OSLER

Les actions collectives canadiennes en matière de protection des renseignements personnels évoluent au-delà des violations de données classiques

11 JANVIER 2023 11 MIN DE LECTURE

Expertises Connexes

- Actions collectives

Auteur: Robert Carson

En 2021, nous avons signalé que les tribunaux de tout le pays avaient exercé leur rôle de contrôleur pour mettre un terme aux actions collectives pour violation de données non fondées sur des preuves de préjudice pour les membres du groupe visé par l'action collective projetée. Les tribunaux de l'Ontario ont également confirmé d'importantes limitations au délit d'intrusion dans la vie privée, estimant qu'il ne s'appliquait pas lorsqu'un défendeur avait simplement échoué à empêcher un incident de piratage. En 2022, dans une victoire importante pour les « défendeurs exploitant des bases de données », la Cour d'appel de l'Ontario a confirmé ce raisonnement.

De nombreux avocats de demandeurs semblent désormais se détourner, du moins en partie, des recours pour violation de données classiques. Les allégations les plus courantes dans le cadre des nouvelles actions collectives vont de la mauvaise utilisation de données au manque de protection des enfants et des adolescents qui utilisent des services en ligne. Les tribunaux canadiens continuent également de se pencher sur de nouveaux délits touchant la vie privée.

Limites du délit d'intrusion dans la vie privée

En 2021, la Cour divisionnaire de l'Ontario a décidé, dans l'affaire *Owsianik v. Equifax Canada Co.* (l'« affaire Owsianik » ; en anglais seulement), que le délit d'intrusion dans l'intimité n'était pas applicable dans les cas de violation de données où les renseignements en cause ont été piratés par un tiers malveillant et où le défendeur a simplement échoué à empêcher l'intrusion. En novembre 2022, la Cour d'appel de l'Ontario a statué sur les appels interjetés dans l'affaire Owsianiket dans d'autres affaires concernant ce délit.

La décision de la Cour atteste de façon importante des droits des défendeurs exploitant des bases de données. Elle établit également de façon importante les limites du délit d'intrusion dans la vie privée et de tout autre nouveau délit touchant la vie privée.

La Cour a expliqué que le délit d'intrusion dans la vie privée comportait trois éléments. Comme premier élément, il y a le comportement, c'est-à-dire que le défendeur doit avoir fait ingérence ou intrusion dans les affaires privées du demandeur sans excuse légitime. Ensuite, il y a l'état d'esprit, c'est-à-dire que le défendeur doit avoir fait intrusion intentionnellement ou par insouciance. Enfin, l'intrusion doit entraîner des conséquences. Il faut pour cela qu'une personne raisonnable considère l'intrusion comme un acte très offensant, qui cause de la détresse, de l'humiliation ou de l'angoisse. La Cour a conclu que, lorsqu'un tiers pirate accède à des renseignements en possession du défendeur exploitant une base de données,

l'élément du délit qui concerne le comportement était absent pour le défendeur exploitant la base de données, car on ne peut pas dire que le défendeur exploitant la base de données a fait « ingérence ou intrusion ».

La décision est une victoire notable pour les défendeurs. Les demandeurs avaient fait valoir que le délit d'intrusion dans la vie privée était nécessaire pour les actions collectives en matière de protection des renseignements personnels parce que « les recours disponibles en matière de contrat et de négligence exigent la preuve d'une perte pécuniaire ». La Cour a expressément rejeté ce raisonnement, estimant que : [TRADUCTION] « Il est vrai que l'impossibilité de réclamer des dommages moraux peut avoir des répercussions négatives sur la capacité des demandeurs à faire autoriser la demande en tant qu'action collective. À mon avis, cette conséquence procédurale ne constitue pas une absence de recours. Les avantages procéduraux ne sont pas des recours. »

Plus tôt cette année, avant la publication de la décision dans l'affaire Owsianik, plusieurs tribunaux s'étaient penchés sur la nature et les limites du délit d'intrusion dans la vie privée. Par exemple, dans l'affaire *Stewart v. Demme* (en anglais seulement), la Cour divisionnaire de l'Ontario a infirmé une décision antérieure autorisant une action collective fondée sur le délit d'intrusion dans la vie privée. La Cour divisionnaire a jugé que l'affaire n'aurait pas dû être autorisée si l'employé de l'hôpital n'avait eu qu'un accès « éphémère et accessoire » (*fleeting and incidental*) à des renseignements médicaux dans le cadre d'un autre acte prétendument illicite.

Dans une décision distincte (en anglais seulement), la Cour d'appel de l'Ontario a rejeté l'appel de cet employé contre un refus de couverture d'assurance. Ce faisant, la Cour a conclu que l'exclusion des actes intentionnels de la police d'assurance s'appliquait aux allégations selon lesquelles l'employé avait commis le délit d'intrusion dans la vie privée. La Cour a conclu que l'exclusion s'appliquait sans égard au fait que la plaidoirie portait sur une intrusion « intentionnelle » (*intentional*) ou « intentionnelle ou insouciante » (*intentional or reckless*).

Dans l'affaire *Campbell v. Capital One Financial Corporation* (en anglais seulement), la Cour suprême de la Colombie-Britannique a autorisé une action collective découlant d'une violation de données. Bien qu'elle ait autorisé l'action, la Cour a refusé la demande du demandeur de reconsidérer la jurisprudence de la Colombie-Britannique selon laquelle le délit d'intrusion dans la vie privée avait été éliminé par la loi de la Colombie-Britannique intitulée *Privacy Act*. Nous avons déjà fait état d'une action parallèle en Ontario, qui a été rejetée.

Dans l'affaire *Sweet v. Canada* (en anglais seulement), la Cour fédérale a autorisé une action collective en matière de protection des renseignements personnels intentée contre le gouvernement du Canada par des contribuables dont les pages Mon dossier de l'ARC avaient été consultées lors d'attaques par un tiers. La Cour fédérale a estimé que les allégations d'insouciance des demandeurs dans cette affaire étaient suffisantes pour autoriser un recours pour intrusion dans la vie privée, et a conclu que l'application du délit aux défendeurs exploitant des bases de données n'était pas « vouée à l'échec » (*bound to fail*).

Responsabilité du fait d'autrui de l'employeur

Les actions collectives dans lesquelles les demandeurs allèguent qu'un employeur-défendeur est responsable de l'acte répréhensible d'un employé sont de plus en plus courantes. Ces affaires pourraient devenir encore plus importantes étant donné la jurisprudence ontarienne qui limite l'application du délit d'intrusion dans la vie privée.

Par exemple, dans l'affaire *Ari v. ICBC* (en anglais seulement), la Cour suprême de la Colombie-Britannique a accordé un jugement sommaire sur certaines questions juridiques autorisées dans le cadre d'une action collective en matière de protection des renseignements personnels remarquable sur le plan factuel. Le défendeur, l'Insurance Company of British Columbia (« ICBC »), administre le régime public d'assurance automobile de la Colombie-Britannique. ICBC avait employé un expert en sinistres qui, contre rémunération, recherchait et fournissait des renseignements sur les adresses associées aux plaques d'immatriculation fournies par une tierce partie. À l'insu de l'expert, la tierce partie agissait au nom d'une quatrième partie qui croyait, sous l'effet de la drogue, être la cible du Justice Institute of British Columbia et qui avait observé les numéros de plaques d'immatriculation dans le stationnement du Justice Institute. La quatrième partie a ensuite commis des incendies criminels et des fusillades à certaines des adresses. L'individu a été condamné à une importante peine de prison.

Ce fait intéressant a donné lieu à une action collective contre ICBC. Dans sa décision, la Cour suprême de la Colombie-Britannique a conclu que le demandeur avait établi que l'expert en sinistres avait enfreint la *Privacy Act*. La Cour a également conclu que, même si ICBC était innocente, elle était responsable du fait d'autrui pour l'inconduite de l'expert, car sa conduite s'inscrivait dans une zone de risque créée par la collecte de renseignements par ICBC. La Cour a également rejeté l'argument d'ICBC selon lequel les attaques de la quatrième partie étaient imprévisibles ou constituaient un *novus actus interveniens.*

L'exigence d'une « base factuelle » pour l'autorisation reste un obstacle important dans les actions collectives en matière de protection des renseignements personnels

Les tribunaux de tout le pays continuent de confirmer que les demandeurs dans les actions en matière de protection des renseignements personnels ne peuvent obtenir la certification sans preuve que le groupe visé par l'action collective a été réellement touché par la violation présumée de la vie privée. Voici deux exemples qui concernent des recours contre Facebook, Inc.

Dans la première affaire, *Simpson v. Facebook, Inc.* (en anglais seulement), le demandeur alléguait qu'un tiers nommé Cambridge Analytica avait obtenu des renseignements sur les utilisateurs de Facebook auprès d'un tiers développeur d'applications. La Cour supérieure de justice de l'Ontario a rejeté la demande d'autorisation du demandeur au motif qu'il n'y avait aucune preuve que des données d'utilisateurs canadiens avaient été partagées avec Cambridge Analytica. Par conséquent, rien ne justifiait une action collective.

En confirmant cette décision en appel, la Cour divisionnaire a souligné que les demandeurs avaient le fardeau de démontrer [TRADUCTION] « qu'une question commune existait au-delà de la simple affirmation dans les plaidoiries ». Osler a défendu Facebook dans cette action.

Dans l'affaire *Chow v. Facebook, Inc.* (en anglais seulement), la Cour suprême de la Colombie-Britannique a refusé d'autoriser une affaire dans laquelle les demandeurs alléguaient que Facebook avait utilisé à mauvais escient les données des journaux d'appels et de messages textes des utilisateurs de son application Messenger sur les téléphones Android. La Cour a conclu que les demandeurs n'avaient pas réussi à établir une base factuelle pour leurs allégations selon lesquelles Facebook [TRADUCTION] « a recueilli, utilisé, conservé et commercialisé des données d'appels et de messages textes et a profité de cette collecte aux dépens des utilisateurs ». En l'absence de base pour ces allégations, rien d'autre ne justifiait une action collective. Osler a également défendu Facebook dans cette action.

Abandon des recours pour violation de données

Nous avons précédemment signalé que, dans leurs demandes d'actions collectives, les demandeurs alléguaient de plus en plus souvent que les défendeurs avaient fait un mauvais usage des données ou que celles-ci ont été collectées de manière inappropriée, plutôt que d'affirmer qu'ils ont été victimes d'une violation de données. De nombreuses actions pour mauvais usage de données ont été intentées en 2022. Il s'agit notamment d'une série d'actions collectives dans lesquelles les demandeurs alléguaient que les gouvernements provinciaux avaient partagé des renseignements concernant de nouvelles mères avec des tiers inappropriés. Nous avons également assisté à un certain nombre de règlements importants en matière de mauvaise utilisation de données en 2022, notamment des règlements concernant la collecte et l'utilisation prétendument inappropriées de renseignements de géolocalisation. La décision dans l'affaire Owsianik renforcera probablement cette tendance.

Conclusion

Malgré la multiplication des actions collectives en matière de protection des renseignements personnels, les tribunaux de tout le pays continuent de préciser que la certification n'est pas une simple formalité et qu'elle ne découle pas automatiquement d'une violation ou d'un incident touchant des données. Les tribunaux s'attendent à ce que les demandeurs démontrent qu'ils ont été réellement touchés par l'incident. Bien qu'il demeure essentiel que les entreprises réagissent rapidement et efficacement lorsque des incidents touchant des données se produisent, les défendeurs disposent de toute une gamme d'outils pour se défendre contre des actions relatives à la protection des renseignements personnels ou pour les résoudre rapidement. Il peut s'avérer profitable de consulter un avocat sans tarder afin d'obtenir des conseils sur la meilleure façon de mettre en œuvre ces outils dans des circonstances où il existe un risque d'action collective ou lorsqu'un recours est exercé.