer leurs demandes devant les tribunaux, en particulier lorsqu'il n'y a pas de données identifiables qui permettent de rendre personnels les renseignements recueillis, que la collecte présumée des données a pris fin et que les données ont été supprimées.

Doan c. Clearview AI inc., 2024 QCCS 3968

Lire les détails de l'affaire

Faits

La demanderesse, Ha Vi Doan (M^me^ Doan), a demandé l'autorisation d'exercer une action collective au nom de tous les résidents du Québec dont les images faciales et les renseignements personnels ont été recueillis, utilisés ou communiqués sans leur consentement par la défenderesse, Clearview AI (Clearview).

Clearview a mis au point un algorithme de reconnaissance faciale qui lui permet de créer une empreinte faciale à partir de données biométriques extraites d'une photographie. Son moteur de recherche explore Internet, localise des photos de visages et les classe dans sa base de données en fonction de leurs empreintes faciales respectives. Ce logiciel permet à Clearview d'offrir à ses clients un service capable de rassembler dans un rapport de recherche toutes les images faciales dont les empreintes correspondent à une image donnée et qui sont disponibles sur Internet.

M^me^ Doan alléguait que Clearview avait violé certains droits fondamentaux des membres du groupe, notamment leur droit à la vie privée, leur droit à la dignité et leur droit de contrôler l'utilisation de leur image. Elle a également allégué que Clearview avait manqué à ses obligations prévues dans les lois applicables à la collecte de renseignements personnels. Clearview a contesté le bien-fondé apparent de certaines des causes d'action invoquées, mais a également fait valoir que les tribunaux québécois n'avaient pas compétence en l'espèce.

Décision

La Cour a statué qu'elle avait compétence pour entendre et trancher l'action collective proposée au nom des résidents du Québec, concluant en outre que l'allégation selon laquelle la collecte de photographies des membres du groupe, leur utilisation pour créer une empreinte faciale et la constitution d'un dossier sur chacun d'eux sans leur consentement constituait une atteinte à la sauvegarde de leur dignité en vertu de l'article 4 de la *Charte des droits et libertés de la personne*, RLRQ c. C 12 (Charte québécoise) n'est pas une allégation frivole. La Cour a jugé que cette question méritait d'être analysée sur le fond et a autorisé l'action collective.

La Cour a souligné que la portée du droit de contrôler l'utilisation de son image n'avait pas encore été examinée par les tribunaux dans de telles circonstances. Elle a conclu qu'il n'était pas exagéré de se demander si l'utilisation d'une image pour, entre autres, créer une empreinte faciale pouvait porter atteinte au droit des membres du groupe à contrôler l'utilisation de leur image.

Point principal à retenir

Cette décision met en évidence les préoccupations juridiques croissantes entourant l'utilisation des données biométriques et de la technologie de reconnaissance faciale. Cette affaire, qui va maintenant passer à l'examen sur le fond, sera suivie de près en raison de son potentiel à façonner le paysage juridique dans ce domaine en rapide évolution, notamment en ce qui concerne les droits de la personne et le droit à l'image.

Imprimeries Transcontinental inc., Re, Commission d'accès à l'information du Québec, 1024350-S

Faits

En octobre 2020, le commissaire à l'information et à la protection de la vie privée du Québec, la Commission d'accès à l'information (CAI), a reçu d'Imprimeries Transcontinental inc. (la société) une déclaration l'informant de la création d'une base de données de caractéristiques ou de mesures biométriques (la déclaration).

À l'origine, la déclaration avait pour objet de justifier la mise en place, dans le contexte de la pandémie de COVID-19, d'un système d'authentification (le système) doté de deux fonctionnalités visant à contrôler l'accès aux locaux de la société, à savoir une fonctionnalité de reconnaissance faciale et une fonctionnalité de mesure de la température corporelle. Au moment de la déclaration, l'objectif de la société concernant le système était d'assurer la sécurité de ses employés et de ses locaux.

Étant donné que la fonctionnalité de prise de température du système n'avait pas été utilisée depuis octobre 2022 et que les données générées par celle-ci avaient été détruites, la décision de la CAI ne concerne que la fonctionnalité de reconnaissance faciale du système.

Décision

La CAI a ordonné à la société de cesser de recueillir des données biométriques permettant la reconnaissance faciale, de cesser d'utiliser un système de reconnaissance faciale utilisant des mesures biométriques pour contrôler l'accès à ses locaux et de détruire les modèles créés et les codes de hachage obtenus par la conversion des photos de visages recueillies.

Après avoir conclu que la société est assujettie à la *Loi sur la protection des renseignements personnels dans le secteur privé*, RLRQ c. P-39.1 (la *Loi sur le secteur privé du Québec*), la CAI a estimé qu'une photographie du visage d'une personne et sa codification sous forme de représentation mathématique — qui font toutes deux partie du processus du système — constituent des données personnelles sensibles.

La *Loi sur le secteur privé du Québec* prévoit que les renseignements personnels ne peuvent être recueillis que s'il existe un intérêt sérieux et légitime. De plus, seuls les renseignements personnels nécessaires aux fins précisées avant la collecte peuvent être recueillis. Pour justifier la nécessité de recueillir ces données, une entreprise doit démontrer le motif légitime, important et réel poursuivi par cette collecte, ainsi que la proportionnalité de l'atteinte à la vie privée par rapport aux fins poursuivies. Une entreprise ne peut déroger à ces exigences, même avec le consentement de la personne concernée.

Tout d'abord, la CAI a estimé que la société avait un motif légitime de garantir la sécurité de ses locaux et de prendre des mesures pour contrôler l'accès à ceux-ci. Toutefois, elle a conclu que la société n'avait pas démontré l'existence de problèmes de sécurité particuliers justifiant une telle collecte de données à caractère personnel.

La CAI a estimé que la société n'avait pas démontré l'importance de l'objectif poursuivi. Le contrôle de l'accès aux locaux d'une entreprise est un objectif courant. Les activités d'une entreprise ou une situation particulière peuvent justifier un niveau de sécurité plus élevé que celui que peuvent offrir les données biométriques, mais rien n'indiquait que tel était le cas en l'espèce.

Ensuite, la CAI a conclu que la collecte effectuée par la société n'était pas proportionnelle à l'objectif sous-jacent compte tenu de la nature biométrique et sensible des renseignements personnels en question. En effet, l'atteinte à la vie privée découlant de la collecte des renseignements personnels n'a pas été minimisée. La société n'a pas non plus établi en quoi la collecte des renseignements personnels nécessaires au

fonctionnement du système procurait des avantages qui l'emportaient sur le préjudice causé par cette collecte.

Point principal à retenir

Cette décision souligne les normes rigoureuses qui s'appliquent à la collecte et à l'utilisation des données biométriques sous le régime des lois québécoises sur la protection de la vie privée. Les organisations doivent justifier d'un intérêt sérieux et légitime et ne peuvent recueillir que les renseignements personnels nécessaires aux fins déterminées avant la collecte. Elles ne peuvent pas se fonder uniquement sur le consentement pour justifier leurs pratiques.

Cette affaire renforce l'importance de privilégier, dans la mesure du possible, des solutions qui portent moins atteinte à la vie privée.

Granger v. Ontario, 2024 ONSC 6503

Lire les détails de l'affaire

Faits

En 2013, Micky Granger, un travailleur agricole migrant, a été soumis à un prélèvement d'ADN par la Police provinciale de l'Ontario (OPP) dans le cadre d'une enquête sur une agression sexuelle violente. M. Granger et 95 autres travailleurs ont fourni des échantillons d'ADN conformément à ce qu'ils croyaient être un consentement éclairé. Cependant, la police n'a pas fourni de copies des formulaires de consentement, et le Centre des sciences judiciaires (CSJ) a conservé les profils génétiques malgré l'obligation prévue au Code criminel de détruire définitivement ces données si les échantillons ne correspondaient à aucun ADN trouvé sur les lieux d'un crime. M. Granger a allégué que la conservation de son ADN violait ses droits garantis par l'article 8 de la *Charte canadienne des droits et libertés* (la Charte canadienne) et a donné lieu à une action en responsabilité délictuelle fondée sur l'intrusion dans l'intimité.

Décision

La Cour a conclu que le CSJ n'avait pas respecté l'obligation légale de supprimer définitivement les résultats électroniques des analyses d'ADN une fois qu'il avait été établi que les échantillons ne correspondaient pas. Ce manquement constituait une violation de l'attente raisonnable des plaignants en matière de vie privée, car ils avaient consenti à la collecte de leur ADN en croyant que leurs profils seraient détruits s'ils n'étaient pas retenus comme correspondances. La Cour a ordonné le versement de dommages-intérêts globaux de 1 000 $ par membre du groupe, soit un total d'environ 7 267 000 $ pour violation des droits garantis par la Charte canadienne. La Cour a souligné que les violations étaient graves et justifiaient des dommages-intérêts à titre de réparation et de dissuasion, malgré l'absence de preuve démontrant un préjudice réel résultant de la conservation des profils ADN. Toutefois, la Cour a refusé d'accorder des dommages punitifs, concluant que le CSJ avait agi de bonne foi et n'avait pas eu de comportement malveillant ou imprudent.

Point principal à retenir

Cette décision souligne l'importance du strict respect des obligations légales lors du traitement de renseignements personnels sensibles, comme l'ADN. Le fait que le CSJ n'ait pas supprimé les résultats électroniques comme l'exige la loi a été un facteur déterminant dans la décision de la Cour. Cela met en évidence les risques juridiques auxquels s'exposent les organisations qui ne respectent pas les mesures de protection de la vie privée prévues par la loi, même en l'absence de preuve d'un préjudice réel.

Clearview AI Inc. v. Alberta (Information and Privacy Commissioner), 2025 ABKB 287

Lire les détails de l'affaire

Faits

Clearview AI Inc. (Clearview), une entreprise américaine, a moissonné des milliards d'images sur Internet, y compris sur les réseaux sociaux, afin de constituer une base de données de reconnaissance faciale destinée aux forces de l'ordre. Cette décision fait suite à une enquête conjointe menée par les autorités canadiennes chargées de la protection de la vie privée (Alberta, Colombie-Britannique, Québec et fédérale) sur les pratiques de Clearview en matière de reconnaissance faciale. Elle a été publiée après la décision connexe de la Cour suprême de la Colombie-Britannique dans l'affaire *Clearview AI Inc. v. Information and Privacy Commissioner for British Columbia*, 2024 BCSC 2311, et est largement conforme à celle-ci sur les points communs.

Le 2 février 2021, les organismes de réglementation ont publié un rapport conjoint dans lequel ils concluaient que Clearview avait enfreint les lois sur la protection des renseignements personnels en moissonnant des milliards d'images sans consentement, en créant des profils biométriques et en commercialisant ses services auprès des forces de l'ordre canadiennes. Ils ont recommandé que Clearview cesse d'offrir son outil de reconnaissance faciale au Canada, mette fin à la collecte et à l'utilisation des données des Canadiens et supprime toutes les données en sa possession.

Le 7 décembre 2021, après que Clearview a refusé d'accepter les recommandations, l'Alberta et son commissaire à l'information et à la protection de la vie privée (le commissaire) ont rendu une ordonnance exécutoire (l'ordonnance) exigeant que Clearview les adopte. Clearview a demandé un contrôle judiciaire, contestant i) la compétence de l'Alberta à son égard en tant que société étrangère; ii) l'interprétation de l'expression renseignements « accessibles au public » au sens de la *Personal Information Protection Act*, S.A. 2003, c. P-6.5 (PIPA) — qui exempte le consentement pour ces données; et iii) la constitutionnalité de l'ordonnance en vertu de l'alinéa 2b) de la *Charte canadienne des droits et libertés* (la Charte canadienne), qui garantit le droit à la liberté d'expression.

Clearview a fait valoir ce qui suit : i) le « moissonnage » d'images accessibles au public était légal et comparable aux pratiques de moteurs de recherche tels que Google; ii) l'obligation de consentement prévue par la PIPA était trop large et décourageait l'utilisation légitime des données publiques (p. ex., les moteurs de recherche); et iii) l'ordonnance était inapplicable, car elle ne permettait pas de distinguer les données des Albertains dans sa base de données.

Le commissaire : i) a soutenu que Clearview avait violé les droits à la vie privée des Albertains garantis par la PIPA; ii) a défendu son interprétation de l'expression de renseignements « accessibles au public » afin d'exclure les médias sociaux; et iii) a fait valoir que toute violation des droits garantis par la Charte canadienne était justifiée en vertu de l'article 1, compte tenu de la faible valeur de l'expression commerciale de Clearview par rapport aux atteintes importantes à la vie privée.

Décision

La Cour a déclaré que les articles 12, 17 et 20 de la PIPA, ainsi que la disposition 7(e) du *Personal Information Protection Act Regulation*, Alta. Reg. 366/2003 (Règlement sur la PIPA), constituait une violation injustifiée de l'alinéa 2b) de la Charte canadienne (liberté d'expression). À titre de réparation, la Cour a supprimé les mots « *including, but not limited to, a magazine, book or newspaper* » de l'article 7(e) du Règlement sur la PIPA, élargissant ainsi considérablement le sens du terme « *publication* » pour inclure les renseignements personnels et les images publiés sur Internet (sans paramètres de confidentialité), de sorte que l'utilisation de ces renseignements n'est pas soumise à une obligation de consentement.

Cette décision constitutionnelle n'a pas invalidé l'ordonnance, car la décision selon laquelle l'objectif de Clearview en matière de collecte et d'utilisation des renseignements personnels était déraisonnable restait valable.

Applicabilité de la PIPA à Clearview (compétence)
La Cour a statué que l'Alberta avait compétence sur Clearview en vertu du critère du « lien réel et substantiel ». Clearview avait commercialisé ses services auprès des forces de l'ordre de l'Alberta et avait moissonné des images stockées sur des serveurs situés en Alberta, établissant ainsi des liens suffisants avec la province. Son retrait du Canada au cours de l'enquête n'a pas invalidé la compétence, car l'ordonnance portait à la fois sur le comportement passé et sur le respect futur des obligations.

Interprétation de l'expression « accessible au public »
La Cour a jugé qu'il était raisonnable d'interpréter l'exception « accessible au public » contenue dans la PIPA et le règlement sur la PIPA comme excluant les médias sociaux. La Cour a reconnu que les lois sur la protection des renseignements personnels justifient des exceptions restreintes aux exigences en matière de consentement. De façon plus générale, lorsqu'elle s'est penchée sur les arguments fondés sur la Charte canadienne, la Cour a commenté un principe important de l'interprétation de la PIPA, à savoir que l'énoncé de l'objet de l'article 3 indique que le législateur cherchait à atteindre un équilibre et non à créer un régime où les droits à la vie privée l'emportaient sur tous les autres. Il en résulte que l'objet ne crée pas une approche extensive ou restrictive de l'interprétation.

Violation de l'alinéa 2b) de la Charte
Toutefois, la Cour a jugé que l'obligation de consentement prévue par la PIPA limitait de manière injustifiée la liberté d'expression, en se fondant sur trois considérations principales :

- **Activité d'expression :** La Cour a estimé que le moissonnage effectué par Clearview facilitait l'expression (p. ex., les résultats de recherche), et était donc protégé par la Charte canadienne. Elle a expressément rejeté l'argument de l'Alberta selon lequel l'expression n'était pas protégée parce qu'elle était commerciale ou motivée par le profit.

- **Portée excessive :** La Cour a estimé que la règle générale du consentement prévue par la loi visait des activités inoffensives (p. ex., l'indexation de données publiques par les moteurs de recherche), restreignant de manière disproportionnée la liberté d'expression légitime.

- **Atteinte minimale :** Tout en reconnaissant que la protection de la vie privée était un objectif urgent et important, la Cour a estimé que les moyens prévus par la loi ne constituaient pas une entrave minimale. Pour remédier à cela, la Cour a adapté le recours en élargissant l'exception « accessible au public » pour inclure les publications publiques sur Internet sans protection inhérente de la vie privée.

Caractère raisonnable de l'objectif de Clearview
La conclusion du commissaire selon laquelle l'utilisation par Clearview des images qu'elle avait collectées n'avait pas d'« objet raisonnable » au sens de la PIPA a été confirmée. La Cour a convenu que le moissonnage sans discrimination, le profilage biométrique et la revente commerciale des données ne satisfaisaient pas au critère de caractère raisonnable de la PIPA. L'argument de Clearview selon lequel ses pratiques étaient conformes aux valeurs de la Charte canadienne a été rejeté comme étant hors de propos.

Caractère exécutoire de l'ordonnance
L'ordonnance était exécutoire malgré l'allégation de Clearview selon laquelle elle ne pouvait pas identifier les données spécifiques à l'Alberta. La Cour a rejeté cet argument, le qualifiant de « défense désordonnée » (*scrambled egg defense*), et a fait remarquer que Clearview pouvait se conformer à l'ordonnance en adoptant des mesures similaires

à celles prévues dans le cadre du règlement conclu en Illinois. Le processus de conformité itératif du commissaire a également été jugé légal.

Point principal à retenir

La Cour a trouvé un équilibre entre la vie privée et la liberté d'expression : même si l'exigence de consentement trop large de la PIPA concernant la collecte et l'utilisation de renseignements accessibles au public a été jugée inconstitutionnelle, les pratiques spécifiques de Clearview ont été jugées déraisonnables au regard de la PIPA. La décision précise que les lois sur la protection des renseignements personnels ne doivent pas entraver les recherches et l'indexation légitimes sur Internet, mais peuvent cibler adéquatement les utilisations déraisonnables de données à caractère personnel, comme l'utilisation de ces renseignements pour créer une base de données de reconnaissance faciale.

Litiges relatifs à la protection des renseignements personnels : importance déterminante du consentement

Hogue c. Société canadienne des postes, 2025 QCCS 49

Lire les détails de l'affaire

Faits

Le demandeur a demandé l'autorisation d'exercer une action collective au nom des clients de la défenderesse, la Société canadienne des postes (Postes Canada), alléguant que leurs renseignements personnels avaient été collectés et vendus sans leur consentement. Il alléguait que Postes Canada avait créé des listes d'envoi à des fins de marketing postal qu'elle avait ensuite vendues à des sociétés privées. Le demandeur réclamait des dommages compensatoires et punitifs au nom du groupe proposé.

Décision

La Cour a autorisé l'action collective en partie et a conclu que les allégations semblaient suffisantes pour conclure que Postes Canada a collecté des renseignements qui vont au-delà de ce qui est nécessaire pour atteindre son objectif, qu'elle a revendu ces renseignements à des tiers à des fins lucratives et qu'elle n'avait pas obtenu le consentement de ses clients pour le faire. Elle a donc autorisé les demandes fondées sur la violation de la *Loi sur la protection des renseignements personnels*, L.R.C. 1985, ch. P-21, et du *Code civil du Québec*, RLRQ c. CCQ-1991.

La Cour a également autorisé la demande fondée sur le droit à la vie privée prévu par la *Chartre des droits et libertés de la personne,* RLRQ c. C-12 (la Charte québécoise). Elle a rejeté l'argument de Postes Canada selon lequel la Charte québécoise ne s'applique pas à Postes Canada au motif que cette dernière est une société d'État fédérale.

Toutefois, la Cour n'a pas autorisé l'allégation de fausses représentations fondée sur la *Loi sur la protection du consommateur,* RLRQ c. P-40.1, parce que le demandeur n'a pas allégué qu'il connaissait la politique de Postes Canada en matière de protection des renseignements personnels ni qu'il s'était fondé sur les déclarations de Postes Canada contenues dans cette politique.

En ce qui concerne les dommages compensatoires, la Cour a notamment déclaré que l'utilisation de renseignements personnels à des fins commerciales sans consentement ni compensation peut causer un préjudice. Elle a donc conclu que les allégations du demandeur ne pouvaient être considérées comme frivoles, notamment celles selon lesquelles ses renseignements personnels ont une valeur et qu'il a le droit de réclamer le paiement d'une somme équivalente à la valeur des renseignements personnels recueillis par Postes Canada.

Quant aux dommages punitifs, la Cour a conclu que les actes de Postes Canada pouvaient être qualifiés d'intentionnels au sens de l'article 49 de la Charte québécoise.

Point principal à retenir

Cette décision réitère l'importance d'obtenir le consentement pour la collecte ou l'utilisation de renseignements personnels et souligne les risques juridiques associés à la collecte et à la revente non autorisées de renseignements personnels. Elle reflète également la reconnaissance croissante des renseignements personnels comme un actif précieux pour les entreprises.

E.G. v. Scotiabank (Bank of Nova Scotia), 2024 QCCS 3979

Lire les détails de l'affaire

Faits

Le demandeur (E.G.), représenté par sa fille, a réclamé des dommages-intérêts pour violation présumée de la *Loi sur la protection des renseignements personnels et les documents électroniques*, L.C. 2000, ch. 5 (LPRPDE) par la défenderesse. E.G. alléguait que la Banque Scotia avait divulgué à tort ses relevés bancaires au Curateur public du Québec (le curateur public) à la suite d'une lettre dans laquelle celui-ci demandait à la Banque Scotia de divulguer les relevés bancaires d'E.G. afin de protéger ses actifs. La Banque Scotia a demandé le rejet de la demande introductive d'instance d'E.G.

Décision

La Cour a accueilli la demande de rejet.

Elle a déclaré que l'alinéa 7(3)i) de la LPRPDE prévoit une exception à la confidentialité des relevés bancaires lorsque la loi exige leur divulgation.

La Cour a conclu que la loi exigeait la divulgation des relevés bancaires d'E.G. En effet, la lettre du curateur public et la demande de divulgation qu'elle contenait ont été envoyées dans le cadre des pouvoirs d'enquête prévus à l'article 27 de la *Loi sur le curateur public*, RLRQ c. C -81. Dans le cadre d'une telle enquête, le curateur public exerce ses pouvoirs avec l'immunité conférée aux commissaires par la *Loi sur les commissions d'enquête*, RLRQ c. C -37, qui l'autorise à exiger la divulgation de renseignements personnels.

Ce raisonnement a suffi pour accueillir la demande de rejet de la Banque Scotia. Cependant, la Cour a souligné l'absence d'allégations quant à la nature du préjudice subi par E.G. comme autre motif justifiant le rejet préliminaire de la demande. La jurisprudence ne permet pas d'accorder des dommages compensatoires au seul motif qu'une personne non autorisée a eu accès à des renseignements personnels.

Point principal à retenir

Cette décision renforce le principe selon lequel les droits à la vie privée en vertu de la LPRPDE ne sont pas absolus et peuvent être outrepassés par des obligations légales de divulguer des renseignements personnels. Elle montre aussi qu'il est important de démontrer l'existence d'un préjudice réel dans les réclamations liées à la vie privée.

Pour les organisations, cette affaire sert à rappeler qu'il faut évaluer soigneusement si une exception légale s'applique avant de divulguer des renseignements personnels.

Protection de la vie privée et responsabilité délictuelle

Clearview AI Inc. v. Information and Privacy Commissioner for British Columbia, 2024 BCSC 2311

Lire les détails de l'affaire

Faits

Cette demande de contrôle judiciaire concernait l'application de la loi sur la protection des renseignements personnels de la Colombie-Britannique, intitulée *Personal Information Protection Act (PIPA)*, à Clearview AI Inc., une entreprise américaine fournissant des services de reconnaissance faciale. La technologie de Clearview collecte (ou « moissonne ») des images de personnes sur Internet, notamment celles de résidents de la Colombie-Britannique, à partir desquelles elle crée des identifiants biométriques destinés à être utilisés par des clients tiers, tels que des forces de l'ordre.

À la suite d'une enquête conjointe menée par les organismes de réglementation canadiens chargés de la protection de la vie privée, le commissaire à l'information et à la protection de la vie privée de la Colombie-Britannique (le commissaire) a conclu que Clearview avait collecté, utilisé et communiqué des renseignements personnels de résidents de la Colombie-Britannique sans leur consentement, en violation de la PIPA. Il a rendu une ordonnance interdisant à Clearview d'offrir ses services en Colombie-Britannique, lui enjoignant de cesser la collecte, l'utilisation et la communication de ces renseignements et de faire tout son possible pour supprimer les renseignements personnels recueillis auprès de personnes de la province sans leur consentement.

Clearview a demandé un contrôle judiciaire, soutenant que la PIPA ne s'appliquait pas à ses activités du fait qu'elle est une entreprise américaine, que l'interprétation du commissaire de l'expression « accessible au public » et « fin raisonnable » était déraisonnable, et que l'ordonnance était inutile, inapplicable ou trop générale.

Décision

La Cour suprême de la Colombie-Britannique a rejeté la requête, confirmant la décision et l'ordonnance du commissaire, et a rendu les conclusions suivantes :

- **Compétence et application extraterritoriale de la PIPA :** La collecte par Clearview de renseignements personnels auprès de personnes de la Colombie-Britannique et la fourniture de services à des entités dans la province établissaient un lien suffisant pour justifier la compétence. Le fait que Clearview n'ait aucune présence physique (bureaux, employés ou serveurs) en Colombie-Britannique n'était pas déterminant, compte tenu de la nature de la collecte de données sur Internet et du modèle commercial en cause.

- **Interprétation de l'expression « accessible au public » :** Le commissaire a interprété de manière raisonnable l'expression de renseignements « accessibles au public » au sens de la PIPA et de son règlement comme excluant les renseignements disponibles sur les médias sociaux ou sur des sources Internet grand public. La conclusion du commissaire selon laquelle les sites de médias sociaux ne constituent pas des sources « accessibles au public » aux fins de la PIPA était étayée par le texte, le contexte et l'objet de la loi, ainsi que par des décisions antérieures et la nature sensible des renseignements biométriques.

- **Consentement et fins raisonnables :** La Cour a convenu que Clearview n'avait pas obtenu le consentement requis pour la collecte, l'utilisation ou la communication des renseignements personnels. L'analyse a tenu compte des éléments suivants : i) la sensibilité des données biométriques moissonnées par Clearview; ii) l'absence de lien entre les fins pour lesquelles les images avaient été publiées et l'utilisation qui en était faite par Clearview; et iii) les risques de préjudice, notamment l'identification erronée et les atteintes à la protection des données.

- **Nécessité, force exécutoire et portée de l'ordonnance :** La Cour a jugé l'ordonnance nécessaire, compte tenu du refus de Clearview de s'engager à se retirer définitivement du marché de la Colombie-Britannique et de la poursuite de sa collecte de renseignements personnels. L'ordonnance n'était pas non plus trop générale, car la PIPA réglemente les activités des organisations en matière de renseignements personnels des personnes en Colombie-Britannique, quel que soit leur statut de résidence.

Point principal à retenir

Les lois provinciales sur la protection des renseignements personnels peuvent avoir une portée extraterritoriale dans le contexte de la collecte de données sur Internet. Les organismes de réglementation de la protection des renseignements personnels peuvent rendre des ordonnances exécutoires à l'encontre d'entités étrangères dont les activités ont un lien réel et substantiel avec la province. Les organisations ne peuvent pas non plus invoquer l'exception de renseignements « accessibles au public » prévue par la PIPA pour justifier le moissonnage sans consentement de renseignements personnels sur les médias sociaux ou sur Internet. Les exceptions aux mesures de protection des renseignements personnels seront interprétées de manière restrictive, et le risque de préjudice — notamment la perte de contrôle sur les renseignements personnels et le risque d'erreur d'identification — sera au cœur de l'évaluation du caractère raisonnable des fins au regard des lois sur la protection de la vie privée. Cette décision fait l'objet d'un appel.

Moon v. International Alliance of Theatrical Stage Employees (Local 891), 2024 BCSC 1560

Lire les détails de l'affaire

Faits

Kelly Moon, ex-déléguée syndicale principale de la section locale 891 de l'International Alliance of Theatrical Stage Employee (IATSE), a intenté une action civile contre le syndicat et plusieurs membres de son comité de direction, alléguant un préjudice causé par la diffusion non autorisée d'un rapport détaillant l'utilisation de sa carte de crédit, qui contenait des allégations contestées et graves à son encontre. La publication du rapport a coïncidé avec sa campagne de réélection en 2019, ce qui a porté gravement atteinte à sa réputation et a finalement conduit à sa défaite électorale. M^me^ Moon a affirmé que le comité de direction, notamment Gary Mitch Davies, avait conspiré pour publier le rapport afin de nuire à sa candidature, et elle a allégué des violations de diverses lois, notamment la loi sur la protection de la vie privée (la *Privacy Act*) de la Colombie-Britannique et la loi sur la protection des renseignements personnels (la *Personal Information Protection Act* ou PIPA) de la Colombie-Britannique, ainsi que des négligences. Les défendeurs ont demandé la radiation de ses réclamations, faisant valoir qu'elle n'avait pas épuisé les recours internes et que ses réclamations étaient dépourvues de motif valable.

Décision

La demande des défendeurs visant à radier les réclamations a été en grande partie rejetée, à l'exception de la contestation de la décision du comité électoral, qui était de nature administrative. L'analyse de la Cour concernant le délit civil de divulgation publique de faits privés, un délit reconnu en Alberta et en Ontario, était particulièrement pertinente. Après avoir examiné les décisions récentes de la Cour d'appel de la Colombie-Britannique en matière d'intrusion dans l'intimité (*Tucci v. Peoples Trust Company*, 2020 BCCA 246) et, de manière plus générale, en matière de délits civils de la common law relatifs à la vie privée (*Insurance Corporation of British Columbia v. Ari*, 2023 BCCA 331), la Cour a conclu que les tribunaux de la Colombie-Britannique pouvaient toujours reconnaître les délits civils en matière de vie privée, y compris la divulgation publique de faits privés, et a refusé de radier la nouvelle réclamation. La Cour a également refusé de radier les réclamations connexes de M^me^ Moon en vertu de la PIPA et de la *Privacy Act*, car le commissaire à la protection de la vie privée avait conclu que la section locale 891 de l'IATSE avait enfreint la PIPA et avait fait preuve de négligence.

Point principal à retenir

La Cour a refusé de rejeter une réclamation pour délit civil de divulgation publique de faits privés, refusant ainsi de fermer la porte aux délits civils liés à la vie privée en Colombie-Britannique et ouvrant la voie à la reconnaissance éventuelle de ce délit civil en particulier.

The Hospital for Sick Children v. Information and Privacy Commissioner of Ontario, 2025 ONSC 385

Lire les détails de l'affaire

Faits

L'Hospital for Sick Children (SickKids) a demandé une ordonnance de mise sous scellés afin de caviarder certains renseignements du dossier de la procédure à la suite d'une cyberattaque par rançongiciel survenue le 18 décembre 2022. Cette attaque a perturbé les systèmes cliniques et administratifs de l'hôpital, entraînant des retards dans la délivrance des ordonnances et la communication des résultats d'analyses. Au 29 décembre 2022, environ 50 % des systèmes prioritaires de l'hôpital avaient été rétablis. À la suite de l'incident, SickKids a signalé les faits au Commissaire à l'information et à la protection de la vie privée de l'Ontario (CIPVP), qui a ouvert une enquête en vertu de la *Loi sur la protection des renseignements personnels sur la santé* (LPRPS) afin d'établir s'il y avait eu divulgation non autorisée ou perte de renseignements personnels sur la santé. SickKids a coopéré avec le CIPVP en lui fournissant des informations sur ses mesures de cybersécurité, que le CIPVP a accepté de garder confidentielles afin de protéger l'hôpital contre de futures attaques.

Décision

SickKids a démontré que la publication des renseignements caviardés demandés augmenterait sa vulnérabilité aux cyberattaques futures, compromettant ainsi la sécurité de ses systèmes informatiques et les soins médicaux essentiels qu'il dispense. La Cour a estimé que les caviardages demandés étaient minimes et nécessaires pour se prémunir contre de nouvelles cybermenaces, ce qui sert un intérêt public important en matière de protection des soins aux patients. La Cour a accueilli la requête, concluant que les caviardages étaient nécessaires pour protéger les activités de l'hôpital et l'intérêt public. En outre, la Cour a jugé que SickKids avait droit au remboursement des frais de la requête, car le CIPVP s'y était initialement opposé sans déposer de mémoire en défense, se contentant d'une lettre qui n'aidait pas la Cour à statuer.

Point principal à retenir

La Cour a reconnu le besoin impérieux de trouver un équilibre entre la transparence et la protection des renseignements sensibles, en particulier dans le contexte de la cybersécurité. Les organisations pourraient s'appuyer sur cette affaire pour demander des caviardages limités lorsqu'elles peuvent démontrer l'existence d'un risque crédible de cybermenaces.

Lamarche v. British Columbia (Securities Commission), 2025 BCCA 146

Lire les détails de l'affaire

Faits

Au cours d'une enquête, la Commission des valeurs mobilières (la *Securities Commission* ou la Commission) de la Colombie-Britannique a saisi les dossiers de courriels de l'appelant, notamment des communications qui, selon lui, étaient protégées par le secret professionnel de l'avocat. L'appelant a intenté une action civile alléguant des violations de la *Charte canadienne des droits et libertés* et de la loi sur la protection de la vie privée de la Colombie-Britannique (la *Privacy Act*), en vue d'obtenir des mesures de redressement déclaratoires et pécuniaires. La Commission a demandé la suspension ou la radiation des réclamations au motif qu'une procédure administrative était en cours et/ou que les réclamations ne révélaient aucune cause d'action raisonnable.

Le juge en chambre a suspendu les réclamations constitutionnelles en attendant que le processus de la Commission soit mené à terme et a radié les réclamations en vertu de la *Privacy Act*. L'appelant a fait appel, soutenant que la Cour ne devrait pas s'en remettre au processus administratif et que ses réclamations en vertu de la *Privacy Act* ont été incorrectement radiées.

Décision

La Cour d'appel a partiellement accueilli l'appel. Elle a confirmé la suspension à statuer sur les réclamations constitutionnelles, estimant qu'en l'absence de circonstances exceptionnelles, les parties doivent épuiser les voies de recours administratives avant de saisir la justice.

Toutefois, la Cour a annulé l'ordonnance rejetant les réclamations fondées sur la *Privacy Act*. Même si la Commission bénéficiait d'une immunité d'origine législative pour les actes accomplis de bonne foi, un degré suffisant d'imprudence peut justifier une présomption de mauvaise foi. Les actes de procédure de l'appelant, selon lesquels la Commission aurait agi de manière imprudente en ne mettant pas en œuvre des protocoles adéquats, étaient suffisants pour étayer une conclusion potentielle de mauvaise foi ou d'absence de bonne foi. La Cour a également rejeté la conclusion du juge en chambre selon laquelle la *Privacy Act* ne pouvait être invoquée pour faire valoir des allégations pouvant également fonder une violation de la Charte canadienne, précisant que les allégations relatives à la vie privée et à la Charte canadienne ne s'excluent pas mutuellement.

La Cour a ordonné que les réclamations fondées sur la *Privacy Act*, notamment les réclamations de dommages punitifs, soient suspendues (plutôt que rejetées) jusqu'à la fin du processus administratif de la Commission, afin d'éviter le dédoublement et la fragmentation des procédures.

Point principal à retenir

Les réclamations fondées sur la *Privacy Act* peuvent survivre à une requête en radiation, même lorsque l'immunité d'origine législative pour conduite de bonne foi est invoquée, car un degré suffisant d'imprudence peut justifier une présomption de mauvaise foi. La décision confirme également que les délits civils en matière de vie privée et les réclamations fondées sur la Charte canadienne peuvent faire l'objet de poursuites parallèles, sous réserve d'un report de procédure afin d'éviter les litiges redondants.

Insurance Corporation of British Columbia v. Ari, 2025 BCCA 131

Lire les détails de l'affaire

Faits

L'action collective sous-jacente découle des actes d'un ex-employé de l'appelant qui avait accédé aux renseignements personnels de 78 clients à des fins illégitimes et vendu certains de ces renseignements à des criminels. Par la suite, 13 personnes ont été la cible d'incendies criminels et de coups de feu. Le groupe a été défini comme comprenant toutes les personnes dont les renseignements avaient été consultés, ainsi que les résidents à leur adresse. Le juge d'instruction sommaire a accordé des dommages-intérêts globaux de 15 000 $ par membre du groupe pour violation de la vie privée en vertu de l'article premier de la loi sur la protection de la vie privée de la Colombie-Britannique (la *Privacy Act*). Ces dommages-intérêts ont été accordés indépendamment du fait que les membres du groupe aient réellement subi un préjudice. Les préjudices individuels seront examinés à un stade ultérieur de la procédure.

Décision

La Cour d'appel a confirmé l'octroi de dommages-intérêts, affirmant que la *Privacy Act* crée un délit civil pour atteinte à la vie privée sans preuve de préjudice. Des dommages-intérêts généraux peuvent être accordés pour indemniser, réparer et dissuader les atteintes à la vie privée proprement dite, reflétant ainsi la nature quasi constitutionnelle du droit à la vie privée.

La Cour a rejeté l'argument selon lequel, en l'absence de preuve de préjudice, seuls des dommages-intérêts symboliques pouvaient être accordés, soulignant que la loi présume qu'un préjudice découle de la simple atteinte à la vie privée. La gravité et le caractère délibéré de l'atteinte, à savoir la diffusion de renseignements à des criminels et les risques qui en découlaient pour les membres du groupe, justifiaient l'octroi d'une indemnité supérieure à un montant purement symbolique. Le fait de limiter les dommages-intérêts à une somme dérisoire aurait porté atteinte à l'intention du législateur de la *Privacy Act* et rendu inefficace le droit à la protection de la vie privée garanti par la loi.

Point principal à retenir

La décision confirme qu'en vertu de la *Privacy Act*, des dommages-intérêts généraux pour atteinte à la vie privée peuvent être accordés sans preuve d'un préjudice consécutif. Même si la décision ne concernait que la *Privacy Act*, d'autres provinces ont des lois similaires, de sorte que le raisonnement de la Cour d'appel pourrait s'appliquer à des lois parallèles sur la protection des renseignements personnels. L'affaire démontre également que des dommages-intérêts globaux potentiellement importants peuvent être accordés pour des atteintes à la protection des données, même en l'absence de preuve d'un préjudice individuel.

Accès à l'information

Centre d'acquisitions gouvernementales c. Teva Canada limitée, 2025 QCCQ 892

Lire les détails de l'affaire

Faits

L'appelant, le Centre d'acquisitions gouvernementales (CAG), un organisme public du Québec, a fait appel d'une décision rendue par la Commission d'accès à l'information (CAI), qui ordonnait au CAG de transmettre à l'intimée, Teva Canada limitée (Teva), des copies de deux demandes d'accès à l'information qu'il avait reçues dans le cadre de l'application de la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, RLRQ c. A-2.1 (la Loi sur l'accès). Teva avait adressé une requête au CAG afin d'obtenir une copie de ces deux demandes qui visaient, notamment, à obtenir une copie d'un contrat conclu avec plusieurs fournisseurs, dont Teva.

La CAI a conclu que ces demandes d'accès à l'information avaient été déposées par le CAG dans l'exercice de ses fonctions. Elle a également établi que les documents demandés ne contenaient pas de renseignements personnels, car les demandes d'accès à l'information avaient été faites pour le compte et au nom de personnes morales.

Décision

La Cour a rejeté l'appel.

La Cour a conclu que la CAI n'avait pas commis d'erreur susceptible de révision en concluant que les demandes d'accès à l'information sont des documents détenus dans l'exercice des fonctions d'un organisme public, qui doivent être interprétés de manière libérale au sens de la Loi sur l'accès. La Cour a souligné que le fait que la loi constitutive d'un organisme ne prévoit pas spécifiquement son obligation de détenir tel ou tel autre document ne permet pas de conclure, en soi, que le document n'est pas détenu dans l'exercice de ses fonctions.

Les fonctions d'un organisme public s'étendent non seulement à l'ensemble de ses fonctions principales, mais également aux fonctions accessoires découlant de celles-ci, aux fonctions assumées volontairement ainsi qu'aux activités lui incombant en raison de sa loi constitutive ou en vertu d'une loi d'application générale comme la Loi sur l'accès. Par conséquent, la Cour a conclu que les documents demandés par Teva dans sa demande d'accès à l'information étaient détenus par le CAG dans l'exercice de ses fonctions.

Par ailleurs, la Cour a jugé que l'identité des demandeurs d'accès à l'information ne constituait pas un renseignement personnel confidentiel. Le nom d'une personne agissant à titre de représentant d'une entreprise n'est toutefois pas considéré comme un renseignement personnel confidentiel s'il n'est associé à aucune information significative le concernant personnellement. Ainsi, les documents demandés par Teva ne contenaient aucun renseignement personnel confidentiel au sens de la Loi sur l'accès.

S'il souhaitait ériger un principe fondamental visant la protection de l'identité des demandeurs d'accès et la confidentialité des demandes d'accès à proprement parler, le législateur l'aurait spécifié. La Cour a réitéré l'avis de la CAI selon lequel il ne lui appartient pas de créer une nouvelle exception au droit d'accès ni de réécrire la Loi sur l'accès.

La Cour ayant conclu qu'aucune exception au droit d'accès n'était applicable en l'espèce, rien n'empêchait le CAG de communiquer les documents demandés à Teva.

Point principal à retenir

Cette décision clarifie la portée de la Loi sur l'accès du Québec en affirmant que les demandes d'accès à l'information visent les documents détenus dans l'exercice des fonctions d'un organisme public et que le droit d'accès doit être interprété de manière libérale, à moins qu'une exception ne soit expressément prévue dans cette loi.

De plus, l'identité des demandeurs d'accès à l'information n'est pas considérée comme un renseignement personnel confidentiel au sens de cette loi si elle n'est pas associée à d'autres renseignements personnels importants.

Office of the Information and Privacy Commissioner for British Columbia v. Airbnb Ireland UC, 2024 BCCA 333

Lire les détails de l'affaire

Faits

Cet appel concernait la divulgation de renseignements sur les titulaires de permis de location à court terme (LCT) dans la ville de Vancouver, collectés par la ville conformément à son accord avec Airbnb. En 2018, la ville a modifié ses règlements municipaux afin d'obliger les exploitants de LCT à obtenir des permis, qui sont délivrés au nom de l'exploitant et indiquent son adresse personnelle. Dans le cadre d'un protocole d'entente, Airbnb a fourni à la ville les noms, numéros de permis, adresses personnelles et adresses électroniques des hôtes, tous considérés comme des « renseignements personnels » au sens de la *Freedom of Information and Protection of Privacy Act* (FIPPA), la loi sur l'accès à l'information et la protection de la vie privée de la Colombie-Britannique.

Un demandeur a sollicité la divulgation des noms, numéros de permis et adresses des hôtes des LCT. La Ville a rejeté la requête en invoquant plusieurs exceptions à la FIPPA, notamment celles liées à la sécurité, à la sûreté des biens, aux intérêts commerciaux de tiers et à la protection des renseignements personnels. Le demandeur a sollicité un examen par le Commissariat à l'information et à la protection de la vie privée (CIPVP).

L'arbitre de la CIPVP a ordonné la divulgation de certains renseignements, estimant que la plupart des préoccupations de la Ville et d'Airbnb concernant les préjudices n'étaient pas fondées, à l'exception d'un cas impliquant une victime de harcèlement. Il a également déterminé que les adresses des LCT étaient des « coordonnées » plutôt que des « renseignements personnels », car elles étaient utilisées à des fins commerciales et n'étaient donc pas protégées contre la divulgation en vertu de l'article 22 de la FIPPA.

Airbnb a demandé un contrôle judiciaire, faisant valoir que l'interprétation qu'avait faite l'arbitre de la FIPPA était déraisonnable et que les hôtes auraient dû être avisés et avoir la possibilité de participer au contrôle. La Cour suprême de la Colombie-Britannique a annulé la décision de la CIPVP, renvoyé l'affaire pour réexamen et ordonné que tous les titulaires de permis soient avisés avant le réexamen.

Décision

La Cour d'appel de la Colombie-Britannique a accueilli en partie l'appel du CIPVP, uniquement sur la question de savoir si les personnes dont les renseignements pourraient être divulgués devaient être informées du fait que le commissaire envisageait de les divulguer. Elle a jugé que la décision d'informer ou non les personnes concernées relevait du pouvoir discrétionnaire du CIPVP en vertu de l'article 54 de la FIPPA.

La Cour a confirmé la décision du tribunal de première instance, soulignant que l'analyse du juge était trop formaliste et ne tenait pas suffisamment compte du contexte législatif et de l'objectif de la loi, ni des conséquences pratiques sur la vie privée que pouvait avoir la divulgation d'adresses privées utilisées à des fins professionnelles.

Point principal à retenir

Cette affaire souligne la nécessité d'adopter une approche contextuelle et téléologique pour interpréter la notion de « renseignements personnels » au sens de la FIPPA, en particulier lorsque l'adresse du domicile est utilisée à des fins personnelles et professionnelles.

Compétence des organismes de protection de la vie privée

Société québécoise d'information juridique c. Commission d'accès à l'information, 2025 QCCQ 859

Lire les détails de l'affaire

Faits

Une personne a formulé une demande de rectification auprès de la Commission d'accès à l'information (CAI) du Québec après que la Société québécoise d'information juridique (SOQUIJ) a rejeté sa demande visant à anonymiser les renseignements personnels la concernant figurant sur le site Web de la SOQUIJ. La SOQUIJ gère une base de données contenant notamment les jugements rendus par le Tribunal administratif du logement (TAL) et le Tribunal administratif du travail (TAT).

La SOQUIJ a présenté une requête en irrecevabilité, faisant valoir que la CAI ne possédait pas la compétence juridictionnelle afin de trancher la demande de rectification. Elle a souligné que la CAI disposait déjà, à ce moment-là, de tous les éléments pertinents lui permettant d'accorder sa requête en irrecevabilité, avant d'entendre le fond. La CAI a rejeté la contestation de compétence et la SOQUIJ a fait appel de la décision.

Décision

La Cour a considéré que la personne qui demandait l'anonymisation à la SOQUIJ n'avait, à aucun moment, demandé au TAL ou au TAT une quelconque forme d'anonymisation, de procédure à huis clos ou de mesures visant à garantir la confidentialité de son identité. La Cour a estimé que la CAI ne pouvait pas imposer la mesure de réparation demandée, car elle n'est pas compétente pour siéger en appel ou en révision des décisions de ces tribunaux. Une audience sur le fond n'était ni nécessaire ni souhaitable pour parvenir à cette conclusion.

Ainsi, la question dont était saisie la CAI était de déterminer l'identité de l'instance compétente pour accorder la réparation demandée par la personne souhaitant garder l'anonymat. Seuls le TAT et le TAL pouvaient rectifier, modifier ou anonymiser les décisions qu'ils avaient rendues.

Les renseignements personnels visés par la demande de rectification sont des renseignements publics, car la personne qui a présenté la demande n'a pas demandé au TAL ni au TAT d'anonymiser leurs décisions. Dans ces circonstances, le recours prévu à l'article 89 de la Loi sur l'accès ne peut être exercé pour rectifier les décisions rendues par des instances juridictionnelles telles que le TAT et le TAL.

En refusant d'accueillir la demande de rejet, et donc en refusant de se dessaisir, la CAI s'est arrogé une compétence qui relève plus spécifiquement du TAT et du TAL. De plus, elle a erré en concluant que les renseignements personnels obtenus dans l'exercice d'une fonction juridictionnelle, qui ne sont pas visés par une ordonnance de non-divulgation, de non-publication ou de non-diffusion, restent assujettis au chapitre III de la Loi sur l'accès du Québec, qui comprend l'article 89.

La CAI a rejeté la requête en irrecevabilité sur la base qu'elle détient une compétence générale quant à la SOQUIJ en raison de son statut d'organisme public en vertu de la Loi sur l'accès. En appel, la Cour a conclu que la CAI avait erré, car elle devait avoir compétence sur le fond du litige, ce qui n'était pas le cas en l'espèce. L'appel de la SOQUIJ a été accueilli en partie, ainsi que sa contestation de compétence.

Point principal à retenir

Cette décision fournit des indications importantes sur les limites de la compétence de la CAI. Elle renforce également le principe selon lequel les ordonnances de confidentialité ne peuvent être rendues que par la cour ou le tribunal saisi de la demande. La CAI ne peut imposer rétroactivement de telles ordonnances aux décisions rendues par ces tribunaux ou ces cours.

IA et vie privée

Svoboda v. Modiface Inc., 2024 ONSC 6249

Lire les détails de l'affaire

Faits

La Cour supérieure de l'Ontario a statué sur une demande visant à faire exécuter des lettres rogatoires délivrées par un tribunal américain dans le cadre d'une action collective, où les demandeurs, représentant un groupe, alléguaient des violations de la loi de l'Illinois sur la protection des renseignements biométriques (la *Illinois Biometric Information Privacy Act*). Le tribunal américain cherchait à contraindre ModiFace Inc., une société canadienne qui a développé une technologie de réalité augmentée (RA), à produire son code source et à fournir des témoignages sous serment. ModiFace s'est opposée à cette demande, arguant que sa portée était trop large et que la divulgation de son code source pourrait nuire gravement et de manière irréparable à ses activités.

Décision

La Cour a estimé que les requérants n'avaient pas démontré la pertinence et la nécessité du code source non obscurci en vertu du droit de l'Ontario, jugeant que la demande était contraire à l'ordre public en raison du risque pour la technologie exclusive de ModiFace. Toutefois, la Cour a ordonné à ModiFace de fournir son code compilé et obscurci et de se soumettre à une déposition, soulignant que la production du code non obscurci n'était pas justifiée. La Cour a également noté que la charge de la conformité ne devait pas incomber à ModiFace, qui n'était pas partie à l'action américaine, et qu'il existait des méthodes moins intrusives pour obtenir les renseignements nécessaires.

Point principal à retenir

Cette décision a souligné l'importance d'équilibrer l'entraide judiciaire internationale et la protection des renseignements confidentiels des entreprises canadiennes. En effet, la divulgation d'un code source non obscurci à un concurrent porterait inutilement et gravement atteinte aux intérêts commerciaux de l'entreprise canadienne.

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 relativement à un large éventail de questions juridiques nationales et transfrontalières. Notre approche « une équipe, un cabinet » nous permet d'offrir un accès direct à l'un de nos 600 avocats afin de fournir des solutions juridiques efficaces, proactives et pratiques dictées par vos besoins. Depuis plus de 160 ans, nous avons acquis la réputation de résoudre les problèmes, d'éliminer les obstacles et de fournir les réponses dont vous avez besoin, quand vous en avez besoin.

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

OSLER