

DEMANDE D'ACTION COLLECTIVE CONTRE FACEBOOK POUR MOISSONNAGE DE DONNÉES : UNE COUR BRITANNO-COLOMBIENNE COUPE L'HERBE SOUS LE PIED AUX PLAIGNANTS

Publié le 22 février, 2022

Catégories: [Perspectives](#), [Publications](#)

Le 27 janvier dernier, la Cour suprême de la Colombie-Britannique a rejeté une demande d'autorisation d'exercer une action collective contre Facebook, Inc. (« **Facebook** »), qui aurait « moissonné » des données sur des appels et messages d'utilisateurs de l'application Messenger sans leur consentement et à leur insu^[1].

Pour la Cour, les plaignants n'ont pas présenté suffisamment de faits à l'appui de leur allégation. Elle aurait rejeté la demande même en présence d'un fondement factuel puisque, les plaignants n'ayant pas établi des questions de fait ou de droit communes à tous les membres du groupe, l'action collective n'était pas le meilleur moyen de résolution. Si la Cour n'a pas fermé la porte à un recours ultérieur similaire pour atteinte à la vie privée, sa décision démontre que la nature personnelle et individuelle de ces dossiers peut compliquer l'établissement de questions communes dans un contexte d'action collective. Le présent bulletin résume la décision et fait ressortir les points à retenir pour les entreprises.

Des arguments « pris sur Internet »

Au-delà de la question de l'atteinte à la vie privée, pour la Cour, la faille fatale du dossier présenté par les plaignants a été [traduction] « l'absence totale de preuve démontrant que Facebook a utilisé, ou utilisé de façon abusive, leurs renseignements à son profit »^[2].

Les plaignants accusent Facebook d'avoir moissonné des données sur des appels et des messages provenant de leurs téléphones Android^[3] (le moissonnage étant l'extraction automatique de renseignements à partir d'une source électronique lisible par l'utilisateur). Ils allèguent que Facebook a exploité une faille dans le système d'exploitation Android pour accéder à leurs données sans leur consentement. Ils estiment par ailleurs qu'une fois le correctif apporté, Facebook a camouflé le fait qu'elle demandait l'accès à ces données précises en montrant une fenêtre de consentement générique, en manipulant les paramètres par défaut et en présentant une interface truquée incitant les utilisateurs à lui donner accès à l'ensemble de leurs

renseignements. Le jugement ne donne pas plus de détails sur la façon dont Facebook aurait procédé selon les plaignants, se contentant d'indiquer qu'il s'agissait pour ces derniers de gestes délibérés et trompeurs posés par Facebook dans le but de causer un préjudice aux membres du groupe^[4].

La Cour a relevé des lacunes importantes dans la preuve des plaignants. Certains de leurs documents clés ont été trouvés sur le Web et produits en preuve par un déposant qui ne connaissait pas personnellement leur contenu.

La fiabilité d'une bonne partie de la preuve documentaire n'a pas pu être établie, et d'autres documents ont été présentés sans qu'aucun lien ne soit fait avec Facebook^[5]. Même s'ils avaient été admissibles, ces documents n'auraient pas suffi pour prouver les allégations des plaignants, puisqu'ils ne prouvaient en rien que Facebook avait recueilli des données sur leurs appels et messages.

Cette conclusion nous rappelle que, comme le cite la Cour, [traduction] « si la barre est basse au stade de l'autorisation, reste qu'il faut l'atteindre »^[6]. À cette étape, la Cour joue un rôle de gardienne pour bloquer les réclamations douteuses et sans fondement qui pourraient accaparer les maigres ressources judiciaires et nuire à l'accès à la justice.

Les critères de la CPA non satisfaits

Même si elle a conclu que les plaignants n'avaient pas établi de fondement probatoire pour leur principale prétention, la Cour a pris la peine d'évaluer les critères d'autorisation prévus dans la *Class Proceedings Act* (la « CPA »)^[7]. Elle s'est penchée sur les trois critères les plus importants en l'espèce : (1) la cause d'action doit être adéquatement formulée, (2) il doit y avoir de véritables questions communes et (3) l'action collective doit représenter le meilleur moyen de régler le dossier.

1. La seule cause d'action soulevée était fondée sur la *Privacy Act*

Atteinte à la vie privée aux termes de la Privacy Act

La réclamation pour atteinte à la vie privée présentée par les plaignants s'appuyait sur la *Privacy Act*^[8] de la Colombie-Britannique, qui crée un délit civil pour atteinte à la vie privée et utilisation non autorisée du nom ou de l'image d'une personne^[9]. D'autres délits pour cause d'infraction du genre existent dans d'autres provinces^[10], et un délit en common law pour atteinte à la vie privée a été reconnu en Ontario^[11].

Pour qu'une cause fondée sur l'article 1 de la *Privacy Act* soit accueillie, le plaignant doit démontrer que le défendeur a, sciemment et sans droit, porté atteinte à sa vie privée^[12]. Les plaignants ont présenté suffisamment de faits importants relativement à la collecte, à la conservation et à l'utilisation alléguées de leurs données obtenues par l'intermédiaire de l'application Messenger de Facebook à leur insu et sans leur

consentement, et leurs actes de procédure établissaient adéquatement les éléments essentiels d'une telle cause[13].

Autres réclamations

La Cour a conclu que les actes de procédure ne révélaient pas de cause d'action pour les autres allégations, soit une fondée sur le paragraphe 3(2) de la *Privacy Act*, une pour enrichissement injustifié et une pour délit d'atteinte par un moyen illégal. Autrement dit, dans chaque cas, les plaignants n'ont pas établi les faits essentiels de leur revendication.

Dans le cas du paragraphe 3(2), les plaignants n'ont pas indiqué que leur nom ou leur image avaient réellement été utilisés, ni que l'utilisation visait à promouvoir la vente ou le commerce de biens ou de services[14]. Pour ce qui est de l'enrichissement injustifié, les plaignants n'ont pas présenté de fait important à l'appui d'une prétendue privation[15]. Enfin, dans le cas de l'atteinte par un moyen illégal, la Cour a rejeté l'argument voulant que la vie privée comporte une valeur économique essentielle, puisqu'une action pour atteinte à la vie privée fondée sur la *Privacy Act* peut être intentée sans preuve de préjudice[16].

2. Absence de réelles questions communes

Il ne restait donc que la réclamation fondée sur l'article 1 de la *Privacy Act*, que la Cour devait évaluer au regard du critère des questions communes de la CPA[17]. L'existence de telles questions relève de l'essence même des actions collectives, qui permettent de ménager les ressources judiciaires en étudiant une question qui concerne nombre de personnes sans avoir à refaire la recherche des faits et l'analyse juridique, et d'améliorer l'accès à la justice en donnant l'occasion à un groupe de plaignants de participer à la résolution de leur affaire. Les plaignants ont proposé les questions communes suivantes[18] :

1. Facebook a-t-elle recueilli des données sur les appels et les messages des utilisateurs de son application Messenger pour téléphones intelligents Android au Canada et, si oui, quand?
2. Facebook a-t-elle demandé aux utilisateurs de son application Messenger pour téléphones intelligents au Canada de consentir à la collecte de données sur leurs appels et leurs messages et, si oui, le consentement était-il suffisant aux termes de l'alinéa 2(2)(a) de la *Privacy Act*?
3. Si la réponse à la première question est affirmative, et la réponse à la seconde négative, Facebook a-t-elle enfreint la *Privacy Act*?

Selon la Cour, les questions 1 et 2 pouvaient être considérées comme étant communes, mais pas la question 3. Elle a également conclu que les deux premières questions ne pouvaient pas être examinées indépendamment de la troisième[19].

La preuve d'une atteinte à la vie privée fondée sur l'article 1 de la *Privacy Act* doit tenir compte de ce qui est

raisonnable au vu des circonstances de chaque personne[20]. La Cour a mentionné des affaires similaires où ce point a été un frein à l'autorisation[21]. Cette conclusion suggère que la nature individuelle et contextuelle de la réclamation pour atteinte à la vie privée peut être un facteur faisant obstacle à la présentation d'actions collectives fondées sur l'article 1 de la *Privacy Act*.

3. L'action collective ne représentait pas le meilleur moyen de procéder

Même s'il y avait eu des questions communes valables, la Cour aurait jugé que l'action collective n'était pas la meilleure voie à emprunter pour régler le dossier.

Cela tient principalement au fait que, si une action peut être intentée en vertu de l'article 1 de la *Privacy Act* sans preuve de préjudice, les actions collectives sont longues et complexes. Il serait donc contraire aux principes de l'économie des ressources judiciaires et de l'accès à la justice d'investir d'importantes ressources dans une affaire où aucun dommage ni aucune perte n'a été prouvé[22]. Au mieux, les plaignants allèguent que leur vie privée est importante et qu'elle mérite d'être protégée, mais pas qu'elle a une valeur pécuniaire ni qu'ils ont subi un préjudice.

Points à retenir

La Cour suprême de la Colombie-Britannique a mis un obstacle de taille sur la route de ceux qui voudraient intenter une action collective pour une atteinte à la vie privée fondée sur la *Privacy Act*, puisque ces dossiers (i) concernent des préjudices souvent difficiles à quantifier et (ii) dépendent de facteurs contextuels individuels qui ne se réunissent pas aisément dans des questions communes.

À mesure que les données, comme les renseignements personnels, prendront de la valeur, les techniques de collecte, d'utilisation et de traitement deviendront plus sophistiquées et donneront lieu à de plus en plus de réclamations pour atteinte à la vie privée. Il ne s'agit pas de la première action collective intentée contre une entreprise de technologie ou de média social pour atteinte à la vie privée, et il ne s'agira certainement pas de la dernière. Qui plus est, le dépôt d'une action collective peut avoir un effet d'entraînement, en ce sens où les allégations d'utilisation malveillante de renseignements personnels peuvent mener à une enquête des organismes de réglementation canadiens et à l'imposition d'amendes[23]. Les entreprises qui commercialisent des données, surtout lorsqu'il s'agit de renseignements personnels, doivent s'assurer que leurs processus et utilisations proposées soient transparents et facilement accessibles pour tous les utilisateurs finaux, de façon à atténuer les risques d'atteintes à la vie privée.

Cette décision démontre qu'une cour n'hésitera pas à rejeter une action mal préparée qui ne présente pas assez d'éléments de preuve à l'appui des prétentions ni à conclure qu'une action n'a pas réussi à atteindre la barre de l'étape de l'autorisation, aussi basse soit-elle. Voilà une bonne nouvelle pour les entreprises qui

craignent d'avoir à se défendre dans des actions collectives sans fondement à une époque où des poursuites inspirées de causes antérieures tiennent à des spéculations plutôt qu'à des faits. La ruée vers les actions collectives pourrait s'essouffler si une approche plus rigoureuse remplace le processus d'autorisation quasi machinal actuel.

[1][ps2id id='1' target=''] *Chow v Facebook*, [2022 BCSC 137](#) [**Chow v Facebook**].

[2][ps2id id='2' target=''] *Chow v Facebook* [au par. 29](#).

[3][ps2id id='3' target=''] *Chow v Facebook* [au par. 14](#).

[4][ps2id id='4' target=''] *Chow v Facebook* [au par. 14](#).

[5][ps2id id='5' target=''] *Chow v Facebook* [aux par. 36-37](#).

[6][ps2id id='6' target=''] *Chow v Facebook* [au par. 43](#), citant le juge Belobaba dans la décision *Simpson v Facebook*, 2021 ONSC 968 au par. 50.

[7][ps2id id='7' target=''] *Class Proceedings Act*, [RSBC 1996, c 50](#) [CPA].

[8][ps2id id='8' target=''] *Privacy Act*, [RSBC 1996, c 373](#).

[9][ps2id id='9' target=''] *Privacy Act*, art 1 et 3.

[10][ps2id id='10' target=''] *The Privacy Act*, [RSS 1978, c P-24](#); *Loi sur la protection de la vie privée*, [CPLM, c P125](#); *Privacy Act*, [RSNL 1990, c P-22](#).

[11][ps2id id='11' target=''] *Jones c Tsige*, [2012 ONCA 32](#).

[12][ps2id id='12' target=''] *Privacy Act*, [RSBC 1996, c 373, art 1](#); *Chow v Facebook* [au para 49](#).

[13][ps2id id='13' target=''] *Chow v Facebook* [aux paras 51 et 54](#).

[14][ps2id id='14' target=''] *Chow v Facebook* [au para 57](#).

[15][ps2id id='15' target=''] *Chow v Facebook* [aux para 58-60](#).

[16][ps2id id='16' target=''] *Chow v Facebook* [aux paras 61-63](#).

[17][ps2id id='17' target=''] *Chow v Facebook* [au para 7](#), citant la CPA.

[18][ps2id id='18' target=''] *Chow v Facebook* [au para 83](#).

[19][ps2id id='19' target=''] *Chow v Facebook* [aux paras 84-86](#).

[20][ps2id id='20' target=''] *Chow v Facebook* [au para 87](#).

[21][ps2id id='21' target=''] *Chow v Facebook* [aux para 88-91](#).

[22][ps2id id='22' target=''] *Chow v Facebook* [aux para 97-102](#).

[23][ps2id id='23' target=''] La Colombie-Britannique a par exemple proposé une loi sur la protection de la vie privée qui donnerait au commissaire à l'information et à la protection de la vie privée de la province de larges pouvoirs d'infliction d'amendes. Voir notre [bulletin précédent](#) à ce sujet.

par [Joan Young](#), [Robert Piasentin](#), [Robbie Grant](#) et [Kristen Shaw](#) (stagiaire en droit)

Mise en garde

Le contenu du présent document ne fournit qu'un aperçu du sujet et ne saurait en aucun cas être interprété comme des conseils juridiques. Le lecteur ne doit pas se fonder uniquement sur ce document pour prendre une décision, mais devrait plutôt obtenir des conseils juridiques précis.

© McMillan S.E.N.C.R.L., s.r.l. 2022