PAS DE DOMMAGES-INTÉRÊTS POUR LE STRESS ET LES INCONVÉNIENTS PASSAGERS : UNE COUR DU QUÉBEC REJETTE UNE ACTION COLLECTIVE POUR ATTEINTE À LA PROTECTION DES DONNÉES

Publié le 14 juin, 2021

Catégories: Perspectives, Publications

En mars, la Cour supérieure du Québec a rendu une rare décision rejetant sur le fond une action collective en matière de protection de la vie privée. L'affaire *Lamoureux* c. *OCRCVM*[1] concerne une action collective à l'encontre de l'Organisme canadien de réglementation du commerce des valeurs mobilières (« **OCRCVM** ») pour des dommages découlant d'une atteinte à la protection des données. Dans sa décision, la Cour a établi un seuil minimal pour l'octroi de dommages-intérêts et elle a apporté des précisions quant aux pratiques exemplaires que devraient adopter les organisations en cas d'atteinte à la protection des données.

UN ORDINATEUR PORTABLE ÉGARÉ

L'atteinte à la protection des données s'est produite en février 2013, lorsqu'un inspecteur de l'OCRCVM a malencontreusement oublié un ordinateur portable de l'entreprise dans le compartiment à bagages d'un train (l'« **incident de l'ordinateur portable** »). L'ordinateur contenait les renseignements personnels de milliers d'investisseurs canadiens. Malgré tous ses efforts, l'OCRCVM n'a jamais réussi à retrouver l'ordinateur portable[2].

Après l'incident, une des personnes concernées, Paul Sofio, a intenté une action collective contre l'OCRCVM. Cette action collective a été rejetée en première instance, le juge ayant conclu que M. Sofio n'avait pas prouvé *prima facie* qu'il avait subi des dommages indemnisables comme l'exigeait l'article 1003 de l'ancien *Code de procédure civile* du Québec[3]. Ce jugement a été confirmé par la Cour d'appel du Québec[4].

Danny Lamoureux a déposé une action collective distincte, réclamant une indemnisation pour le stress, l'anxiété, l'inquiétude et la colère ressentis par les membres du groupe ainsi que les inconvénients, les pertes de temps et les dépenses occasionnés par les mesures de protection mises en place par l'OCRCVM. Certains membres revendiquent également une compensation pour l'usurpation de leur identité ou la commission d'une fraude ou la tentative de fraude dont ils ont été victimes et qu'ils croient liées à l'incident de l'ordinateur

portable.

ACTION COLLECTIVE REJETÉE

La Cour a rejeté l'action pour les motifs suivants :

i. Les membres n'ont pas réussi à prouver qu'ils avaient subi des dommages susceptibles d'être indemnisés.
ii. Il n'existe aucune preuve permettant d'établir un lien probant entre l'usurpation d'identité ou la fraude dont certains membres ont été victimes et l'incident de l'ordinateur portable.
iii. Le comportement du défendeur après l'atteinte à la protection des données satisfait aux standards attendus dans des circonstances semblables et, par conséquent, il n'a commis aucune faute intentionnelle justifiant de le condamner à des dommages-intérêts punitifs.

i. Les inconvénients normaux ne donnent pas lieu à une indemnisation

La Cour a jugé que même si les membres du groupe n'avaient pas à prouver l'existence réelle d'un vol d'identité pour obtenir des dommages-intérêts, ils devaient démontrer qu'ils avaient subi davantage que des inconvénients normaux[5]. La Cour a estimé que les membres du groupe n'avaient pas satisfait à ce critère minimal, soulignant l'absence de preuve documentaire ou médicale et concluant que les craintes, les angoisses et le stress des membres ainsi que les retards dans l'obtention d'un crédit sont des désagréments ordinaires que toute personne vivant en société doit régulièrement accepter[6].

Après la découverte de l'atteinte à la protection des données, le défendeur a entre autres offert aux personnes touchées, gratuitement, une surveillance de crédit et des mesures de protection par l'entremise d'Equifax et de TransUnion. La Cour a jugé que le stress et les inconvénients liés à l'instauration du service de surveillance étaient trop peu importants pour justifier une indemnisation[7].

ii. Le témoin expert réfute certaines allégations

L'OCRCVM a produit une imposante preuve d'experts non contredite démontrant que le vol d'identité allégué par certains membres du groupe ne pouvait être lié aux renseignements qui auraient été soi-disant volés de l'ordinateur perdu[8]. Cette preuve démontre que le vol d'identité et la fraude dont certains membres affirment avoir été victimes manquent de similitudes et dans certains cas, exigeaient des renseignements qui ne figuraient pas dans l'ordinateur portable[9]. La Cour en a conclu que les données mises en cause dans ces infractions criminelles n'avaient aucun lien avec l'incident de l'ordinateur portable[10].

iii. Pas de dommages punitifs sans preuve de faute

Au Québec, les dommages-intérêts punitifs constituent leur propre cause d'action et découlent des

agissements de la partie défenderesse[11]. Par conséquent, même si les membres du groupe n'ont pas réussi à démontrer qu'ils avaient subi un préjudice susceptible d'être indemnisé en lien avec l'incident de l'ordinateur portable, la Cour a examiné la possibilité d'adjuger des dommages-intérêts punitifs fondés uniquement sur les agissements de l'OCRCVM.

La Cour a refusé d'adjuger des dommages-intérêts punitifs, estimant que l'OCRCVM avait réagi conformément aux standards attendus de lui[12]. Cette décision offre donc un bon aperçu du type de mesures qu'une cour attend d'une organisation en cas d'atteinte à la protection des données. L'OCRCVM a notamment pris les mesures suivantes compte tenu de la menace à la sécurité :

- Lancement d'une enquête interne approfondie aussitôt qu'il a eu connaissance de l'atteinte.
- Recrutement d'une équipe d'enquête technique indépendante.
- Envoi d'un avis à toutes les parties concernées, y compris :
    - le Service de police de la Ville de Montréal;
    - la Commission d'accès à l'information du Québec et le Commissariat à la protection de la vie privée du Canada;
    - les maisons de courtage représentant des investisseurs touchés;
    - les personnes dont les renseignements personnels ont été compromis.
- Offre d'un service de surveillance de crédit pendant un an, gratuitement, aux personnes touchées, entre autres mesures de protection du crédit.
- Publication d'un communiqué expliquant l'incident.

La Cour a reconnu que l'organisme n'avait pas pris des mesures de prévention parfaites. L'OCRCVM a admis qu'il avait omis d'assurer la protection maximale des renseignements personnels de ses membres en ne chiffrant pas l'ordinateur perdu[13]. Néanmoins, en ce qui concerne la réaction à l'atteinte à la protection des données, la Cour a accepté l'opinion du témoin expert du défendeur voulant que l'OCRCVM eût respecté les pratiques exemplaires[14].

Le principal argument du demandeur au soutien de sa réclamation de dommages punitifs repose sur le délai qui s'est écoulé avant que l'OCRCVM publie l'avis. Effectivement, l'OCRCVM a avisé les personnes touchées de l'atteinte à la protection des données plus d'un mois après la découverte de la perte[15]. Pour expliquer ce retard, il a indiqué qu'il lui a fallu un certain temps pour déterminer avec précision quels étaient les renseignements personnels concernés ainsi que les maisons de courtage et les personnes touchées, et pour mettre en œuvre des mesures en vue d'assurer la protection en amont des renseignements et de répondre aux questions que soulèverait l'annonce de l'incident.

L'OCRCVM a fait valoir que s'il avait communiqué l'information trop hâtivement, il y aurait eu un risque que

l'ordinateur non identifié soit ciblé et tombe dans de mauvaises mains.

POINTS À RETENIR

Il y a deux points importants à retenir de cette décision sur lesquels nous aimerions insister.

Premièrement, la décision aide à établir un jalon pour les mesures adéquates à prendre en cas d'atteinte à la protection des données. Elle rappelle la décision *Lozanski* v. *Home Depot* rendue en 2016 en Ontario[16]. Dans cette affaire, le système de cartes de paiement de Home Depot avait été piraté par des intrus au moyen d'un maliciel conçu sur mesure, ce qui leur avait permis d'avoir accès aux renseignements de près de 500 000 clients. Même si la décision *Home Depot* visait à approuver un règlement à l'amiable, le juge a tenu à préciser qu'à son avis, Home Depot n'avait commis aucune faute. Selon la décision, [traduction] « Home Depot a réagi de façon responsable, rapide, généreuse et exemplaire aux actes criminels perpétrés à son encontre par les pirates informatiques » en offrant douze mois gratuits de services de protection de l'identité, de surveillance du crédit et de redressement du crédit[17]. Le juge a même écrit (en obiter) qu'il aurait approuvé le désistement de l'instance sans que les membres putatifs du groupe aient obtenu le moindre avantage[18].

La décision *Lamoureux* c. *OCRCVM* offre un sceau d'approbation encore plus inébranlable que celui de la décision *Home Depot* quant aux mesures mises en œuvre par l'OCRCVM. Cependant, ces mesures ne devraient pas être traitées comme une feuille de route exemplaire pour tous les types d'atteintes à la protection des données. La meilleure réaction en cas d'atteinte à la protection des données dépend du contexte. Par exemple, lorsqu'on peut immédiatement discerner le préjudice que risquent de subir les consommateurs et que les données sont déjà passées dans de mauvaises mains, une cour peut attendre d'une organisation qu'elle avise bien plus rapidement les consommateurs de l'atteinte potentielle.

Deuxièmement, la décision renforce le principe voulant que les inconvénients normaux ne soient pas indemnisables dans le cadre d'une action collective en protection de la vie privée. Cela pourrait changer dorénavant le résultat des décisions relatives à l'autorisation des actions collectives semblables aux affaires *Zuckerman* c. *Target* et *Lévy* c. *Nissan*, dans lesquelles les inconvénients et le temps passé à déployer des mesures de protection ont été considérés comme des préjudices indemnisables[19].

[1][ps2id id='1' target='/] *Lamoureux* c. *OCRCVM*, 2021 QCCS 1093 (« ***Lamoureux c. OCRCVM*** »); OCRCVM est l'acronyme de l'Organisme canadien de réglementation du commerce des valeurs mobilières.
[2][ps2id id='2' target='/] *Lamoureux* c. *OCRCVM*, paragr. 9.
[3][ps2id id='3' target='/] *Sofio* c. *Organisme canadien de réglementation du commerce des valeurs mobilières (OCRCVM)*, 2014 QCCS 4061.
[4][ps2id id='4' target='/]*Sofio* c. *Organisme canadien de réglementation du commerce des valeurs mobilières (OCRCVM)*, 2015 QCCA 1820.

[5][ps2id id='5' target='/] *Lamoureux* c. *OCRCVM*, paragr. 72.
[6][ps2id id='6' target='/] *Lamoureux* c. *OCRCVM*, paragr. 68-72.
[7][ps2id id='7' target='/] *Lamoureux* c. *OCRCVM*, paragr. 85.
[8][ps2id id='8' target='/] *Lamoureux* c. *OCRCVM*, paragr. 102.
[9][ps2id id='9' target='/] *Lamoureux* c. *OCRCVM*, paragr. 105-107, 113-115.
[10][ps2id id='10' target='/]*Lamoureux* c. *OCRCVM*, paragr. 118.
[11][ps2id id='11' target='/] *Lamoureux* c. *OCRCVM*, paragr. 120, citant *de Montigny* c. *Brossard (Succession)*, 2010 CSC 51, paragr. 47.
[12][ps2id id='12' target='/] *Lamoureux* c. *OCRCVM*, paragr. 134.
[13][ps2id id='13' target='/]La Cour a fait remarquer que l'ordinateur portable était protégé par un mot de passe, mais que les données qu'il contenait n'étaient pas chiffrées, même s'il s'agissait de données de nature très délicate. *Lamoureux* c. *OCRCVM*, paragr. 10. Le Commissariat à la protection de la vie privée recommande régulièrement que les renseignements personnels de nature délicate soient protégés par chiffrement : voir les rapports d'enquête du CPVP sur Vtech Holdings Limited, Equifax Inc., TJX/Winners, WhatsApp, CIBC, Adobe et la base de données de l'Agence mondiale antidopage.
[14][ps2id id='14' target='/]*Lamoureux* c. *OCRCVM*, paragr. 130.
[15][ps2id id='15' target='/] *Lamoureux* c. *OCRCVM*, paragr. 9-18. L'incident de l'ordinateur portable s'est produit le 22 février 2013. Après l'enquête interne, l'OCRCVM a déterminé le 4 mars 2013 que l'ordinateur portable contenait probablement des renseignements concernant des milliers de personnes et d'entités juridiques. Malgré ce fait, les maisons de courtage concernées ont été informées de la situation seulement lors de réunions en personne les 8 et 9 avril 2013 et par le communiqué de presse publié le 11 avril 2013.
[16][ps2id id='16' target='/] *Lozanski* v. *The Home Depot, Inc.* 2016 ONSC 5447 (« ***Home Depot*** »).
[17][ps2id id='17' target='/] *Home Depot*, paragr. 10.
[18][ps2id id='18' target='/] *Home Depot*, paragr. 74.
[19][ps2id id='19' target='/]*Zuckerman* c. *Target Corporation*, 2017 QCCS 110, paragr. 73; *Lévy* c. *Nissan Canada inc.*, 2019 QCCS 3957, paragr. 104-108 (« ***Lévy*** »).

par Mitch Koczerginski et Robbie Grant

Mise en garde


mcmillan