Date: 20250610

Dossier: 566-34-43563

Référence: 2025 CRTESPF 70

Loi sur la Commission des relations de travail et de l'emploi dans le secteur public fédéral et *Loi sur les relations de travail dans le secteur public fédéral*

Devant une formation de la Commission des relations de travail et de l'emploi dans le secteur public fédéral

ENTRE

MOHAMMED TIBILLA

fonctionnaire s'estimant lésé

et

AGENCE DU REVENU DU CANADA

défenderesse

Répertorié
Tibilla c. Agence du revenu du Canada

Affaire concernant un grief individuel renvoyé à l'arbitrage

Devant : Audrey Lizotte, une formation de la Commission des relations de travail et de l'emploi dans le secteur public fédéral

Pour le fonctionnaire s'estimant lésé : Michael Cohen, avocat

Pour la défenderesse : Mathieu Cloutier, avocat

Affaire entendue à Montréal (Québec),
du 14 au 17 mai 2024,
et par vidéoconférence,
le 5 juillet 2024.
(Traduction de la CRTESPF)

MOTIFS DE DÉCISION (TRADUCTION DE LA CRTESPF)

I. Grief individuel renvoyé à l'arbitrage

[1] Au moment de son licenciement, Mohammed Tibilla, le fonctionnaire s'estimant lésé (le « fonctionnaire »), occupait un poste d'agent des services aux contribuables, classé SP-04, à l'Agence du revenu du Canada (ARC ou l'« employeur »).

[2] Selon la lettre de licenciement, datée du 18 février 2021 et signée par Chantal Tourigny, directrice, Bureau des services fiscaux de Montréal de l'ARC, le fonctionnaire aurait accédé sans autorisation à son compte de contribuable de l'ARC à cinq reprises et aurait tenté de dissimuler cette inconduite lorsqu'il avait été interrogé à ce sujet. La lettre se lit comme suit :

> [Traduction]
>
> […]
>
> *L'objet de la présente lettre est de vous informer de ma décision concernant le maintien de votre emploi à l'Agence du revenu du Canada et de ma décision concernant vos accès non autorisés à votre propre compte le 4 avril 2019, les 23 et 24 mars 2020, le 1er avril 2020 et le 15 octobre 2020. Par suite du rapport #02886 de la Division des affaires internes et du contrôle de la fraude (DAICF) qui vous a été remis le 7 janvier 2021 et de l'audience disciplinaire tenue le 13 janvier 2021, je conclus que vous avez contrevenu au* Code d'intégrité et de conduite professionnelle *(le « Code ») de l'Agence du revenu du Canada (ARC) et à la* Directive sur l'utilisation des systèmes informatiques et des réseaux électroniques.
>
> *En tant qu'employé de l'ARC, vous êtes tenu de respecter le Code ainsi que toutes les autres directives et politiques de l'ARC. Vous avez reçu des rappels annuels sur le comportement que vous êtes censé adopter à l'égard du Code et vous avez reconnu avoir pris connaissance du Code.*
>
> *Pour parvenir à ma décision, j'ai pris en considération les circonstances présentées. J'ai également pris en compte des facteurs aggravants, notamment le fait qu'il y a eu plusieurs accès non autorisés entre avril 2019 et octobre 2020. En outre, vous avez tenté, à trois occasions différentes, de dissimuler la faute et de tromper la direction en faisant des allégations infondées et incohérentes. Ces comportements sont inacceptables et ne peuvent être tolérés. J'ai également pris en compte le fait que vous n'avez pas reconnu la gravité de votre comportement et que vous n'avez pas non plus fait preuve d'un quelconque remords.*
>
> *Étant donné que le lien de confiance a été irrévocablement rompu, et conformément au pouvoir qui m'a été conféré par le*

> *commissaire en vertu de l'article 51(1)(f) de la* Loi sur l'Agence du revenu du Canada*, je mets immédiatement fin par la présente à votre emploi auprès de l'ARC pour cause d'inconduite.*
>
> […]

[3] Le fonctionnaire a déposé son grief le 24 février 2021. Le grief a été renvoyé à l'arbitrage le 22 septembre 2021 au titre de l'article 209(1)b) de la *Loi sur les relations de travail dans le secteur public fédéral* (L.C. 2003, ch. 22, art. 2).

[4] Pour les motifs qui suivent, j'estime que l'inconduite alléguée a été établie, qu'elle a justifié l'imposition d'une mesure disciplinaire et que le licenciement n'était pas excessif dans les circonstances.

II. Résumé de la preuve

[5] L'employeur a appelé les six témoins suivants, tous ses employés :

- Rosaria Stockdale, qui était la directrice adjointe de la Division des affaires internes et du contrôle de la fraude (DAICF) de l'ARC. Elle était chargée de superviser l'enquête sur les allégations d'accès non autorisés du fonctionnaire et ses explications;
- Mme Tourigny;
- James Jones, qui était le gestionnaire du fonctionnaire et qui l'a interrogé sur ses accès à son compte;
- Robert Fazio, qui était conseiller technique et formateur et qui a fourni une formation au fonctionnaire;
- Sébastien Mongrain, qui était chef d'équipe au sein du bureau de service national des technologies de l'information (TI) de l'ARC et qui a vérifié les interactions du fonctionnaire avec le bureau de service des TI;
- Sergio Romanelli, qui était le chef d'équipe du fonctionnaire à compter du 4 avril 2019. Il a été appelé à témoigner en réplique pour réfuter un élément du témoignage du fonctionnaire.

[6] Le fonctionnaire a témoigné en son propre nom pour établir que les faits ne s'étaient pas produits de la manière alléguée et que la mesure disciplinaire était excessive dans les circonstances.

A. Pour l'employeur

1. Mme Stockdale

[7] Mme Stockdale a déclaré qu'à la date de l'audience, elle travaillait pour l'ARC depuis 22 ans et qu'elle occupait le poste de directrice adjointe au moment des faits en litige. Dans le cadre de ses fonctions, elle était chargée de superviser les enquêtes sur les inconduites soupçonnées d'employés. Le 29 décembre 2020, elle a publié un rapport d'enquête concernant le fonctionnaire. Elle n'avait aucune relation préexistante avec lui et ne le connaissait pas.

[8] Mme Stockdale a expliqué que les employés n'ont accès qu'aux bases de données de l'ARC nécessaires à l'exercice de leurs fonctions. Voici les systèmes électroniques de l'ARC concernés par la présente affaire :

- l'Aire de travail de l'agent des services aux contribuables – Particuliers (ATASC-P), qui permet d'accéder aux renseignements sur les contribuables;
- le Système en direct d'information de contribuable (RAPID) qui est plus ancien et permet également d'accéder aux renseignements sur les contribuables;
- RQCH (l'acronyme n'a pas été expliqué), qui est le système de stockage et de récupération hors site géré par la société Iron Mountain.

[9] Pour accéder à ces comptes, l'employé doit entrer son code d'utilisateur et son mot de passe confidentiel. Pour plus de sécurité, les employés sont tenus de changer leur mot de passe tous les 90 jours. Les renseignements sur les contribuables sont récupérés en utilisant leur numéro d'assurance sociale (NAS).

[10] Au cours du contre-interrogatoire, Mme Stockdale n'a pas pu dire avec certitude si tous les mots de passe utilisés pour accéder à ces systèmes de l'ARC devaient être changés tous les 90 jours.

[11] L'ATASC-P est conçue pour permettre aux agents d'accéder aux renseignements nécessaires afin de répondre aux demandes des contribuables en automatisant la collecte de renseignements à partir de systèmes particuliers de l'ARC, afin de faciliter l'analyse des comptes. Les données disponibles pour les utilisateurs de l'ATASC-P comprennent, entre autres, l'identification, les déclarations d'impôt sur le revenu, les cotisations, les allocations, les revenus, les entrées de journal et la correspondance.

[12] Pour ce qui est des contrôles, l'ARC dispose du formulaire d'accès électronique des employés [*Employee Electronic Access Form*], qui fournit un journal de vérification dressant une liste de tous les accès par les employés aux renseignements sur les contribuables. Chaque page du journal de vérification indique en colonnes les renseignements pertinents suivants :

- le nom d'utilisateur [*User ID*], qui identifie la personne qui a accédé à un système électronique de l'ARC;
- l'identificateur du système [*System ID*], qui précise le système auquel on a accédé; par exemple, ATASC-P, RAPID, etc.;
- l'identificateur d'écran [*Screen ID*], qui précise l'écran qui a été visualisé. Chaque écran est identifié par un code unique;
- le CIDP [*PRI*], le code d'identification du dossier personnel de l'employé. Chaque employé se voit attribuer un numéro unique qui permet de l'identifier;
- l'heure et la date de l'accès;
- le contribuable [*TP*] dont le dossier a été consulté ou le nom de la personne ou de l'organisation qui a soumis le document consulté;
- le numéro du centre de responsabilité [*RC number*] où travaille l'employé;
- le numéro de compte, qui est le NAS du compte auquel il a été accédé;
- le nom de l'employé, qui est identifié par son nom d'utilisateur, indique qui a accédé au système.

[13] Mme Stockdale a déclaré que l'ARC dispose d'un système de surveillance proactive, le système de gestion de la fraude électronique [*Electronic Fraud Management System*] (EFM). Ce système est conçu pour surveiller tous les accès. Des règles prédéfinies s'appliquent à toutes les opérations. Lorsqu'un employé effectue un accès qui déclenche l'une des règles, une alerte électronique est envoyée à la DAICF pour examen. Une règle est souvent déclenchée lorsqu'un employé accède à son compte, auquel cas l'EFM alerte automatiquement la DAICF pour examen.

[14] Au cours du contre-interrogatoire, Mme Stockdale a déclaré que l'EFM est en place depuis 2017 et qu'une fois que la DAICF reçoit une alerte, celle-ci est enregistrée dans un système de gestion des dossiers et attribuée à un enquêteur pour examen. Elle a précisé que les alertes sont générées en temps réel et qu'elles sont immédiatement intégrées dans un registre des dossiers. Toutefois, elles peuvent ne pas faire l'objet

d'une enquête immédiate, selon la disponibilité des enquêteurs. Elle a déclaré que des alertes sont reçues tous les jours, mais qu'elles ne donnent pas toutes lieu à une enquête. Si la DAICF examine l'information et détermine qu'il s'agit d'un accès valide qui n'est pas contestable, elle ferme le dossier.

[15] À titre d'exemple, Mme Stockdale a expliqué que l'une des règles qui génèrent une telle alerte est déclenchée chaque fois que l'on accède aux comptes de certaines personnes très connues. Dans ce cas, une vérification est effectuée auprès du gestionnaire afin de confirmer que l'accès était prévu. Si c'est le cas, l'accès est considéré comme valide. Elle a affirmé qu'il n'est jamais considéré comme légitime qu'un employé accède à son propre compte.

[16] Les alertes indiquent la règle qui a été déclenchée ainsi que la date et l'heure auxquelles elle s'est produite. Dans la plupart des cas, l'EFM fournit également une rediffusion d'écran. Cela permet à la DAICF de voir chacune des étapes que l'employé a suivies lorsqu'il a accédé à un système de l'ARC. Elle a expliqué que la rediffusion d'écran est disponible lorsque l'on accède à certains systèmes, tels que RAPID. Dès que ces systèmes sont consultés, l'EFM enregistre automatiquement les actions de l'employé.

[17] Mme Stockdale a déclaré que deux alertes EFM visant le fonctionnaire avaient été générées, indiquant qu'il avait accédé à son compte le 1er avril et le 15 octobre 2020.

[18] Au cours du contre-interrogatoire, Mme Stockdale a été interrogée pour savoir pourquoi l'incident du 1er avril 2020 n'avait pas fait l'objet d'une enquête plus tôt. Elle a expliqué que, le 16 mars 2020, tous les employés avaient été renvoyés chez eux en raison de la pandémie de COVID-19 et que seuls les employés considérés comme essentiels avaient été maintenus sur le lieu de travail. Elle a déclaré que la DAICF n'était pas considérée comme essentielle, et que ses travaux étaient donc suspendus jusqu'à ce que les membres de son personnel reprennent leurs fonctions en juillet 2020.

[19] À cette époque-là, il y avait un arriéré d'enquêtes à mener. Mme Stockdale a déclaré que la DAICF avait continué à surveiller l'EFM pendant le confinement, mais qu'elle n'avait examiné que les cas d'inconduite grave ou flagrante. Interrogée pour

savoir si l'accès d'un employé à son compte était considéré comme un cas d'inconduite grave, elle a répondu par l'affirmative.

[20] L'enquête a commencé par une vérification des accès du fonctionnaire depuis le 1er janvier 2016. Selon les rapports de pistes de vérification, il a également accédé à son compte le 4 avril 2019 et les 23 et 24 mars 2020, soit un total de cinq accès.

[21] Lorsqu'on lui a demandé au cours du contre-interrogatoire si des alertes avaient été générées le 4 avril 2019 et les 23 et 24 mars 2020, Mme Stockdale a répondu que l'ATASC-P était considérée comme un système relativement récent et que l'ARC était en train de migrer les renseignements de RAPID vers l'ATASC-P. Elle a déclaré qu'étant donné que tous les systèmes n'avaient pas été définis dans l'EFM, il était possible que l'ATASC-P n'y ait été définie qu'ultérieurement.

[22] Mme Stockdale a pris des mesures pour confirmer si des alertes EFM avaient été générées à ces dates antérieures. Elle a par la suite confirmé, dans un affidavit qu'elle a signé, qu'aucune alerte n'avait été générée. Elle a expliqué que l'EFM n'avait pas la capacité de définir et de saisir tous les systèmes à tout moment, compte tenu des constants changements et mises à niveau des systèmes de l'ARC.

[23] Mme Stockdale a décrit les renseignements contenus dans les journaux de vérification et les rediffusions d'écran disponibles pour les cinq incidents.

Incident no 1 - Accès le 4 avril 2019

[24] Selon le journal de vérification, le nom d'utilisateur du fonctionnaire a été utilisé pour se connecter à l'ATASC-P à 11 h 15 et une recherche a été effectuée à l'aide de son NAS. Les écrans « résumé de l'identification » [*identification summary*] et « renseignements sur le contribuable » [*taxpayer information*] ont été consultés.

Incident no 2 - Accès le 23 mars 2020

[25] Selon le journal de vérification, le nom d'utilisateur du fonctionnaire a été utilisé pour se connecter à l'ATASC-P et à RQCH de 8 h 36 à 8 h 50 et une recherche a été effectuée à l'aide de son NAS. Les écrans « résumé de l'identification » [*identification summary*] et « renseignements sur le contribuable » [*taxpayer information*] de l'ATASC-P ont été consultés. Plusieurs écrans de comptabilité ont également été consultés, montrant l'historique du compte, le solde, les débits, les crédits, les montants dus et les remboursements. Le journal montrait également

qu'une recherche avait été effectuée dans RQCH et que plusieurs écrans de ce système avaient été consultés.

Incident no 3 - Accès le 24 mars 2020

[26] Selon le journal de vérification, le nom d'utilisateur du fonctionnaire a été utilisé pour se connecter à l'ATASC-P et à RAPID de 20 h 47 à 20 h 52 et une recherche a été effectuée à l'aide de son NAS. Les écrans consultés étaient similaires à ceux du 23 mars, ainsi que le « menu vue du client » [*client vue menu*] dans RAPID.

Incident no 4 - Accès le 1er avril 2020

[27] Selon le journal de vérification, le nom d'utilisateur du fonctionnaire a été utilisé pour se connecter à l'ATASC-P et à RAPID de 9 h 04 à 9 h 24 et une recherche a été effectuée à l'aide de son NAS. Les écrans « résumé du solde de l'année de base » [*base year balance summary*], « demandes de paiement » [*payment inquiries*] et « renseignements sur les enfants » [*children information*] ont été consultés dans RAPID. Les écrans « résumé de l'identification du contribuable » [*taxpayer identification summary*], « allocations pour enfants – admissibilité et versements » [*benefits for children — eligibility and payments*] et « historique des impressions » [*print history*] ont été consultés dans l'ATASC-P.

[28] Mme Stockdale a déclaré que le fonctionnaire avait également examiné les allocations versées par le gouvernement fédéral et le gouvernement de l'Alberta.

[29] Mme Stockdale a également fait référence aux rediffusions d'écran obtenues de l'EFM pour cette date, qui indiquent les écrans qui ont été consultés. Elles indiquent également les commandes que le fonctionnaire a saisies pendant qu'il effectuait la recherche. Elle a déclaré qu'il avait examiné des chèques individuels d'allocations pour enfants remontant à 1998.

Incident no 5 - Accès le 15 octobre 2020

[30] Selon le journal de vérification, le nom d'utilisateur du fonctionnaire a été utilisé pour se connecter à l'ATASC-P et à RAPID de 17 h 36 à 17 h 41 et une recherche a été effectuée à l'aide de son NAS. Les écrans « renseignements sur le contribuable » [*taxpayer information*], « solde du compte » [*account balance*], « débits » [*debits*], « crédits » [*credits*], « montants dus » [*amounts owing*] et « remboursements » [*refunds*]

ont été consultés dans l'ATASC-P. Un écran de demande de renseignements sur les paiements a été consulté dans RAPID.

[31] Là encore, Mme Stockdale a mentionné les rediffusions d'écran de l'EFM pour cette date, qui décrivent les commandes utilisées lors de la recherche. Elle a déclaré que les écrans affichaient des renseignements sur un remboursement que le fonctionnaire avait reçu ou allait recevoir. Elle a déclaré que l'écran de demande de renseignements sur les paiements dans RAPID concernait son formulaire T1 et était lié à ses propres déclarations d'impôt sur le revenu. L'écran indiquait si un paiement était en suspens ou si un remboursement était dû.

[32] Mme Stockdale a déclaré que, d'après les rediffusions d'écran, les commandes saisies pour accéder aux écrans comprenaient le nom d'utilisateur, le mot de passe et le NAS du fonctionnaire. Elle a déclaré que, pour naviguer entre les écrans, le fonctionnaire utilisait des touches de clavier rapide, comme les fonctions F8 et F3. Elle a précisé qu'il était parfois possible de placer le curseur sur un élément et d'appuyer sur la touche « Entrée » pour le visualiser. Elle a déclaré que les renseignements consultés montraient que le fonctionnaire avait un remboursement de 4 884,06 $. L'écran suivant affichait les détails du remboursement, le numéro du chèque et la date d'exécution, c'est-à-dire la date à laquelle le remboursement a été traité.

[33] Mme Stockdale a confirmé que les rediffusions d'écran n'étaient disponibles que pour les alertes du 1er avril et du 15 octobre 2020. Elle a précisé qu'en général, elles ne sont disponibles que pour les écrans visualisés dans RAPID.

[34] Mme Stockdale a déclaré qu'après avoir examiné tous les journaux de vérification et les rediffusions d'écran, son équipe avait préparé une liste de questions pour l'entrevue avec le fonctionnaire, afin de connaître les raisons de ces accès. La liste avait été remise au gestionnaire du fonctionnaire, M. Jones, aux fins de l'entrevue.

[35] M. Jones a mené l'entrevue le 23 octobre 2020, au cours de laquelle le fonctionnaire a fourni quelques explications. Le 27 octobre 2020, il a envoyé des renseignements supplémentaires à M. Jones par courriel.

[36] Mme Stockdale a déclaré que la DAICF avait enquêté sur chacune des explications du fonctionnaire.

[37] Mme Stockdale a remis son rapport d'enquête le 29 décembre 2020. Selon son rapport, le fonctionnaire avait accédé à son compte à cinq reprises et, ce faisant, il avait enfreint le *Code d'intégrité et de conduite professionnelle* (le « Code ») et la *Directive sur l'utilisation des systèmes informatiques et des réseaux électroniques* (la « Directive ») de l'ARC. Le rapport faisait mention de ce qui suit :

> [Traduction]
>
> […]
>
> *Le 23 octobre 2020, lors d'une entrevue par téléconférence menée par James Jones, gestionnaire, centre de contact régional du Québec, BSF de Montréal, en présence d'Andréanne Leblanc (preneuse de notes), conseillère en relations de travail, Division des ressources humaines, et de Suzanne Ehrhardt, représentante syndicale, Syndicat des employé(e)s de l'impôt (SEI), Mohammed Tibilla a déclaré qu'il travaillait pour l'Agence du revenu du Canada (ARC) depuis 2006. Il travaillait comme agent des services aux contribuables et répondait aux appels des contribuables, au cours desquels il effectuait des vérifications de confidentialité à l'aide de l'ATASC-P ou de l'ordinateur central de l'ARC afin de valider l'identité des appelants avant de répondre à leurs questions. Il a déclaré qu'il avait lu et compris le Code d'intégrité et de conduite professionnelle au cours de la dernière année et qu'il savait qu'il n'était autorisé à accéder qu'aux renseignements sur les contribuables dans le cadre de ses fonctions.*
>
> *Interrogé pour savoir s'il avait déjà accédé à son propre compte, Mohammed Tibilla a répondu par l'affirmative. Il a expliqué que, lors de la formation du 15 octobre 2020 sur les gains en capital, animée par Robert Fazio, agent principal des services aux particuliers, centre de contact régional du Québec, BSF de Montréal, Robert Fazio a tenté d'extraire des renseignements sur les gains en capital. Mohammed Tibilla a mentionné qu'il avait demandé à Robert Fazio s'il pouvait utiliser son propre numéro d'assurance sociale (NAS) pour consulter les renseignements relatifs à son propre compte, étant donné qu'il avait déjà vendu un bien qui avait généré un gain en capital. Mohammed Tibilla a déclaré que Robert Fazio avait répondu par l'affirmative.*
>
> *Interrogé sur ses accès à son propre compte les 23 et 24 mars et le 1er avril 2020, Mohammed Tibilla a déclaré qu'il ne se souvenait pas d'avoir effectué ces accès. Il a indiqué que, parfois, lorsqu'il saisissait un NAS et commettait une erreur typographique, il accédait au mauvais compte sans s'en rendre compte. Il a déclaré qu'il était certain de ne pas avoir accédé intentionnellement à son propre compte en mars et avril 2020, et qu'il avait dû le faire par erreur. Il convient de noter que l'examen par la DAICF des accès effectués par Mohammed Tibilla à son propre compte en mars et avril 2020 a révélé plusieurs accès à chacune des dates. Cela*

n'appuie pas l'explication selon laquelle les accès étaient le résultat d'une erreur typographique.

Le 27 octobre 2020, Mohammed Tibilla a envoyé un courriel à la direction dans lequel il déclarait qu'en mars et avril 2020, il avait rencontré un nombre anormalement élevé de problèmes avec les systèmes informatiques, notamment des gels fréquents et l'incapacité d'enregistrer un NAS lorsqu'il était saisi. Il a déclaré que, pour résoudre ces problèmes, il avait contacté le bureau de service des technologies de l'information (TI), et qu'un employé avait pris le contrôle à distance de son poste de travail. Selon lui, les tests de résolution ont été effectués par un employé des TI afin de s'assurer que les systèmes fonctionnaient normalement, et il a indiqué qu'il ne savait pas comment ces tests avaient été effectués. Il a déclaré qu'il croyait qu'il était possible qu'une erreur involontaire ou un incident soit survenu lors de ces tests effectués par l'employé des TI, qui se sont ensuite traduits par des accès effectués par lui. Il a déclaré qu'il croyait que cette explication devait être prise en considération.

Selon l'examen par la DAICF du rapport de billets Remedy pour la période du 1er janvier 2019 au 31 mai 2020, aucun billet de TI concernant les types de problèmes de système décrits par Mohammed Tibilla lors de l'entrevue n'a été créé pour lui les 23 et 24 mars ou le 1er avril 2020, ou autour de ces dates. Il convient également de noter que les employés du bureau de service des TI ne demandent que l'identifiant de l'utilisateur d'un employé (nom d'utilisateur), et non son NAS.

Dans son courriel du 27 octobre 2020, Mohammed Tibilla a également déclaré que le rapport de piste de vérification de ses accès montrait qu'il avait accédé à son compte le 4 avril 2019, ce qui n'avait pas été mentionné lors de l'entrevue du 23 octobre 2020. Il a déclaré qu'il se souvenait qu'à son retour au centre de contact régional du Québec après la vérification, il avait rencontré des problèmes d'accès à l'ordinateur central et avait communiqué avec le bureau de service des TI pour obtenir de l'assistance. Il a déclaré qu'il en avait informé son superviseur et que le problème avait été résolu.

Selon l'examen par la DAICF du rapport de billets Remedy pour la période du 1er janvier 2019 au 31 mai 2020, un billet de TI avait été créé le 2 avril 2019, dans lequel Mohammed Tibilla signalait qu'il n'était pas en mesure de se connecter à Windows. À ce moment-là, l'employé des TI l'a informé qu'il était déjà connecté à un autre compte avec son mot de passe. Par conséquent, après avoir suivi les instructions pour redémarrer son système, le problème était résolu. L'examen a également révélé qu'un billet de TI avait été créé le 4 avril 2019 par le gestionnaire de Mohammed Tibilla, qui avait envoyé une demande de modification de ses accès à l'ordinateur central, car il avait changé de poste de travail. Encore une fois, il convient de noter que les employés du bureau de service des TI ne demandent pas le NAS d'un employé lorsqu'un employé appelle pour obtenir de l'aide; la seule

> *information demandée est le nom d'utilisateur de l'employé. Les renseignements recueillis concernant les billets de TI créés les 2 et 4 avril 2019 ne semblent pas étayer l'explication de la situation donnée par Mohammed Tibilla.*
>
> ***Entrevue avec un témoin – Roberto Fazio***
>
> *Le 30 octobre 2020, lors d'une entrevue par téléconférence avec James Jones, et en présence d'Andréanne Leblanc (preneuse de notes), Roberto Fazio a déclaré que Mohammed Tibilla était présent à la formation relative aux gains en capital le 15 octobre 2020. Interrogé pour savoir si Mohammed Tibilla lui avait demandé s'il pouvait utiliser son propre NAS pour examiner le système, il a répondu par la négative. Robert* [*sic*] *Fazio a déclaré qu'il avait peut-être mal compris la question de Mohammed Tibilla et pensait qu'il avait peut-être demandé s'il pouvait utiliser un NAS, mais il ne se souvenait pas d'avoir eu une conversation avec Mohammed Tibilla au cours de la formation sur l'utilisation de son propre NAS. Cette information est contraire au récit que Mohammed Tibilla a fait de la conversation entre lui et Roberto Fazio.*
>
> *Le Code d'intégrité et de conduite professionnelle prévoit que les employés ne doivent jamais accéder à des renseignements qui ne font pas partie de leurs fonctions et de leur charge de travail officielles, y compris leurs propres renseignements, car il s'agit là d'un exemple d'inconduite grave. Il est strictement interdit d'accéder aux renseignements recueillis par l'Agence, sauf si le travail de l'employé l'exige expressément.*
>
> *La Directive sur l'utilisation des systèmes informatiques et des réseaux électroniques prévoit que les employés ne peuvent accéder aux systèmes et aux réseaux électroniques de l'ARC que dans le cadre de l'exécution de leur charge de travail et de leurs tâches autorisées et assignées. L'annexe D – Exemples d'utilisation inacceptable des systèmes et des réseaux électroniques de l'ARC prévoit que les employés ne sont pas autorisés à accéder à leurs propres renseignements en tant que contribuable ou à ceux de leurs parents ou de leurs connaissances.*
>
> *Les renseignements recueillis au cours de cette enquête ont permis de déterminer que Mohammed Tibilla a enfreint le Code d'intégrité et de conduite professionnelle et la Directive sur l'utilisation des systèmes informatiques et des réseaux électroniques en accédant à son propre compte sans autorisation. Les détails des accès non autorisés figurent à l'annexe 1 – Vue d'ensemble des accès non autorisés et la description des systèmes et des écrans se trouve à l'annexe 2.*
>
> […]

[38] Mme Stockdale a déclaré qu'elle ne jugeait pas l'explication du fonctionnaire crédible. D'après son expérience, les journaux de vérification étaient toujours exacts puisqu'ils étaient établis automatiquement, sans intervention manuelle. Elle a déclaré

que le fait que le fonctionnaire se soit connecté à cinq occasions distinctes ne corroborait pas son explication selon laquelle il aurait pu commettre par accident une erreur typographique. En outre, chaque incident s'est déroulé sur une période prolongée et plusieurs écrans avaient été consultés. S'il s'agissait d'une erreur typographique, il aurait quitté l'écran immédiatement. D'ailleurs, des procédures sont en place pour permettre aux employés de signaler les incidents. Ces accès n'ont pas été signalés à la direction. Tout bien considéré, le fait d'affirmer que ses accès étaient des erreurs ne rendait pas le fonctionnaire crédible.

[39] Mme Stockdale a déclaré que l'affirmation selon laquelle une autre personne aurait utilisé le compte du fonctionnaire n'avait pas été jugée crédible. Il aurait fallu que cette personne connaisse son mot de passe pour chacun des cinq accès sur une période de plus de 18 mois, même si les mots de passe changeaient tous les 90 jours. En ce qui concerne son explication selon laquelle l'agent de soutien des TI aurait pu utiliser son NAS, Mme Stockdale a déclaré que ces agents ne demandent jamais le NAS d'un employé, et ils n'effectuent pas non plus de dépannage dans l'environnement de production en direct.

2. M. Mongrain

[40] M. Mongrain a déclaré qu'à la date de l'audience, il travaillait au bureau de service des TI depuis plus de neuf ans. Le rôle du bureau est d'être le premier point de contact pour tous les problèmes informatiques rencontrés par les employés de l'ARC. En tant que chef d'équipe, il gérait le rendement de ses employés et la qualité du service des appels en veillant au respect de l'ensemble des procédures.

[41] M. Mongrain a déclaré que les données relatives aux appels sont saisies dans Remedy, le logiciel du bureau de service des TI. Une fois entrées, elles ne peuvent pas être modifiées ou supprimées. Au début de chaque appel, l'appelant est invité à fournir son nom d'utilisateur, son nom, son lieu de travail, le bureau où il travaille, son numéro de téléphone et la raison de l'appel. L'agent des TI ne demande jamais de NAS, car il n'en a pas besoin, et Remedy ne comporte aucun champ pour le saisir. Les agents des TI utilisent également un logiciel appelé Vocals qui permet de suivre tous les appels qu'ils reçoivent.

[42] M. Mongrain a déclaré que le bureau de service des TI aide à réinitialiser les mots de passe et qu'il peut fournir des mots de passe temporaires. Lorsqu'un mot de

passe temporaire est utilisé, le système en question demande immédiatement au client de créer un nouveau mot de passe. La procédure consiste à rester avec le client jusqu'à ce qu'il confirme qu'il a changé son mot de passe. Le logiciel gère les mots de passe; les agents des TI n'y ont pas accès. Lorsqu'un agent consulte un écran, le mot de passe lui apparaît toujours chiffré et il ne dispose d'aucun moyen de le déchiffrer.

[43] M. Mongrain a déclaré que, pour accéder aux renseignements sur les contribuables dans l'ordinateur central de l'ARC, un employé doit entrer son nom d'utilisateur et un mot de passe. Si un mot de passe incorrect est saisi, l'utilisateur verra son accès bloqué après trois tentatives infructueuses. Le mot de passe de l'ordinateur central doit être modifié tous les 90 jours, et le même mot de passe ne peut pas être utilisé pour les 24 mots de passe suivants. Les mots de passe doivent comporter huit caractères et inclure des lettres et des chiffres ainsi qu'un caractère spécial. Les seuls caractères spéciaux qui peuvent être utilisés sont le dièse (« # »), l'arobas (« @ ») ou le signe du dollar (« $ »), et ils ne peuvent pas être utilisés comme premier ou dernier caractère du mot de passe.

[44] En ce qui concerne l'accès à RAPID ou à l'ATASC-P, M. Mongrain a déclaré que le bureau de service des TI peut seulement accorder l'accès, mais ne peut pas accéder à ces systèmes. Les agents des TI ne savent pas comment ces systèmes fonctionnent.

[45] M. Mongrain a déclaré qu'il avait vérifié les appels du fonctionnaire au bureau de service des TI.

[46] D'après les dossiers du bureau de service des TI, le fonctionnaire a communiqué avec le bureau le 2 avril 2019 et a parlé à Greg Morris, l'un des agents des TI de M. Mongrain. L'appel a duré de 8 h 40 à 8 h 58.

[47] Selon les dossiers, le fonctionnaire a essayé de se connecter à son ordinateur, sans se rendre compte qu'un autre compte était connecté. Il a déclaré que cela arrivait souvent, lorsque plusieurs employés utilisaient le même ordinateur. Dans une situation où quelqu'un n'a pas fermé sa session, le mot de passe de l'employé suivant ne fonctionnera pas, car celui-ci ne se rendra pas compte qu'il essaie de se connecter à un autre compte. Le bureau de service des TI demande alors à la personne de se déconnecter et de redémarrer l'ordinateur, afin de forcer la fermeture de la session précédente. La procédure consiste à attendre avec le client pendant qu'il redémarre l'ordinateur. Une fois l'opération réussie, l'agent des TI signale dans Remedy que le

problème a été résolu. C'est la procédure qui a été suivie lors de l'appel du fonctionnaire.

[48] Au cours du contre-interrogatoire, M. Mongrain a déclaré qu'une autre façon pour quelqu'un d'autre de se connecter à l'ordinateur d'un employé était lorsqu'un agent des TI devait mettre à jour un logiciel et, pour ce faire, devait se connecter à l'ordinateur du client en utilisant son propre compte. M. Mongrain a mentionné que cela se produit parfois durant la nuit et que le bureau de service des TI demande aux employés de laisser leurs ordinateurs allumés pendant la nuit afin que les mises à jour puissent être envoyées aux ordinateurs. Il a déclaré qu'une trace est laissée sur l'ordinateur si cela se produit.

[49] Interrogé pour savoir si un employé pouvait accéder au compte d'un autre employé, M. Mongrain a répondu que les employés n'ont accès qu'à leur propre compte, selon les exigences de leur poste. Aucun employé n'a accès au compte d'un autre employé. L'accès à un compte se fait à l'aide du nom d'utilisateur et du mot de passe de l'employé. Les accès sont suivis sur la base des noms d'utilisateur. L'accès aux systèmes électroniques de l'ARC est accordé selon le principe du « besoin de savoir » et doit être autorisé par un chef d'équipe ou un gestionnaire, selon le niveau d'approbation requis.

[50] Les dossiers indiquent également qu'un appel a été passé le 5 avril 2019. Le fonctionnaire a parlé avec un autre agent des TI. L'appel a duré de 10 h 14 à 10 h 53. M. Mongrain a déclaré que, d'après son examen du dossier dans Remedy, la configuration du clavier du fonctionnaire ne fonctionnait pas correctement pour une raison inconnue, de sorte que le bureau de service des TI l'a remplacé par le clavier par défaut, et que ce clavier fonctionnait normalement par la suite.

[51] Selon les dossiers, le fonctionnaire a communiqué avec le bureau de service des TI le 26 mars 2020 et a parlé avec un autre agent informatique. M. Mongrain a déclaré que le fonctionnaire avait appelé parce qu'il n'arrivait pas à se connecter à l'ATASC-P; cependant, il a affirmé qu'il s'agissait d'un problème à l'échelle du ministère et que personne n'était en mesure d'accéder à l'ATASC-P à ce moment-là.

[52] M. Mongrain a déclaré qu'il avait extrait les dossiers du 30 mars au 16 août 2019 et que, d'après son examen, rien ne laissait supposer que le compte du fonctionnaire avait été piraté. Il a mentionné que la marche à suivre dans de tels cas consiste d'abord

à désactiver le compte et à demander à l'équipe de sécurité des TI d'entamer une enquête. Si quelque chose semble indiquer la présence d'une anomalie dans le compte, celui-ci est supprimé et un nouveau nom d'utilisateur est attribué.

[53] M. Mongrain a déclaré qu'aucune de ces mesures n'avait été prise à l'égard du fonctionnaire et qu'il n'avait pas non plus connaissance du piratage du compte d'un employé. Il a déclaré que l'ARC gère des renseignements essentiels et que la sécurité de ces renseignements est prise très au sérieux. L'ARC dispose de nombreux pare-feu et d'un des protocoles de mot de passe les plus stricts qu'il connaisse.

[54] Lors du contre-interrogatoire, M. Mongrain a déclaré que son témoignage était basé uniquement sur son examen des dossiers et qu'il n'avait pas discuté de ces appels avec les agents des TI qui avaient créé les dossiers. Il a déclaré que les agents des TI devaient prendre en note tout ce qu'ils faisaient pour résoudre un problème en saisissant l'information dans Remedy. Toutefois, il n'était pas en mesure de confirmer que cela avait été fait. Lorsqu'il a été avisé que le fonctionnaire allait déclarer que M. Morris lui avait dit que son ordinateur avait été mis sur écoute, M. Mongrain a répondu qu'il ne disposait d'aucun renseignement permettant de confirmer ou d'infirmer cette déclaration.

[55] Je souligne que, d'après les documents déposés en preuve, Cédric Roberge a contacté le bureau de service des TI le 30 mars 2019 et a demandé que le compte du fonctionnaire soit modifié et que sa configuration soit mise à jour. M. Roberge était alors le chef d'équipe du fonctionnaire.

3. M. Jones

[56] M. Jones a déclaré qu'il travaillait au sein de l'ARC depuis 1997. Il est devenu gestionnaire du centre de contact régional du Québec en 2020. M. Roberge était l'un de ses chefs d'équipe et, lors des incidents en cause, le fonctionnaire relevait de lui.

[57] M. Jones est devenu le gestionnaire du fonctionnaire pour la première fois en décembre 2019. Il a déclaré que les heures de travail du fonctionnaire étaient de 9 h à 17 h. Il a décrit sa relation avec le fonctionnaire comme étant très cordiale. Il a déclaré que le fonctionnaire avait toujours un grand sourire et qu'il était amical. Il a déclaré qu'avant que les incidents en question ne soient révélés, il n'avait jamais eu de problèmes avec lui.

[58] M. Jones a déclaré que les employés de l'ARC ne sont pas autorisés à se connecter à leurs propres comptes et à les consulter. Lorsque les employés se connectent à l'ordinateur central, trois écrans s'affichent, chacun d'entre eux indiquant que l'accès se fait sur la base du besoin de savoir. Les bureaux du commissaire adjoint et du directeur envoient également des rappels périodiques à cet effet.

[59] M. Jones a déclaré qu'on lui avait demandé d'interroger le fonctionnaire sur les accès non autorisés et qu'on lui avait fourni les questions à poser. L'entrevue a eu lieu le 23 octobre 2020. Comme ils travaillaient à domicile à l'époque, la rencontre a eu lieu par téléphone. Une représentante de l'équipe des relations de travail de l'ARC, Andréanne Leblanc, et une représentante de l'agent négociateur, Suzanne Ehrhardt, ont également participé à l'appel, qui n'a pas été enregistré. Lui et Mme Leblanc ont tous deux posé des questions au fonctionnaire, mais seule Mme Leblanc a pris des notes.

[60] Durant l'entrevue, le fonctionnaire a nié avoir accédé à son compte plus d'une fois, le 15 octobre 2020, dans le cadre d'une formation. Il a dit à M. Jones qu'il avait suivi une formation sur les gains en capital et qu'il avait demandé au formateur s'il pouvait utiliser son compte, étant donné qu'il avait récemment vendu des biens et que le formateur, M. Fazio, lui avait dit qu'il pouvait utiliser son NAS.

[61] M. Jones a déclaré qu'il avait été surpris par cette déclaration, car M. Fazio était l'un des formateurs les plus anciens et les plus compétents dont disposait l'ARC. Il a déclaré qu'il avait du mal à croire que M. Fazio ait pu dire à quelqu'un d'utiliser son NAS.

[62] M. Jones a déclaré qu'il avait envoyé un courriel chiffré au fonctionnaire pendant l'entrevue, pour lui montrer les journaux de vérification du 4 avril 2019, des 23 et 24 mars, du 1er avril et du 15 octobre 2020, et qu'ils les avaient examinés ensemble. Il a déclaré que le fonctionnaire avait reconnu avoir accédé à son compte le 15 octobre 2020, mais qu'il n'avait pas accédé à son compte, ou qu'il n'en avait aucun souvenir, en dehors du 15 octobre. Il avait mentionné qu'il était possible qu'il y ait accédé par accident, par erreur.

[63] Lors du contre-interrogatoire, M. Jones a été informé que le fonctionnaire avait nié avoir reçu une copie chiffrée du journal de vérification. M. Jones a répondu qu'il l'avait envoyée et s'est engagé à trouver une copie de son courriel pour confirmer son affirmation. J'ai été informée que cela a été fait.

[64] Lors du contre-interrogatoire, M. Jones a également été interrogé pour savoir ce qu'il pensait du commentaire du fonctionnaire selon lequel il entrait parfois le mauvais NAS. M. Jones s'est dit perplexe, car il ne comprenait pas comment une personne pouvait accidentellement saisir son NAS. Interrogé pour savoir s'il était possible qu'il ait mal compris l'explication du fonctionnaire et que ce dernier n'ait parlé qu'en termes généraux, M. Jones a répondu qu'il savait ce qu'il lui avait dit. Il convenait qu'il était mathématiquement impossible pour le fonctionnaire de saisir accidentellement son propre NAS.

[65] Le 26 octobre 2020, M. Jones a envoyé par courriel au fonctionnaire les notes d'entrevue préparées par Mme Leblanc. Il a confirmé qu'elles représentaient fidèlement la conversation tenue au cours de l'entrevue. Interrogé lors du contre-interrogatoire pour savoir s'il s'agissait d'une reproduction mot à mot de ce qui avait été dit, M. Jones a répondu que les notes reprenaient 95 % de ce qui avait été dit.

[66] Voici le courriel que M. Jones a envoyé au fonctionnaire :

> [Traduction]
>
> *Veuillez les examiner et, si vous souhaitez y apporter des modifications, envoyez-les-moi dans un courriel chiffré distinct avant le mercredi 28 octobre 2020. Une fois que vous aurez examiné le document, et s'il n'y a pas de modifications, vous devez parapher chaque page avant d'apposer votre signature électronique. Une fois paraphé et signé, renvoyez-moi le document avant la fin de la journée du mercredi 28 octobre 2020.*

[67] M. Jones a mentionné un courriel reçu du fonctionnaire le 27 octobre 2020, dans lequel ce dernier déclarait ce qui suit : [traduction] « Vous trouverez ci-joint les documents paraphés et signés conformément aux instructions. De légères modifications peuvent suivre sur une feuille distincte. » Il a reçu un autre courriel qui contenait des renseignements supplémentaires le 27 octobre 2020.

[68] M. Jones a envoyé les deux documents à son directeur adjoint. Il a ensuite rencontré M. Fazio le 30 octobre 2020 pour lui demander s'il se souvenait d'une conversation avec le fonctionnaire au cours de laquelle il lui avait demandé s'il pouvait utiliser son NAS. M. Fazio a répondu qu'il en doutait, mais que s'il l'avait fait, c'était parce qu'il n'avait pas compris la question.

[69] Mme Leblanc était également présente et a pris des notes de la réunion. M. Jones a confirmé l'exactitude des notes. Lors du contre-interrogatoire, il a déclaré que les notes n'étaient pas textuelles, mais qu'elles étaient aussi fidèles que possible. Il a reconnu que la déclaration selon laquelle M. Fazio doutait d'avoir dit au fonctionnaire qu'il pouvait utiliser son NAS n'était pas consignée dans les notes.

[70] Les notes d'entrevue ont été déposées en preuve. Elles se lisent en partie comme suit :

> [Traduction]
>
> […]
>
> ***JJ :*** *Il a accédé à son propre compte puisqu'il n'avait pas de NAS pour consulter les systèmes. Est-ce qu'il t'a demandé s'il pouvait utiliser son propre NAS? Lui as-tu dit qu'il pouvait le faire?*
>
> ***RFG :*** *Non, je ne lui ai pas dit. Peut-être que je n'avais pas compris la question. Non, si j'avais compris la question, je n'aurais pas dit qu'il pouvait accéder à son propre compte. Si je n'avais pas compris, j'aurais pu dire qu'il pouvait utiliser un NAS.*
>
> […]
>
> ***AL :*** *Robert, te souviens-tu d'une conversation avec M. Tibilla ou d'une question de M. Tibilla concernant un NAS ou l'utilisation de son propre NAS?*
>
> ***RFG :*** *Je ne me souviens d'aucune conversation. J'ai peut-être mal compris ce qu'il a dit et j'ai dit OK. Nous nous penchions sur les NAS. Je n'aurais certainement pas dit oui si j'avais compris qu'il aurait accédé à son propre compte.*
>
> […]

[71] M. Jones a déclaré avoir reçu le rapport d'enquête du 29 décembre 2020 de Mme Stockdale. Il avait ensuite envoyé un courriel au fonctionnaire le 7 janvier 2021, le convoquant à une audience disciplinaire. Le courriel l'informait que l'examen de la piste de vérification avait confirmé qu'il avait accédé à son compte sans autorisation le 4 avril 2019, ainsi que les 23 et 24 mars, le 1er avril et le 15 octobre 2020. Le courriel se lisait comme suit : [traduction] « À ce stade du processus, l'objectif de cette réunion est de recueillir vos commentaires. » Le fonctionnaire était informé qu'une décision serait rendue après l'audience et une copie du rapport d'enquête était jointe au courriel.

[72] M. Jones a déclaré qu'au cours de l'audience disciplinaire, le fonctionnaire continuait à nier avoir accédé à son compte aux quatre premières dates. En ce qui

concerne les accès du 15 octobre 2020, M. Jones a déclaré qu'il avait signalé au fonctionnaire que certains des écrans consultés n'avaient rien à voir avec les gains en capital, mais que le fonctionnaire avait nié les avoir consultés. Il a déclaré que le fonctionnaire avait expliqué que les TI avaient peut-être accédé à son compte.

[73] M. Jones a déclaré qu'il ne jugeait pas crédibles les explications du fonctionnaire. Il a demandé à ce dernier s'il voulait dire que quelqu'un avait obtenu son NAS, son nom d'utilisateur et ses mots de passe, ce à quoi il a répondu que cela avait pu se produire. M. Jones a déclaré que l'affirmation du fonctionnaire selon laquelle les TI auraient pu accéder à ses dossiers par inadvertance ne tenait pas la route, car il n'avait pas contacté le bureau de service des TI à ces dates.

[74] Une copie des notes prises au cours de l'audience disciplinaire a été déposée en preuve. M. Jones a confirmé qu'elles représentaient fidèlement la conversation.

[75] Il a déclaré qu'il avait quitté la réunion avec le sentiment que le fonctionnaire avait été malhonnête et qu'il avait inventé des histoires juste pour se protéger. Il ne pensait pas que le fonctionnaire avait été crédible. Il estimait que le lien de confiance avait été rompu et qu'il ne pouvait plus lui faire confiance. Il avait décidé de s'adresser à son directeur adjoint, car son pouvoir délégué en matière de mesures disciplinaires se limitait à une suspension de 30 jours. M. Jones a déclaré que sa participation à ce processus a pris fin à cette étape. Il avait été informé plus tard de la décision de mettre fin à l'emploi du fonctionnaire.

[76] Au cours du contre-interrogatoire, M. Jones a convenu que, lors des cinq accès non autorisés, aucune modification n'avait été apportée aux dossiers – ils avaient seulement été consultés. Il a déclaré que, si le fonctionnaire lui avait avoué ce qu'il avait fait et s'était excusé, il aurait recommandé une suspension de 30 jours. Il a convenu qu'une telle sanction était conforme à la directive de l'ARC en matière de discipline.

4. M. Fazio

[77] M. Fazio a déclaré qu'en date de l'audience, il travaillait à l'ARC depuis 20 ans. En 2020, il était agent principal des services aux contribuables de groupe et niveau SP-05; il s'agissait d'un poste syndiqué. Son rôle principal était d'aider les agents des

services aux contribuables avec leurs appels et de les former et les encadrer. Il occupait ces fonctions depuis 15 ans.

[78] M. Fazio a qualifié sa relation avec le fonctionnaire [traduction] « d'excellente » et a déclaré qu'ils avaient de très bons rapports. Il a déclaré qu'il aimait bien le fonctionnaire et qu'ils avaient passé de bons moments ensemble. Il a déclaré avoir formé le fonctionnaire à deux reprises et l'avoir encadré une dizaine de fois.

[79] Du 5 octobre au 13 novembre 2019, M. Fazio donnait des formations sur les gains et pertes en capital, les déclarations de fiducies, les revenus locatifs et les déclarations internationales. Le fonctionnaire était l'un des 15 participants. Les cours se déroulaient virtuellement de 9 h à 17 h chaque jour.

[80] M. Fazio a déclaré qu'au début de chaque séance de formation, il avertissait les participants qu'ils verraient des NAS et que s'ils connaissaient le contribuable qui détenait l'un de ces NAS, ils devaient immédiatement l'en informer, afin qu'un autre NAS soit choisi. En effet, ils n'étaient pas autorisés à consulter le NAS et les renseignements fiscaux d'une personne qu'ils connaissaient.

[81] Au cours de cette formation, l'ATASC-P et le système de cas T1 ont été utilisés. RAPID n'a pas été utilisé.

[82] M. Fazio a mentionné que RAPID était plus ancien et qu'il était rarement utilisé depuis que certains renseignements comme les gains en capital en avaient été supprimés. Ce système contenait encore d'anciens renseignements, comme les allocations pour enfants. Il a déclaré qu'il connaissait très bien RAPID puisqu'il l'a utilisé pendant 20 ans. Il a mentionné que les touches de fonction du clavier servaient à naviguer dans RAPID. Il a précisé qu'il n'est pas possible de naviguer sans ces touches, mais que, dans certaines de ses zones, il est possible d'utiliser des clics de souris. Il a précisé que la touche F3 permet de revenir en arrière et que les touches F7 et F8 permettent de passer d'un écran à l'autre. Il a déclaré qu'il n'y avait aucune raison d'utiliser RAPID pour la formation sur les gains en capital.

[83] M. Fazio a été prié de visionner les rediffusions d'écran du fonctionnaire à partir du 15 octobre 2020. Il a affirmé qu'aucun de ces écrans ne concernait les gains en capital. Il a déclaré qu'il n'était en fait pas nécessaire d'accéder à RAPID pour les gains en capital, car ce système ne contenait aucun renseignement de ce type. Il a déclaré

que la touche de fonction G1 qui avait été utilisée permettait à l'utilisateur d'accéder à une liste de remboursements reçus par un contribuable. M. Fazio a déclaré que la fonction suivante qui avait été utilisée dans les rediffusions d'écran montrait que le fonctionnaire consultait des renseignements sur l'état d'un chèque. L'écran indiquait qu'un paiement avait été envoyé le 14 octobre 2019. Il a déclaré qu'aucun de ces renseignements n'était lié à la formation sur les gains en capital.

[84] M. Fazio a déclaré qu'il n'a jamais autorisé un étudiant à accéder à son propre compte parce qu'il n'en a pas le droit. Il a déclaré que ce principe était enseigné dans le cadre de la formation de base des agents. Les systèmes électroniques de l'ARC comportent également des avertissements rappelant aux employés qu'ils ne sont autorisés à y accéder qu'à des fins liées au travail.

[85] Interrogé pour savoir pourquoi il avait permis au fonctionnaire d'utiliser son NAS dans RAPID, M. Fazio a répondu qu'il ne l'avait pas fait et qu'il ne le ferait jamais.

[86] Lors du contre-interrogatoire, M. Fazio a été interrogé pour savoir s'il se souvenait de l'entrevue du 30 octobre 2019 et s'il avait déclaré qu'il était possible qu'il ait autorisé le fonctionnaire à utiliser son NAS, dans le cas où il aurait mal compris la demande du fonctionnaire. Il a répondu qu'il se souvenait d'avoir tenu de tels propos. Il a toutefois ajouté qu'il n'aurait jamais dit que les employés pouvaient accéder au système en utilisant leur propre NAS. Il a ajouté ceci : [traduction] « Mais j'aime bien [le fonctionnaire], nous avons passé de bons moments ensemble. J'ai donc dit que j'avais peut-être mal compris sa question. Beaucoup de gens me posent des questions. »

5. Mme Tourigny

[87] Mme Tourigny a déclaré qu'elle travaillait à l'ARC depuis 1992. Au moment des faits en cause, elle était directrice du Bureau des services fiscaux de Montréal de l'ARC. Sa relation avec le fonctionnaire au moment des faits était strictement professionnelle. Elle n'avait jamais eu de problèmes avec lui auparavant.

[88] Mme Tourigny a déclaré que le système fiscal de l'ARC repose sur les piliers de la confiance, de l'honnêteté et de l'intégrité. Ces valeurs fondamentales sont présentes dans toutes les activités de l'ARC et sont essentielles au maintien de la confiance du public. Leur importance est soulignée dans le Code et dans la Directive.

[89] Mme Tourigny a déclaré que ces documents dictent les comportements exigés des employés. Ils prévoient clairement que les employés de l'ARC doivent faire preuve d'une conduite irréprochable et qu'ils ne peuvent dissimuler aucune inconduite. L'accès aux renseignements sur les contribuables est un privilège, pas un droit. Ces documents donnent des exemples d'inconduite, notamment l'accès d'un employé à ses propres renseignements. Elle a précisé qu'en aucun cas un employé n'est autorisé à consulter son dossier. Les employés reçoivent des rappels à cet égard tous les jours lorsqu'ils se connectent à leur ordinateur. Cela fait également partie de la formation des employés et est répété lors de plusieurs campagnes de sensibilisation annuelles.

[90] Si un employé tente de dissimuler un accès non autorisé, cela crée une situation de méfiance et nuit à la capacité de l'ARC à maintenir la confiance des Canadiens.

[91] Mme Tourigny a déclaré qu'elle a été informée pour la première fois que des accès non autorisés lorsqu'elle a reçu un courriel de la DAICF l'informant de l'enquête. Elle est ensuite intervenue après l'entrevue disciplinaire, car M. Jones n'avait pas le pouvoir de licencier un employé.

[92] Avant de décider de licencier le fonctionnaire, Mme Tourigny a examiné le rapport d'enquête de la DAICF, les journaux de vérification et les rediffusions d'écran, ainsi que les notes de la procédure disciplinaire, les entrevues et les renseignements supplémentaires fournis par le fonctionnaire dans un courriel.

[93] Mme Tourigny a affirmé que la décision de licencier le fonctionnaire a été prise sur la base des faits suivants : allégations non fondées, manque de responsabilité, répétition des accès non autorisés, manque d'honnêteté et rejet de la faute sur les autres. Par conséquent, il a manqué de respect aux valeurs de l'ARC. Elle a déclaré que les agents des services aux contribuables sont le visage de l'ARC, qu'il faut les responsabiliser et qu'ils doivent protéger et renforcer le système fiscal. Ils ne peuvent accéder à un compte que si cela fait partie de leur travail.

[94] Mme Tourigny a déclaré qu'elle a considéré comme des facteurs aggravants aux fins de sa décision le nombre de fois où le fonctionnaire avait accédé à son compte sans autorisation et qu'il avait dissimulé son inconduite, fait des allégations non fondées, manqué de responsabilité et de remords et rejeté la faute sur d'autres personnes. Elle a également tenu compte de la position du fonctionnaire au sein de l'ARC et de l'atteinte réelle ou potentielle à l'intégrité de l'ARC et de son incapacité à la

protéger. Elle a déclaré que la dissimulation de conduite répréhensible constitue la violation la plus grave qu'un employé de l'ARC puisse commettre. Le fonctionnaire a rompu le lien de confiance avec l'ARC. C'est la principale raison pour laquelle elle a décidé de le licencier.

[95] Mme Tourigny a déclaré qu'elle a pris en compte les années de service du fonctionnaire, puisqu'il travaillait pour l'ARC depuis 2006. Mais elle a également tenu compte du nombre de séances de formation qu'il avait reçues et d'avertissements qui lui avaient été donnés pendant cette période.

[96] Mme Tourigny a déclaré qu'elle ne s'est appuyée sur aucune mesure disciplinaire antérieure dont le fonctionnaire avait fait l'objet.

[97] Mme Tourigny a déclaré qu'elle a informé le fonctionnaire de sa décision lors d'une réunion le 18 février 2021. Elle lui a expliqué les raisons de son licenciement et lui a remis la lettre de licenciement signée. Mme Leblanc a pris des notes lors de cette réunion, qui ont été déposées en preuve. Mme Tourigny a confirmé leur exactitude.

[98] Au cours du contre-interrogatoire, Mme Tourigny a déclaré que le journal de vérification montrait que les 23 et 24 mars, le 1er avril et le 15 octobre 2020, le fonctionnaire avait accédé à des renseignements pour l'année « 19MY ». Elle a précisé qu'il s'agissait de renseignements pluriannuels et qu'ils incluaient les gains en capital, les reports à des exercices ultérieurs et antérieurs, ainsi que les pertes ou revenus locatifs.

[99] Toujours lors du contre-interrogatoire, Mme Tourigny s'est vu présenter des renseignements provenant des journaux de vérification qui indiquaient que plus d'un écran était consulté à la fois. Elle a expliqué que cela était dû au fait que tous les agents des services aux contribuables disposaient de deux écrans et travaillaient à partir de ceux-ci, de sorte qu'ils pouvaient les regarder tous les deux en même temps.

B. Pour le fonctionnaire

[100] Le fonctionnaire a déclaré qu'il travaillait pour l'ARC depuis 2006. Il avait obtenu plusieurs contrats à durée déterminée au fil des ans et quelques interruptions de service. Il a obtenu son statut d'employé permanent le 1er novembre 2020.

[101] Le fonctionnaire a fait référence à deux griefs antérieurs. Le premier est daté du 10 juin 2019, dans lequel il se plaignait d'une réprimande écrite datée du 22 mai 2019 pour insubordination les 28 et 29 mars 2019. Le second est daté du 20 décembre 2019, dans lequel il se plaignait de l'évaluation de son rendement pour la période allant du 1er septembre 2018 au 31 mars 2019. Les deux documents ont été déposés en preuve sur consentement. Les parties ont reconnu que je n'étais saisie d'aucun de ces documents. La réprimande écrite avait été réduite à un avertissement verbal, tandis que le grief relatif à l'évaluation du rendement était resté en suspens.

[102] Le fonctionnaire a également déposé en preuve une plainte pour harcèlement psychologique, traitement différentiel et favoritisme datée du 4 avril 2019 (la « plainte pour harcèlement »). La plainte porte sur des incidents survenus sur le lieu de travail entre 2018 et le 29 mars 2019. L'employeur s'est opposé à ce qu'elle soit déposée en preuve, car le grief dont je suis saisie n'allègue aucune discrimination, et la Commission canadienne des droits de la personne (CCDP) n'en a pas été avisée, comme l'exigent les lois auxquelles la Commission des relations de travail et de l'emploi dans le secteur public fédéral (la « Commission ») est assujettie. L'avocat du fonctionnaire a fait valoir que le document servait à illustrer le contexte des incidents survenus juste avant la première violation alléguée, le 4 avril 2019.

[103] J'ai autorisé le dépôt de la plainte pour harcèlement comme preuve de son existence, mais non comme preuve de son contenu, car je n'en suis pas saisie, et le grief n'y fait pas non plus référence. La plainte mettait en évidence les tensions sur le lieu de travail, principalement entre le fonctionnaire et son chef d'équipe à l'époque.

[104] Il convient de souligner que le contrat à durée déterminée du fonctionnaire a pris fin le 31 mars 2019. Les incidents du 29 mars 2019 se sont produits un vendredi, le dernier jour ouvrable de son contrat à durée déterminée. Le lundi 1er avril 2019, il a commencé un nouveau contrat à durée déterminée dans une unité différente et a été placé sous la responsabilité d'un gestionnaire et d'un chef d'équipe différents.

[105] Le fonctionnaire a déclaré qu'à un moment donné, le 29 mars 2019, il s'est rendu aux toilettes. Avant de quitter son poste, il avait fermé sa session, mais n'avait pas éteint son ordinateur. À son retour, on lui a demandé de se rendre dans le bureau de son superviseur. Il a ensuite été conduit à son bureau pour récupérer ses affaires et

on lui a demandé de rentrer chez lui pour le reste de la journée. Il a déclaré que sa cheffe d'équipe avait pris son ordinateur.

[106] Le fonctionnaire a déclaré qu'il pensait que cet incident était lié à son licenciement. Il a déclaré que, lorsque sa cheffe d'équipe a pris son ordinateur, elle ne s'est pas assurée qu'il était éteint, comme elle aurait dû le faire, conformément aux protocoles habituels, afin d'éviter toute compromission. Il a déclaré qu'étant donné qu'il s'agissait du dernier jour de son contrat, certains protocoles auraient dû être suivis. Il a déclaré qu'à la fin de ses contrats précédents, le superviseur s'assurait que toutes les mesures de sécurité étaient en place et que le fonctionnaire avait quitté les systèmes de l'ARC et avait fermé sa session avant de prendre l'ordinateur. Ces protocoles n'avaient pas été suivis le 29 mars 2019.

[107] Le fonctionnaire a déclaré que, le 4 avril 2019, M. Morris du bureau de service des TI l'a informé que son ordinateur avait été piraté. Compte tenu de la proximité des deux incidents et du fait que cela ne lui était jamais arrivé auparavant, il a cru que ce piratage était la source des problèmes qui se sont ensuite produits.

[108] Le fonctionnaire a déclaré que, le 4 avril 2019, il a informé son nouveau superviseur, M. Romanelli, que le bureau de service des TI avait détecté le piratage de son ordinateur. Il a déclaré que M. Romanelli lui avait demandé si le problème avait été résolu, ce à quoi il a répondu par l'affirmative. Il a déclaré qu'il n'avait pas été informé de l'existence d'une enquête à ce sujet par la suite.

[109] Le fonctionnaire a déclaré que, lorsqu'il a été licencié, il travaillait en tant qu'agent de service à la clientèle. Son rôle consistait à recevoir les appels transférés depuis le centre de contact et, le cas échéant, il devait suivre un processus. Il demandait le numéro d'assurance sociale de l'appelant pour accéder à ses renseignements. Après avoir correctement identifié l'appelant, il lui demandait l'objet de l'appel et tentait d'y répondre. La plupart des appels concernaient le formulaire d'impôt T1 et les régimes enregistrés d'épargne-retraite.

[110] Le fonctionnaire a affirmé qu'il n'était pas en mesure de modifier quoi que ce soit dans les systèmes de l'ARC et qu'il ne pouvait que demander une modification et entrer les renseignements fournis par l'appelant. Cela se faisait dans l'ATASC-P. Il a déclaré qu'une fois les renseignements entrés dans l'ATASC-P, ils ne pouvaient plus être modifiés.

[111] Le fonctionnaire a déclaré que, même s'il disposait de deux écrans d'ordinateur lorsqu'il travaillait au bureau, il n'en utilisait qu'un seul. Lorsqu'il a commencé à travailler à domicile en mars 2020, il disposait d'un ordinateur portable et d'un écran d'ordinateur.

[112] En ce qui concerne la navigation dans les systèmes de l'ARC, le fonctionnaire a déclaré que l'ATASC-P était simple et qu'il utilisait un clavier ou une souris. La navigation dans RAPID s'effectue normalement à l'aide de touches de fonction. Il a déclaré qu'il utilisait les flèches vers le haut ou vers le bas pour naviguer d'une page à l'autre. Il a déclaré qu'il n'utilisait pas la touche F7. Il a déclaré qu'il n'utilisait jamais les touches de fonction parce qu'il y en avait beaucoup. Il a déclaré qu'il préférait utiliser les flèches.

[113] Au cours du contre-interrogatoire, interrogé pour savoir s'il était possible que les flèches vers le haut et vers le bas permettent uniquement de se déplacer vers le haut et vers le bas d'une page, mais non de changer de page, le fonctionnaire a répondu qu'il n'avait pas accédé à ce système depuis longtemps et qu'il ne s'en souvenait plus très bien. Il n'utilisait pas vraiment RAPID la plupart du temps, et son témoignage constituait ce dont il se souvenait. Il a déclaré que, la plupart du temps, il se rendait à la page dont il avait besoin et utilisait ensuite la touche de fonction F3 pour la quitter. Il a reconnu qu'il travaillait pour l'ARC depuis 2006 et qu'il utilisait RAPID depuis le début.

[114] Le fonctionnaire a déclaré qu'au moment de parapher les notes d'entrevue qu'il a envoyées à M. Jones, il n'avait pas compris qu'il en acceptait le contenu. Il a déclaré que M. Jones lui avait dit de les signer pour confirmer que toutes les pages avaient été reçues.

[115] Au cours du contre-interrogatoire, le fonctionnaire a reconnu avoir été informé avant et après l'entrevue qu'il pouvait apporter des modifications aux notes d'entrevue et a dit avoir compris. Il a reconnu avoir eu le temps de les examiner, les avoir signées et les avoir renvoyées à M. Jones. Il a déclaré n'avoir pris aucune note pendant l'entrevue et a ajouté que son témoignage était fondé sur ses souvenirs.

[116] Le fonctionnaire a déclaré qu'après avoir lu les notes d'entrevue, il a remarqué que l'incident du 4 avril 2019 avait été ajouté, même s'il n'avait pas été interrogé à ce sujet au cours de l'entrevue. Il a décidé d'envoyer un courriel pour soulever cette

question. Il a déclaré qu'il souhaitait aviser M. Jones du fait que son compte avait été piraté le 4 avril 2019 et que l'ARC devait enquêter à ce sujet. Il a déclaré que son courriel mentionnait que son ordinateur était [traduction] « bourré » [*budded*], mais qu'il voulait dire [traduction] « sur écoute » [*bugged*].

[117] J'ai noté que, lors de son témoignage, le fonctionnaire employait de façon interchangeable les termes [traduction] « sur écoute » et [traduction] « piraté ».

[118] Au cours du contre-interrogatoire, le fonctionnaire a déclaré que le journal de la piste de vérification qui lui avait été remis lors de l'entrevue du 23 octobre 2020 n'était pas le même que celui qui a été déposé en preuve. Il a déclaré qu'il ne se souvenait pas exactement de ce qu'il avait vu, car cela lui avait été montré [traduction] « très rapidement », avant d'être supprimé. Il a déclaré qu'on lui avait demandé de regarder le document, ce qu'il a fait. On lui avait ensuite demandé s'il l'avait regardé. Après avoir répondu par l'affirmative, le document a été supprimé. Il a déclaré qu'il ne pouvait pas décrire en quoi les documents étaient différents de ce qu'il avait vu puisqu'il ne se souvenait de rien à propos de ces documents. Cependant, il savait simplement que c'était différent de ce qu'on lui avait montré le 23 octobre 2020.

[119] En ce qui concerne les notes d'entrevue et les commentaires sur la saisie accidentelle d'un NAS, le fonctionnaire a déclaré qu'il avait parlé en termes généraux parce que la conversation portait sur l'accès au mauvais compte. Il a mentionné qu'il arrivait qu'un NAS soit mal saisi et qu'après avoir réalisé qu'il s'agissait du mauvais dossier, celui-ci était fermé. Il ne faisait pas référence à la saisie accidentelle de son NAS.

[120] Le fonctionnaire a déclaré qu'il connaissait le Code et la Directive et qu'il était interdit à un employé d'accéder à son propre compte. Il a déclaré que c'était la raison pour laquelle il ne l'aurait jamais fait. Il n'aurait jamais accédé à son compte et mis en péril son emploi.

[121] Il a déclaré qu'il n'avait aucune raison de consulter les renseignements sur les allocations pour enfants. Il a ajouté qu'il n'avait pas d'enfant ou de parent qui recevait des allocations. Son enfant était âgé de 39 ans et avait cessé de recevoir des allocations en 1996. Il a déclaré que l'employeur prétendait qu'il avait regardé les allocations pour l'Alberta; pourtant il avait toujours vécu au Québec et il n'avait regardé aucune des allocations qu'on lui reprochait d'avoir consultées.

[122] En ce qui concerne le 15 octobre 2020, le fonctionnaire a déclaré qu'il reconnaissait avoir accédé à son compte à cette date pour les raisons qu'il avait mentionnées. Toutefois, il a déclaré qu'il n'avait pas besoin de regarder l'écran G1, comme il a été prétendu, puisqu'il disposait déjà de tous ces renseignements.

[123] Lors du contre-interrogatoire, le fonctionnaire a reconnu que l'ARC mène plusieurs campagnes pour rappeler aux employés qu'ils ne peuvent accéder aux comptes qu'à des fins professionnelles. Il a reconnu que la confiance, l'honnêteté et l'intégrité sont les piliers de l'ARC et constituent un élément essentiel de la relation employé-employeur. Il a déclaré qu'il comprenait qu'il devait être honnête au travail et, lors de son témoignage, il s'est souvenu d'avoir prêté serment d'agir avec intégrité et honnêteté.

[124] Lors du contre-interrogatoire, le fonctionnaire a reconnu que les déclarations de revenus doivent être transmises à l'ARC avant la fin du mois d'avril de chaque année. Il a également reconnu avoir reçu un chèque de l'ARC en octobre 2020 pour un remboursement qui lui était dû au titre des impôts d'années précédentes. Il a déclaré qu'il n'avait jamais rempli de documents pour recevoir ce montant.

[125] Lors du contre-interrogatoire, le fonctionnaire a déclaré qu'il avait communiqué avec le bureau de service des TI peut-être deux fois en avril 2019. Il n'a pas été en mesure de se souvenir du nombre de fois où il avait communiqué avec les TI en mars 2019. Il a déclaré qu'il se souvenait d'avoir parlé à M. Morris depuis le bureau le 4 avril 2019. Interrogé pour savoir s'il était possible qu'il ait parlé à M. Morris le 2 avril, le fonctionnaire a répondu par la négative, mais il a déclaré qu'il lui avait parlé plusieurs fois.

[126] Le fonctionnaire a déclaré qu'il n'avait pas pris de notes concernant ces appels. Interrogé pour savoir comment il pouvait se souvenir de cette date précise, il a affirmé que c'était parce que la date était importante pour lui et qu'il avait signalé la conversation à son superviseur. Il a déclaré s'être rendu dans le bureau de son superviseur et lui avoir parlé.

[127] Au cours du contre-interrogatoire, le fonctionnaire a déclaré qu'il était convaincu que l'appel avec M. Morris avait eu lieu le 4 avril 2019. Selon ses dires, il ne se souvenait pas de l'appel du 2 avril 2019. Il a ajouté que M. Morris ne lui avait pas dit que son ordinateur était « bourré », mais que c'est ce qu'il avait compris. Il a déclaré

que M. Morris s'est montré surpris et a dit [traduction] « Oh, ton compte est sur écoute! », puis lui a demandé d'éteindre et de redémarrer son système. Ensuite, M. Morris lui a dit que son ordinateur était en bon état. Le fonctionnaire a déclaré qu'il n'en avait pas discuté avec quelqu'un d'autre des TI. Il a déclaré avoir appelé le bureau de service des TI ce jour-là parce qu'il ne pouvait pas accéder aux systèmes de l'ARC.

[128] Au cours du contre-interrogatoire, le fonctionnaire a convenu que son mot de passe était nécessaire pour entrer dans les systèmes de l'ARC. Il a reconnu avoir accédé à son dossier dans l'ATASC-P le 15 octobre 2020. Il a déclaré qu'il se souvenait de l'avoir fait le matin. Il a déclaré qu'il ne se souvenait pas d'avoir accédé au système de cas T1 et a nié avoir accédé à RAPID.

[129] Les notes de l'audience disciplinaire du 13 janvier 2021 ont été montrées au fonctionnaire. Elles indiquent qu'il a reconnu avoir accédé à RAPID, à l'ATASC-P et au système de cas T1 concernant les gains en capital. Interrogé pour savoir s'il était possible que sa mémoire de l'incident soit meilleure à ce moment-là qu'à l'audience disciplinaire, il a déclaré que les notes étaient erronées et qu'il n'avait pas dit à M. Jones qu'il avait accédé à RAPID. Il a déclaré que, pour la formation, l'ATASC-P et le système de cas T1 étaient pertinents, mais qu'il n'y avait rien à consulter dans RAPID.

[130] Le fonctionnaire a déclaré qu'au cours de l'entrevue, il a été interrogé sur le remboursement et a répondu qu'il n'avait pas eu besoin de jeter un coup d'œil dans ce système. Il a convenu qu'il n'y avait aucun lien entre la formation sur les gains en capital et les renseignements contenus dans RAPID. Il a reconnu avoir reçu une copie des notes d'entrevue et avoir eu la possibilité de les modifier, mais ne pas l'avoir fait.

[131] Lors du contre-interrogatoire, interrogé sur l'explication qu'il a donnée selon laquelle les employés des TI auraient pu accéder à son compte par inadvertance, le fonctionnaire a répondu qu'il ne les accusait pas. Il a déclaré qu'il répondait en termes généraux et qu'il disait que quelque chose avait dû se produire et que l'ARC devait enquêter davantage.

[132] Le fonctionnaire a demandé de déposer en preuve un formulaire de la CCDP dûment rempli, dans lequel il alléguait qu'il avait été victime de discrimination fondée sur la race, l'origine nationale ou ethnique et la couleur. Le formulaire fait référence à ce qui s'est passé à partir du 23 octobre 2020, lorsqu'il a été interrogé sur les accès non autorisés à son compte, jusqu'à son licenciement le 18 février 2021. Il a déclaré

avoir déposé le formulaire auprès de la CCDP. L'employeur s'y est opposé au motif qu'il n'est pas daté ni signé et qu'il ne l'avait jamais reçu.

[133] Le 17 mai 2024, le représentant du fonctionnaire s'est engagé à obtenir une version signée et datée du formulaire. Au début de l'audience, le 5 juillet 2024, il a déclaré que la question de savoir si le formulaire avait été déposé restait un mystère. Cependant, il avait l'intention de déposer une plainte. L'employeur a accepté le dépôt en preuve du formulaire pour prouver son existence, mais non son contenu. Je souligne que le fonctionnaire y déclarait ce qui suit :

> [Traduction]
>
> […]
>
> *J'ai accédé à mon compte personnel le 15 octobre 2020 dans une salle de classe à des fins d'apprentissage, avec l'autorisation du formateur de la salle de classe, car il ne trouvait pas de numéro de compte avec les renseignements nécessaires pour faire la démonstration à la classe. Ce fait a été précisé à l'enquêteur et aux observateurs au cours de l'entrevue.*
>
> […]

C. Contre-preuve de l'employeur

1. M. Romanelli

[134] M. Romanelli a déclaré qu'il travaillait pour l'ARC depuis 2004. D'avril à août 2019, il était le chef d'équipe du fonctionnaire. Il a déclaré qu'il entretenait de bonnes relations professionnelles avec le fonctionnaire et qu'il n'avait aucun problème avec lui.

[135] M. Romanelli a déclaré n'avoir jamais discuté avec le fonctionnaire des problèmes informatiques ou du piratage de son compte. Il a déclaré n'avoir jamais entendu parler d'un employé dont le compte avait été piraté au cours des 20 années qu'il a passées à l'ARC.

[136] Au cours du contre-interrogatoire, M. Romanelli a admis qu'il ne se souvenait pas de toutes les conversations qu'il avait eues avec le fonctionnaire en 2019.

[137] En réinterrogatoire, M. Romanelli a déclaré qu'il était certain de n'avoir jamais abordé la question du piratage du compte du fonctionnaire, car il s'agirait d'un problème grave qui aurait été signalé à la direction et aurait nécessité une enquête. Il a

mentionné qu'il se serait souvenu d'une conversation de cette importance, car il s'agissait d'un problème de sécurité majeur. Si le fonctionnaire lui avait parlé d'un problème avec sa souris, ou d'un problème similaire, cela aurait été quelque chose de mineur dont il ne se serait pas souvenu, mais le piratage d'un compte constituait un problème de sécurité majeur dont on se souviendrait pendant des années.

III. Analyse et motifs

[138] Pour parvenir à une décision, il convient tout d'abord de savoir si l'employeur a établi l'existence d'une inconduite justifiant la prise d'une mesure disciplinaire à l'encontre du fonctionnaire. Dans l'affirmative, je dois ensuite déterminer si la décision de mettre fin à son emploi était une réponse excessive dans les circonstances et s'il convient d'y substituer une autre mesure corrective (voir *Wm. Scott & Company Ltd. v. Canadian Food and Allied Workers Union, Local P-162*, [1977] 1 Can. L.R.B.R. 1).

[139] Il incombait à l'employeur d'établir les faits selon la prépondérance des probabilités à l'aide d'une preuve claire et convaincante (voir *F.H. c. McDougall*, 2008 CSC 53, aux par. 46 à 49).

[140] Le fonctionnaire ayant nié toute conduite répréhensible, l'affaire repose entièrement sur la crédibilité. Je me suis appuyée sur l'approche suivante, souvent citée, dans *Faryna c. Chorny*, 1951 CanLII 252 (BC CA) à la p. 357, pour évaluer la crédibilité des témoignages qui m'ont été présentés :

> *La crédibilité des témoins intéressés, en particulier dans le cas où des divergences interviennent entre les témoignages, ne saurait être évaluée uniquement à l'aune du comportement personnel du témoin en question, lequel comportement emporterait la conviction qu'il dit vrai. Le critère consiste à soumettre son récit des faits à un examen raisonnable afin d'en vérifier la cohérence avec les probabilités qui entourent les circonstances existantes. En bref, le véritable critère pour vérifier la véracité du récit d'un témoin dans un tel cas doit être sa concordance avec la prépondérance des probabilités qu'une personne douée du sens pratique et bien informée tiendrait facilement pour raisonnables dans les circonstances* […]

[141] Le fonctionnaire a aussi invoqué les décisions *Turmel c. Conseil du Trésor (Service correctionnel du Canada)*, 2009 CRTFP 122; *Syndicat québécois des employées et employés de service, section locale 298 (FTQ) c. Centre d'hébergement Saint-Vincent-Marie (Mireille Davilmar)*, 2016 QCTA 396; et *Syndicat des employés de métier de la*

Buanderie centrale de Montréal (CSN) c. Buanderie Centrale de Montréal, 2024 CanLII 18619 (QC SAT) qui soutiennent toutes essentiellement la même affirmation.

A. Y a-t-il eu une conduite qui a donné lieu à des mesures disciplinaires?

[142] Selon la lettre de licenciement de l'employeur, le fonctionnaire aurait accédé à son compte sans autorisation le 4 avril 2019, ainsi que les 23 et 24 mars, le 1er avril et le 15 octobre 2020, et il aurait enfreint le Code et la Directive. Comme facteurs aggravants, la lettre s'appuyait sur le fait que les accès non autorisés avaient été répétés plusieurs fois sur une période de 18 mois, qu'à trois reprises différentes le fonctionnaire avait tenté de dissimuler son inconduite et de tromper l'employeur, et qu'il n'avait manifesté aucun remords ou compréhension de la gravité de son inconduite.

[143] Après avoir soigneusement évalué la preuve, j'estime que l'employeur a établi qu'il avait des motifs suffisants pour imposer une mesure disciplinaire au fonctionnaire. Voici mes motifs.

1. Les accès non autorisés

[144] Mme Stockdale a déclaré avoir été avisée des accès non autorisés lorsqu'elle a reçu des alertes générées par le système. Elle a expliqué que des alertes sont générées automatiquement lorsque certaines règles ne sont pas respectées. En l'espèce, la violation concernait l'accès par un employé à son propre compte, ce que le Code et la Directive interdisent. Le fonctionnaire n'a pas contesté ce fait. Il a reconnu que cette pratique était interdite et qu'il était au courant de cette règle tout au long de la période en cause.

[145] Ces alertes ont amené la DAICF à vérifier le compte du fonctionnaire. La vérification a révélé que son compte avait été consulté à cinq reprises à l'aide de son nom d'utilisateur et de son NAS. Un journal de vérification corroborant ces renseignements a été déposé en preuve.

[146] Le fonctionnaire a reconnu avoir accédé à son compte le 15 octobre 2020. Il a cependant nié avoir accédé à tous les écrans figurant dans le journal de vérification ou l'avoir fait à l'heure indiquée.

[147] Pour donner raison au fonctionnaire, il faudrait que je tire les conclusions suivantes : les journaux de vérification de l'ARC ont été falsifiés pour en modifier le contenu, l'EFM a généré des rapports erronés, ou quelqu'un d'autre s'est connecté aux systèmes de l'ARC en utilisant le nom d'utilisateur et le NAS du fonctionnaire le même jour. Aucune de ces conclusions n'est étayée par la preuve.

[148] Selon le fonctionnaire, le 15 octobre 2020, M. Fazio lui aurait donné la permission d'accéder à son compte pendant la formation sur les gains en capital à laquelle il participait. Il a affirmé avoir accédé à son compte au cours de la matinée, et non à 17 h 36, comme l'indique le journal de vérification. J'estime que son récit manque de crédibilité pour les motifs suivants.

[149] Premièrement, M. Fazio a nié avoir donné cette autorisation ou avoir eu une conversation avec le fonctionnaire à ce sujet. S'il est vrai qu'il a déclaré qu'il avait peut-être mal compris la question du fonctionnaire, je suis d'avis que ce commentaire était motivé par sa relation avec le fonctionnaire. En effet, il a déclaré qu'il avait encadré le fonctionnaire une dizaine de fois et qu'il l'appréciait. Cependant, il a déclaré très clairement qu'il n'aurait jamais autorisé un tel accès.

[150] Deuxièmement, l'entrevue avec M. Fazio a eu lieu le 30 octobre 2020, soit à une date proche de celle de la prétendue conversation. Il est donc probable que la mémoire du fonctionnaire était encore relativement fraîche. Si M. Fazio avait eu une conversation avec le fonctionnaire ressemblant à une demande d'accès au système de l'ARC à l'aide d'un NAS, il est probable qu'il s'en serait souvenu.

[151] Troisièmement, M. Fazio a confirmé que les écrans consultés, comme l'indique le journal de vérification, n'avaient rien à voir avec la formation sur les gains en capital. Cela milite en faveur du fait que les accès ont été effectués pour des raisons personnelles et non aux fins de formation, comme l'a prétendu le fonctionnaire.

[152] Quatrièmement, la formation a eu lieu entre 9 h et 17 h, et le journal de vérification indique que l'accès a été effectué à 17 h 35. Cela contredit directement l'allégation du fonctionnaire selon laquelle il a accédé aux écrans au cours de la matinée, dans le cadre de la formation.

[153] Cinquièmement, le fonctionnaire avait un motif pour accéder à son compte le 15 octobre 2020, car il s'attendait à un remboursement important de la part de l'ARC.

En effet, l'un des écrans consultés montrait qu'un chèque de 4 884,06 $ avait été créé la veille. Il était donc sur le point de le recevoir.

[154] Sixièmement, le fonctionnaire a affirmé avoir accédé à son compte au cours de la matinée. Cependant, aucun journal de vérification ne vient étayer cette affirmation. Cela milite en faveur du fait qu'il a effectué l'accès d'une manière contraire à ce qu'il prétendait.

[155] Septièmement, l'accès faisait partie d'un comportement habituel car, comme l'indiquent les journaux de vérification, il avait accédé à son compte quatre fois auparavant.

[156] Huitièmement, toutes les personnes impliquées dans l'enquête sur les accès non autorisés avaient de bonnes relations de travail avec le fonctionnaire ou ne le connaissaient pas. Personne n'avait donc de raison de falsifier le journal de vérification.

[157] Neuvièmement, l'accès aux renseignements contenus dans le journal de vérification nécessitait le nom d'utilisateur et le mot de passe du fonctionnaire, ainsi que son NAS. Il était le seul à connaître son mot de passe. Cela milite fortement en faveur de son accès aux systèmes de l'ARC, comme l'indique le journal de vérification.

[158] À la lumière de l'ensemble de la preuve, je conclus que le récit du fonctionnaire sur l'incident du 15 octobre 2020 n'est tout simplement pas crédible. Comme il est énoncé dans l'arrêt *Faryna*, le critère pour vérifier la véracité du récit d'un témoin doit être sa concordance avec la prépondérance des probabilités qu'une personne douée du sens pratique et bien informée tiendrait facilement pour raisonnables dans les circonstances. En l'espèce, les éléments de preuve étayent de manière indiscutable la conclusion selon laquelle le fonctionnaire a accédé à son compte le 15 octobre 2020, comme le montre le journal de vérification.

[159] Je conclus en outre que l'employeur a fourni un témoignage clair, logique et convaincant selon lequel le fonctionnaire avait également accédé à son propre compte le 4 avril 2019, ainsi que les 23 et 24 mars et le 1er avril 2020. Je tire cette conclusion pour les motifs exposés ci-après.

[160] Mme Stockdale a déclaré que le journal de vérification indiquait que le nom d'utilisateur et le NAS du fonctionnaire avaient été utilisés pour accéder à plusieurs

systèmes de l'ARC contenant des renseignements sur les contribuables. Le journal de vérification a été déposé en preuve et a corroboré l'accès aux comptes du fonctionnaire aux quatre dates concernées. Elle a déclaré qu'au cours de ses années d'expérience, les journaux de vérification n'ont jamais fourni de faux renseignements.

[161] Mme Stockdale et M. Mongrain ont tous deux déclaré que, pour accéder au compte du fonctionnaire, comme le montrent les journaux de vérification, quelqu'un devait d'abord entrer le nom d'utilisateur et le mot de passe du fonctionnaire. Celui-ci était le seul à connaître le mot de passe, qui n'était pas accessible autrement. Le mot de passe changeait tous les 90 jours, et le même mot de passe ne pouvait pas être utilisé lors des 24 changements de mot de passe suivants. Étant donné que les accès non autorisés se sont produits sur une période de 18 mois, cela signifie forcément que son mot de passe a changé plusieurs fois au cours de cette période. Le fonctionnaire n'a contesté aucun de ces renseignements. Il n'a pas non plus déclaré avoir divulgué son mot de passe à qui que ce soit.

[162] Comme il a été mentionné précédemment, le fardeau de la preuve incombait à l'employeur. J'estime que les faits mentionnés dans les deux derniers paragraphes constituent à eux seuls une preuve convaincante selon laquelle le fonctionnaire a accédé à son propre compte aux quatre dates susmentionnées. Toutefois, avant de rendre une décision finale, il est nécessaire d'examiner attentivement tous les éléments de preuve restants et d'évaluer la crédibilité du récit des faits présentés par le fonctionnaire.

[163] Le fonctionnaire a résolument nié avoir accédé à son compte le 4 avril 2019, ainsi que les 23 et 24 mars et le 1er avril 2020. Il a fait valoir que son compte avait été piraté le 4 avril 2019, date du premier accès non autorisé, ce qui pourrait être à l'origine de tous les autres accès non autorisés. Plus précisément, il a affirmé que le fait que son chef d'équipe ait pris son ordinateur le 29 mars 2019 étayait sa théorie selon laquelle son ordinateur avait été compromis de telle sorte que tous les accès ultérieurs étaient liés à cet incident. Il a affirmé que, le 4 avril 2019, il avait téléphoné au bureau de service des TI parce qu'il ne parvenait pas à ouvrir une session dans son ordinateur. Il a affirmé avoir parlé à M. Morris, qui l'a informé que son ordinateur avait été piraté. Il a affirmé en avoir ensuite parlé à son chef d'équipe, M. Romanelli. Il a affirmé que la proximité de ces deux incidents augmentait la probabilité que son compte ait été compromis lorsque son ordinateur a été saisi le 29 mars 2019.

[164] Pour les motifs qui suivent, je conclus que le récit du fonctionnaire n'est pas crédible.

[165] Tout d'abord, en ce qui concerne l'incident au cours duquel le chef d'équipe avait pris l'ordinateur du fonctionnaire le 29 mars 2019, celui-ci a déclaré que juste avant, il avait fermé sa session, mais n'avait pas complètement éteint son ordinateur avant de se rendre aux toilettes. Lorsqu'il était revenu, son chef d'équipe avait pris son ordinateur, mais ne l'avait pas éteint correctement, comme c'était habituellement le cas lorsque ses contrats temporaires prenaient fin. Il a laissé entendre que son chef d'équipe, avec lequel il entretenait une relation tendue, ou quelqu'un d'autre avait pu s'emparer de son ordinateur et le compromettre de manière à pouvoir se connecter ultérieurement à ses comptes.

[166] Je note que ces incidents sont survenus un vendredi et qu'il s'agissait du dernier jour de travail du contrat temporaire du fonctionnaire qui devait se terminer le 31 mars 2019, un dimanche. De son propre aveu, à la fin de chacun de ses contrats temporaires, son chef d'équipe prenait son ordinateur. Ainsi, j'estime que le fait que son chef d'équipe ait pris son ordinateur le 29 mars 2019 n'était pas inhabituel, mais faisait plutôt partie d'un protocole normal de fin de contrat. En outre, pour que son chef d'équipe ou toute autre personne puisse se connecter à son compte, immédiatement ou ultérieurement, ils auraient eu besoin des mots de passe du fonctionnaire. Mme Stockdale et M. Mongrain ont tous deux déclaré que des mots de passe étaient nécessaires pour se connecter aux systèmes de l'ARC. Le fonctionnaire n'a pas déclaré qu'il les avait divulgués. Ces éléments de preuve militent en faveur de l'argument selon lequel personne ne s'est connecté ultérieurement à son compte.

[167] Le fonctionnaire allègue que le 4 avril 2019, il a téléphoné au bureau de service des TI, car il ne parvenait pas à se connecter à son compte sur son ordinateur. Il a déclaré avoir parlé à l'agent des TI, M. Morris, qui lui a dit que son ordinateur avait été piraté. Il a déclaré que M. Morris lui avait alors demandé d'éteindre son ordinateur afin de le redémarrer et qu'il lui avait ensuite dit que son ordinateur était en bon état.

[168] Aucune preuve ne corrobore cette prétention. Mme Stockdale et M. Mongrain ont tous deux déclaré que tous les appels au bureau de service des TI sont enregistrés. Les agents des TI sont tenus d'enregistrer les renseignements relatifs à un appel dans Remedy. En outre, Vocals crée automatiquement un journal de tous les appels passés

au bureau de service des TI, qu'ils aient été répondus ou abandonnés. Des copies de ces journaux ont été déposées en preuve. D'après celles-ci, le fonctionnaire n'a pas téléphoné au bureau de service des TI le 4 avril 2019.

[169] Lors de la procédure d'arbitrage, le fonctionnaire a insisté sur le fait que l'appel au bureau de service des TI avait eu lieu le 4 avril 2019 et non le 2 avril 2019. Cependant, cette croyance était basée uniquement sur sa mémoire et ne correspondait pas à son courriel du 27 octobre 2020, dans lequel il déclarait se souvenir très précisément que l'incident s'était produit [traduction] « à peu près à la même époque ». L'exactitude de sa mémoire a aussi été remise en question par le fait qu'il avait déclaré n'avoir pris aucune note de l'appel et que son témoignage a eu lieu environ cinq ans après les faits.

[170] Bien qu'il n'existe aucune trace d'un appel téléphonique le 4 avril 2019, les dossiers des TI indiquent que le fonctionnaire a communiqué avec le bureau de service des TI les 2 et 5 avril 2019. Aucun des deux appels ne concernait l'écoute ou le piratage de son ordinateur.

[171] L'appel du 2 avril 2019 semblait correspondre à la description qu'en fait le fonctionnaire, puisqu'il concernait l'impossibilité d'ouvrir une session dans son ordinateur. M. Morris avait pris l'appel.

[172] M. Mongrain a déclaré qu'il ne s'agissait pas d'un type d'appel inhabituel. Il a expliqué que cela se produisait lorsqu'un utilisateur ouvrait une session sur l'ordinateur d'un autre employé et oubliait de se déconnecter. Il a précisé qu'une telle situation pouvait se produire lorsqu'un agent des TI devait effectuer une mise à jour du système pour un utilisateur. Je souligne que le fonctionnaire avait commencé un nouveau contrat temporaire dans un lieu de travail différent le 1er avril 2019, et que le 30 mars 2019, son superviseur de l'époque avait demandé que le compte du fonctionnaire soit modifié. Il s'agit là d'une explication plausible du problème rencontré par le fonctionnaire le 2 avril 2019.

[173] Plus convaincant encore, M. Mongrain a déclaré qu'un ordinateur mis sur écoute ou piraté constitue une situation extrêmement grave pour l'ARC, et qu'il aurait été nécessaire d'acheminer le problème à un niveau d'intervention supérieur au sein de sa direction générale et de mener une enquête. Compte tenu de la gravité du problème, j'estime qu'il est hautement improbable que M. Morris ait simplement demandé au

fonctionnaire de redémarrer son ordinateur pour le réparer, qu'il n'ait rien fait d'autre et qu'il n'ait rien consigné.

[174] Le fonctionnaire a également déclaré qu'il avait signalé à son superviseur, M. Romanelli, que son ordinateur avait été piraté. M. Romanelli a catégoriquement contredit le récit du fonctionnaire. Il a confirmé qu'il était le chef d'équipe du fonctionnaire en avril 2019. Cependant, il a fermement nié que celui-ci lui ait dit que son ordinateur avait été mis sur écoute ou piraté. Il a déclaré qu'il s'agirait d'un problème très grave et qu'il s'en souviendrait si cela s'était produit. Il a déclaré qu'en 20 ans à l'ARC, il n'avait jamais entendu parler du piratage de l'ordinateur d'un employé.

[175] Tous ces éléments de preuve militent fortement en faveur de la fausseté du récit du fonctionnaire.

[176] Le fonctionnaire a fait valoir que les allégations n'avaient pas de sens puisqu'il n'avait aucune raison de consulter les renseignements de son compte de l'ARC. J'estime que les éléments de preuve indiquaient le contraire. Tout comme il existait des éléments de preuve selon lesquels il avait des raisons de consulter les renseignements sur le remboursement le 15 octobre 2020, tous les autres accès ont eu lieu entre la fin mars et le début avril – soit à la période où il devait produire sa déclaration de revenus. Encore une fois, cela fournissait une explication plausible de sa motivation à consulter son compte de l'ARC.

[177] Le fonctionnaire a également fait valoir qu'il n'était pas possible qu'il ait consulté les écrans mentionnés dans certains des journaux RAPID puisqu'il n'avait pas utilisé les touches de fonction F7 et F8 qui avaient été identifiées dans les rediffusions d'écran. M. Fazio a déclaré que RAPID était très ancien et qu'il fallait utiliser les touches de fonction pour y naviguer. Le fonctionnaire a déclaré avoir utilisé la touche de fonction F3. Il a également reconnu avoir fondé son témoignage sur ce dont il se souvenait, mais que cela faisait un certain temps qu'il n'avait pas utilisé RAPID. Compte tenu de tous les autres éléments de preuve, j'estime qu'il est plus probable que le contraire que le fonctionnaire ait commis une erreur lorsqu'il a affirmé ne pas avoir utilisé F7 et F8.

[178] Le fonctionnaire a également tenté de faire valoir qu'il n'était pas possible qu'il ait consulté plusieurs écrans à la fois, puisqu'il n'en utilisait qu'un seul, même s'il en

avait deux à sa disposition. Compte tenu de la preuve accablante, j'estime que cette explication est peu crédible.

[179] Pour en revenir à l'arrêt *Faryna*, le récit d'un témoin doit concorder avec la prépondérance des probabilités qu'une personne douée du sens pratique et bien informée tiendrait facilement pour raisonnables dans les circonstances. Le récit du fonctionnaire n'y parvient pas. J'estime que les éléments de preuve militent fortement en faveur d'une conclusion selon laquelle il a accédé à son compte le 4 avril 2019, ainsi que les 23 et 24 mars et le 1er avril 2020, comme indiqué dans le journal de vérification.

2. Facteurs aggravants

[180] Outre les accès non autorisés, la lettre de licenciement de l'employeur invoquait également plusieurs facteurs aggravants :

- les accès non autorisés sont survenus plusieurs fois sur une période de 18 mois;
- le fonctionnaire a tenté à trois reprises de dissimuler sa faute et de tromper l'employeur;
- son absence de remords ou de compréhension de la gravité de son inconduite.

[181] Je vais maintenant examiner chaque facteur.

a. Inconduite répétée

[182] Pour les motifs susmentionnés, je conclus que le fonctionnaire a accédé à son compte, comme l'indiquent les journaux de vérification. Cette inconduite répétée a eu lieu à cinq reprises sur une période de 18 mois. Il a déclaré qu'au cours de cette période, il savait qu'il lui était interdit d'accéder à son propre compte. Pourtant, comme la preuve l'a établi, il l'a quand même fait. Il est possible qu'il se soit laissé porter par un faux sentiment de sécurité en pensant qu'il ne se ferait pas prendre puisque rien ne s'était passé avant octobre 2020. Cependant, cela n'enlève rien au fait qu'il était conscient chaque fois qu'il ne devait pas le faire.

[183] Le fait que les incidents se soient déroulés sur une période de 18 mois signifie également que le fonctionnaire a continué à recevoir des rappels de l'employeur pendant cette période pour lui signifier que ce comportement n'était pas autorisé. Il a quand même décidé de le faire à cinq reprises.

b. Dissimulation et tromperie

[184] M. Jones a déclaré avoir rencontré le fonctionnaire pour la première fois le 23 octobre 2020 pour discuter des accès non autorisés. Au cours de cette rencontre, le fonctionnaire a nié avoir accédé à son compte le 4 avril 2019, ainsi que les 23 et 24 mars et le 1er avril 2020. Il a reconnu avoir accédé à son compte le 15 octobre 2020, mais a précisé que c'était dans le cadre d'une formation et qu'il avait reçu l'autorisation de son formateur.

[185] Le fonctionnaire a reçu une copie des notes d'entrevue et a eu la possibilité d'y apporter des modifications. Il n'en a pas fait. Il a toutefois envoyé un autre courriel le 27 octobre 2020, qui contenait des explications supplémentaires. Dans ces documents, il mentionnait avoir rencontré de nombreux problèmes informatiques au cours de la période pertinente, ce qui l'avait obligé à fournir un accès à distance au bureau de service des TI pour les résoudre. Il a laissé entendre qu'il était possible qu'un agent des TI ait pu accéder à son ordinateur. Il a également affirmé qu'un agent des TI lui avait dit que son compte avait été piraté.

[186] Mme Stockdale a déclaré que chaque explication avait fait l'objet d'une enquête. M. Jones a déclaré que le fonctionnaire avait reçu une copie du rapport d'enquête de Mme Stockdale et qu'il avait été invité à assister à une audience disciplinaire pour discuter des conclusions du rapport. Lors de cette audience, le fonctionnaire a maintenu qu'il n'avait pas accédé à son compte les quatre premières fois mais qu'il avait reçu l'autorisation de le faire le 15 octobre 2020. Il a soutenu qu'en avril 2019, il avait été informé que son ordinateur avait été piraté.

[187] Le fonctionnaire a déclaré qu'il avait reçu une copie des notes de l'audience disciplinaire et qu'il avait eu la possibilité d'y apporter des modifications. Il n'en a pas fait.

[188] Lors de l'audience d'arbitrage, le fonctionnaire a témoigné en son nom. Il a eu l'occasion de rectifier les faits. Il a choisi de ne pas le faire. Comme l'a déclaré son représentant, le fonctionnaire a maintenu le même récit.

[189] J'ai déjà abordé en détail les raisons pour lesquelles j'ai conclu que le fonctionnaire avait accédé à son propre compte aux cinq occasions indiquées dans les

journaux de vérification et les raisons pour lesquelles son récit des faits du 15 octobre 2020 et du piratage en avril 2019 n'est pas crédible.

[190] En ce qui concerne l'affirmation du fonctionnaire selon laquelle un agent des TI aurait pu accéder à son compte par inadvertance après avoir accédé à son ordinateur à distance, je souligne qu'aucun des accès n'a eu lieu à une date à laquelle le fonctionnaire a téléphoné au bureau de service des TI. En outre, M. Mongrain a déclaré que les agents des TI n'ont pas accès aux mots de passe des employés et ne demandent pas de NAS. Cette explication n'est donc pas plausible.

[191] Compte tenu de l'ensemble de la preuve, je conclus que l'employeur a établi que le fonctionnaire a tenté à trois reprises de dissimuler son inconduite et de le tromper.

c. Absence de remords

[192] Il n'est pas contesté que le fonctionnaire a toujours refusé d'admettre qu'il s'était livré à une conduite répréhensible. Par conséquent, il n'y a aucune preuve de remords.

[193] En conséquence de tout ce qui vient d'être dit, je conclus que tous les facteurs aggravants invoqués par l'employeur ont été établis, comme il l'alléguait.

[194] Étant donné que j'ai conclu que le fonctionnaire a sciemment accédé à son compte sans autorisation à cinq reprises sur une période de 18 mois, qu'il a tenté à plusieurs reprises de dissimuler les accès après les avoir découverts, qu'il a induit l'employeur en erreur et qu'il a refusé de reconnaître sa conduite répréhensible ou de faire preuve de remords, il est tout à fait clair que sa conduite justifiait une mesure disciplinaire.

B. Le licenciement était-il excessif dans les circonstances?

[195] Je conclus que le licenciement n'était pas excessif dans les circonstances, pour les motifs qui suivent.

[196] Mme Tourigny a déclaré que le fait que le fonctionnaire ait accédé à son compte à cinq reprises sur une longue période illustre qu'il ne s'agissait pas d'incidents spontanés. Elle a ajouté que s'il avait reconnu avoir effectué les accès non autorisés lorsqu'il avait été confronté pour la première fois, il n'aurait probablement reçu qu'une suspension de 30 jours. Cependant, étant donné le comportement du fonctionnaire

une fois les accès révélés, elle a changé d'avis. Elle a déclaré que l'absence de remords, le refus d'admettre toute conduite répréhensible et les tentatives de dissimuler la vérité et d'orienter l'enquête l'ont amenée à conclure que le lien de confiance avait été irrémédiablement rompu.

[197] Le fonctionnaire a fait valoir à titre d'argument subsidiaire que, si je devais conclure qu'il avait accédé à son compte de manière inappropriée, je devrais considérer comme facteurs atténuants le fait qu'il n'avait consulté que ses renseignements et non ceux d'un tiers et qu'il n'y avait pas eu d'effet négatif sur l'employeur puisque les incidents étaient restés au sein de l'ARC. En outre, le fait qu'il soit au courant des alertes rend peu probable qu'il récidive. Enfin, à l'exception d'un chef d'équipe, il avait de bonnes relations avec les autres et n'était pas un employé problématique.

[198] Malheureusement pour le fonctionnaire, aucun de ces facteurs atténuants ne l'emporte sur la gravité des circonstances aggravantes. La confiance est au cœur de la relation employé-employeur, surtout si l'employé a accès à des renseignements très sensibles et personnels sur les contribuables.

[199] Les passages suivants de la décision *Campbell c. Agence du revenu du Canada*, 2016 CRTEFP 66, résument bien l'importance du lien de confiance dans le contexte de l'ARC :

> […]
>
> ***49*** *Je rejette l'argument voulant que le long bilan de bons services du fonctionnaire devrait constituer un facteur atténuant. Qui plus est, ses nombreuses années de service devraient être considérées comme un facteur aggravant. On lui avait offert des douzaines d'auxiliaires didactiques et d'aide-mémoire, ainsi que de l'appui conjoint de la part de l'employeur et de l'agent négociateur pour veiller à ce qu'il comprenne bien le code de conduite et s'y conforme. Un employé de longue date devrait être plus sensibilisé à son milieu de travail et, par conséquent, plus digne de la confiance de l'employeur.*
>
> ***50*** *Finalement, le fonctionnaire n'a exprimé aucun remords démontrant qu'il comprend le préjudice potentiel que son inconduite pouvait causer à son employeur. Il a d'emblée reconnu qu'il savait que ce qu'il faisait constituait une violation de son code de conduite, mais il a choisi de récidiver à de nombreuses reprises. Il a déclaré qu'il souhaitait ne pas avoir commis les actes d'inconduite, mais j'ai interprété ce commentaire au sens où il regrette d'avoir perdu son indemnité de départ, plutôt que comme*

> *un regret à l'égard de ce qu'il a fait à son employeur. À ce titre, je dois rejeter le grief.*
>
> ***51*** *Agir autrement et autoriser la réintégration du fonctionnaire, et d'autres fonctionnaires ayant agi ainsi, aurait nécessairement pour effet d'augmenter le risque d'inconduite de la part d'un employé qui comprend parfaitement que ce qu'il a fait est répréhensible, mais qui, pour ses propres motifs, décide de commettre régulièrement des actes d'inconduite contre son employeur. Le fonctionnaire n'a démontré aucune compréhension du préjudice potentiel pour le système fiscal canadien que sa décision d'ignorer le code de conduite de l'employeur pouvait occasionner.*
>
> ***52*** *Il ne s'agit pas d'un cas où des mesures disciplinaires progressives justifieraient une mesure disciplinaire moindre, afin de favoriser la réintégration de l'employé. Pour les motifs énoncés ci-dessus, un préjudice irréparable a été porté au lien de confiance sous-jacent aux relations employeur-employé par suite de la décision du fonctionnaire d'ignorer le code de conduite de l'employeur, et ce, à répétition.*
>
> […]

[200] Bien que les faits dans l'affaire *Campbell* ne soient pas les mêmes qu'en l'espèce, je suis d'avis qu'il convient de tirer les mêmes conclusions. Le fonctionnaire était un employé de longue date et avait reçu à plusieurs reprises des rappels du Code et de la Directive. Il aurait donc dû être mieux informé. Contrairement à l'affaire *Campbell*, le fonctionnaire en l'espèce a refusé de reconnaître toute conduite répréhensible ou d'assumer la responsabilité de ses actes. Il est d'ailleurs révélateur qu'il n'ait pas été en mesure de me citer un seul cas dans lequel un employé a refusé d'admettre sa conduite répréhensible et a néanmoins été réintégré. Il m'a renvoyé aux cinq décisions suivantes dans lesquelles des sanctions disciplinaires moins sévères ont été substituées ou envisagées.

[201] Dans l'affaire *Nova Scotia (Public Service Commission) v. NSGEU (Hillier)* (2013), 238 L.A.C. (4 th) 62, la fonctionnaire avait été licenciée pour avoir accédé de manière inappropriée à des renseignements relatifs au service à la clientèle à des fins non professionnelles. Elle n'avait pas contesté qu'il existait une cause juste et suffisante pour imposer une mesure disciplinaire, mais elle avait fait valoir que le licenciement était excessif dans les circonstances. Bien que la fonctionnaire ait manqué de franchise lorsqu'elle avait été confrontée pour la première fois à la violation, la discussion s'était déroulée dans un cadre décontracté et elle a avoué son inconduite immédiatement dans les 24 heures qui ont suivi. Elle s'est excusée, a fourni des documents expliquant

à l'employeur ses actions et a coopéré pendant l'enquête. Compte tenu de ces faits, l'arbitre était d'avis que la relation de travail n'avait pas subi de dommage irréparable au point de ne pas pouvoir être rétablie. Dans ce contexte, l'arbitre a conclu que le licenciement était excessif.

[202] Dans l'affaire *Eastern Regional Integrated Health Authority v. NAPE (O. (L.))* (2015), 259 L.A.C. (4 th) 188, la fonctionnaire travaillait dans un hôpital et avait été suspendue pour avoir accédé sans autorisation à des dossiers de patients. Elle avait consulté ses dossiers et ceux de son père comme outil de formation pour ses collègues et un médecin. Elle a reconnu sa conduite répréhensible.

[203] De même, dans l'affaire *Newfoundland and Labrador Nurses' Union v. Eastern Regional Integrated Health Authority*, 2014 CanLII 83846 (NL LA), une fonctionnaire a été licenciée pour avoir accédé à des renseignements sans autorisation. Une fois de plus, la fonctionnaire a reconnu sa conduite répréhensible.

[204] Dans l'affaire *Mercer c. Administrateur général (ministère des Ressources humaines et du Développement des compétences)*, 2016 CRTEFP 11, un fonctionnaire a été licencié pour avoir accordé un traitement préférentiel à des membres de sa famille dans le cadre de ses fonctions. Bien que le fonctionnaire ait pleinement coopéré à l'enquête, il avait nié avoir eu une conduite répréhensible au motif qu'il n'en avait pas conscience. L'ancienne Commission a refusé de réduire la sanction disciplinaire et a noté que le fonctionnaire n'avait manifesté aucun remords pour ses actes et avait tenté à plusieurs reprises de se décharger de sa responsabilité en rejetant la faute sur son employeur, prétextant son ignorance ou en faisant allusion à d'autres personnes qui auraient agi de la même manière.

[205] Dans l'affaire *Peel (Regional Municipality) v. CUPE, Local 966 (Trotman)* (2016), 273 L.A.C. (4 th) 117, la fonctionnaire était une agente chargée du traitement des cas et a été licenciée après avoir accédé au dossier de sa fille. Dans cette affaire, il s'agissait de savoir si son action avait permis à sa fille de recevoir un paiement. Bien que la fonctionnaire n'ait pas été tout à fait sincère lorsqu'elle a été confrontée à la situation, elle a reconnu par la suite avoir consulté les renseignements. Mais elle a nié avoir déclenché le paiement. L'arbitre lui a donné raison, a réintégré la fonctionnaire et a remplacé la sanction par une suspension de cinq jours.

[206] Je tire de toute cette jurisprudence l'importance d'admettre une faute, d'en accepter la responsabilité, de faire preuve de remords et de coopérer à une enquête. La confiance étant à la base de la relation employeur-employé, je vois mal comment le fonctionnaire pourrait être réintégré en l'absence d'une telle preuve. Le lien de confiance ne peut être rétabli sans preuve de remords.

[207] L'ARC se voit confier les renseignements les plus personnels et les plus sensibles concernant les contribuables. Elle doit agir en cas de violation, car la confiance du public en dépend. S'il est vrai que le fonctionnaire n'a consulté que son compte et qu'il n'en a sans doute tiré que peu d'avantages, cela n'enlève rien au fait qu'il a agi de la sorte en contravention au Code et à la Directive et qu'il l'a quand même fait à plusieurs reprises.

[208] Si l'on ajoute à cela les dommages causés par son refus d'admettre la conduite répréhensible, les tentatives de dissimulation, la fabrication de récits pour éviter toute responsabilité et l'absence de tout remords, je conclus que le licenciement était justifié.

[209] Pour ces motifs, la Commission rend l'ordonnance qui suit :

(L'ordonnance apparaît à la page suivante)

IV. Ordonnance

[210] Le grief est rejeté.

Le 10 juin 2025.

Audrey Lizotte,
une formation de la Commission
des relations de travail et de l'emploi
dans le secteur public fédéral