

Le 7 mai 2024

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



TABLE DES MATIÈRES

- [Highland Cannabis Inc. v. Alcohol and Gaming Commission of Ontario, 2024 ONSC 423](#)
- [Carter v. LifeLabs Inc., 2023 ONSC 6104](#)
- [Option Consommateurs c. Home Depot of Canada Inc., 2023 QCCS 3493](#)
- [Insurance Corporation of British Columbia v. Ari, 2023 BCCA 331](#)
- [G.D. v. South Coast British Columbia Transportation Authority, 2023 BCSC 958](#)
- [Broutzas v. Rouge Valley Health System, 2023 ONSC 540](#)

Lire l'édition complète : *Revue de la jurisprudence sur la protection de la vie privée*

HIGHLAND CANNABIS INC. V. ALCOHOL AND GAMING COMMISSION OF ONTARIO, 2024 ONSC 423

En savoir plus sur la décision : [Highland Cannabis Inc. v. Alcohol and Gaming Commission of Ontario, 2024 ONSC 423](#)

FAITS

La défenderesse, High Tide Inc., et la demanderesse, Highland Cannabis Inc., exercent leurs activités dans le secteur de la vente au détail de cannabis. Highland Cannabis a intenté une action en justice contre High Tide et la Commission des alcools et des jeux de l'Ontario (CAJO) relativement à une atteinte à la protection des données à la CAJO. Des données précises concernant le chiffre d'affaires des magasins de vente au détail de cannabis pour les mois de juillet et décembre 2021 ont fait l'objet d'une fuite ou d'un détournement. Highland Cannabis a prétendu que High Tide avait accédé à ces données et les avait utilisées au détriment de Highland Cannabis. High Tide a présenté une requête en rejet de l'action au motif qu'elle était frivole et vexatoire et qu'elle constituait un abus de procédure.

DÉCISION

Le tribunal a accédé à la requête de High Tide et a rejeté l'action à son encontre. Il a conclu que la demande était frivole et vexatoire, et qu'il était clair et évident que la demanderesse ne pouvait pas obtenir gain de cause. Le tribunal a conclu qu'il n'y avait pas de cause d'action pour l'intrusion dans l'intimité, parce que High Tide ne s'est pas immiscée intentionnellement dans les affaires ou entreprises privées de la demanderesse, et une personne raisonnable ne considérerait pas l'intrusion (accès aux données de vente) comme une atteinte très offensante causant détresse, humiliation ou angoisse. Le tribunal a en outre conclu qu'il n'y avait pas de cause d'action pour le détournement, puisque le délit ne s'applique pas en cas d'atteinte à la protection des données, et que High Tide n'a pas nui au droit ou au titre de propriété de la demanderesse à l'égard des données. Le tribunal a conclu que le simple fait que des données ont été vues par des destinataires passifs, dans le contexte de cette atteinte, ne peut pas équivaloir à un acte illégal.

Point principal à retenir

Cette affaire illustre les limites des délits d'intrusion et de détournement dans le contexte des atteintes à la protection des données. Le tribunal a souligné que le délit d'intrusion dans l'intimité exigeait une conduite intentionnelle ou imprudente, et que High Tide avait également été victime de l'atteinte à la protection des données. Il a conclu que le délit de détournement ne s'appliquait pas à de l'information, à de la propriété intellectuelle ou à des biens intangibles, et que High Tide n'a pas nui au droit ou au titre de propriété de Highland Cannabis à l'égard des données.

CARTER V. LIFELABS INC., 2023 ONSC 6104

En savoir plus sur la décision : [Carter v. LifeLabs Inc., 2023 ONSC 6104](#)

FAITS

Les demandeurs, qui sont des clients actuels ou anciens de LifeLabs, une société de tests de laboratoire médical, ont poursuivi LifeLabs pour une atteinte à la protection des données qui a potentiellement compromis les renseignements personnels de 8,6 millions de clients. Ils ont invoqué diverses causes d'action, notamment la négligence, la rupture de contrat, les recours en matière de protection des consommateurs, les atteintes à la vie privée prévues par la loi et l'enrichissement sans cause, et ont demandé des dommages-intérêts et la restitution des bénéfices. Après quatre ans de litige, les parties ont convenu de régler l'action sous réserve de l'approbation du tribunal. L'entente de règlement prévoyait un paiement de 4,9 millions de dollars en fonds de règlement garantis et de 4,9 millions de dollars en fonds de règlement conditionnels par LifeLabs aux membres du groupe, en fonction du nombre de réclamations déposées. L'entente de règlement indiquait également que l'avocat du groupe demandait des honoraires conditionnels de 25 % des fonds de règlement et que chaque représentant des demandeurs devait recevoir une rémunération de 2 500 \$, sous réserve de l'approbation du tribunal.

DÉCISION

L'entente de règlement et les honoraires d'avocat ont été approuvés, mais la demande de rémunération a été rejetée. La contribution des représentants des demandeurs était typique du bon travail effectué par des représentants de demandeurs, et le tribunal a conclu qu'il ne s'agissait pas d'un cas exceptionnel qui justifierait l'octroi d'une rémunération.

Point principal à retenir

Le tribunal examine minutieusement le caractère équitable et raisonnable d'une entente de règlement et des honoraires des avocats dans le cadre d'une action collective. À cette fin, il tient compte de divers facteurs, comme la probabilité de recouvrement, le montant et la nature du règlement, la recommandation et l'expérience de l'avocat, les frais futurs et la durée du litige, le nombre et la nature des objections et l'existence d'une négociation de bonne foi.

OPTION CONSOMMATEURS C. HOME DEPOT OF CANADA INC., 2023 QCCS 3493

En savoir plus sur la décision : [Option Consommateurs c. Home Depot of Canada Inc., 2023 QCCS 3493](#)

FAITS

Le tribunal a accordé à la défenderesse la permission de produire en preuve la *Home Depot's Privacy and*

Security Statement (Déclaration de confidentialité et de sécurité de Home Depot), mais a refusé la permission de produire la *Facebook's Privacy Policy* (Politique de confidentialité de Facebook) et les *Tools pertaining to Off-Facebook Activity* (Outils relatifs aux activités hors Facebook).

Le tribunal a décidé que la Déclaration de confidentialité et de sécurité de Home Depot constituait une preuve essentielle et indispensable dans le cadre factuel sur lequel repose la demande d'autorisation d'une action collective. Selon le tribunal, cette preuve permettrait à la défenderesse de contester les allégations contenues dans la demande relativement aux conditions d'utilisation ou de partage de renseignements personnels. Le tribunal a en outre conclu que cette preuve permettrait à la défenderesse de présenter des arguments pour souligner la différence entre les achats en magasin et ceux faits sur le site Web de la défenderesse, ces derniers n'ayant pas fait l'objet de l'enquête du CPVP. Dès lors, cette preuve serait utile à la composition du groupe ainsi que la formulation des questions de fait.

En ce qui concerne les documents de Facebook, le tribunal a décidé que la défenderesse ne s'était pas acquittée du fardeau de preuve qui lui incombait. Bien que la défenderesse ait soutenu que ces documents, mentionnés dans le rapport du CPVP, étaient nécessaires pour démontrer les outils offerts aux usagers de Facebook pour contrôler leurs renseignements personnels, le tribunal a souligné qu'il n'était pas suffisant de vouloir compléter une pièce si la pertinence de cette preuve n'est pas démontrée.

DÉCISION

The court granted the defendant permission to file Home Depot's Privacy and Security Statement in evidence, but denied permission relating to Facebook's Privacy Policy and Tools pertaining to Off-Facebook Activity.

The court decided that Home Depot's Privacy and Security Statement is a relevant and essential piece of evidence in the factual framework on which the request to authorize a class action is based. According to the court, this evidence would allow the defendant to contest allegations contained in the application in connection with the conditions of use or sharing of personal information. The court further found that this evidence would enable the defendant to present arguments highlighting the difference between in-store purchases and those made on the defendant's website, which were not the subject of the OPC's investigation, and would therefore be useful for the composition of the class and the formulation of questions of fact.

With respect to Facebook's documents, the court ruled that the defendant had not met its burden of proof. While the defendant argued that these documents, referred to in the OPC's report, are necessary to demonstrate the tools available to Facebook users to control their personal information, the court pointed out that it is not sufficient to wish to complete an exhibit if the relevance of the evidence is not demonstrated.

Point principal à retenir

Les déclarations de confidentialité et de sécurité peuvent être déposées en tant que preuves pertinentes en vertu de l'article 574 du C.p.c. lorsqu'elles permettent à un défendeur de contester les allégations contenues dans la demande en rapport avec les conditions d'utilisation ou de partage des renseignements personnels, et de présenter des arguments en rapport avec la composition du groupe et la formulation des questions de fait.

Toutefois, il ne suffit pas de faire valoir que la preuve que l'on souhaite déposer complète une pièce si la pertinence de la preuve n'est pas démontrée.

INSURANCE CORPORATION OF BRITISH COLUMBIA V. ARI, 2023 BCCA 331

En savoir plus sur la décision : [Insurance Corporation of British Columbia v. Ari, 2023 BCCA 331](#)

FAITS

L'Insurance Corporation of British Columbia (ICBC) a porté en appel une décision dans laquelle elle a été jugée responsable du fait que son employé avait commis une atteinte à la vie privée des clients de l'ICBC en vendant des renseignements personnels reliant les plaques d'immatriculation des clients à leur adresse domiciliaire. Plusieurs de ces clients ont ensuite été la cible d'incendies criminels et de fusillades. En appel, l'ICBC a soutenu que le juge avait commis une erreur en concluant que les renseignements étaient confidentiels, en imposant la responsabilité du fait d'autrui et en concluant que les dommages-intérêts généraux pouvaient être déterminés dans le cadre d'une action collective.

DÉCISION

La Cour d'appel de la Colombie-Britannique a rejeté l'appel, affirmant que le juge de première instance n'avait pas commis d'erreur dans ses conclusions à l'égard de tous les arguments soulevés par l'appelante. Plus précisément, elle a déclaré qu'il n'avait commis aucune erreur en concluant que les renseignements vendus étaient confidentiels au sens de la loi de la Colombie-Britannique intitulée *Privacy Act*. Les clients de l'ICBC pouvaient raisonnablement s'attendre à ce que l'appelante n'utilise les renseignements qu'ils lui avaient fournis qu'à des fins commerciales légitimes. Ils avaient par ailleurs le droit de contrôler l'utilisation de leurs renseignements personnels. En outre, la Cour a déclaré que le juge n'avait pas commis d'erreur en imposant la responsabilité du fait d'autrui, car des motifs de principe justifient l'imposition de la responsabilité.

Point principal à retenir

Le comportement de l'employé, qui a vendu certains renseignements à des tiers dans un but criminel, a entaché tous ses actes en accédant aux dossiers des clients sans but professionnel légitime.

La décision confirme également que la loi de la Colombie-Britannique intitulée *Privacy Act* n'exige pas de preuve de dommages réels. Des dommages-intérêts généraux peuvent être accordés dans le cadre d'une action collective, sans qu'il soit nécessaire d'apporter une preuve individualisée.

G.D. V. SOUTH COAST BRITISH COLUMBIA TRANSPORTATION AUTHORITY, 2023 BCSC 958

En savoir plus sur la décision : [G.D. v. South Coast British Columbia Transportation Authority, 2023 BCSC 958](#)

FAITS

Les demandeurs, d'anciens employés de la défenderesse, la South Coast British Columbia Transportation Authority, demandent la certification de leur projet d'action collective en vertu de la loi de la Colombie-Britannique intitulée *Class Proceedings Act* en leur nom propre et au nom de toutes les autres personnes dont les renseignements personnels ont été compromis par une atteinte à la sécurité des données survenue en 2020, qui a touché les réseaux et systèmes informatiques de la défenderesse.

En décembre 2020, l'équipe des TI de TransLink a découvert un logiciel rançonneur sur son réseau, confirmant qu'une partie de son infrastructure de TI avait été la cible d'une attaque par logiciel rançonneur. Malgré la présence des programmes de cybersécurité du réseau, les cybercriminels sont parvenus à accéder à la sécurité du réseau de TransLink et ont inséré le logiciel rançonneur à la suite d'une tentative d'hameçonnage réussie auprès d'un employé de l'une des filiales d'exploitation de TransLink. La défenderesse a pris de nombreuses mesures pour riposter à la menace. Les demandeurs ont invoqué les causes d'action suivantes : violation des obligations légales de protection de la vie privée, négligence, délit civil de détournement et enrichissement sans cause. Ils ont principalement soutenu que la défenderesse avait causé ou permis l'atteinte à la protection des données, car elle violait ses propres normes en matière de protection des renseignements personnels.

DÉCISION

Le tribunal a conclu que les réclamations étaient vouées à l'échec et a donc rejeté la demande de certification des demandeurs.

Point principal à retenir

Le tribunal a déclaré que le responsable d'un délit civil pour cause d'infraction dans le contexte d'une atteinte à la sécurité d'une base de données ne peut être que le pirate de la base de données, et non pas la défenderesse.

BROUTZAS V. ROUGE VALLEY HEALTH SYSTEM, 2023 ONSC 540

En savoir plus sur la décision : [*Broutzas v. Rouge Valley Health System, 2023 ONSC 540*](#)

FAITS

Les demanderesses sont des femmes qui ont accouché à un hôpital du Rouge Valley Health System ou au Scarborough and Rouge Hospital entre 2009 et 2014 et dont les renseignements personnels ont été consultés par des employés malhonnêtes des hôpitaux et divulgués à des vendeurs de régimes enregistrés d'épargne-études (REEE) sans leur consentement. Elles ont intenté deux actions collectives contre les hôpitaux, les employés malhonnêtes, les vendeurs de REEE et les sociétés de REEE, alléguant le délit d'intrusion dans l'intimité et réclamant des dommages-intérêts. Le juge saisi de la requête a rejeté leurs demandes de certification, estimant qu'elles ne répondraient pas aux critères de l'article 5 de la *Loi de 1992 sur les recours collectifs*. Les demanderesses ont fait appel de ce rejet, en se concentrant sur l'action en responsabilité délictuelle contre les défendeurs individuels et sur les actions en responsabilité du fait d'autrui correspondantes contre les hôpitaux et les sociétés de REEE.

DÉCISION

La Cour divisionnaire a convenu avec le juge saisi de la requête que les employés malhonnêtes avaient consulté ou divulgué, non pas des renseignements médicaux confidentiels concernant les demanderesses, mais uniquement leurs coordonnées, qui sont des renseignements personnels, mais non confidentiels, dans le contexte de cette affaire. La Cour a également convenu qu'une personne raisonnable ne considérerait pas l'intrusion comme très offensante, causant de la détresse, de l'humiliation ou de l'angoisse, comme l'exige le troisième élément du délit. La Cour a estimé que le juge saisi de la requête n'avait pas commis d'erreur en concluant qu'il n'y avait pas de cause d'action contre les vendeurs de REEE, qui ne s'étaient pas immiscés dans l'intimité des demanderesses, et qu'il n'était pas nécessaire d'étendre le champ d'application du délit à ces derniers. La Cour a également conclu que

le juge saisi de la requête n'avait pas commis d'erreur en concluant que les sociétés de REEE ne pouvaient pas être responsables du fait d'autrui pour les actes des vendeurs de REEE.

Point principal à retenir

Ce qu'il faut retenir de cette décision, c'est que le délit d'intrusion dans l'intimité se limite aux atteintes délibérées et importantes à la vie privée qu'une personne raisonnable trouverait très offensantes.

RESTER INFORMÉ

Recevez une notification par courriel vous informant de la disponibilité de la prochaine édition de *la Revue de la jurisprudence sur la protection de la vie privée*.

Abonnez-vous maintenant

© Osler, Hoskin & Harcourt S.E.N.C.R.L./s.r.l. Le contenu de la présente est fourni à titre d'information générale seulement et ne constitue ni un conseil juridique ni un conseil professionnel ou autre avis de quelque nature que ce soit. Vous pouvez vous inscrire pour recevoir des mises à jour sur une foule de sujets liés à différents secteurs d'activité à l'adresse osler.com/abonnez-vous.