Cour fédérale Federal Court

Date : 20240606

Dossier : T-226-13

Référence : 2024 CF 851

[TRADUCTION FRANÇAISE]

Ottawa (Ontario), le 6 juin 2024

En présence de madame la juge en chef adjointe Gagné

RECOURS COLLECTIF ENVISAGÉ

ENTRE :

JOHN MARK JACQUES,
GORDON ALBERT MEHEW ET CRAIG ROBAR

demandeurs

et

SA MAJESTÉ LE ROI

défendeur

ORDONNANCE ET MOTIFS

I. Aperçu

[1] La Cour est saisie d'une requête en autorisation d'un recours collectif envisagé. Les demandeurs font valoir qu'un employé (ou des employés) du ministère des Ressources humaines et du Développement des compétences du Canada (RHDCC), maintenant Emploi et Développement social Canada (Emploi Canada), a fait preuve de négligence et a commis un abus de confiance à l'endroit de personnes ayant présenté une demande de prestations d'invalidité au titre du Régime de pensions du Canada en perdant une clé USB contenant leurs renseignements personnels.

[2] Les faits qui ont donné naissance à la présente réclamation sont survenus en novembre 2012 et la déclaration a été déposée en janvier 2013, quelques semaines après le dépôt de réclamations semblables dans les dossiers T-132-13 (le dossier *Condon*) et T-166-13.

[3] Les avocats représentant les parties dans les trois dossiers connexes ont convenu de regrouper les dossiers T-132-13 et T-166-13 et d'utiliser le dossier *Condon* comme dossier principal, tout en laissant le présent dossier en suspens jusqu'à ce qu'une décision définitive soit rendue dans le dossier *Condon*.

[4] Le dossier *Condon* a été autorisé et un jugement de notre Cour a approuvé le règlement, qui a pris effet le 17 juillet 2018.

[5] En plus de faire valoir que le critère relatif à l'autorisation n'est pas satisfait dans ce dossier, le défendeur affirme maintenant que les réclamations de la plupart des membres du groupe sont prescrites en raison de l'expiration des délais de prescription prévus par la loi.

II. Faits

A. *La perte de la clé USB*

[6] En novembre 2012, un employé anonyme d'Emploi Canada a fourni à un avocat du ministère de la Justice une clé USB non chiffrée contenant les renseignements personnels de 5 045 particuliers ayant interjeté appel du refus de leurs demandes de prestations d'invalidité.

[7] Le lendemain, la clé USB était perdue. Des recherches ont été effectuées chez l'employé, dans son bureau et dans le taxi qu'il a pris ce jour-là pour se rendre chez lui, mais personne n'a réussi à trouver la clé USB, qui est toujours manquante.

[8] En décembre 2012, les demandeurs, et vraisemblablement tous les membres du groupe, ont reçu une lettre d'Emploi Canada les informant qu'une clé USB contenant leurs renseignements personnels avait été égarée. Voici un extrait de la lettre :

> [TRADUCTION]
>
> […] J'ai le regret de vous informer qu'un employé a égaré un support de données électroniques, aussi appelé une clé USB, qui contenait certains de vos renseignements personnels. Ce support contenait les types de renseignements suivants : numéro d'assurance sociale (NAS); nom; problème de santé principal, et s'il y a lieu, secondaire; date de naissance; présence d'autres payeurs (p. ex. indemnisation des victimes d'accidents de travail); niveau de scolarité; type d'emploi; centre de traitement de Service Canada.

[9] Les membres du groupe sont définis en ces termes :

> [TRADUCTION]
>
> Toutes les personnes dont les renseignements personnels étaient conservés sur un support de données électroniques, aussi appelé une clé USB, sous le contrôle de Ressources humaines et Développement des compétences Canada ou du ministère de la Justice, renseignements qui ont été perdus ou divulgués à autrui en novembre 2012 ou vers novembre 2012.

[10] Le défendeur a depuis confirmé que la clé USB contenait les renseignements suivants :

> Nom de famille; date de naissance; numéro d'assurance sociale (NAS); niveau de scolarité et type d'emploi; centre de traitement de Service Canada; codes d'affection génériques provenant de la Classification internationale des maladies; confirmation des autres payeurs, comme les programmes d'indemnisation des victimes d'accidents de travail.

[11] En décembre 2012, Emploi Canada a informé le Commissariat à la protection de la vie privée du Canada (le Commissariat à la protection de la vie privée) de l'incident. Emploi Canada a annoncé publiquement la perte de ces données dans un communiqué de presse publié le 11 janvier 2013, dont voici un extrait :

> À la fin de 2012, RHDCC a informé le Commissariat à la protection de la vie privée qu'une clé USB avait été égarée. Cette dernière contenait des renseignements personnels au sujet de plus de 5 000 Canadiens.

[12] Plus tard le même mois, les membres du groupe proposé ont reçu une seconde lettre de la part d'Emploi Canada, dans laquelle on leur offrait de placer une annotation dans leur dossier de crédit (un avertissement relatif au crédit) afin d'avertir les créanciers de confirmer l'identité de ces particuliers avant de leur accorder du crédit. En octobre 2014, le Commissariat à la

protection de la vie privée a publié une annonce concernant les conclusions de son enquête, intitulée « La perte de la clé USB d'Emploi et Développement social Canada confirme les leçons tirées ».

[13] Le Commissariat à la protection de la vie privée s'est exprimé en ces termes :

> Le même mois, une clé USB contenant les renseignements personnels de 5 045 particuliers ayant interjeté appel de décisions relatives à des prestations d'invalidité du Régime de pensions du Canada a disparu du bureau de travail d'un employé dans un local d'EDSC. Comme le disque dur, la clé USB n'était ni protégée par un mot de passe ni chiffrée, et elle n'a jamais été retrouvée. Les renseignements personnels suivants étaient notamment stockés sur la clé USB disparue, pour chaque personne : NAS, date de naissance, nom, état de santé, niveau de scolarité, type d'emploi; l'information indiquait également si d'autres paiements étaient versés, par exemple des indemnités d'accident du travail. Si des renseignements de ce type tombent entre de mauvaises mains, cela peut donner lieu au vol d'identité ou à la fraude.

[14] Le Commissariat à la protection de la vie privée a conclu que le ministère de la Justice, dont un avocat avait la garde de la clé USB lorsqu'elle a été perdue, « n'a pas réussi à transposer ses propres politiques en matière de protection de la vie privée et de sécurité en pratiques opérationnelles judicieuses ». Autrement dit, l'employé, soit un avocat qui avait la garde de la clé USB, n'a pas respecté les politiques de sécurité et de protection des renseignements personnels établies ou en a fait abstraction.

[15] Les faits de l'espèce sont similaires à ceux du dossier *Condon*, dans lequel un disque dur portable contenant des demandes de prêt étudiant a été perdu.

[16] Le dossier *Condon* a été mis au jour en même temps que la perte de la clé USB en l'espèce. Selon un Rapport spécial au Parlement du 25 mars 2014 préparé par le Commissariat à la protection de la vie privée :

> […] le 5 novembre 2012, un employé de l'unité du PCPE a voulu prendre un disque dur externe dans un classeur et a constaté qu'il ne s'y trouvait pas. […] Selon les observations d'EDSC, le disque dur était conservé dans un classeur pouvant être verrouillé et qui se trouvait dans le cubicule de cet employé. Le disque dur était dans une enveloppe dissimulée sous d'autres dossiers. […] Il n'était pas protégé par un mot de passe et l'information qu'il contenait n'était pas chiffrée. Le numéro de série du disque dur demeure inconnu. […] Après un examen approfondi des fichiers et dossiers conservés sur le réseau du Ministère et visés par le projet de migration, EDSC a informé le Commissariat que la perte du disque dur externe avait mis en péril la confidentialité des renseignements contenus dans les fichiers de données suivants, chacun d'eux étant décrit plus en détail ci-dessous :
>
> > • fichiers se rapportant aux sondages sur la satisfaction de la clientèle; • fichiers renfermant des rapports d'enquête; • fichiers contenant des données financières, le plan d'activités et des renseignements sur les ressources humaines du PCPE; • fichiers renfermant de l'information sur la planification de la continuité des opérations.
>
> Malgré ce qui précède, comme le disque dur a disparu, EDSC affirme qu'il est impossible de savoir avec certitude quels renseignements avaient effectivement été sauvegardés sur ce disque.

[17] Tout comme dans son rapport sur la perte de la clé USB, le Commissariat à la protection de la vie privée a conclu, relativement au dossier *Condon*, qu'Emploi Canada n'avait pas réussi à transposer ses propres politiques en matière de protection de la vie privée et de sécurité en pratiques opérationnelles judicieuses.

[18] Dans la foulée du dossier *Condon*, le Commissariat à la protection de la vie privée a formulé plusieurs recommandations, qu'Emploi Canada a acceptées, y compris, non exclusivement, les suivantes :

> • Nous avons recommandé qu'EDSC revoie ses pratiques de contrôle de la sécurité physique de sorte que son programme de sécurité comporte des activités de surveillance et des inspections régulières. Cette mesure contribuera à faire en sorte que les renseignements personnels soient conservés dans des classeurs approuvés lorsque les employés ne sont pas à leur bureau pendant un certain temps; que les classeurs soient verrouillés en conséquence; que les clés des classeurs soient protégées comme il se doit; et que les biens attrayants ou précieux (p. ex. disques durs externes, ordinateurs portatifs, etc.) contenant des renseignements personnels soient protégés adéquatement.
>
> • Nous avons recommandé que les appareils portatifs de stockage ne servent qu'en dernier recours pour la conservation ou le transfert de renseignements personnels et uniquement si cela est manifestement nécessaire pour atteindre une fin précise et documentée. Tous les renseignements délicats ou personnels stockés sur un appareil portatif doivent être protégés par des mesures technologiques robustes, dont le chiffrement.
>
> • Nous avons recommandé que le programme de formation et de sensibilisation d'EDSC privilégie […] Des stratégies pour faire en sorte que tous les employés comprennent leurs rôles et leurs responsabilités dans la gestion des renseignements personnels […] Les exigences relatives à la sécurité physique énoncées dans le Manuel des politiques et méthodes de sécurité d'EDSC […] Les exigences relatives à la protection des renseignements personnels […] [et] Les conséquences du non-respect des normes de sécurité et de protection de la vie privée du Ministère.

[19] Les demandeurs sont des représentants membres du groupe qui ont été avisés par Emploi Canada que leurs renseignements personnels étaient stockés sur la clé USB qui a été perdue.

B. *L'enquête*

[20] Le défendeur a fourni des éléments de preuve indiquant que les deux ministères responsables des employés avaient mené des enquêtes administratives officielles sur des allégations de traitement inadéquat des renseignements. L'auteur de l'affidavit du défendeur a affirmé que les enquêtes internes avaient mené à la conclusion que les employés d'Emploi Canada et du ministère de la Justice n'avaient pas traité les renseignements classifiés conformément à la politique ministérielle, mais que rien n'indiquait que la clé USB avait été volée, consultée à des fins frauduleuses ou emportée à l'extérieur du bureau.

III. Critère d'autorisation

[21] Le paragraphe 334.16(1) des *Règles des Cours fédérales*, DORS/98-106 (les Règles), énonce les conditions qui doivent être réunies pour qu'une instance soit autorisée comme recours collectif. Il prévoit qu'un recours collectif doit être autorisé si : a) les actes de procédure révèlent une cause d'action valable; b) il existe un groupe identifiable formé d'au moins deux personnes; c) les réclamations soulèvent des points de droit ou de fait communs; d) le recours collectif est le meilleur moyen de régler, de façon juste et efficace, les points de droit ou de fait communs; e) il existe un représentant demandeur approprié.

[22] Toutes les conditions sauf la dernière sont en cause dans la présente requête.

[23] Le critère prévu à l'alinéa a), à savoir si les actes de procédure révèlent une cause d'action valable, est le même qu'en regard d'une requête en radiation – « s'il est clair et évident

que les actes de procédure ne révèlent aucune cause d'action valable » (*Sweet c Canada*, 2022 CF 1228 au para 75). Cette analyse ne doit pas être effectuée en fonction de la preuve, mais doit plutôt être fondée sur la présomption selon laquelle les faits allégués sont véridiques.

[24] Afin d'atteindre le seuil pour satisfaire aux exigences relatives à l'autorisation (alinéas b) à e)), les demandeurs doivent présenter des éléments de preuve montrant un « certain fondement factuel » pour étayer l'ordonnance d'autorisation. La norme applicable à cet égard n'exige pas que la partie qui cherche à obtenir l'autorisation établisse, selon la prépondérance des probabilités, que les conditions relatives à l'autorisation sont respectées. Elle n'exige pas que la Cour se prononce sur les éléments de fait et les éléments de preuve contradictoires. Elle reflète plutôt le fait que, à l'étape de l'autorisation, la Cour n'est pas en mesure de statuer sur les éléments contradictoires de la preuve ni de déterminer sa valeur probante à l'issue d'une analyse nuancée (*Pro-Sys Consultants Ltd c Microsoft Corporation*, 2013 CSC 57 aux para 101-102). Cependant, la norme de preuve appliquée à cette étape ne donne pas lieu à un examen du caractère suffisant de la preuve qui soit superficiel au point d'être strictement symbolique (*Pro-Sys*, au para 103).

[25] Le critère relatif à l'autorisation est conjonctif. Si un demandeur ne satisfait pas à l'une des cinq conditions, l'autorisation doit être refusée.

[26] Récemment, dans l'arrêt *Jensen c Samsung Electronics Co Ltd*, 2023 CAF 89 [*Jensen CAF*], la Cour d'appel fédérale a souligné que l'étape de l'autorisation n'en reste pas moins un important mécanisme de contrôle qui doit fonctionner comme un mécanisme de

filtrage efficace et qui ne doit pas être considéré comme une simple formalité. La Cour d'appel fédérale a retenu l'approche énoncée par le juge Denis Gascon de notre Cour (*Jensen c Samsung Electronics Co Ltd*, 2021 CF 1185) [*Jensen CF*] :

> [292] Je ne remets pas en question le fait que les recours collectifs constituent un moyen procédural spécifique pour les parties et qu'une requête en autorisation n'est pas l'instrument approprié pour se concentrer sur le fond et le bien-fondé d'un recours collectif envisagé. Cependant, l'étape de l'autorisation n'en reste pas moins un important mécanisme de contrôle qui doit fonctionner comme un « mécanisme de filtrage efficace » et qui ne doit pas être considéré comme une « simple formalité » (*Desjardins* au para 74; *Oratoire* au para 62; *Pro-Sys* au para 103). Contrairement à ce que les demandeurs semblaient laisser entendre, le fait pour un tribunal de procéder à un examen rigoureux […] [d]es faits substantiels […] dans le cadre d'une requête en autorisation ne signifie pas que l'examen se métamorphose en un examen du fond de l'affaire. Comme la [Cour suprême du Canada] l'a souvent affirmé, ceci s'inscrit plutôt dans le rôle et l'obligation qu'ont les tribunaux de faire plus qu'approuver sans discussion et de procéder à un examen symbolique des recours collectifs envisagés à l'étape de l'autorisation, et de s'assurer que les conditions d'autorisation sont effectivement respectées.

IV. Questions en litige

[27] La présente requête en autorisation soulève les questions suivantes :

A. *Les actes de procédure révèlent-ils une cause d'action valable?*

B. *Existe-t-il un groupe identifiable formé d'au moins deux personnes ou les réclamations de la plupart des membres du groupe sont-elles prescrites en raison de l'expiration des délais de prescription prévus par la loi?*

C. *La réclamation soulève-t-elle des points de droit ou de fait communs?*

D. *Le recours collectif est-il le meilleur moyen de régler, de façon juste et efficace, les points communs?*

V. Analyse

A. *Les actes de procédure révèlent-ils une cause d'action valable?*

[28] La première condition à remplir pour obtenir l'autorisation est celle prévue à l'alinéa 334.16(1)a) des Règles, à savoir que les actes de procédure doivent révéler une cause d'action valable. Le critère appliqué à cette condition est le même que dans le cas d'une requête en radiation, c'est-à-dire qu'il faut déterminer s'il est clair et évident que les actes de procédure ne révèlent aucune cause d'action valable. Cette analyse ne doit pas être effectuée en fonction de la preuve présentée par les parties, mais doit plutôt être fondée sur la présomption selon laquelle les faits allégués sont véridiques (*Condon c Canada*, 2015 CAF 159 aux para 11-13 [*Condon CAF*]).

[29] Le défendeur ne conteste pas le fait que les actes de procédure révèlent une cause d'action valable visant une négligence (bien qu'il fasse valoir qu'il n'y ait aucun fondement factuel à l'appui du préjudice ou des dommages subis par les demandeurs ou les membres du groupe; j'y reviens plus loin). Cependant, le défendeur conteste fortement que les actes de procédure révèlent une cause d'action visant une violation de la confidentialité.

[30] L'abus de confiance est un délit intentionnel dans le cadre duquel : a) le demandeur doit avoir communiqué des renseignements confidentiels; b) à titre confidentiel; c) le défendeur doit avoir fait un usage abusif des renseignements; d) intentionnellement; e) au détriment du

demandeur (*Lac Minerals Ltd c International Corona Resources Ltd*, 1989 CanLII 34 (CSC) à la p 576).

[31] Les parties s'entendent sur la définition du délit. Elles ne s'entendent cependant pas sur ce qui constitue l'« intention ». Les demandeurs font valoir que c'est l'usage abusif des renseignements qui doit être intentionnel, tandis que le défendeur fait valoir que la personne qui a reçu les renseignements confidentiels doit avoir utilisé ces renseignements dans l'intention de causer un préjudice à la personne qui les a communiqués.

[32] Les demandeurs affirment que les renseignements (particulièrement les numéros d'assurance sociale et les renseignements médicaux) étaient confidentiels et avaient été communiqués à titre confidentiel. Ils font valoir que le stockage des renseignements sur une clé USB non chiffrée et le retrait de celle-ci du bureau (au lieu de la conserver dans un coffre de sécurité approuvé, comme une armoire fermée à clé) constituaient un usage abusif intentionnel, car les employés savaient qu'ils contrevenaient au manuel du Ministère, ainsi qu'aux politiques et aux pratiques ministérielles relatives aux renseignements Protégé B. Les demandeurs estiment que l'allégation d'abus de confiance est plaidée en détail et que les faits substantiels sont énoncés. Ils s'appuient sur l'arrêt récent de la Cour suprême de la Colombie-Britannique *Lam v Flo Health*, 2024 BCSC 391, et sur le fait que la demande fondée sur la même allégation a été autorisée dans le dossier *Condon.* Par conséquent, il n'est pas évident et manifeste que cette demande ne pourrait pas être accueillie.

[33] Dans la décision *Sweet*, le juge Richard Southcott a dû trancher un débat similaire entre les parties. Les demandeurs ont vu leurs comptes en ligne du gouvernement piratés en raison de manquements opérationnels allégués de la défenderesse à sécuriser adéquatement les portails donnant accès à ces comptes. Entre autres, les demandeurs ont avancé une cause d'action fondée sur le délit d'abus de confiance. Comme en l'espèce, la défenderesse a fait valoir que son défaut d'avoir empêché les cyberattaques ne constitue pas un usage abusif au sens du délit d'abus de confiance.

[34] Bien que le juge Southcott ait reconnu que la position de la défenderesse était étayée par la jurisprudence, il a conclu qu'il n'était pas évident et manifeste que la cause d'action des demandeurs fondée sur l'abus de confiance était vouée à l'échec, essentiellement parce qu'une cause d'action similaire avait été autorisée dans le dossier *Condon* et le dossier T-1931-13 (le dossier *Untel*) :

> [121] Dans l'affaire de piratage *Del Giudice* décrite précédemment dans les présents motifs, la Cour supérieure de justice de l'Ontario n'a trouvé aucun fondement à une demande fondée sur l'abus de confiance, sur la base des faits substantiels invoqués, tant parce que la plupart des renseignements n'étaient pas confidentiels que parce que, de l'avis de la Cour, les défendeurs n'ont pas fait une utilisation non autorisée des renseignements qui constituerait une utilisation abusive (au para 197). De même, dans la décision *Kaplan v. Casino Rama Services Inc.*, 2019 ONSC 2025 [*Kaplan*], la Cour supérieure de justice de l'Ontario a conclu que, à moins que le mot « utilisation abusive » ne soit dénaturé de toute forme et de toute signification, le défaut des défendeurs d'empêcher la cyberattaque en cause dans cette affaire ne constituait pas une utilisation abusive de renseignements confidentiels au sens du délit d'abus de confiance (au para 31).
>
> [122] En réponse à cet argument, le demandeur s'appuie sur les arrêts *Condon CAF* et *Untel CAF*, qui ont tous deux permis l'autorisation de demandes fondées sur l'abus de confiance dans des circonstances où le gouvernement n'avait pas protégé adéquatement les renseignements confidentiels. Dans l'arrêt *Tucci*

BCCA, sur lequel je me suis déjà appuyé dans les présents motifs, la Cour d'appel de la Colombie-Britannique a examiné l'arrêt *Condon CAF*, ainsi que la décision de la Cour fédérale dans l'affaire *Untel*, comme précédents relevés par les demandeurs et dans lesquels les demandes fondées sur l'abus de confiance avaient été autorisées dans des circonstances similaires à l'atteinte à la protection des données en ligne qu'ils envisageaient. La Cour d'appel a souligné qu'aucun de ces précédents des Cours fédérales ne traitait spécifiquement de la question de savoir si le délit d'abus de confiance exigeait une utilisation abusive intentionnelle de renseignements confidentiels (au para 112). Bien que l'autorisation des procédures dans ces deux affaires semble incompatible avec l'opinion selon laquelle l'utilisation abusive doit être intentionnelle, la Cour d'appel de la Colombie-Britannique a néanmoins conclu que l'abus de confiance est un délit intentionnel (aux para 112 à 113).

[123] Par conséquent, l'arrêt *Tucci BCCA* représente un autre précédent qui étaye la position de la défenderesse selon laquelle l'abus de confiance ne s'applique pas aux circonstances de l'espèce. Néanmoins, je suis conscient du principe adopté par le juge Martineau dans la décision *Arsenault c. Canada*, 2008 CF 299 [*Arsenault*], au paragraphe 27, selon lequel, pour satisfaire au critère d'une requête en radiation [qui est le même critère que celui qui s'applique en vertu de l'alinéa 334.16(1)a)], il doit y avoir un dossier portant exactement sur la même question, issu de la même juridiction, et démontrant que cette même question a été clairement examinée et rejetée.

[124] Conformément à l'observation formulée dans l'arrêt *Tucci BCCA*, ni l'arrêt *Condon CAF* ni l'arrêt *Untel CAF* n'ont traité expressément de la question dont la Cour est actuellement saisie, c'est-à-dire de la question de savoir si l'exigence relative à l'utilisation abusive dans le cadre du délit d'abus de confiance peut être satisfaite en l'absence d'intention de la part de l'auteur allégué du délit. En effet, comme le prétend la défenderesse, l'espèce se distingue quelque peu des affaires *Condon CAF* et *Untel CAF*, car aucune de ces affaires ne mettait en cause un tiers. Toutefois, je comprends que le demandeur ait invoqué ces précédents, car tous deux concernaient le défaut du gouvernement, d'une manière ou d'une autre, de protéger adéquatement les renseignements confidentiels. Compte tenu de ce degré de similitude, du fait que l'autorisation a été accordée dans les deux cas, et du fait qu'il s'agit de décisions de la Cour d'appel fédérale, et compte tenu du principe de la décision *Arsenault*, je ne suis pas en mesure de conclure que la cause d'action du demandeur fondée sur l'abus de confiance est vouée à l'échec.

[35] Outre le fait que dans les arrêts *Condon CAF* et *Canada c M Untel*, 2016 CAF 191 [*Untel CAF*], la question dont la Cour était saisie n'était pas aussi bien formulée par les parties, dans la décision *Sweet*, et en l'espèce, il y a maintenant un « dossier portant exactement sur la même question, issu de la même juridiction, et démontrant que cette même question a été clairement examinée et rejetée » (*Sweet*, au para 123).

[36] Après que la Cour a finalement autorisé le dossier *Untel* dans *M Untel c Canada*, 2022 CF 587, la Cour a été saisie d'une requête en jugement sommaire déposée par les demandeurs, qui ont déclaré que toutes les questions communes devraient être tranchées en leur faveur et qu'il n'existait pas de véritable question litigieuse. La juge Catherine Kane a accueilli la requête en partie, mais a rejeté la réclamation fondée sur le délit d'abus de confiance (*M Untel c Canada*, 2023 CF 1636) [*jugement sommaire Untel*].

[37] Dans cette affaire, les allégations des demandeurs découlaient d'un envoi postal de masse dans le cadre duquel Santé Canada avait transmis plus de 41 000 lettres à des participants du Programme d'accès à la marihuana à des fins médicales en novembre 2013. Les lettres avaient été acheminées dans des enveloppes à fenêtre transparente qui exposaient le nom du programme, à savoir le « Programme d'accès à la marihuana à des fins médicales », dans l'adresse de l'expéditeur, ainsi que le nom complet et l'adresse du destinataire. Les demandeurs ont fait valoir que cet envoi postal de masse avait [TRADUCTION] « exposé » leur participation au programme, avait divulgué leurs renseignements personnels et avait porté atteinte à leur droit à la vie privée.

[38] Les points communs relativement à l'abus de confiance étaient les suivants :

- Les membres du groupe ont-ils communiqué les renseignements personnels à Santé Canada?
- Dans l'affirmative, Santé Canada a-t-il fait un mauvais usage des renseignements personnels lorsqu'il a recueilli, utilisé, conservé et divulgué les renseignements personnels?
- Dans l'affirmative, ce mauvais usage des renseignements personnels a-t-il été préjudiciable aux membres du groupe?
- Dans l'affirmative, Santé Canada a-t-il abusé de la confiance des membres du groupe lorsqu'il a recueilli, utilisé, conservé et divulgué les renseignements personnels?

[39] La juge Kane a répondu par l'affirmative aux deux premières questions et par la négative aux troisième et quatrième questions.

[40] Les demandeurs ont fait valoir que la common law devrait continuer d'évoluer pour reconnaître le délit d'abus de confiance sans qu'il soit nécessaire de prouver l'existence d'un préjudice, et pour reconnaître que l'abus de confiance devrait en soi donner ouverture à une action.

[41] La juge Kane a rejeté cet argument et a conclu que l'application du critère de la façon dont le proposent les demandeurs « créerait, dans le cadre des allégations relatives à la protection de la vie privée, un nouveau délit assorti d'un critère moins rigoureux que le délit d'intrusion dans l'intimité et que les délits d'origine législative qui existent dans certaines provinces » (*jugement sommaire Untel*, au para 148).

[42] Après avoir conclu que les membres du groupe avaient communiqué des renseignements personnels à Santé Canada, qui en avait fait un usage abusif, la juge Kane a affirmé que l'usage abusif en soit n'établissait pas l'existence du délit. Selon le critère établi dans l'arrêt *Lac Minerals* et la jurisprudence subséquente appliquant le critère, d'une part, l'usage abusif doit avoir été préjudiciable à la personne qui a communiqué les renseignements, et d'autre part, l'usage abusif, et l'abus de confiance subséquent, doivent être intentionnels (voir par exemple *Tucci v Peoples Trust Company*, 2020 BCCA 246, et *Lysko v Braley et al*, 2006 CanLII 11846 (ON CA)).

[43] Même si l'usage abusif des renseignements des membres du groupe n'était pas accidentel – Santé Canada avait approuvé les enveloppes à fenêtre transparente –, la juge Kane a conclu que l'usage abusif n'était pas intentionnel. Selon la preuve dont elle disposait, Santé Canada n'avait pas l'intention de faire un usage abusif des renseignements confidentiels et n'avait pas l'intention de trahir la confiance des membres du groupe ni de leur causer un quelconque préjudice.

[44] Les demandeurs font valoir que l'arrêt *Lam*, rendu par la Cour suprême de la Colombie-Britannique quelques mois après la décision de notre Cour dans le *jugement sommaire Untel*, contredit manifestement cette conclusion. Les demandeurs affirment que s'il existe une jurisprudence contradictoire, il n'est pas évident et manifeste que la demande est vouée à l'échec.

[45] L'arrêt *Lam* portait sur une demande d'autorisation d'un recours collectif en vertu de la *Class Proceedings Act*, RSBC 1996, c 50, de la Colombie-Britannique. La demanderesse a fait valoir que la défenderesse avait intentionnellement violé la vie privée des personnes qui

utilisaient l'application Flo Health & Period Tracker pour suivre leur cycle de reproduction. La représentante du groupe proposé a affirmé qu'elle avait, comme d'autres utilisateurs, utilisé l'application et saisi des renseignements médicaux personnels de nature très délicate concernant son système de reproduction en se fondant sur l'assurance que lui avait donnée la défenderesse, à savoir que la confidentialité de ces renseignements serait préservée. En fait, la défenderesse avait vendu les renseignements personnels des utilisateurs de l'application à des tiers, comme Facebook, à des fins de publicité.

[46] Après avoir énoncé le critère établi par la Cour suprême du Canada dans l'arrêt *Lac Minerals*, la juge Blake a affirmé que le délit d'abus de confiance [TRADUCTION] « est bien défini comme un délit intentionnel » (*Lam*, au para 71). Quant à la question fondamentale de savoir si les renseignements confidentiels avaient été utilisés d'une manière abusive, elle a conclu que cet élément du délit était présent, car Flo avait fait un mauvais usage [TRADUCTION] « des renseignements en ne respectant pas ses propres politiques en matière de protection de la vie privée, la *Loi sur la protection des renseignements personnels et les documents électroniques* et les normes de l'industrie, et avait agi ainsi pour son propre gain financier, d'une façon préjudiciable aux membres du groupe » (*Lam*, aux para 72, 73, 76).

[47] Autrement dit, dans l'arrêt *Lam*, l'usage abusif était la divulgation intentionnelle de renseignements confidentiels à des tiers (*Lam*, au para 76).

[48] Dans l'affaire dont je suis saisie, la preuve non contredite indique que des employés d'Emploi Canada (du secteur opérationnel et juridique) travaillaient sur des appels en instance

devant l’ancien tribunal lorsque la clé USB a été perdue. La clé servait à stocker et à transmettre les renseignements des appelants dont le dossier d’appel faisait l’objet d’un triage par un avocat.

[49] Les demandeurs mettent l’accent sur les différents termes utilisés pour expliquer ce qui s’est produit : la clé USB a disparu ou a été perdue (termes utilisés par le Commissariat à la protection de la vie privée), ou elle a été [TRADUCTION] « égarée » (terme utilisé dans la lettre qu’Emploi Canada a envoyée aux membres du groupe en décembre).

[50] Toutefois, rien n’indique que la clé USB a été volée, et contrairement à ce que font valoir les demandeurs, la disparition de la clé évoquée par le Commissariat à la protection de la vie privée ne permet pas de déduire que la clé a été volée. Selon moi, il s’agit d’un mauvais choix de mot, car on sait bien que sans l’intervention de David Copperfield, une clé USB ne peut pas simplement disparaître. En fait, ce choix de mot ne change rien à la réalité; personne ne sait ce qu’il est réellement advenu de la clé USB.

[51] Plus important encore, les demandeurs n’affirment pas que leurs renseignements confidentiels ont été divulgués ou consultés par un tiers en raison de la perte de la clé USB.

[52] S’appuyant sur l’arrêt *Lam*, les demandeurs demandent à la Cour de sauter quelques étapes : ils affirment essentiellement qu’en raison du fait que la clé USB a été utilisée d’une façon non autorisée (elle aurait dû être chiffrée et conservée dans un classeur verrouillée, ce qui n’a pas été fait), la Cour devrait conclure que les renseignements ont été divulgués intentionnellement et que cette divulgation a été préjudiciable aux membres du groupe.

Autrement dit, ils veulent que la Cour en vienne à la conclusion que l'usage abusif est synonyme d'intention et que l'intention est synonyme de préjudice.

[53] En tout respect, la Cour ne peut pas faire abstraction des éléments manquants du délit.

[54] Pour ces motifs, en présumant que les faits allégués sont avérés, j'estime que les demandeurs n'ont pas prouvé l'existence d'une cause d'action fondée sur l'abus de confiance.

B. *Existe-t-il un groupe identifiable formé d'au moins deux personnes ou les réclamations de la plupart des membres du groupe sont-elles prescrites en raison de l'expiration des délais de prescription prévus par la loi?*

[55] Bien que le défendeur affirme que le délai de prescription a une incidence sur plusieurs éléments du critère d'autorisation, il fait valoir que les demandeurs ne remplissent pas les conditions prévues à l'article 334.16 des Règles, car les réclamations des membres du groupe proposé sont prescrites en raison de l'expiration des délais de prescription prévus par la loi.

[56] Les demandeurs s'appuyaient initialement sur une décision de la Cour suprême de la Nouvelle-Écosse pour faire valoir que l'expiration du délai de prescription est un moyen de défense qui doit être invoqué dans une défense. Comme les défendeurs ont décidé de ne pas déposer de défense avant l'autorisation, la prescription n'était pas une question à trancher au moment de l'autorisation (*MacQueen v Sydney Steel Corporation*, 2011 NSSC 484 (CanLII) au para 73).

[57] À l'audience, les demandeurs ont demandé l'autorisation de déposer l'affidavit de Luciana Brasil pour décrire les communications entre les avocats et la Cour qui ont conduit à la demande des parties de suspendre la présente instance jusqu'à ce qu'une décision définitive soit rendue dans le dossier *Condon*. La Cour a accordé l'autorisation et a entendu les arguments des parties sur cette question.

[58] Aux termes de la *Loi sur la responsabilité civile de l'État et le contentieux administratif*, LRC 1985, c C-50, lorsqu'une cause d'action survient « ailleurs que dans une province », la procédure « se prescrit par six ans » (art 32). Le libellé du paragraphe 39(2) de la *Loi sur les Cours fédérales*, LRC 1985, c F-7, est identique.

[59] Le défendeur fait valoir que les réclamations des membres du groupe proposé ont expiré en décembre 2018, soit six ans après que les membres du groupe ont été informés de l'incident en décembre 2012. Quant à eux, les demandeurs estiment que les réclamations expireront le 23 septembre 2024. Le raisonnement des demandeurs est le suivant :

- Les parties conviennent que le délai de prescription applicable pour intenter l'action est de six ans.
- En supposant que tous les membres du groupe ont découvert leur cause d'action grâce à une lettre du 19 décembre 2012, ce qui n'est pas admis, le délai de prescription du recours collectif a commencé à courir le 20 décembre 2012.
- Les parties ont convenu de suspendre le litige le 14 avril 2013. Cette suspension a finalement été prolongée jusqu'à ce qu'une décision définitive soit rendue dans le dossier *Condon*.
- Le dossier *Condon* a été réglé et l'entente de règlement a été approuvée le 18 mai 2018. La question aurait été

complètement réglée dans un délai de 60 jours, ce qui porte la fin de la suspension au 17 juillet 2018.

- Enfin, le délai de prescription a été suspendu pendant six mois (du 13 mars au 13 septembre 2020) en raison de la pandémie de COVID-19.

- Une période de six ans compte 2 190 jours.

- En supposant que le délai a commencé à courir le 20 décembre 2012, ce qui n'est pas admis, 116 jours se sont écoulés avant que les parties conviennent de suspendre le dossier.

- Selon les demandeurs, le délai de prescription a recommencé à courir le 18 juillet 2018, lorsque l'ordonnance d'approbation du règlement dans le dossier *Condon* est devenue définitive, et a continué de courir jusqu'à ce qu'il soit suspendu à nouveau en raison de la pandémie de COVID-19 le 13 mars 2020. La période s'échelonnant entre le 18 juillet 2018 et le 13 mars 2020 représente 605 jours supplémentaires.

- À ce moment-là, il restait 1 469 jours avant que le délai de prescription soit expiré.

- Le délai de prescription du recours collectif a recommencé à courir le 15 septembre 2020, lorsque la suspension liée à la pandémie de COVID-19 a pris fin. Ainsi, la date correspondant à 1 469 jours après le 15 septembre 2020 est le 23 septembre 2024.

[60] Conformément au régime des recours collectifs de notre Cour, le délai est suspendu seulement à partir du moment où le recours est autorisé. En l'absence d'une disposition suspendant le délai de prescription pour les membres du groupe proposé, ceux-ci doivent déposer des demandes individuelles ou préserver autrement leur droit au moyen d'une entente entre les parties visant à repousser le point de départ du délai de prescription en attendant que le recours collectif soit autorisé.

[61] Un document de travail du Comité des règles de la Cour fédérale illustre la question. Ce comité a décidé de ne pas adopter une disposition suspendant le délai de prescription en attendant que le recours collectif soit autorisé (Comité des règles de la Cour fédérale du Canada, Le recours collectif en Cour fédérale du Canada : Document de travail (9 juin 2000), XVII DÉLAIS DE PRESCRIPTION, aux p 93-96, dossier de requête du défendeur, onglet 6). Le comité s'est exprimé en ces termes :

> Il serait utile pour les demandeurs qu'une disposition prévoie la suspension du délai de prescription. Toutefois, les contraintes imposées à la compétence du Comité l'empêchent d'incorporer cette question dans la règle sur le recours collectif; en effet, les délais de prescription sont clairement des questions de droit substantiel. En l'absence d'une telle disposition, le membre du groupe peut avoir à déposer une déclaration pour préserver ses droits en attendant la décision concernant la certification du groupe. La nécessité de déposer une déclaration dans de telles circonstances, ou de chercher à s'entendre avec le défendeur pour que le délai de prescription ne soit pas soulevé en défense, peut être un fardeau, mais il n'est pas très lourd. Quoi qu'il en soit, une telle exigence imposée aux membres du groupe ne devrait pas autrement porter atteinte à la viabilité de la règle sur le recours collectif. Il faudrait peut-être que les avis communiqués aux membres du groupe, avant le jugement statuant sur le fond du recours collectif, les informent que les délais de prescription pertinents continuent de s'appliquer.

[62] Notre Cour a conclu qu'un recours collectif ne peut pas servir à faire renaître les droits de personnes dont les réclamations sont prescrites en raison de l'expiration des délais de prescription prévus par la loi en participant à un recours collectif (*Tihomirovs c Canada* (*Ministre de la Citoyenneté et de l'Immigration*), 2006 CF 197 au para 92; *Vézina c Canada (Défense)*, 2011 CF 79 au para 43).

[63] Autrement dit, contrairement aux régimes des recours collectifs provinciaux, le régime des recours collectifs de notre Cour exige une entente de prorogation ou une autorisation pour repousser le point de départ du délai de prescription.

[64] Le défendeur fait valoir que bien que les demandeurs aient déposé leur déclaration le 31 janvier 2013, les parties n'ont jamais convenu de repousser le point de départ du délai de prescription pour le groupe proposé et le défendeur n'a jamais accepté de renoncer à son droit d'invoquer la prescription.

[65] Le 15 avril 2013, lors d'une conférence de gestion de l'instance, les parties ont convenu de suspendre le présent dossier pendant le déroulement du litige dans le dossier *Condon*. Cependant, les délais de prescription sont des droits substantiels. La Cour peut uniquement suspendre le délai de dépôt au tribunal des documents de procédure pour les représentants demandeurs aux termes des Règles.

[66] Les demandeurs renvoient à la décision *McCrea c Canada (Procureur général)*, 2015 CF 592, que notre Cour a rendue, pour affirmer qu'il n'est pas nécessaire d'établir les délais de prescription à l'étape de l'autorisation. Cependant, la décision *McCrea* portait sur une situation dans laquelle le délai était échu pour certaines demandes des membres du groupe et pas pour d'autres. Dans une telle situation, la juge Kane a conclu que le délai de prescription n'empêchait pas l'autorisation du recours collectif. La présente affaire se distingue de la décision *McCrea*, car en l'espèce, tous les demandeurs ont découvert leur cause d'action en même temps, soit lorsqu'ils ont reçu un avis d'Emploi Canada au sujet de la perte des données. Par conséquent, la

question du délai de prescription est déterminante pour tous les membres du groupe (exception faite des trois demandeurs). Compte tenu du mécanisme de contrôle de la requête en autorisation, le facteur de l'économie des ressources judiciaires ne milite pas en faveur de l'autorisation d'un recours collectif qui était complètement prescrit pour tous les demandeurs proposés.

[67] Par conséquent, la question consiste à savoir s'il existait une entente de prorogation entre les parties ou si le défendeur a accepté de renoncer au délai de prescription.

[68] Les demandeurs affirment premièrement que le défendeur a accepté de suspendre le délai de prescription lorsqu'ils ont convenu de suspendre le dossier.

[69] Cependant, les demandeurs n'ont pas été en mesure de renvoyer à une quelconque entente explicite ou implicite, conclue oralement ou par écrit, et le défendeur affirme qu'il n'a jamais accepté de renoncer à son droit d'invoquer la prescription.

[70] Dans son affidavit, M^{me} Brasil affirme que les demandeurs ont appris que le défendeur s'appuyait sur le délai de prescription en février 2024, lorsque le mémoire des faits et du droit du défendeur leur a été signifié. Cependant, la correspondance déposée à l'appui de son affidavit indique clairement que les parties ont discuté de cette question en juin 2023. Les avocats des demandeurs ont demandé aux avocats du défendeur si celui-ci avait l'intention de s'appuyer sur le délai de prescription à l'étape de l'autorisation. Cela confirme également que les parties n'avaient jusque-là conclu aucune entente pour repousser le point de départ du délai de prescription.

[71] Les demandeurs soutiennent également que le défendeur est préclus d'invoquer le délai de prescription. La préclusion promissoire est un moyen de défense d'equity qui nécessite qu'une partie établisse que :

> (1) l'autre partie a, par ses paroles ou sa conduite, fait une promesse ou donné une assurance destinées à modifier leurs rapports juridiques et à inciter à l'accomplissement de certains actes;
>
> (2) la partie qui invoque la préclusion promissoire a pris, sur la foi de la promesse ou de l'assurance, une mesure quelconque ou a de quelque manière changé sa position.
>
> (*Maracle c Travellers Indemnity Co of Canada*, 1991 CanLII 58 (CSC), [1991] 2 RCS 50 à la p 57.)

[72] Selon les directives les plus récentes de la Cour suprême du Canada, le moyen de défense d'equity fondé sur la préclusion promissoire nécessite 1) que les parties entretiennent des rapports juridiques au moment de la promesse ou de l'assurance; 2) que la promesse ou l'assurance ait été destinée à modifier ces rapports et à inciter à l'accomplissement de certains actes; et 3) que l'autre partie se soit fiée à la promesse ou à l'assurance (*Trial Lawyers Association of British Columbia c Royal & Sun Alliance du Canada, société d'assurances*, 2021 CSC 47 au para 15).

[73] Il ne fait aucun doute, selon notre jurisprudence, que la promesse doit être « claire et non équivoque » ou « non ambiguë » (*Trial Lawyers Association of British Columbia c Royal & Sun Alliance du Canada, société d'assurances*, 2021 CSC 47 aux para 46, 59).

[74] La réussite du moyen de défense des demandeurs fondé sur la préclusion promissoire dépend en grande partie de la question de savoir s'ils ont fourni des éléments de preuve clairs et

non équivoques indiquant que le défendeur avait l'intention de promettre de renoncer au délai de prescription.

[75] Selon moi, la conduite du défendeur n'indique pas clairement que celui-ci avait l'intention de renoncer au délai de prescription. En outre, la conduite des demandeurs – qui cherchent à obtenir des renseignements sur la position du défendeur à cet égard – montre qu'ils n'avaient pas interprété la conduite du défendeur comme celle d'une partie qui avait renoncé à un droit substantiel. Par conséquent, ils n'auraient pas pu s'appuyer sur une telle promesse.

[76] Notre Cour n'a pas compétence inhérente pour autoriser une action qui est entièrement prescrite en raison de l'expiration des délais de prescription prévus par la loi (*Tacan c Canada*, 2005 CF 385, [2005] ACF N^{o} 497 aux para 87, 88; *Nicholson c Canada*, [2000] 3 CF 225, ACF N^{o} 211 aux para 38 à 41). En l'absence d'un pouvoir discrétionnaire expressément prévu par la loi, la Cour ne peut supprimer ou proroger un délai de prescription.

[77] En l'absence d'une entente de prorogation par laquelle le défendeur renonce à des droits substantiels prévus par la loi, j'estime que le point de départ du délai de prescription n'a pas été repoussé et que les réclamations des membres du groupe sont prescrites en raison de l'expiration des délais de prescription prévus par la loi.

[78] Selon moi, cette conclusion permet de trancher la requête des demandeurs. Cependant, dans l'éventualité où je commettrais une erreur en ce qui concerne la question du délai de

prescription, je tiens à examiner quelques autres motifs pour lesquels j'estime que les demandeurs ne satisfont pas au critère d'autorisation.

C. *La réclamation soulève-t-elle des points de droit ou de fait communs?*

[79] Les demandeurs cherchent à faire autoriser les questions communes suivantes :

> **Négligence**
>
> 1. Le défendeur avait-il envers les membres du groupe une obligation de diligence lorsqu'il a recueilli, utilisé ou divulgué les renseignements personnels?
>
> 2. Si la réponse à la question n^{o} 1 est « oui », le défendeur a-t-il enfreint la norme de diligence lorsqu'il a recueilli, conservé, perdu ou divulgué les renseignements personnels? Dans l'affirmative, pour quelle raison?
>
> **Abus de confiance**
>
> 3. Les membres du groupe ont-ils communiqué les renseignements personnels au défendeur à titre confidentiel?
>
> 4. Le défendeur a-t-il fait un usage abusif des renseignements personnels lorsqu'il a recueilli, conservé, perdu ou divulgué les renseignements personnels, et cet usage abusif a-t-il été préjudiciable aux membres du groupe?
>
> 5. Si les réponses aux questions n^{os} 3 et 4 sont « oui », le défendeur a-t-il abusé de la confiance des membres du groupe, et dans l'affirmative, de quelle façon?
>
> **Responsabilité du fait d'autrui**
>
> 6. Le défendeur est-il responsable du fait d'autrui ou autrement responsable des actes et des omissions de ses dirigeants, administrateurs, employés, mandataires et représentants pendant qu'il est en possession des renseignements personnels?
>
> **Dommages-intérêts**
>
> 7. Si la réponse à au moins une des questions communes est affirmative, le défendeur devrait-il payer des dommages indemnisables du fait de :

a. sa négligence?

b. l’abus de confiance?

8. Les dommages-intérêts dus aux membres du groupe peuvent-ils faire l’objet d’une évaluation globale en vertu du paragraphe 334.28(1) des *Règles des Cours fédérales*? Dans l’affirmative, à quel montant devraient-ils s’élever?

9. Les membres du groupe ont-ils droit à des intérêts avant jugement et après jugement en application de la *Loi sur la responsabilité civile de l’État et le contentieux administratif*, LRC 1985, c C-50? Dans l’affirmative, quel devrait être le taux de ces intérêts?

[80] Comme je l’indique plus haut, afin d’atteindre le seuil pour satisfaire aux exigences d’autorisation, il est nécessaire d’établir un « certain fondement factuel » pour étayer l’ordonnance d’autorisation.

[81] Ce critère compte deux composantes. Premièrement, les membres du groupe proposé doivent avoir une réclamation ou, à tout le moins, une preuve minimale à l’appui de la réclamation. Deuxièmement, il doit y avoir des éléments de preuve établissant que les questions communes sont telles que leur résolution est nécessaire pour le règlement des demandes de chaque membre du groupe (*Jensen CAF*, au para 78; *Hollick c Toronto (Ville)*, 2001 CSC 68 au para 25).

[82] Selon le critère à deux volets, la cour doit examiner la preuve produite à l’appui de la requête. Dans la décision *Jensen CF*, notre Cour a utilisé l’expression « examen rigoureux » (au para 292) pour décrire cette tâche et a souligné que cette norme nécessite un certain fondement factuel, et non une preuve de fait selon la norme civile. Un examen de la preuve

visant à établir l'existence d'une réclamation à cette étape de l'analyse diffère de l'appréciation du bien-fondé de la réclamation. Comme notre Cour l'a affirmé dans la décision *Jensen CF*, « [i]l existe une différence fondamentale entre l'appréciation du bien-fondé de la réclamation (ce que les tribunaux ne peuvent pas faire au moment de l'autorisation) et la recherche d'une preuve minimale à l'appui de la réclamation » (c.-à-d. le critère à deux volets) (au para 212, *Jensen CAF*, au para 79).

[83] Le défendeur reconnaît que les questions 1 et 2 peuvent être tranchées ensemble. Cependant, il affirme, d'une part, que les questions 4 et 5 n'ont aucun fondement factuel, et d'autre part, que les questions 7 et 8 (dommages-intérêts) ne peuvent pas être tranchées ensemble et n'ont aucun fondement factuel.

(1) Questions 4 et 5 – Manquement à l'obligation de confidentialité

[84] Les demandeurs n'ont pas présenté d'arguments détaillés sur ces questions communes proposées ni sur ce qui permettrait de satisfaire au critère du « certain fondement factuel », particulièrement en ce qui concerne l'allégation d'abus de confiance.

[85] Selon moi, il n'existe aucun fondement factuel à l'égard des questions communes proposées 4 et 5. Les demandeurs n'ont aucun fondement factuel pour établir qu'Emploi Canada avait l'intention de trahir la confiance des demandeurs ou de leur causer préjudice, ni qu'il leur a causé préjudice. Aucun des affidavits des représentants demandeurs n'a apporté un quelconque éclairage sur le caractère intentionnel. Ils n'ont pas non plus exposé de faits substantiels ou de

détails concernant le préjudice qu'ils auraient subi. Au contraire, ils font valoir qu'à leur connaissance, aucun tiers n'a consulté leurs renseignements.

(2) Questions 7 et 8 – Dommages-intérêts

a) *Dommages-intérêts communs pour négligence*

[86] À l'audience, les avocats des demandeurs ont décrit en détail les éléments de preuve déposés. La question est de savoir s'il existe un certain fondement factuel établissant l'existence de préjudices indemnisables suffisants pour étayer l'allégation de négligence, et s'il existe certains éléments de preuve indiquant que le règlement des questions communes est nécessaire au règlement des demandes de chaque membre du groupe.

[87] Les demandeurs ont porté à l'attention de la Cour le rapport d'enquête du Commissariat à la protection de la vie privée, qui indique que les renseignements personnels figurant dans la clé USB, pourraient, s'ils tombaient entre de mauvaises mains, ouvrir la porte au vol d'identité et à la fraude.

[88] Ensuite, les demandeurs renvoient au rapport d'expert de M. Nicholas Scheurkogel, un expert en cybersécurité. M. Scheurkogel confirme que les types de renseignements stockés dans la clé USB peuvent être désignés Protégé B conformément à une évaluation respectant les politiques et les lignes directrices du gouvernement du Canada. Par définition, il s'agit de renseignements qui « pourraient porter un préjudice grave à une personne, à une organisation ou à un gouvernement s'ils étaient compromis ».

[89] M. Scheurkogel souligne qu'il est difficile de savoir quelles techniques et procédures d'enquête ont été appliquées après la perte de la clé USB. [TRADUCTION] « Sans ces détails, il est impossible de se prononcer sur la rigueur de l'enquête et sur ce qu'il est advenu de la clé USB. »

[90] Les demandeurs font valoir qu'en l'absence de certaines mesures d'enquête, il est possible que la clé USB ait été volée. Le gouvernement n'a pas écarté la possibilité du vol.

[91] Les demandeurs soutiennent également que les éléments de preuve sur la façon dont le gouvernement a désigné les renseignements stockés sur la clé USB, sur le risque auquel les personnes sont exposées et sur la façon dont les renseignements ont été recueillis sont insuffisants pour établir un certain fondement factuel quant au bien-fondé de l'allégation de négligence.

[92] Les demandeurs ont présenté des éléments de preuve tirés de la base de données du système d'inscription au recours, selon lesquels environ 7 % des personnes ont déclaré avoir été victimes de vol d'identité en raison du manquement. Les avocats ont affirmé qu'ils ne s'appuient pas sur ces éléments de preuve pour la véracité de leur contenu, mais plutôt pour établir un certain fondement factuel quant à la possibilité qu'il existe un préjudice.

[93] Quant à lui, le défendeur fait valoir qu'il n'existe aucun fondement factuel permettant d'établir qu'un membre du groupe a subi un préjudice indemnisable. Toute allégation de préjudice est entièrement conjecturale. Les affidavits des demandeurs ne fournissent aucun détail ni aucun renseignement significatif sur les préjudices allégués pour établir qu'ils sont communs

aux membres du groupe proposé. Les demandeurs avancent des hypothèses sur le préjudice qui pourrait exister, mais ne fournissent pas les éléments de preuve minimaux nécessaires aux fins de l'autorisation.

[94] En ce qui a trait aux dommages-intérêts réclamés pour le préjudice psychologique, le défendeur fait valoir que les demandeurs n'ont pas présenté les éléments de preuve minimaux nécessaires à l'étape des questions communes. Les préjudices subis en raison du stress et de l'anxiété doivent être « graves et prolongés », et il ne doit pas s'agir « simplement des désagréments, angoisses et craintes ordinaires » (*Saadati c Moorhead*, 2017 CSC 28 au para 37).

[95] La loi établit très clairement que les demandeurs ne sont pas tenus de prouver l'existence de dommages selon la norme civile à l'étape de l'autorisation (*Sweet*, au para 17). Les demandeurs sont tenus d'établir un certain fondement factuel, ce qui nécessite la présentation de certains éléments de preuve.

b) *Risque accru de vol*

[96] Selon M. Scheurkogel, l'analyse de l'enquête révèle plusieurs lacunes qui minent les conclusions du gouvernement selon lesquelles [TRADUCTION] « rien n'indiquait que la clé USB avait été volée, consultée à des fins frauduleuses ou emportée à l'extérieur du bureau » :

> a) Il souligne que [TRADUCTION] « [l]es affidavits et les renseignements fournis ne décrivent pas de façon assez détaillée les activités d'enquête pour être utiles. Les affidavits indiquent qu'une enquête a été réalisée, mais ne précisent pas les dates de début et de fin de l'enquête, les activités précises qui ont été menées, les éléments pris en compte, les personnes interrogées et les mesures techniques déployées pour chercher la clé USB ».

> Selon lui, cela mine la solidité de toute conclusion, car il est impossible d'évaluer la rigueur de l'enquête.
>
> b) Il souligne que la conclusion selon laquelle rien n'indiquait que la clé USB avait été emportée à l'extérieur du bureau était directement minée par la fouille réalisée chez les employés et dans le taxi que l'employé a pris pour se rendre chez lui, car [TRADUCTION] « la clé USB a manifestement été emportée chez l'avocat, sinon, pourquoi une fouille aurait-elle été réalisée à cet endroit; d'autant plus qu'une fouille réalisée dans le bureau n'a pas permis de trouver la clé USB. Manifestement, la clé USB a dû être sortie du bureau, sans quoi elle s'y trouverait encore. Manifestement, l'avocat en question a déjà utilisé et consulté la clé USB à partir de chez lui ».
>
> c) Il souligne qu'on ignore à quel moment l'avocat a consulté la clé USB pour la dernière fois, bien que les enquêteurs soient en mesure d'obtenir ce renseignement. En déterminant l'identifiant unique associé à l'utilisation de la clé USB, les enquêteurs auraient pu établir où se trouvait l'avocat lorsqu'il a utilisé la clé USB pour la dernière fois (l'avocat aurait alors été vraisemblablement chez lui ou au bureau), et savoir [TRADUCTION] « si le dispositif avait été inséré dans un autre appareil ailleurs dans l'organisation ». Il souligne ceci : [TRADUCTION] « Ce renseignement aurait été important pour savoir précisément à quel moment la clé USB a été perdue ou volée. Il aurait aussi été pertinent pour éliminer ou confirmer à partir de quel endroit les renseignements de nature délicate auraient pu avoir été consultés. » Il aurait aussi permis aux enquêteurs de savoir qui avait consulté la clé USB au moment où elle a disparu.
>
> d) Enfin, il souligne que rien n'indique qu'une [TRADUCTION] « surveillance a été effectuée dans le Web invisible pour repérer dans les forums criminels toute donnée qui était stockée dans la clé USB qui a été perdue ou volée. Il s'agit d'une étape qui va de soi, car la vente de données canadiennes aux groupes criminels peut être effectuée à un endroit où il est possible d'assurer une surveillance, particulièrement parce que les données stockées dans la clé USB ont une valeur évidente pour les groupes criminels ».

[97] En ce qui a trait aux risques auxquels les membres du groupe demeurent exposés,

M. Scheurkogel affirme que [TRADUCTION] « [l]e fait que [la clé USB] n'a pas été retrouvée

malgré la fouille est une variable à prendre en compte – la possibilité que le support de données ait été volé n'a pas été écartée. Au gouvernement, dans le domaine de la sécurité des TI, il est pratique courante de considérer que des renseignements susceptibles d'avoir été violés ont été violés tant qu'il n'est pas prouvé qu'ils ne l'ont PAS été ». Autrement dit, le fait que la clé USB n'a pas été retrouvée après une fouille aussi rigoureuse donne à penser qu'elle a été prise, et non « perdue ». M. Scheurkogel souligne que rien dans la preuve présentée par le défendeur (exception faite d'une simple conclusion) n'exclut la possibilité que la clé USB ait été ciblée. Sur le fondement de son expertise, la description que le défendeur a donnée de ses propres activités est insuffisante pour écarter la possibilité d'un vol, c'est-à-dire que [TRADUCTION] « [l]es renseignements sont insuffisants pour déterminer si le risque de préjudice a été éliminé ». Il souligne que sans autre élément de preuve, il lui est impossible de tirer une conclusion sur la question de savoir si les membres du groupe ont subi un préjudice. Cependant, il reconnaît que la protection de six ans offerte grâce à l'avertissement placé dans le dossier de crédit des membres du groupe était excellente et que le préjudice était limité, dans l'hypothèse où l'enquête a été réalisée avec diligence.

[98] Le défendeur a retenu les services de M. Fred Cate, un professeur de droit à l'Université d'Indiana. M. Cate a préparé un rapport d'expert sur le risque de préjudice auquel sont exposées les personnes touchées. Il a exprimé les avis suivants :

> a) La preuve en l'espèce donne à penser que nul n'a consulté les données et qu'il n'y a eu aucun vol d'identité;
>
> b) Les violations consistant en la perte ou le vol de matériel ou de supports ne semblent pas contribuer de façon statistiquement significative au vol d'identité;
>
> c) Le risque financier découlant du vol d'identité est principalement assumé par les institutions financières et d'autres

> entreprises – il est rare que les particuliers subissent une perte financière;
>
> d) Les données personnelles volées sont habituellement utilisées rapidement, soit dans les jours ou les mois suivant l'incident, et non des années plus tard;
>
> e) Le service d'avertissement de fraude offert pendant six ans va bien au-delà de ce qui est nécessaire pour protéger les personnes dont les données sont stockées sur la clé USB manquante.

[99] En toute déférence, j'accorde plus de poids à la preuve préparée par M. Cate qu'à celle de M. Scheurkogel.

[100] Si la Cour adoptait la position de M. Scheurkogel, le fardeau de la preuve reviendrait au défendeur. Cela inverserait le fardeau de la preuve et le défendeur serait donc tenu de présenter certains éléments pour prouver qu'il n'y a pas eu de préjudice. Le défendeur devrait prouver, selon une norme se rapprochant de la norme de la preuve hors de tout doute raisonnable, que la clé USB n'a pas été ciblée. Il ne s'agit pas du critère que je dois appliquer. Ce sont les demandeurs qui avaient le fardeau d'établir un certain fondement factuel quant au risque accru de vol d'identité auquel ils sont exposés, ce qu'ils n'ont pas fait. M. Scheurkogel affirme que rien n'indique qu'une surveillance a été effectuée dans le Web invisible pour repérer tout renseignement qui était stocké dans la clé USB. Toutefois, il ne précise pas s'il a lui-même, à titre d'expert en cybersécurité, effectué une telle recherche, et dans cette éventualité, quels ont été les résultats de cette recherche.

[101] Le rapport de M. Scheurkogel est très conjectural et s'appuie sur des généralités. Il ne traite d'aucune question concrète soulevée par M. Cate, mis à part qu'il reconnaît que la

protection de six ans offerte grâce à l'avertissement placé dans le dossier de crédit était excellente et que le préjudice était donc limité.

[102] Enfin, quant à l'argument des demandeurs selon lequel environ 7 % des personnes ont déclaré avoir été victimes d'un vol d'identité en raison du manquement, il faut mettre les choses en contexte. Il s'agit de 163 des 5 045 (3,2 %) membres du groupe proposé qui se sont inscrits auprès des avocats, car ils souhaitaient participer au recours collectif proposé. Ce sont donc 7 % de 3,2 % qui ont déclaré avoir été victimes d'un vol d'identité, ce qui est largement inférieur aux 3 % de la population qui sont généralement victimes d'un vol d'identité.

c) *Angoisse et anxiété*

[103] Dans l'arrêt *Saadati c Moorhead*, 2017 CSC 28, la Cour suprême du Canada a conclu que les contrariétés émotionnelles graves et de longue durée qui vont au-delà des désagréments ordinaires de la vie sont considérées comme des préjudices personnels indemnisables sans qu'il soit nécessaire d'établir l'existence d'un diagnostic psychiatrique.

[104] J'estime que les demandeurs n'ont fourni aucun élément de preuve établissant que les préjudices subis en raison du stress et de l'anxiété sont graves et prolongés, et vont au-delà des désagréments ordinaires de la vie. Bien que les demandeurs invoquent un préjudice en raison de [TRADUCTION] « la souffrance, la détresse, l'humiliation, l'angoisse, la perte de confiance, le sentiment d'atteinte à la vie privée et l'augmentation du niveau de stress de façon continue », les demandeurs n'ont présenté aucun élément de preuve et n'ont fourni aucun détail établissant que

ces préjudices ne sont pas simplement des désagréments ou vont au-delà des désagréments de la vie quotidienne.

[105] Les demandeurs n'ont pas fourni les éléments de preuve minimaux nécessaires à l'étape des questions communes pour étayer l'existence de préjudices indemnisables à l'échelle individuelle ou à l'échelle du groupe. Les représentants demandeurs proposés n'apportent aucune preuve à cet égard; ils affirment plutôt qu'à leur connaissance, leurs renseignements n'ont pas été utilisés de façon abusive.

[106] Je conclus également que les demandeurs n'atteignent pas le seuil de preuve établi dans l'arrêt *Jensen CAF*, que le préjudice invoqué constitue ou non une perte purement économique. La loi établit très clairement que les demandeurs ne sont pas tenus de prouver l'existence de dommages selon la prépondérance des probabilités à l'étape de l'autorisation (*Sweet*, au para 17). Cependant, les demandeurs sont tenus d'établir un certain fondement factuel, ce qui nécessite la présentation de certains éléments de preuve.

[107] Les demandeurs n'ont fourni aucun élément de preuve établissant qu'un membre du groupe a subi un préjudice en raison des actions du défendeur. Je suis d'accord avec le défendeur pour dire que les demandeurs ont fourni des éléments de preuve concernant un risque conjectural et non un quelconque risque réel et important. Ils ont apporté la preuve que certains membres du groupe proposé prétendent avoir été victimes d'un vol d'identité et ont fourni une preuve d'expert selon laquelle il est impossible d'écarter complètement la possibilité que la clé USB ait été volée. Cela ne suffit pas à apporter la preuve minimale nécessaire pour étayer le bien-fondé

d’une demande fondée sur la négligence ou pour établir que le règlement de cette question commune est nécessaire.

d) *Dommages-intérêts globaux*

[108] Dans l’arrêt *Pro-Sys*, la Cour suprême du Canada a conclu que les questions concernant l’octroi de dommages-intérêts globaux peuvent être certifiées (au para 128).

[109] Dans les dossiers *Condon* et *Untel*, notre Cour a conclu que les questions concernant l’octroi de dommages-intérêts globaux peuvent être certifiées. Notre Cour peut ordonner l’octroi de dommages-intérêts globaux dans les circonstances appropriées en vertu de l’article 333.28 des Règles.

[110] Le défendeur fait valoir que les demandeurs doivent démontrer, par des éléments de preuve, qu’il existe une démarche utilisable pour déterminer les questions à l’échelle du groupe sans que des membres n’aient à en faire la preuve individuellement. Dans l’arrêt *Canada c Greenwood*, 2021 CAF 186, la Cour d’appel fédérale a conclu qu’il n’existait aucun fondement factuel pour une question commune liée à une évaluation globale des dommages-intérêts, car les demandeurs n’avaient produit aucune preuve montrant comment effectuer une telle évaluation (au para 188).

[111] Je suis d’accord avec le défendeur pour dire que les demandeurs ne se sont pas acquittés du fardeau d’établir pour la Cour un fondement factuel pour une question commune concernant

les dommages-intérêts globaux. Les demandeurs n’ont produit aucune preuve montrant comment la Cour pourrait effectuer une telle évaluation.

D. *Le recours collectif est-il le meilleur moyen de régler, de façon juste et efficace, les points communs?*

[112] L’alinéa 334.16(1)d) des Règles prévoit qu’un recours collectif proposé doit être « le meilleur moyen de régler, de façon juste et efficace, les points de droit ou de fait communs ».

[113] Il convient de tenir compte de la liste non exhaustive suivante pour décider si le recours collectif est le meilleur moyen (paragraphe 334.16(2) des Règles) :

> a) la prédominance des points de droit ou de fait communs sur ceux qui ne concernent que certains membres;
>
> b) la proportion de membres du groupe qui ont un intérêt légitime à poursuivre des instances séparées;
>
> c) le fait que le recours collectif porte ou non sur des réclamations qui ont fait ou qui font l’objet d’autres instances;
>
> d) l’aspect pratique ou l’efficacité moindres des autres moyens de régler les réclamations;
>
> e) les difficultés accrues engendrées par la gestion du recours collectif par rapport à celles associées à la gestion d’autres mesures de redressement.

[114] En ce qui concerne le facteur énoncé à l’alinéa a), le défendeur ne conteste pas l’existence de points de droit ou de fait communs en ce qui concerne la négligence dont a fait preuve le défendeur dans le traitement des renseignements personnels des demandeurs. Les points communs se rapportant à la négligence prédominent sur les réclamations individuelles.

[115] Cependant, les autres facteurs prévus au paragraphe 334.16(2) des Règles ne militent pas en faveur d'un recours collectif.

[116] Rien n'indique qu'une proportion importante de membres du groupe ont un intérêt légitime à poursuivre des instances séparées.

[117] En outre, près de douze ans se sont écoulés depuis la perte de la clé USB et rien n'indique que les représentants demandeurs ont subi un quelconque préjudice ou que les renseignements ont été utilisés d'une manière abusive. Comme l'indique le rapport d'expert de M. Cate, le groupe proposé n'est pas exposé à un risque accru de vol d'identité en raison de la perte.

[118] Comme la grande majorité, si ce n'est la totalité, des réclamations individuelles sont prescrites en raison de l'expiration des délais de prescription prévus par la loi, il est impossible d'utiliser un recours collectif pour faire renaître ces réclamations et il ne serait pas dans l'intérêt de la justice d'autoriser un recours collectif pour le bénéfice exclusif des trois représentants demandeurs.

[119] Enfin, un recours collectif en l'espèce ne permettrait pas de réaliser l'objectif de changement de comportement; Emploi Canada a déjà pris des mesures pour modifier ses politiques et ses pratiques après avoir rapidement informé les personnes touchées et le Commissariat à la protection de la vie privée qu'un employé avait égaré une clé USB; Emploi Canada a appliqué les recommandations du Commissariat à la protection de la vie privée; compte

tenu du temps qui s’est écoulé depuis l’incident et de l’évolution de la technologie, l’autorisation du recours collectif proposé ne permet pas de réaliser l’objectif de changement de comportement.

VI. Conclusion

[120] Je rejette la requête des demandeurs parce que, d’une part, la grande majorité, si ce n’est la totalité, des réclamations des membres du groupe sont prescrites en raison des délais de prescription prévus par la loi, et d’autre part, les demandeurs ne satisfont pas au critère conjonctif d’autorisation.

[121] Le défendeur ne sollicite pas de dépens et aucuns ne seront adjugés.

ORDONNANCE dans le dossier T-226-13

LA COUR ORDONNE ce qui suit :

1. La requête en autorisation des demandeurs est rejetée.

2. Aucuns dépens ne sont adjugés.

« Jocelyne Gagné »

Juge en chef adjointe

Traduction certifiée conforme
Claude Leclerc

COUR FÉDÉRALE

AVOCATS INSCRITS AU DOSSIER

DOSSIER :	T-226-13
INTITULÉ :	JOHN MARK JACQUES, GORDON ALBERT MEHEW et CRAIG ROBAR c SA MAJESTÉ LE ROI
LIEU DE L'AUDIENCE :	TORONTO (ONTARIO)
DATE DE L'AUDIENCE :	LES 18 ET 19 MARS 2024
ORDONNANCE ET MOTIFS :	LA JUGE EN CHEF ADJOINTE GAGNÉ
DATE DES MOTIFS :	LE 6 JUIN 2024

COMPARUTIONS :

Theodore P. Charney Caleb Edwards	POUR LES DEMANDEURS
Sean Stynes Sarah Rajguru	POUR LE DÉFENDEUR

AVOCATS INSCRITS AU DOSSIER :

Charney Lawyers PC Toronto (Ontario)	POUR LES DEMANDEURS
Strosberg Sasso Sutts LLP Windsor (Ontario)	
Branch MacMaster LLP Vancouver (Colombie-Britannique)	
Bob Buckingham Law St. John's (Terre-Neuve-et-Labrador)	
Procureur général du Canada	POUR LE DÉFENDEUR

Ottawa (Ontario)