

employés autorisent la vérification de leurs antécédents criminels, leur dossier de crédit et autres informations personnelles, Le processus de vérification forcera aussi les employées et employés à fournir leurs empreintes digitales sur demande.

Par cette politique, la Société exigera de toutes les employées et employés qu'ils acceptent de se soumettre à ce processus, sous peine de sanctions disciplinaires ou administratives pouvant aller jusqu'à leur congédiement.

Le STTP soutient que cette politique contrevient aux dispositions de la convention collective, qu'elle cause préjudice aux employées et employés et est injuste et inéquitable à leur endroit. De plus, le STTP considère que cette politique porte illégalement atteinte à la liberté et à la vie privée des employées et employés.»

[2] Le grief demandait alors l'émission d'une ordonnance intérimaire aux termes des articles 987 et suivants de la convention collective. Le 26 avril 2013, l'arbitre Kenneth P. Swan émettait une telle ordonnance :

«I therefore order that the Corporation cease and desist from implementing the «Practice Regarding Security Clearance of Personnel» to the extent that it involves reliability checks on current employees...»

Cette ordonnance a été reconduite par la suite.

[3] Le «*redressement demandé par décision finale*» se lisait comme suit dans le grief du 11 avril 2013 :

«Le STTP demande par ailleurs que, par décision finale, l'arbitre :

a) Déclare que la «Pratique en matière d'enquête de sécurité sur le personnel» de la Société est illégale parce que portant atteinte à la liberté et à la vie privée

des employées et employés et parce qu'elle leur cause préjudice et est injuste et inéquitable à leur endroit et, qu'à ce titre, elle viole les dispositions de la convention collective, de la Charte canadienne des droits et libertés et de toute autre loi pertinente.

- b) Ordonne à la Société de cesser d'exiger des employées et employés qu'ils autorisent la vérification de leurs antécédents criminels, leur dossier de crédit et autres informations personnelles et soient tenus de fournir leurs empreintes digitales à la Société ou à ses représentants.*
- c) Ordonne à la Société de ne pas chercher, de quelque façon que ce soit, à s'immiscer dans la vie privée des employées et employés.*
- d) Ordonne à la Société de cesser d'imposer des mesures administratives ou disciplinaires ou autres représailles aux employées et employés ayant refusé d'autoriser la vérification de leurs antécédents criminels, leur dossier de crédit et autres informations personnelles, notamment en refusant de fournir leurs empreintes digitales à la Société ou à ses représentants.*
- e) Ordonne à la Société de procéder à la destruction des informations détenues illégalement par elle ou ses représentants en application de la «Pratique en matière d'enquête de sécurité sur le personnel».*
- f) Ordonne à la Société de s'assurer de la destruction desdites informations qui auront été transmises à des tiers dans le cadre de l'application de la «Pratique en matière d'enquête de sécurité sur le personnel»*

Le STTP se réserve le droit de demander tout redressement additionnel».

[4] Conformément à une partie de l'ordonnance de l'arbitre Swan, aux termes de l'article 9.96 de la convention collective, l'arbitre soussigné a été choisi par les parties pour entendre la présente affaire au fond.

[5] Une première audition a été tenue à Ottawa le 9 octobre 2013. L'enquête s'est continuée aux dates suivantes :

23 octobre 2013

25 octobre 2013

21 novembre 2013

04 décembre 2013

17 avril 2014

15 mai 2014

02 juillet 2014

Les procureurs au dossier ont convenu de soumettre leurs argumentaires pour le 27 août 2014 en vue des auditions prévues pour les 9 et 10 septembre 2014.

La Preuve

[6] Au début de la première journée d'enquête, une fois déposés la convention collective, le grief du 11 avril 2013 et la décision de l'arbitre Swan, et une fois consenties les admissions d'usage (procédure et compétence), les parties ont versé au dossier, de consentement, la version du 30 mai 2013, de cette «*Pratique relative à l'enquête de sécurité sur le personnel*». Vu que ce document est au cœur du litige entre les parties, je crois qu'il est opportun de le reproduire intégralement aux quatorze pages qui suivent. (C'est le document qui a été transmis, à cette date du 30 mai 2013, par Madame Shannon Hurst, gestionnaire, Relations du travail, à Madame Rona Eckert, permanente syndicale nationale, STTP.)

Pratique de Postes Canada

1. Énoncé de la pratique

Postes Canada doit s'assurer que les personnes qui ont accès au courrier, aux renseignements de l'entreprise et à ses biens sont fiables, dignes de confiance et ont une cote de fiabilité/cote de sécurité valide en fonction des exigences liées à leurs tâches et à leur poste. Les enquêtes de sécurité s'inscrivent dans le processus pour conserver la confiance de nos clients en assurant la sécurité du courrier, en maintenant un milieu de travail sûr pour tous les employés et en sélectionnant un effectif de qualité.

2. Portée

L'objet de la présente pratique est de décrire les processus d'enquête de sécurité de Postes Canada utilisés pour les employés actuels et tous les candidats à un poste.

La pratique vise les Ressources humaines, les Services de sécurité et d'enquête (SSE) et les titulaires de procédé dans leurs fonctions à titre de responsables de l'embauche, les employés actuels ainsi que toute personne qui fait une demande d'emploi ou désire conserver son emploi au sein de Postes Canada. La pratique régit l'ensemble des activités liées aux enquêtes de sécurité du personnel et aux cotes de sécurité. La présente pratique complète les pratiques d'embauche et les pratiques relatives à la sécurité en milieu de travail de Postes Canada.

3. Définitions

Enquête de sécurité – Procédé lié à l'utilisation de vérifications normalisées pour obtenir des renseignements sur une personne. Ainsi, une évaluation des risques et un degré d'assurance permettront de déterminer si une personne peut obtenir ou non une cote de fiabilité ou une cote de sécurité.

Vérification de fiabilité - Type d'enquête de sécurité minimale requise pour toutes les personnes engagées par Postes Canada. Pour les candidats externes, l'enquête de sécurité exige une vérification des données personnelles, y compris les attestations d'études, les titres et les antécédents professionnels ainsi que les références. Pour toutes les enquêtes de sécurité, une vérification du casier judiciaire est requise et, dans certains cas, une vérification des empreintes digitales, une vérification de solvabilité et une entrevue sont requises.

Vérification de sécurité - Type d'enquête qui s'impose lorsque les fonctions ou les tâches liées à un poste exigent l'accès à des renseignements ou à des biens classifiés. La personne qui se voit accorder une cote de sécurité peut accéder, lorsqu'elle justifie son besoin de savoir, à des renseignements et à des biens dont la classification va jusqu'au niveau d'autorisation accordé. La cote de fiabilité est préalable à l'obtention d'une cote de sécurité, mais une évaluation effectuée par le Service canadien du renseignement de sécurité s'avère aussi nécessaire.

Vérification du casier judiciaire - Type de recherche par nom et date de naissance effectué pour déterminer si la personne en question a un casier judiciaire. La vérification est effectuée dans le répertoire national des casiers judiciaires tenu par la Gendarmerie royale du Canada (GRC).

4. Autres détails relatifs à la pratique

Un processus d'enquête de sécurité cohérent et respectueux des droits individuels. Pour les candidats externes, l'enquête de sécurité exige une vérification des données personnelles, y compris les attestations d'études, les titres et les antécédents professionnels ainsi que les références. Pour toutes les enquêtes, la vérification du casier judiciaire est requise et, dans certains cas, la vérification des empreintes digitales, une vérification de la solvabilité et une entrevue peuvent être nécessaires. Il est essentiel d'obtenir le consentement de la personne pour mener l'enquête. L'utilisation du formulaire de consentement à l'enquête de sécurité approprié pour les tâches spécifiques permet d'assurer l'uniformité du procédé dans toute la Société et le respect de la *Loi sur la protection des renseignements personnels*.

Établissement du niveau d'enquête de sécurité pour un poste. L'enquête de sécurité préalable à l'emploi pour l'obtention d'au moins une cote de fiabilité est une condition d'emploi et est essentielle au processus d'embauche. Le niveau de cote pertinent doit être maintenu pendant toute la durée d'emploi. Si l'employé n'est pas en mesure de maintenir le niveau de la cote exigée pour son poste, il se peut qu'il soit congédié. Avant de déterminer le niveau d'enquête de sécurité requis, il faut évaluer la classification des renseignements et des biens auxquels l'employé devra avoir accès pour l'exécution de ses fonctions. Le niveau exigé doit toujours correspondre au classement le plus élevé de renseignements et de biens que l'employé utilisera pour exécuter les tâches habituelles de son poste. La cote de fiabilité est le niveau de sécurité minimale que doit avoir une personne avant sa nomination à Postes Canada. Les personnes qui ont besoin d'avoir accès à des biens et à des renseignements classifiés doivent avoir une cote de fiabilité valide pour ensuite obtenir une cote de sécurité du niveau pertinent. Les renseignements classifiés peuvent exiger une cote de sécurité de niveau Secret ou Très secret.

Communication aux demandeurs du niveau d'enquête de sécurité exigée pour le poste. Le niveau d'enquête de sécurité requis pour la plupart des postes à Postes Canada est une cote de fiabilité. Lorsqu'un niveau d'enquête de sécurité plus élevé est requis en raison du poste ou de la nature des tâches, les RH ou les responsables de l'embauche en aviseront les candidats.

Obtention du consentement écrit du candidat avant d'entreprendre une vérification. Chaque candidat doit signer les formulaires pertinents afin d'autoriser Postes Canada à effectuer les vérifications nécessaires.

Exécution des vérifications de base concernant la fiabilité des candidats ou des évaluations de sécurité des candidats. Les vérifications de base suivantes doivent être menées dans le cadre de l'évaluation de la fiabilité pour les candidats :

- confirmation de l'identité d'une personne, grâce à la vérification des données personnelles (y compris la date de naissance, l'adresse, le pays de naissance et la date d'arrivée au Canada, le cas échéant), à l'aide de deux pièces d'identité canadiennes acceptables (dont l'une avec photo);
- vérification des renseignements pertinents sur les études, les emplois, les titres et les antécédents professionnels, y compris l'évaluation de la fiabilité, en vérifiant auprès d'anciens employeurs et des personnes mentionnées comme références (conformément aux lignes directrices établies par les Ressources humaines);
- exécution d'une vérification du casier judiciaire, au minimum;
- au besoin, vérification des empreintes digitales afin de confirmer l'existence possible d'un casier judiciaire. La vérification des empreintes digitales est obligatoire dans le cadre de la vérification au niveau de la cote de fiabilité à titre d'exigence préalable à une cote de sécurité.

Exécution des premières vérifications de fiabilité ou des évaluations de sécurité des employés actuels. Les vérifications de base suivantes doivent être menées dans le cadre de l'évaluation de la fiabilité pour les employés actuels :

- exécution d'une vérification du casier judiciaire, au minimum;
- au besoin, vérification des empreintes digitales afin de confirmer l'existence possible d'un casier judiciaire. La vérification des empreintes digitales est obligatoire dans le cadre de la vérification au niveau « cote de fiabilité » à titre d'exigence préalable à une cote de sécurité.

Exécution de vérifications supplémentaires, le cas échéant, à l'appui de la vérification de fiabilité. En sus des vérifications de base, le titulaire de pratique peut effectuer d'autres vérifications requises en raison de la nature délicate des renseignements ou des biens auxquels la personne devra avoir accès et des exigences de sécurité de postes semblables. Il pourrait ainsi être nécessaire d'effectuer les vérifications suivantes :

- Une vérification de la solvabilité si les tâches du poste l'exigent ou si l'individu a un casier judiciaire qui pourrait laisser croire à une faiblesse en matière de transactions financières. La vérification de la solvabilité peut également être effectuée lorsque les autres tentatives d'obtention de renseignements suffisants sont peu fructueuses, ou lorsque nécessaire pour un autre motif valable. La vérification de la solvabilité est

Établissement du niveau d'enquête de sécurité pour un poste. L'enquête de sécurité préalable à l'emploi pour l'obtention d'au moins une cote de fiabilité est une condition d'emploi et est essentielle au processus d'embauche. Le niveau de cote pertinent doit être maintenu pendant toute la durée d'emploi. Si l'employé n'est pas en mesure de maintenir le niveau de la cote exigée pour son poste, il se peut qu'il soit congédié. Avant de déterminer le niveau d'enquête de sécurité requis, il faut évaluer la classification des renseignements et des biens auxquels l'employé devra avoir accès pour l'exécution de ses fonctions. Le niveau exigé doit toujours correspondre au classement le plus élevé de renseignements et de biens que l'employé utilisera pour exécuter les tâches habituelles de son poste. La cote de fiabilité est le niveau de sécurité minimale que doit avoir une personne avant sa nomination à Postes Canada. Les personnes qui ont besoin d'avoir accès à des biens et à des renseignements classifiés doivent avoir une cote de fiabilité valide pour ensuite obtenir une cote de sécurité du niveau pertinent. Les renseignements classifiés peuvent exiger une cote de sécurité de niveau Secret ou Très secret.

Communication aux demandeurs du niveau d'enquête de sécurité exigée pour le poste. Le niveau d'enquête de sécurité requis pour la plupart des postes à Postes Canada est une cote de fiabilité. Lorsqu'un niveau d'enquête de sécurité plus élevé est requis en raison du poste ou de la nature des tâches, les RH ou les responsables de l'embauche en aviseront les candidats.

Obtention du consentement écrit du candidat avant d'entreprendre une vérification. Chaque candidat doit signer les formulaires pertinents afin d'autoriser Postes Canada à effectuer les vérifications nécessaires.

Exécution des vérifications de base concernant la fiabilité des candidats ou des évaluations de sécurité des candidats. Les vérifications de base suivantes doivent être menées dans le cadre de l'évaluation de la fiabilité pour les candidats :

- confirmation de l'identité d'une personne, grâce à la vérification des données personnelles (y compris la date de naissance, l'adresse, le pays de naissance et la date d'arrivée au Canada, le cas échéant), à l'aide de deux pièces d'identité canadiennes acceptables (dont l'une avec photo);
- vérification des renseignements pertinents sur les études, les emplois, les titres et les antécédents professionnels, y compris l'évaluation de la fiabilité, en vérifiant auprès d'anciens employeurs et des personnes mentionnées comme références (conformément aux lignes directrices établies par les Ressources humaines);
- exécution d'une vérification du casier judiciaire, au minimum;
- au besoin, vérification des empreintes digitales afin de confirmer l'existence possible d'un casier judiciaire. La vérification des empreintes digitales est obligatoire dans le cadre de la vérification au niveau de la cote de fiabilité à titre d'exigence préalable à une cote de sécurité.

Exécution des premières vérifications de fiabilité ou des évaluations de sécurité des employés actuels. Les vérifications de base suivantes doivent être menées dans le cadre de l'évaluation de la fiabilité pour les employés actuels :

- exécution d'une vérification du casier judiciaire, au minimum;
- au besoin, vérification des empreintes digitales afin de confirmer l'existence possible d'un casier judiciaire. La vérification des empreintes digitales est obligatoire dans le cadre de la vérification au niveau « cote de fiabilité » à titre d'exigence préalable à une cote de sécurité.

Exécution de vérifications supplémentaires, le cas échéant, à l'appui de la vérification de fiabilité. En sus des vérifications de base, le titulaire de pratique peut effectuer d'autres vérifications requises en raison de la nature délicate des renseignements ou des biens auxquels la personne devra avoir accès et des exigences de sécurité de postes semblables. Il pourrait ainsi être nécessaire d'effectuer les vérifications suivantes :

- Une vérification de la solvabilité si les tâches du poste l'exigent ou si l'individu a un casier judiciaire qui pourrait laisser croire à une faiblesse en matière de transactions financières. La vérification de la solvabilité peut également être effectuée lorsque les autres tentatives d'obtention de renseignements suffisants sont peu fructueuses, ou lorsque nécessaire pour un autre motif valable. La vérification de la solvabilité est

Pratique de Postes Canada

obligatoire dans certains cas, notamment dans le cas d'une vérification de fiabilité à titre d'exigence préalable à une cote de sécurité.

- Une entrevue avec la personne afin de clarifier des imprécisions ou des contradictions, de combler les lacunes dans les renseignements vérifiables ou pour tout autre motif valable.

À mesure que la Société poursuit l'amélioration de ses activités, il faut reconnaître que les services fournis par Postes Canada aux entreprises et aux consommateurs canadiens nous placent dans une situation de confiance et exigent un haut niveau de responsabilité. La vérification de sécurité est un élément essentiel de notre capacité à respecter nos obligations en matière de conformité et nous permet de maintenir la confiance de nos clients. Les exigences en matière d'enquête de sécurité peuvent faire l'objet de changements en fonction des modifications apportées aux tâches, aux ententes contractuelles, aux lois ou aux autres obligations.

à faire en
plan!

Suivi à l'égard de renseignements défavorables ou manquants repérés au cours de l'enquête de sécurité.

Dans certains cas, les responsables de la sécurité du personnel peuvent noter des renseignements défavorables ou ne peuvent confirmer des renseignements nécessaires afin de prendre une décision favorable à l'égard de la vérification de fiabilité. Toutes les personnes doivent être traitées de façon juste et équitable, et il faut leur donner l'occasion d'expliquer tout point défavorable avant qu'une décision soit prise. En voici quelques exemples :

- L'existence d'un casier judiciaire ne constitue pas forcément un motif de refus de l'approbation d'une cote de fiabilité. Les responsables de la sécurité du personnel peuvent interviewer la personne afin d'obtenir des renseignements supplémentaires pour l'examen. Voici des éléments à prendre en considération lors de l'examen d'un casier judiciaire :
 - la gravité de l'infraction;
 - le lien entre l'infraction et les tâches du poste à effectuer;
 - s'il y a récidive;
 - les dates des infractions et le temps écoulé depuis l'infraction;
 - si les infractions ont été déclarées sur le formulaire de consentement.
- Un mauvais dossier de solvabilité ne constitue pas forcément un motif de refus de l'approbation d'une cote de fiabilité. Les responsables de la sécurité du personnel doivent évaluer l'incidence des renseignements défavorables en tenant compte du contexte dans lequel la personne exécuterait les tâches du poste ainsi que les circonstances atténuantes. Les renseignements sur la solvabilité n'étant pas toujours exacts ou à jour, les responsables de la sécurité du personnel donneront l'occasion à la personne d'expliquer la situation.

Si la cote de fiabilité est accordée à titre d'exigence préalable à l'obtention d'une cote de sécurité, les responsables de la sécurité du personnel demanderont au Service canadien du renseignement de sécurité (SCRS) une évaluation de la cote de sécurité. Les responsables de la sécurité du personnel accorderont ou refuseront l'approbation de la cote de sécurité à la lumière des résultats des enquêtes de sécurité et de l'évaluation faite par le SCRS.

Les RH et le responsable de l'embauche effectuent l'embauche seulement lorsque toutes les vérifications préalables sont terminées et que la cote de fiabilité est accordée. Les lettres d'offre ne doivent pas être remises avant que la cote de fiabilité ne soit accordée. Pour les postes qui nécessitent une cote de sécurité, il est possible de remettre une lettre d'offre d'emploi conditionnelle puisque le processus pour obtenir une cote de sécurité peut prendre des mois. L'accès aux renseignements ou aux biens classifiés doit être limité jusqu'à ce que la personne se voit accorder une cote de sécurité du niveau pertinent.

Les responsables de la sécurité du personnel consignent la décision d'accorder la cote de fiabilité dans le formulaire pertinent et permettent aux Ressources humaines d'inclure la lettre d'offre du candidat. Les formulaires signés, accompagnés du formulaire de déclaration relatif au courrier, doivent être retournés aux RH

Pratique de Postes Canada

avant la date de début d'emploi. Lorsqu'une cote de sécurité est accordée, les responsables de la sécurité du personnel établiront le profil de sécurité et s'assureront que les formulaires pertinents sont dûment remplis.

Obtention de l'approbation du directeur général, Services de sécurité et d'enquête, l'agent de sécurité de l'entreprise ou de son délégué pour les cas particuliers. Dans des circonstances particulières, le directeur général, Services de sécurité et d'enquête, et l'agent de sécurité de l'entreprise (ASE) ou son délégué peut accorder à une personne l'accès à des renseignements de nature délicate avant l'exécution de toutes les vérifications nécessaires à l'appui de la procédure pertinente d'enquête de sécurité pour la cote de fiabilité ou la cote de sécurité. Cette autorisation ne doit être accordée qu'en de très rares cas, et uniquement comme mesure d'urgence, temporaire et pour un accès restreint (par exemple, pour la fermeture d'un bureau de poste en raison de l'incapacité d'exécuter le recrutement à un bureau de l'ACMPA). Le vice-président, Ressources humaines, ou son délégué auprès de l'agent de sécurité de l'entreprise ou le délégué de celui-ci, fournira la justification à l'appui de ces demandes.

Préparation en vue d'enquêtes de sécurité hors de la procédure d'embauche. Afin d'assurer le maintien de la fiabilité des personnes, une mise à jour régulière des enquêtes de sécurité doit être effectuée. Les questions liées à l'enquête de sécurité doivent être réglées et signalées aux responsables de la sécurité du personnel lorsque les exigences d'un poste en matière de sécurité sont modifiées. Lorsque des renseignements partagés ou appris pourraient remettre en question la capacité d'un individu de détenir une cote de fiabilité ou une autorisation de sécurité valide, un examen de la cause pourrait s'avérer nécessaire. La cote de fiabilité ou les cotes de sécurité doivent être annulées lorsque l'employé refuse de participer au procédé. Ce refus fera en sorte que l'employé ne sera plus qualifié pour ce poste et peut entraîner des mesures disciplinaires pouvant aller jusqu'au congédiement.

5. Rôles et responsabilités

Les employés doivent :

- respecter les exigences minimales en matière de vérifications de sécurité relatives à leur poste;
- signaler aux responsables de la sécurité du personnel tout changement de sa situation (p. ex. accusations ou condamnations criminelles) par courriel à l'adresse suivante : personnel.securite@postescanada.ca.

Les chefs d'équipe et les responsables de l'embauche doivent :

- consulter la Pratique commerciale relative à la classification de l'information afin de s'assurer que toutes les personnes qui ont accès à des renseignements ou à des biens détiennent la cote de fiabilité ou la cote de sécurité appropriée pour travailler avec ces données ou ces biens. (Les renseignements et biens de catégorie Protégés A et B et C exigent une cote de fiabilité, soit le niveau de la cote de sécurité que doivent détenir tous les employés au moment de leur embauche et qu'ils sont tenus de conserver);
- s'il y a lieu, examiner le formulaire de consentement pour en assurer l'exactitude et le caractère complet, puis vérifier l'identité des candidats externes;
- signaler aux responsables de la sécurité du personnel les incidents ou les situations qui pourraient avoir des répercussions sur le niveau de la cote du personnel ou poser un risque pour l'entreprise ou l'image de la marque de Postes Canada. De temps à autre, les chefs d'équipe peuvent prendre connaissance de renseignements concernant des employés actuels, des agents et des entrepreneurs qui ont été accusés ou reconnus coupables d'un acte criminel ou qui ont été incarcérés. Même si l'infraction ou l'incident a eu lieu à l'extérieur du milieu de travail, il est essentiel que ces renseignements soient communiqués au personnel chargé de la sécurité. À la soumission des renseignements à l'adresse personnel.securite@postescanada.ca, il faut inclure les détails suivants :
 - nom de l'employé ou de l'entrepreneur;
 - matricule de l'employé, le cas échéant;
 - poste, rôle ou titre actuel;
 - nom et adresse de l'installation postale;
 - bref résumé;
 - pièces jointes : inclure des documents de soutien (articles de journaux, relevés, notes, etc.);
 - coordonnées du chef d'équipe.

Les Ressources humaines – agents de dotation doivent :

- assurer la conformité aux processus d'enquête de sécurité, à la *Politique sur la sécurité du gouvernement* et à la *Loi sur la protection des renseignements personnels*;
- consulter les autorités d'embauche au sujet des exigences pertinentes à l'égard des enquêtes sur les employés et candidats;
- s'assurer que les candidats sont informés de la procédure d'enquête de sécurité et qu'ils y consentent;
- passer en revue l'exactitude et le caractère complet du formulaire de consentement, puis vérifier l'identité des candidats externes;
- consulter les responsables de la sécurité du personnel pour toute question liée à une enquête de sécurité.

Les Services de sécurité et d'enquête – personnel de sécurité doivent :

- donner des conseils sur les niveaux de sécurité requis pour les postes;
- consulter les RH, les Services juridiques et les Relations du travail, le cas échéant, pour toute question liée aux enquêtes de sécurité;
- passer en revue les casiers judiciaires et autres renseignements défavorables dans le but de prendre une décision;
- évaluer la nécessité d'effectuer une autre enquête de sécurité pour un motif valable;
- remettre au SCRS les Formulaires d'autorisation de sécurité remplis aux fins d'une évaluation de sécurité exhaustive;
- accorder, refuser ou retirer une cote de fiabilité ou une cote de sécurité;
- signer chaque formulaire requis dans le cadre du processus d'enquête de sécurité et conserver en dossier les copies nécessaires.
- informer les personnes de leurs responsabilités à l'égard de leur cote de sécurité;
- tenir à jour les dossiers d'enquête et aviser le SCRS de toute démission et cessation d'emploi;
- mettre à jour les cotes de sécurité conformément au calendrier de renouvellement en vigueur;
- établir et maintenir à jour la cote de sécurité de l'employé dans la section des compétences du SAP;
- effectuer à intervalles réguliers des examens afin de cerner les problèmes de non-conformité ou d'améliorer la procédure;
- s'assurer que les exigences en matière d'enquête de sécurité sont satisfaites;
- conserver les dossiers d'enquête de sécurité de façon à les protéger contre toute utilisation non autorisée et perte.

6. Non-conformité

Il incombe à tous les employés de Postes Canada, à tous les niveaux, de se conformer à cette pratique. Le refus de coopérer au cours du procédé de vérification de sécurité ou le non-respect de cette pratique pourrait entraîner l'application des mesures disciplinaires suivantes :

- Un candidat à un emploi qui ne coopère pas au cours du processus d'enquête de sécurité ou qui ne se conforme pas à cette pratique n'est pas admissible à l'emploi au sein de Postes Canada;
- Un employé actuel qui ne coopère pas au cours de la mise à jour ou de la révision du processus de vérification de sécurité visant à trouver une cause ou qui ne se conforme pas à cette pratique est susceptible d'être suspendu (avec ou sans paie, conformément à la convention collective pertinente ou aux conditions d'emploi des employés cadres et exempts) jusqu'à ce que toutes les exigences de cette pratique soient atteintes et peut même être congédié;
- Un employé actuel qui ne parvient pas à conserver le niveau de la cote requis pour son poste pourrait, par mesure d'adaptation, être réaffecté ou renommé pour un autre poste ou ses tâches pourraient être modifiées. Postes Canada peut aussi prendre d'autres mesures qu'elle juge raisonnables dans les circonstances et qui sont conformes aux dispositions de la convention collective. Si les mesures d'adaptation, à la discrétion de Postes Canada, ne sont pas possibles ou pratiques compte tenu des circonstances, Postes Canada peut décider de congédier l'employé, selon le nombre d'infractions, la nature et les circonstances de l'infraction, les tâches particulières effectuées, les antécédents professionnels de l'employé et tout autre facteur qui pourrait être pertinent dans les circonstances;

Pratique de Postes Canada

- Un employé actuel accusé d'une infraction qui, si elle entraînait une condamnation, modifierait le niveau de cote requise pour son poste, pourrait, à la discrétion de Postes Canada, être réaffecté à d'autres tâches, renommé ou suspendu, jusqu'à ce que les accusations aient été résolues par les autorités compétentes;
- Si un employé n'avise pas la Société de changements apportés au statut et que Postes Canada en prend connaissance par la suite au cours d'une mise à jour régulière ou d'une autre façon, cela sera pris en compte pendant le processus d'enquête de sécurité et pourrait constituer un motif de refus ou de révocation de la cote de fiabilité.

7. Impact au niveau réglementaire

La présente pratique est adoptée à l'appui de la Norme sur la sécurité du personnel de la *Politique sur la sécurité du gouvernement*, du Code de conduite de Postes Canada et de la section 5 de la partie I de la *Loi sur la Société canadienne des postes*.

8. Où trouver des renseignements supplémentaires

- [Politique sur la sécurité du gouvernement](#)
- [Foire aux questions](#)
- [Planification de la sécurité dans l'adjudication des contrats](#)
- [Pratique sur les contrats de produits et de services](#)
- [Pratique commerciale relative à la classification de l'information](#)
- [Sécurité en milieu de travail](#)

Titulaire de la pratique : Services de sécurité et d'enquête

Services consultatifs : [Services de sécurité et d'enquête \(sécurité du personnel\)](#)

Commentaires/questions : Cliquez [ici](#) pour envoyer un courriel à la personne-ressource responsable de la pratique.

Liens relatifs à la pratique

Vérification du casier judiciaire	<p>Dans le cadre d'une vérification de fiabilité, une vérification du casier judiciaire (VCJ) est effectuée en vue de déterminer si une personne aurait, par le passé, participé à des activités criminelles qui indiqueraient un risque inacceptable dans le contexte des responsabilités de la personne exercées à Postes Canada. Le formulaire de consentement offre aux personnes l'occasion de déclarer une condamnation pour infraction criminelle pour laquelle elles n'ont pas obtenu un pardon. Peu importe qu'une déclaration soit faite ou non, les responsables de la sécurité du personnel doivent faire une vérification du casier judiciaire.</p> <p>Les demandes de vérification du casier judiciaire doivent être transmises à la GRC par moyen électronique. La GRC peut renvoyer les résultats de la vérification accompagnés d'une demande d'empreintes digitales. La vérification des empreintes digitales vise à confirmer l'identité de la personne et à s'assurer que les</p>
---	---

	<p>renseignements fournis concernent bien la personne visée).</p> <p>Si des empreintes digitales sont requises, mais ne sont pas fournies, la vérification du casier judiciaire sera déclarée incomplète et la demande d'enquête de sécurité sera annulée. La GRC ne libérera aucun casier judiciaire sans avoir reçu au préalable les empreintes digitales permettant de confirmer l'identité positive.</p>
<p><u>Formulaire pertinent de vérification de la sécurité</u></p>	<p>Afin d'assurer la mise en œuvre uniforme de l'approche sur la collecte des renseignements pertinents et de respecter les exigences de la <i>Loi sur la protection des renseignements personnels</i> visant la collecte, l'utilisation et la protection des renseignements personnels, un formulaire de consentement à l'enquête de sécurité sera utilisé pour toutes les demandes. Les formulaires approuvés indiqués ci-dessous sont utilisés dans le cadre du processus d'enquête de sécurité :</p> <p>a) un <u>formulaire de consentement à l'enquête de sécurité</u> doit être utilisé dans les cas suivants :</p> <ul style="list-style-type: none"> i) toutes les demandes d'enquête de sécurité afin de déterminer les exigences et les niveaux de sécurité; ii) à l'appui des décisions générales sur la cote de fiabilité, pour obtenir des renseignements biographiques sur une personne, ainsi que des données sur sa résidence et sur son casier judiciaire; iii) aux fins d'obtention du consentement d'une personne au sujet du type et du niveau de la cote requise; iv) aux fins de la confirmation de l'exécution des enquêtes de sécurité et l'approbation ou le refus de la cote de sécurité demandée. <p>b) un <u>formulaire de consentement à l'enquête de sécurité</u> doit être utilisé dans les cas suivants :</p> <ul style="list-style-type: none"> i) pour tous les niveaux de cote de sécurité. Le formulaire ne doit pas être utilisé pour la collecte de renseignements à l'appui de l'enquête pour la cote de fiabilité. Comme l'indique le formulaire, la quantité de renseignements à fournir dépend du type et du niveau de la cote de sécurité requise; ii) aux fins de l'accès à des lieux d'intérêt national. <p>c) un <u>Formulaire normalisé de la GRC pour les empreintes digitales</u> (pour une demande d'empreintes digitales).</p> <p>d) un <u>certificat d'enquête de sécurité</u> dans les cas suivants :</p> <ul style="list-style-type: none"> i) attestation officielle du niveau de cote accordée; ii) formulaire sur le profil de sécurité d'une personne ayant reçu une cote de sécurité ou une cote de fiabilité.
<p><u>Niveau de la cote de sécurité requise</u></p>	<p>Lien au tableau ci-dessous</p>

Types / Niveaux de la cote de sécurité / Privilèges d'accès / Exigences de mise à jour

Catégorie de	Niveau de la	Niveau d'accès ou de sensibilité	Exigences de mise à jour
--------------	--------------	----------------------------------	--------------------------

Pratique de Postes Canada

l'enquête de sécurité	cote de sécurité	(maximal)	
Vérification de fiabilité	Cote de fiabilité	Renseignements et biens PROTÉGÉS (niveau A, B ou C)	Tous les 10 ans**
Vérification de sécurité	Secret	Renseignements et biens SECRETS et personnes qui détiennent un « accès privilégié » aux systèmes essentiels et/ou aux processus d'identification du gouvernement du Canada	Tous les 10 ans*
	Très secret	Renseignements et biens TRÈS SECRETS	Tous les 5 ans

* Mise à jour une fois tous les 10 ans ou plus souvent (selon les modifications apportées aux tâches, aux ententes contractuelles, aux lois ou aux autres obligations; dans un tel cas, les employés touchés seront avisés de l'exigence modifiée).

<u>Vérification des données personnelles</u>	<p>La vérification des renseignements personnels permet de confirmer l'identité de la personne et de s'assurer que tous les autres dossiers vérifiés concernent la personne visée. Les personnes doivent fournir tous les renseignements indiqués sur le formulaire de consentement.</p> <p>Pour les nouvelles demandes (et non les mises à jour ou les demandes d'employés actuels), en plus de fournir les renseignements requis sur le formulaire de consentement :</p> <ul style="list-style-type: none"> a) la personne doit fournir des photocopies de deux pièces d'identité émises par le gouvernement du Canada (p. ex. acte de naissance, passeport, permis de conduire) pour permettre de confirmer son identité. L'une de ces photocopies doit être celle d'une pièce d'identité acceptable avec photo; b) Si la personne demeure au Canada depuis moins de cinq ans ou a vécu à l'étranger pendant plus de six mois, elle doit fournir : <ul style="list-style-type: none"> i) une copie de son passeport, de l'attestation de son statut de résident permanent, de la fiche relative au droit d'établissement, de l'attestation de son statut de résident temporaire ou de tout autre document émis par Citoyenneté et Immigration Canada; ii) des documents justificatifs du pays d'origine (p. ex. preuve de résidence, copies de factures; iii) un certificat de police du pays d'origine.
<u>Vérification des renseignements pertinents concernant les études, les antécédents professionnels, les compétences professionnelles et l'expérience de travail des candidats externes</u>	<p>La vérification des attestations d'études, des titres et des antécédents professionnels ainsi que des références pour évaluer les compétences d'une personne aux fins de dotation se distingue des vérifications effectuées dans le cadre de la vérification de fiabilité. Bien que ces deux types de vérification puissent être effectués simultanément, elles sont utilisées à des fins différentes. Le tableau ci-dessous précise les exigences, les utilisations et les différences de ces vérifications :</p>

Vérification	Évaluation des compétences dans le	Critères d'évaluation pour la
--------------	------------------------------------	-------------------------------

	cadre du procédé de dotation	vérification de fiabilité
Attestations d'études	S'assurer que le candidat possède le niveau d'études établi pour le travail à accomplir.	S'assurer que le candidat dit la vérité au sujet de ses antécédents.
Antécédents professionnels	Évaluer l'expérience par rapport aux exigences du poste.	Évaluer la fiabilité lors des emplois précédents et s'assurer que le candidat est honnête au sujet de ses antécédents.
Références	Évaluer les qualités personnelles, comme le jugement, le tact, l'entregent.	Déterminer si le candidat est honnête, discret, digne de confiance et fiable.

Vérification des empreintes digitales	<p>La vérification des empreintes digitales est nécessaire :</p> <ul style="list-style-type: none"> • si la personne déclare avoir eu une condamnation pour infraction criminelle pour laquelle elle n'a pas obtenu un pardon; • la GRC en fait la demande afin de mener à bien la vérification du casier judiciaire; • la demande de vérification est remplie comme préalable à l'obtention d'une cote de sécurité. <p>Si la personne déclare une condamnation pour infraction criminelle dans le formulaire de consentement, elle peut choisir de soumettre ses empreintes digitales avec sa demande d'enquête de sécurité. Cela permettra tout simplement de gagner du temps au cours du procédé.</p> <p>La personne dont les empreintes digitales sont requises doit se rendre à un bureau de la GRC, un poste de police local ou un organisme privé accrédité pour prendre les empreintes digitales et ensuite les envoyer (uniquement par la poste) aux responsables de la sécurité du personnel.</p> <p>Une fois les empreintes reçues, les responsables de la sécurité du personnel les enverront à la GRC par voie électronique. Les résultats seront envoyés aux responsables de la sécurité du personnel qui décideront d'accorder ou non la cote de fiabilité.</p>
--	---

Profil de sécurité	<p>Une fois le processus d'enquête de sécurité terminé, le candidat ou l'employé sera informé du niveau approuvé de cote, ainsi que de ses responsabilités, telles qu'elles sont décrites ci-dessous.</p> <p>Les employés doivent respecter l'exigence applicable en tout temps de :</p> <ol style="list-style-type: none"> a. signaler toute nouvelle accusation criminelle ou infraction; b. protéger les renseignements et les biens, y compris le courrier, conformément à la <u>Politique</u> sur la sécurité du gouvernement ainsi qu'aux politiques et aux pratiques en vigueur de Postes Canada; c. signaler tout incident où des personnes non autorisées
---------------------------	---

	cherchent à accéder à de l'information de nature délicate ou lorsqu'ils croient être la cible d'une tentative d'exploitation.
<u>Agent de sécurité de l'entreprise (ASE)</u>	Le directeur général et chef inspecteur des postes, Services de sécurité et d'enquête, est l'ASE de Postes Canada.
<u>Vérifications à l'extérieur du pays</u>	<p>Voici les trois types de vérification à l'extérieur du pays pour les candidats externes :</p> <ul style="list-style-type: none"> • Personnes qui ne résidaient pas Canada au cours des cinq dernières années; • Immigrants admis ayant le statut de <u>résidents permanents</u> • <u>Résidents temporaires</u> <p>1. Demandeur ayant résidé à l'extérieur du Canada – Cote de fiabilité avec restrictions</p> <p>Si le demandeur n'a pas résidé au Canada au cours des cinq dernières années, il faut obtenir un dossier de police, des lettres d'attestation d'employeurs à l'étranger et d'autres documents à l'appui, comme des factures comportant une adresse, etc.</p> <p>Il est important de noter qu'il n'est pas toujours possible de valider ou de confirmer les renseignements. Dans de tels cas, les responsables de la sécurité du personnel passeront en revue le dossier et décideront des prochaines étapes.</p> <p>Dans certains cas, une évaluation de la menace et des risques sera effectuée afin de déterminer si une cote de fiabilité avec restrictions peut être accordée.</p> <p>2. Statut de résident permanent – Examen de renseignements de Citoyenneté et immigration Canada</p> <p>Un candidat ayant le statut de résident permanent doit fournir une copie certifiée conforme du document de confirmation de résidence permanente, d'une fiche d'établissement ou d'une carte de résident permanent, le cas échéant.</p> <p>Pour les besoins de l'enquête de sécurité, les responsables de la sécurité du personnel effectueront une inspection visuelle des documents du candidat sur le statut de résident permanent afin de satisfaire aux exigences de vérification des renseignements personnels et du casier judiciaire pour la cote de fiabilité visant la période antérieure à l'arrivée du candidat au Canada.</p> <p>Les responsables de l'embauche ou les Ressources humaines sont chargés de tenter de confirmer les attestations d'études, les titres et les antécédents professionnels ainsi que les références du candidat pour toute la période visée par la vérification (y compris les périodes passées à l'extérieur du pays) en vérifiant les renseignements et en communiquant avec les références. Il incombe au candidat de fournir tous les renseignements supplémentaires afin de faciliter cette tâche.</p> <p>3. Résident temporaire</p> <p>Citoyenneté et Immigration Canada peut accorder à une personne</p>

	<p>établie au Canada, qui n'est pas résident permanent ni citoyen canadien, la permission de résider au pays à titre de visiteur ou de travailleur temporaire, d'étudiant ou de demandeur du statut de réfugié).</p> <p>Les personnes dans les catégories susmentionnées ne sont pas assujetties à une vérification du casier judiciaire et à une enquête de sécurité avant leur arrivée au Canada et aucun certificat de police d'administrations étrangères n'aurait été obtenu. À ce titre, à moins d'être en mesure d'obtenir des renseignements auprès du candidat, y compris le certificat de police, les responsables de la sécurité du personnel pourraient refuser d'accorder la cote de fiabilité en raison de leur incapacité de recueillir les renseignements pertinents.</p>
<u>Mise à jour</u>	<p>Les Services de sécurité et d'enquête doivent mettre à jour la cote de sécurité d'une personne à la fréquence décrite ci-dessous et dans les circonstances où une révision est nécessaire pour tout autre motif valable.</p> <p>a) Cote de fiabilité : une fois tous les dix ans ou plus souvent (en fonction des modifications apportées aux tâches, aux ententes contractuelles, aux lois ou aux autres obligations. Dans un tel cas, les employés concernés seront avisés de l'exigence modifiée)</p> <p>b) Cote de sécurité de niveau Secret : tous les dix ans</p> <p>c) Cote de sécurité de niveau Très secret : tous les cinq ans</p>
<u>Conséquences</u>	<p>Un employé actuel qui ne coopère pas au cours de la mise à jour ou de la révision du processus de vérification de sécurité visant à trouver une cause ou qui ne se conforme pas à cette pratique est susceptible d'être suspendu (avec ou sans paie, conformément à la convention collective pertinente ou aux conditions d'emploi des employés cadres et exempts) jusqu'à ce que toutes les exigences de cette pratique soient atteintes et peut même être congédié.</p>
<u>Politique sur la sécurité du gouvernement</u>	<p>Postes Canada a adopté la <u>Politique sur la sécurité du gouvernement</u>.</p> <p>(La section 10.9 de la Politique porte sur l'enquête de sécurité.)</p>
<u>Foire aux questions</u>	<p>Q. Le candidat refuse de signer le formulaire de consentement. Puis-je poursuivre la procédure d'embauche?</p> <p>R. Non. Le candidat doit donner son approbation écrite avant que vous puissiez présenter une demande d'enquête de sécurité aux Services de sécurité et d'enquête. Il faut informer le candidat qui refuse de signer le formulaire que sa candidature pour le poste sera refusée et que la procédure d'embauche sera immédiatement abandonnée.</p> <p>Q. Quels autres renseignements ou vérifications pourraient être exigés au cours d'une enquête de sécurité pour des candidats externes?</p> <p>R. Dans des cas particuliers, la vérification d'autres renseignements, comme le visa, l'autorisation d'emploi de travailleur étranger ou le dossier de conducteur, pourrait être exigée dans le cadre du processus d'enquête de sécurité.</p> <p>Q. Dans quelles circonstances les empreintes digitales sont-elles exigées?</p>

	<p>R. Le prélèvement d'empreintes digitales serait requis dans les cas suivants :</p> <ol style="list-style-type: none"> 1. Le candidat doit obtenir une cote de sécurité. 2. Les résultats de la vérification du casier judiciaire exigent la vérification des empreintes digitales afin de confirmer l'identité du candidat. 3. Le candidat déclare avoir eu une condamnation pour infraction criminelle à l'intérieur ou à l'extérieur du pays et pour laquelle il n'a pas obtenu de pardon. 4. La Société peut exiger des empreintes digitales en cas de modification aux fonctions de l'employé, aux ententes contractuelles ou à la loi, ou encore pour satisfaire à d'autres obligations. <p>Q. Qu'arrive-t-il si le candidat ou l'employé a obtenu un pardon?</p> <p>R. Le candidat ou l'employé n'est pas tenu de déclarer une condamnation pour infraction criminelle pour laquelle il a obtenu un pardon. Lorsqu'un pardon est accordé, tous les renseignements au sujet de l'infraction criminelle visée doivent être supprimés du dossier d'enquête du candidat. Si un pardon est obtenu après la tenue de l'enquête sur l'infraction criminelle déclarée, la GRC en informera les responsables de la sécurité du personnel, conformément à la procédure en vigueur.</p> <p>Q. Quand la cote de fiabilité ou la cote de sécurité doit-elle être mise à jour?</p> <p>R. Le niveau de la cote de l'employé doit être mis à jour conformément au <u>tableau</u>, ou lorsqu'un changement est apporté au poste et que celui-ci exige un niveau de cote supérieur.</p> <p>Q. Comment les entrepreneurs peuvent-ils obtenir une cote de fiabilité ou une cote de sécurité?</p> <p>R. Par l'entremise du ministère des Travaux publics et des Services gouvernementaux du Canada, les responsables de la sécurité du personnel mènent une enquête de sécurité pour tout entrepreneur qui a besoin d'une cote ou valident les niveaux des cotes actuelles. Pour obtenir plus de renseignements, veuillez consulter le document <u>Planification de la sécurité dans l'adjudication des contrats</u> de Postes Canada.</p> <p>Q. Je comprends que la cote de fiabilité est le niveau minimal d'enquête de sécurité exigé pour les employés de Postes Canada. Quels autres postes nécessitent une cote de sécurité?</p> <table border="1" style="width: 100%;"> <thead> <tr> <th>Type d'employé</th> <th>Niveau de cote de sécurité</th> </tr> </thead> <tbody> <tr> <td>Inspecteurs des postes</td> <td>Très secret</td> </tr> <tr> <td>Quelques postes d'employés cadres et exempts</td> <td>Secret ou Très secret</td> </tr> </tbody> </table>	Type d'employé	Niveau de cote de sécurité	Inspecteurs des postes	Très secret	Quelques postes d'employés cadres et exempts	Secret ou Très secret
Type d'employé	Niveau de cote de sécurité						
Inspecteurs des postes	Très secret						
Quelques postes d'employés cadres et exempts	Secret ou Très secret						

	<p>Q. En tant qu'employé, comment puis-je maintenir ma cote de fiabilité?</p> <p><i>R. Votre cote de fiabilité est maintenue aussi longtemps que vous ne faites pas l'objet d'une accusation ou d'une condamnation criminelle. Cependant, il pourrait être nécessaire d'effectuer un examen si l'information communiquée remet en question la capacité de l'employé de conserver sa cote de fiabilité actuelle. À noter que toute cote de sécurité peut être retirée si l'employé refuse de participer</i></p>
--	---

[7] Madame Eckert a d'ailleurs été le premier témoin de la partie syndicale. Elle occupe ce poste au syndicat depuis 2011. Elle compte une expérience de vingt-six ans comme employée de Postes Canada.

[8] C'est lors d'une rencontre de consultation au niveau national que ce sujet a été abordé pour la première fois, comme en fait foi le procès-verbal de la rencontre du 7 décembre 2012:

«Security and Investigation (S & I) stated they are looking at a draft practice on the security screening of personnel, in order to bring in clarity and consistency to the practice...»

[9] La teneur de cette *pratique* a alors été communiquée verbalement aux représentants du syndicat, comme en a témoigné Madame Eckert. Le procès-verbal fait cependant état d'un engagement de la Société.

«CPC to provide a copy of the draft Security Screening Practice.

Sent via email 2012-12-11.»

(Il avait été convenu, le 7 décembre 2012, que le sujet serait discuté plus en détail lors d'une rencontre prévue pour le 12 décembre 2012.)

Toujours le 7 décembre 2012, la Société s'était engagée à transmettre au syndicat une copie d'une *«letter of confirmation between CPC and the Treasury Board Secretariat of Canada regarding the Policy on Government Security»*. On peut lire la note suivante à ce sujet dans le procès-verbal :

«CPC to look into providing a copy of letter, date of signature. »

Dans les faits, cette lettre, portant la date du 14 septembre 2012, a été envoyée à Madame Eckert le 17 janvier 2013. Elle est reproduite à la page qui suit (Document S-10).

[10] Une rencontre a effectivement été tenue le 12 décembre 2012, mais comme le projet de cette «Pratique» n'avait été reçu que la veille par le syndicat, il a été convenu que le sujet serait de nouveau abordé lors d'une rencontre subséquente. Fait à noter : la partie syndicale a signalé, lors de cette rencontre du 12 décembre 2012, l'existence d'une décision arbitrale de 1988 de l'arbitre Richard B. Bird, relativement au droit de la Société d'exiger que ses employés fournissent leurs empreintes digitales. Nous y reviendrons.

[11] A cette rencontre du 12 décembre 2012, la partie syndicale a réitéré sa demande au sujet de cette lettre confirmant l'entente entre la Société et le gouvernement (le document S-10, transmis le 17 janvier 2013), accompagnée d'une demande additionnelle :

«CUPW also requested a copy of the policy on Government Security. »

(On peut lire la note qui suit à ce sujet dans le procès-verbal :

«Provided by email on 2013-01-08»)

[12] Toujours à cette même rencontre du 12 décembre 2012, le syndicat a requis d'autres renseignements :

«CUPW also requested statistics such as the number of criminal acts related to mail occurring within Canada Post, as well as the number of employees committing these criminal acts that have previous criminal records...»

CUPW asked for examples of partners and contracts that did not use CPC due to their current reliability status...»

S-10



SEP 14 2012

Deepak Chopra
President and Chief Executive Officer
Canada Post Corporation
Président-directeur général
Société canadienne des postes

MS. MICHELLE D'AURAY
SECRETARY OF THE TREASURY BOARD OF CANADA
TREASURY BOARD SECRETARIAT
140 O'CONNOR ST
OTTAWA ON K1A 0R5

Re: Restating Canada Post's Intent to adopt and apply the requirements of the Policy on Government Security and of its associated standards (including the Personnel Security Standard)

Dear Ms. d'Auray:

Since 1987, Canada Post has an agreement with the Treasury Board Secretariat with respect to the adoption and application of the provisions of the Government Security Policy (GSP) and its operational standards. These provisions include security screening and clearance requirements and the protection and sharing of classified information.

In July 2003, following issuance of a revised GSP, Canada Post reiterated to the Treasury Board Secretariat its commitment to adopt and apply the provisions of the GSP and its operational standards.

The purpose of this letter is to reassert our commitment. We believe it is both beneficial and appropriate for Canada Post to restate our intent to adopt and apply the provisions of the Treasury Board's Policy on Government Security (PGS) issued in July 2009 and its associated standards. Please be assured that meeting security requirements is an important matter for Canada Post, as it is to continue to be recognized within the federal public sector as a Crown corporation that applies and complies with the PGS and the Personnel Security Standard.

To this effect, we are liaising with the Security Policy Division, CIOB, and are taking the necessary measures to formalize the process and maintain our mutually beneficial relationship. Canada Post's Chief Postal Inspector and General Manager, Ted Upshaw, is the official responsible to coordinate and direct the implementation of the PGS, and he can be reached at 613-734-4010 or by email at ted.upshaw@canadapost.ca.

Yours sincerely,

Deepak Chopra

[13] Le même jour, après la rencontre, Madame Hurst a transmis à Madame Eckert un projet de cette «*Pratique en matière d'enquête de sécurité sur le personnel*». On peut lire le passage suivant dans la lettre d'accompagnement :

«Ce document a pour principal objectif de décrire le processus d'enquête de sécurité de la Société et de veiller à ce que les exigences en matière de sécurité soient respectées. Cette pratique nous aidera à maintenir la confiance de nos clients grâce au transport sécuritaire du courrier, à un environnement de travail où tous les employés sont en sécurité et à une main-d'œuvre de qualité. Non seulement est-il essentiel de renforcer ces aspects pour conserver nos clients actuels, mais également pour être plus concurrentiel et en acquérir de nouveaux.»
(sic)

(Il était également indiqué dans cette lettre que la date d'entrée en vigueur de cette pratique avait été fixée au 1^{er} avril 2013.)

[14] Une autre rencontre a eu lieu le 25 janvier 2013.

Le syndicat a demandé que lui soit transmis un exemplaire de cette «*entente*» de 1987 dont il est question dans la lettre du 14 septembre 2012 reproduite plus haut (document S-10).

Il a de nouveau été fait mention de la décision de l'arbitre Bird (2 mai 1988) où il avait été déclaré que la Société n'avait pas le droit d'exiger que ses salariés fournissent leurs empreintes digitales. Voici un extrait pertinent du procès-verbal de cette rencontre du 25 janvier 2013 :

«Le STTP soutient que cette décision est toujours valable et, par conséquent, exécutoire. La SCP répond qu'en 1988, le monde était très différent de ce qu'il

est aujourd'hui et que les attentes du marché en matière de sécurité ont considérablement changé depuis.»

[15] Toujours à cette rencontre du 25 janvier 2013, la Société a fourni au syndicat, «à titre confidentiel, des exemples d'exigences en matière de sécurité devant être pris en considération pour diverses possibilités de marché», comme elle s'y était engagée lors de la rencontre du 12 décembre 2012. D'ailleurs, dans l'intervalle, soit le 14 janvier 2013, Madame Anne-Marie Somerville, agente, Relations de travail, avait adressé à Madame Eckert un courriel dont voici un extrait :

«Examples of partners/contracts having security compliance requirements

- *All government related contracts have security requirements (e.g. HRSDC, Passport, etc.)*

- *Other examples of RFP's or contracts include – Capital One, Grand and Toy, Johnson and Johnson, etc. »*

[16] Par lettre du 20 mars 2013, le syndicat a été avisé que la date d'entrée en vigueur de la pratique avait été reportée au 29 avril 2013.

[17] Une autre rencontre de consultation nationale a été tenue le 22 mai 2013, alors que le sujet a de nouveau été abordé. Les parties ont maintenu leurs positions respectives.

[18] En contre-interrogatoire, Madame Eckert a reconnu volontiers que le volume du courrier avait considérablement diminué au cours des dernières années. Elle a ajouté que le syndicat avait toujours été prêt à collaborer avec la Société en vue de rechercher des nouveaux débouchés d'affaires, entre autres pour les paquets et les services. On peut lire, d'ailleurs, dans le procès-verbal de la rencontre du 25 janvier 2013, que le syndicat

«...est disposé à poursuivre les discussions dans un cadre lié à la vente au détail. Toutefois, il veut s'assurer que ces marchés apporteront des avantages à ses membres de la vente au détail sous forme de niveaux de dotation élevés ou d'une augmentation du nombre d'heures de quart de jour.»

[19] Finalement, Madame Eckert a tenu à préciser que le syndicat qu'elle représente n'avait jamais eu de réponse satisfaisante à sa demande de précisions quant aux possibilités de débouchés d'affaires.

[20] Madame Stephanie Nystedt occupe depuis 2010 le poste de directrice des services de sécurité et d'enquête à Postes Canada. Elle a été libérée en vue de la mise sur pied de *«Pratique relative à l'enquête de sécurité sur le personnel»* dont le texte est reproduit à la suite du paragraphe (6) ci-dessus.

[21] Auparavant, ces *«enquêtes de sécurité»* n'avaient lieu que dans les cas de nouveaux employés, ainsi que pour l'accès à des postes à un plus haut niveau de sécurité (chef d'unité, inspecteur du service de sécurité, etc.) Dans le cadre de ces enquêtes, on utilisait une formule émise pour le Gouvernement du Canada aux termes de la *«Norme sur la sécurité du personnel»*. Cette formule avait pour titre : *«Formulaire de vérification de sécurité, de consentement et d'autorisation du personnel»*.

La *«Politique sur la sécurité»* du gouvernement fédéral s'applique à tous les employés du gouvernement du Canada. On peut y lire ce qui suit à la fin du paragraphe 5 :

«Certains organismes et sociétés d'état peuvent conclure des ententes avec le Secrétariat du Conseil du Trésor du Canada afin d'adopter les exigences de cette politique et les appliquer à leur organisation.»

[22] Ceci est à l'origine de la lettre que le président-directeur général de la Société a écrite à la secrétaire du Conseil du Trésor le 14 septembre 2012. Cette lettre est reproduite plus haut au paragraphe (8) (document S-10). On peut y lire qu'une telle *«entente»* remonte à l'année

1987. En effet, dans une lettre qu'il écrivait alors à son collègue du Conseil du Trésor, le ministre responsable de la Société canadienne des Postes avait précisé ce qui suit :

«This is to advise you that Canada Post Corporation will be complying with national interest provisions of the Security Policy of the Government of Canada...

It is my understanding that, by entering into this compliance agreement and taking the required action, Canada Post Corporation will meet the conditions specified for continued access to classified information and to Canadian Security Intelligence Service security clearance services. »

[23] Au cours des années 2010 et 2011, il y a eu des mises à jour dans le service que dirige Madame Nystedt, et on y a abouti, en août 2011, à la centralisation des démarches au service de la sécurité et à la mise sur pied d'un système électronique pour procéder plus rapidement et plus efficacement à la vérification des renseignements colligés dans les formules dont il a été question plus haut, au paragraphe (21).

[24] C'est en 2012 que Madame Nystedt a été chargée de mettre par écrit cette pratique de sécurité qui serait dorénavant applicable à tous les employés de la Société.

[25] Le sujet a été ajouté à la dernière minute à l'ordre du jour de la rencontre du 7 décembre 2012, vu l'existence d'une possibilité d'affaires avec le Ministère des transports de l'Ontario. Madame Nystedt a participé à cette rencontre, de même qu'à celles du 12 décembre 2012, du 25 janvier et du 22 mars 2013. Les positions des deux parties ont été exprimées lors de cette dernière rencontre (22 mars 2013). Le procès-verbal est reproduit aux deux pages qui suivent (Document S-14).

[26] Le syndicat a été conséquent avec lui-même en levant le grief du 11 avril 2013. La pratique proposée n'a pas été mise en œuvre à ce jour, vu la décision rendue par l'arbitre Swan, le 26 avril 2013.

5.14

**Procès-verbal de la consultation nationale
entre
la Société canadienne des postes et le Syndicat des travailleurs et travailleuses des
postes
pour des questions concernant les factrices et facteurs ruraux et suburbains (FFRS)
tenue au 2701, promenade Riverside, Ottawa (Ontario)**

Le 22 mars 2013

Postes Canada (SCP)

**Syndicat des travailleurs et travailleuses des
postes (STTP)**

Carlo Raponi
Shannon Hurst
Stephanie Nystedt
Tom Baltzer

Rona Eckert
P. Arbour
F. Bénard

Pratique relative à la vérification de sécurité des employés

La SCP et le STTP discutent de la mise en œuvre d'une pratique mise à jour relative à la vérification de sécurité qui aura une incidence sur tous les employés, y compris les FFRS membres du Syndicat. Cette pratique mise à jour entrera en vigueur le 29 avril 2013. Il incombera aux employés de déclarer toute accusation criminelle ou condamnation qui pourrait avoir une incidence sur le résultat de la vérification de sécurité effectuée à leur égard. Les employés seront également tenus de conserver leur cote de sécurité en fonction des exigences de leur poste. La SCP explique que, pour des motifs d'ordre administratif, le processus de vérification de sécurité des employés actuels sera progressivement mis en œuvre en commençant par l'Île-du-Prince-Édouard.

La SCP précise que la pratique assurera un environnement de travail sécuritaire pour nos employés, tout en assurant à Postes Canada le maintien de la confiance que nous avons à l'égard de nos clients en raison d'une main-d'œuvre plus stable, ainsi que la possibilité d'accéder à des marchés nécessitant une autorisation de sécurité plus élevée. En vertu de la Loi sur la Société canadienne des postes, la Société a comme mandat d'assurer son exploitation dans les meilleures conditions de sécurité du courrier. Cette pratique consolide notre engagement visant à satisfaire à cette obligation légale. La SCP précise que, selon la nouvelle pratique, tous les FFRS actuellement membres du Syndicat seraient tenus de subir une vérification de sécurité tous les 10 ans et que, par ailleurs, ce seuil de 10 ans pourrait être revu à la baisse si les conditions le justifient.

Le STTP indique que ce programme ne lui convient pas et qu'il étudie ses options en fonction des besoins à l'avenir. Le STTP soulève également des préoccupations en ce qui concerne l'application de ce programme à l'égard de ses membres et il demande des renseignements supplémentaires sur la façon dont le programme sera géré et sur la question de savoir si le Syndicat sera convoqué à des réunions dont le résultat serait de

congédier un membre du STTP. Le STTP craint également que des personnes puissent être congédiées d'une façon arbitraire et non professionnelle et il demande si la SCP fera preuve de discrétion lorsqu'il sera question d'accusations qui ne sont pas considérées comme graves. La SCP précise que tout congédiement sera effectué de manière professionnelle et non arbitraire; les questions seront examinées avec discrétion et logique et au cas par cas. La SCP enverra des renseignements supplémentaires concernant les procédures de la SCP relativement à cette question et elle a de plus indiqué que la convention collective sera respectée.

Le STTP demande ce qui arriverait si un FFRS membre du Syndicat refusait de se conformer à la pratique. La SCP indique qu'il s'agirait d'une situation de non-respect de la pratique et que la personne en cause serait assujettie à des mesures disciplinaires progressives. Le STTP demande à qui il incomberait de déterminer si une personne dispose de l'autorisation de sécurité exigée par le poste qu'elle occupe. La SCP indique qu'il incombera à la direction générale des Services de sécurité et d'enquête (SSE) d'examiner le dossier et de déterminer s'il y a lieu d'accorder la cote de sécurité visée à la personne en question. S'il est impossible d'accorder l'autorisation de sécurité relativement au poste en cause, une mesure de réintégration sera examinée à l'égard de la personne dans la mesure du possible. Le STTP demande quels représentants de la SCP s'occuperaient de ces employés. La SCP indique que le processus serait similaire à notre processus actuel (les SSE, les RT et le gestionnaire de zone locale). Le STTP indique que, compte tenu des changements apportés par le travail à temps partiel et du stress supplémentaire dans l'aire de travail engendré par la réorganisation, ce nouveau programme ne fera qu'ajouter un stress supplémentaire aux employés et le Syndicat étudiera ses options en fonction des besoins à l'avenir.

Mesure de suivi

SCP	Faire parvenir au STTP le site Web du Conseil du Trésor, un exemplaire du formulaire de consentement et de tout bulletin qui sera émis pour les régions relativement à cette affaire. Faire parvenir la position de la SCP à l'égard de la participation du STTP aux réunions des cadres avec les membres en ce qui concerne l'autorisation de sécurité de ces derniers. Faire parvenir une mise en jour du processus lié à la pratique qui sera en vigueur dans les régions.
-----	---

[27] Madame Rita Eswick est au service de la Société depuis dix-huit ans. Depuis 1995, elle a été affectée à des tâches relatives à la sécurité (enquêtes, activités préventives, etc.) et, depuis 2005, aux contacts avec les clients de la Société plus particulièrement exigeants en cette matière, par exemple les banques. Depuis 2011, en sa qualité de directrice des stratégies de sécurité, elle s'occupe de la prévention des fraudes (collecte de renseignements, de statistiques, élaboration d'une base de données relatives aux pertes de cartes de crédit, etc.)

[28] A ces fins, elle rencontre des clients de la Société sur une base quotidienne, ou elle communique avec eux pour répondre à leurs questionnements en matière de sécurité. Elle participe également aux rencontres avec des clients, afin de les rassurer quant à leurs exigences en cette matière.

[29] A l'une de ces rencontres avec les représentants de l'entreprise Capital One, on lui a demandé à quelle fréquence les salariés des Postes étaient soumis à des vérifications de sécurité, ce à quoi elle a été obligée de répondre qu'ils n'étaient pas obligés de se soumettre à de telles vérifications s'ils étaient déjà à l'emploi de la Société.

[30] En 2013, Madame Eswick a préparé, à partir de ses dossiers, un relevé des cas d'offenses criminelles en rapport avec le courrier au cours des années 2011, 2012 et une partie de 2013. On retrouve ces données dans le document reproduit aux pages qui suivent (document E-8). Commentant un des exemples cités dans ce document, Madame Eswick a précisé qu'elle avait dû elle-même faire pression auprès de l'entreprise Telus pour les assurer que leurs produits étaient en sécurité lorsqu'ils étaient confiés à la Société. Elle a dû faire de même auprès des autres clients mentionnés dans ces exemples, y compris l'engagement pris auprès de l'Association des banquiers du Canada.



E-8

Vide 5-15

Mail-Related * Investigative Results

	2011 Year End Total = 43		2012 Year End Total = 69		2013 Sept-30 YTD Total = 43	
	Criminally Charged	Terminated/ Resigned	Criminally Charged	Terminated/ Resigned	Criminally Charged	Terminated/ Resigned
Employees	18	20	20	26	9	21
- CUPW	- 18	-20	-18	-25	- 8	- 20
Contractors	2	3	16	7	7	6
Total	20	23	36	33	16	27

*Mail Related includes any of the following:

- Mail Theft,
- Mail Opening,
- Mail Tampering,
- Mail Delay,
- Mail Abandonment

Key Messages

- The majority of Canada Post employees are good.
- But even one incident can have a serious impact on the company's ability to maintain and attract business opportunities.

Some examples below

1. In September 2012, Canada Post acquired the TELUS Business-to-consumer parcel business. Part of the acquisition included many discussions on Canada Post's security program in order to give the customer confidence that their product (high valued iPhones) would be delivered securely and efficiently. Within one month of the acquisition, TELUS began to experience a high number of consumer non-receipt complaints within the Calgary area. An investigation undertaken by Canada Post Security & Investigation Services resulted in Calgary Police Services arresting and charging a CUPW employee at the Calgary Mail Processing Plant for Theft of Mail. At the time of the individual's arrest, Police recovered \$8K in cash (believed to have been resulting from the sale of the stolen product) and the recovery of two iPhones which were being sold by the individual on an online website auction. The incident appeared in several media channels including the Calgary Beacon, The Canadian Press, Lethbridge Herald, HuffingtonPost (online) Global Calgary (TV) and the Penticton Herald. Canada Post had to provide \$40K financial compensation to TELUS and there were numerous subsequent discussions with TELUS to provide reassurances relating to the security of their product.
 Consumer comment on HuffingtonPost.ca (online) dalethompson: "Yet another reason for the Canadian government to sell off Canada Post to a private company and let them run it their way. You don't see mass fraud or theft with Fed-Ex, UPS or other major parcel delivery companies, just with Canada Post. Get rid of Canada Post already, it's a huge monkey on the backs of Canadians now and we're paying way too much for what we get back in return from these bozos"

→
 might 2 de
 5-15
 29, 18 78



2. On January 30, 2012, a 24-year employee (64-year old) CUPW employee at the South Central Plant was arrested and charged with Theft of Mail by Toronto Police Services following an investigation undertaken by S&IS. At the time of the arrest, she was found to be in possession of 20 gift cards removed from the mailstream. Story profiled in The Toronto Star, CTV Toronto (CFTO-TV), Cable Pulse 24 and CFRB Radio Toronto. This prompted many banks to contact S&IS enquiring if there was any evidence of this individual tampering/handling their payment cards. WHY? Because of the case in September 2010 (see below)
3. In September 2010, an investigation by S&IS resulted in the arrest of a full-time 9-year employee CUPW postal clerk employee at the Woodbridge delivery centre – at the time of the arrest, she was in possession of 108 stolen credit cards. Investigation was initiated in May (over 100 credit card non-receipts – fraud exposures in excess of \$250K). Agreement made with Canadian Bankers Association (CBA) to communicate investigative results impacting their product (credit cards, cheques, etc).
4. On February 14, 2012, a part-time 4-year employee working at the Cobble Hill Post Office (Cobble Hill is a small community on Vancouver Island – 2006 census indicated population of 1775 people) was arrested and charged with Theft of Mail. At time of the arrest, 34 depredated greeting cards were found within the employee's vehicle and facility's washroom dated between February 7-14th. She was discharged from Canada Post in March 2012 (after failing to appear to her scheduled interview) Media included BC Local News (Online), Cowichan News Leader, Saanich News, Terrance Standard & North Shore Outlook.

The former employee entered a guilty plea in Criminal Court on February 18, 2013 and received a 12 month conditional discharge, 12 months probation and ordered to pay a \$50 fine. Her court appearance details appeared in the Cowichan Valley citizen as well as Canada.com (online)
5. On January 28th 2011; full time night clerk (employed since September 1989) was arrested and charged for Theft of Mail – stealing small parcels containing DVDs from Game Access. Company is now suing Canada Post for \$250K in lost sales/damages.

These stories are but a few that shows how only one incident has significant impacts on our business and our customer's security.

[31] Au mois de novembre 2012, la Gendarmerie Royale du Canada a produit un rapport d'évaluation du service postal. Voici quelle était la conclusion de cette évaluation :

«This assesment confirmed that the Canadian postal system, more specifically Canada Post, is utilized by criminals to transport various contraband both domestically and internationally. »

Ce rapport a été porté à l'attention d'un représentant de Postes Canada chargé des communications avec les médias par un journaliste de la Presse canadienne.

Il s'est avéré que ce rapport avait été largement commenté dans les médias à travers le pays.

(Invité par le journaliste de la Presse canadienne à commenter ce rapport, le porte-parole de la Société lui a écrit ce qui suit :

«Canada Post takes the security and integrity of the postal service very seriously. Our team of Postal Inspectors is responsible for investigating any potential fraudulent or criminal activity related to the postal service and works closely with police, from across the county. This approach has worked well, leading to seizures and charges in many cases. It should be noted that Canada Post was not involved in the creation of this report. »)

[32] Un représentant d'un client de la Société (Best Buy) a même demandé à Madame Eswick si les allégations contenues dans ce rapport de la G.R.C. correspondaient à la réalité, et dans quelle mesure de telles activités criminelles risquaient d'affecter la sécurité de leurs produits lorsqu'ils étaient confiés à la Société. Il est allé jusqu'à s'enquérir du niveau de sécurité des employés des Postes.

[33] La partie syndicale a demandé que lui soient transmis, entre autres, les détails des cas ayant servi à la compilation du relevé produit plus tôt par Madame Eswick (document E-8). Ces détails ont alors été transmis au procureur du syndicat, et ils ont ensuite été versés au dossier, en liasse pour cent-cinq (105) des cas, et de façon plus particulière pour les cinq (5) cas mentionnés dans ce document E-8.

[34] En contre-interrogatoire, Madame Eswick a reconnu que pour l'année 2012, il y avait eu un total de soixante-neuf (69) cas de telles offenses criminelles (tel qu'indiqué dans le document E-8) sur un total d'au-delà de neuf (9) millions de pièces de courrier... De surcroît, elle n'a pas été en mesure de préciser combien de ces délinquants avaient des antécédents judiciaires.

[35] En plus des détails relatifs aux cas d'offenses criminelles en rapport avec le courrier, la Société a transmis au syndicat, à sa demande, les documents suivants :

«- copie de la documentation fournie par la Société ou Madame Eswick pour démontrer les éléments du programme de sécurité lors de rencontres avec les clients ou clients potentiels».

(En guise d'illustration, le document produit a été celui d'une présentation à Best Buy Canada, en février 2012.)

«- copies des contrats de services conclus entre la Société et MBNA Canada Bank, et entre la Société et Capital One Bank, plus particulièrement les clauses relatives à la sécurité. (Madame Eswick a précisé qu'il n'y avait pas de contrat avec MEDIJEAN, et que les contrats avec TELUS et BEST BUY ne contenaient pas de telles clauses relatives à la sécurité.)

- copies des documents échangés avec le regroupement de banquiers «Partenaires-cartes de paiements», dont le but était d'améliorer l'aspect sécurité dans les opérations de transmission de ces cartes.

[36] Madame Eswick a reconnu que les passeports, les cartes de crédit, les permis de conduire, les certificats d'état civil, les chèques, et toutes sortes de documents légaux étaient distribués par la Société depuis de nombreuses années, sans que n'existe la pratique contestée.

[37] Monsieur Rod Hart est à l'emploi de la Société depuis quelque dix-neuf années. Depuis le mois de juillet 2011, il occupe le poste de «*General Manager, domestic parcels and commerce market development*». Voici comment il décrit ses tâches dans son C.V. :

«Responsible for the design, development, deployment and overall performance of the \$900M parcels, products and services delivered to all customer segments in the domestic market.

Key strategic focus is on expansion of Canada Post's capabilities in the e Commerce/eRetail segment to improve the customers experience for online shoppers. »

[38] Étant dans le domaine des colis depuis plusieurs années, ce témoin a précisé qu'au cours des dernières années la livraison des colis occupait la plus grande partie du marché, d'où une concurrence de plus en plus féroce de la part des autres entreprises spécialisées dans le domaine (Canpar, UPS, Federal Express, etc.).

[39] Ceci est d'autant plus vrai vu la diminution endémique du volume du courrier ordinaire depuis les années 2007-2008, tel qu'illustré par les données colligées dans les rapports annuels pour les années 2012 et 2013, dont des extraits sont reproduits aux deux pages qui suivent (documents E-13 et E-39).

The Year in Review: 2012

2012 Annual Report pg. 4

*pm 2013 E-13 1 of 1
min E-39*

The mail that built Canada Post is eroding like never before

Canada Post's core business has been the delivery of letters, bills, invoices, notices and statements. This mail built our network and workforce. This mail is our foundation – and our foundation is eroding.

Volumes of domestic Lettermail began to decline slightly in 2007. In 2009, the decline picked up speed. In 2012, the decline accelerated like never before. Canadians and Canadian businesses mailed almost one billion fewer Lettermail pieces in 2012 than they did in 2006. And, almost 30 per cent of that nearly one-billion drop occurred in 2012 alone. What does this decline look like on a typical workday?

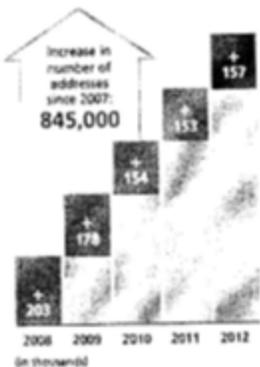
In 2012, we had nearly 1.1 million fewer pieces of domestic Lettermail in our system per business day than the year before; 1.7 million fewer pieces than two years ago, and 3.7 million fewer pieces than 2006, the year before the decline began.

Volumes are falling faster than ever. Nobody expects them to rebound. Mail will be with us for many years to come, but nobody knows how far or how fast volumes will drop. That is Canada Post's starkest challenge.

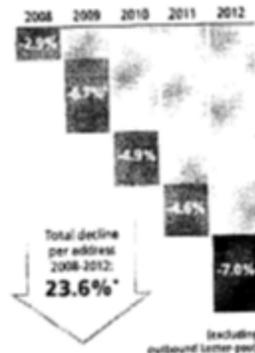


Transaction Mail decline per address

The number of addresses to which we deliver grows steadily each year...



...while the number of pieces of mail we deliver to each address is decreasing dramatically each year.



* Note: Due to a methodology change implemented in 2010, volumes for 2009 have been restated for comparability. Had 2008 volumes been restated, the decline per address for 2009 would have been 5.1% and the five-year total would have been 22.3%.

© 2012 Canada Post Annual Report

et cetera

Domestic Lettermail's decline: Picking up speed in 2012

In 2006, we delivered roughly five billion pieces of domestic Lettermail.

That number has dropped to roughly four billion pieces, and about 30 per cent of that decline was in 2012 alone.

In 2012, we delivered roughly **255 million** fewer pieces of domestic Lettermail than we did in 2011.

Year in Review: 2013

E-39

THE CONTINUING DECLINE IN LETTERMAIL VOLUMES...

Transaction Mail is Canada Post's core product. In 2013, volumes declined for the seventh consecutive year, as Canadians increasingly paid their bills and received their statements online.

Over the last seven years, Domestic Lettermail, our largest and most profitable product, has declined on average by more than 150 million pieces a year. In 2013, Domestic Lettermail volumes declined by 4.8 per cent. Canadians mailed almost 1.2 billion fewer pieces in 2013 than they did in 2006.



What does this decline look like on a typical workday?

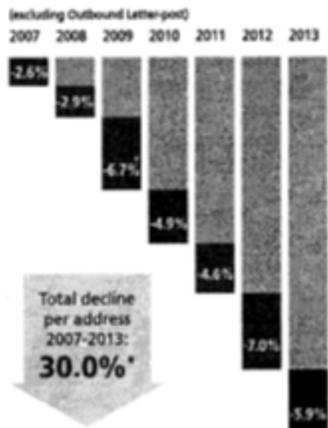
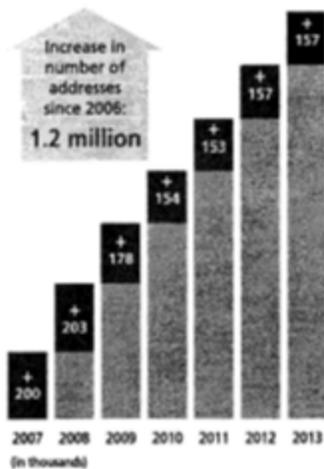
In 2013, we had roughly 760,000 fewer pieces of Domestic Lettermail in our system per business day than the year before, 1.8 million fewer pieces per day than two years ago, and 4.5 million fewer pieces per day than 2006.

Meanwhile, the number of addresses we serve has grown on average by more than 170,000 a year since Domestic Lettermail volumes began to decline in 2007.

Delivering fewer pieces of mail to an increasing number of addresses is not a formula for success.

Nobody expects Lettermail volumes to rebound, or knows how far and fast they will continue to drop before they level off. But the overall decline makes an indisputable case for significant change in the postal system.

Transaction Mail decline per address
The number of addresses to which we deliver grows steadily each year ...



... while the number of pieces of mail we deliver to each address has been decreasing dramatically each year.

Domestic Lettermail decline
In 2006, we delivered roughly **five billion** pieces of Domestic Lettermail.

That number has dropped to roughly **3.8 billion** in 2013.

Over the last seven years, Domestic Lettermail has declined on average by more than 150 million pieces per year.

In 2013, we delivered roughly **491 million** fewer pieces of Domestic Lettermail than we did in 2012, a year-over-year drop of **4.8 per cent**.

* Due to a methodology change implemented in 2010, volumes for 2009 were restated for comparability. Had 2008 volumes been restated, the decline per point of call for 2009 would have been 5.1% and the seven-year decline would have been 28.8%.

...AND THE GROWING DEMAND FOR PARCEL DELIVERY...



With the popularity of online shopping, Canada's business-to-consumer parcel delivery market is expected to grow significantly in the coming years. By 2017, the value of physical goods delivered to online shoppers in Canada is expected to climb to \$16.9 billion, up from \$9 billion in 2012, according to a leading Canadian market research firm.

While parcel delivery is a highly competitive business, Canada Post is in a strong position to meet the growing demand. It continues to be the market leader in business-to-consumer parcel delivery. Our parcel volumes grew by five million pieces compared to 2012, generating a revenue increase of 7.2 per cent. Revenues from our top e-commerce customers grew 29 per cent in 2013.

The 2013 holiday season was especially strong for Canadian e-commerce. Canada Post delivered over one million parcels on 10 different days during the six-week holiday period – up from two such days in 2012. Overall, parcel volumes for the holiday season increased by three million pieces compared to the 2012 holiday period.

...HAVE CREATED A NEED FOR A NEW POSTAL SYSTEM

Computers, tablets and smartphones are eroding the demand for traditional Domestic Lettermail. At the same time, online shopping is fuelling a growing need for convenient and reliable parcel delivery. As a result of these trends, Canada Post needs to make fundamental changes, and in 2013, it explored options to do so.

In April 2013, a Conference Board of Canada study projected Canada Post could lose close to \$1 billion a year by 2020, unless it makes fundamental changes to its business.

From May to September of 2013, our senior leaders visited 46 communities across Canada to consult with a cross-section of Canadians about their current and future postal needs. They met residential and business customers in every province. We also invited Canadians to comment online or in writing. Thousands responded, and the feedback helped form the basis for our Five-point Action Plan, which was released December 11, 2013.

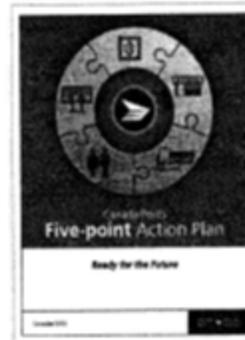
The plan introduced five initiatives, four that will reduce costs significantly, to meet

the changing needs of Canadians while helping to secure the future of the postal service for all Canadians:

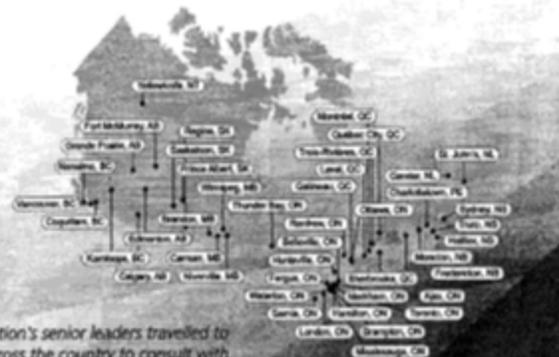
1. converting the one third of Canadian households that have door-to-door delivery to community mailbox delivery,
2. introducing a new tiered pricing structure for Lettermail,
3. expanding convenience through postal franchises,
4. streamlining operations,
5. addressing the cost of labour.

These initiatives will help return the Corporation to financial sustainability. Canada Post estimates that four of the five initiatives will improve its finances by between \$700 million and \$900 million a year.

The Corporation's senior leaders travelled to 46 communities across the country to consult with Canadians about their current and future postal needs.



Canada Post released the Five-point Action Plan on December 11, 2013.



Canada Post Corporation 2013 Annual Report

(On se souviendra que Madame Eckert avait reconnu cet état de fait. Voir le paragraphe 18 ci-dessus.)

[40] Parallèlement, la livraison des colis a augmenté considérablement au cours de la même période. En effet, en 2012, cette activité a correspondu à 22% des revenus de la Société. Néanmoins cette augmentation s'est avérée insuffisante pour compenser les pertes encourues par la livraison du courrier ordinaire.

[41] Il s'en est suivi que le secteur dirigé par Monsieur Hart a déployé des efforts en vue d'améliorer le service dans le but d'attirer de nouveaux clients (diriger les colis à des points de service désignés, livrer en soirée, etc.)

[42] Sans surprise, Monsieur Hart a également parlé des envois perdus ou volés, de même que des produits endommagés. Dans tous les cas, le destinataire se tourne vers le fournisseur, et ce dernier s'en prend ensuite à la Société. En 2012, ces réclamations ont coûté près de 5 millions de dollars à la Société. (Ce chiffre n'a pas varié en 2013, en dépit de l'augmentation du volume.)

[43] Pour les réclamations qui ne sont pas réglées, il existe un recours à l'ombudsman, dont le rapport parcellaire pour l'année 2013 fait état d'une diminution par rapport aux dix années précédentes, comme en fait foi le document reproduit à la page suivante (E-14).

(Le témoin n'a pas été en mesure de préciser dans quelle proportion ces réclamations provenaient de pertes ou de vol.)

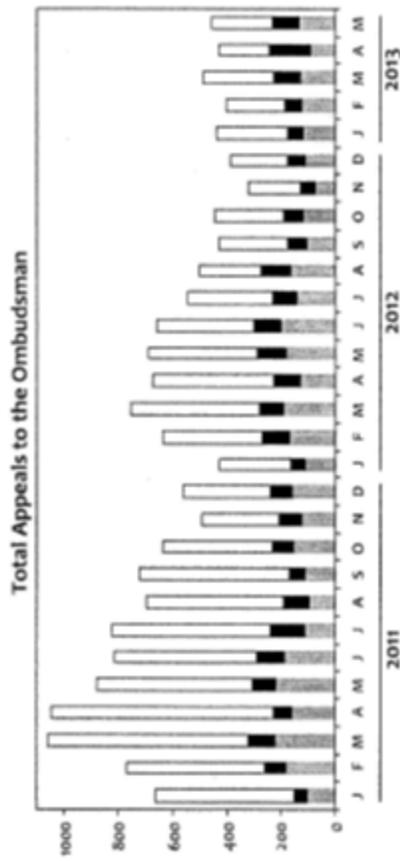
[44] Monsieur Hart a cependant affirmé sans ambages que la perte et le vol du courrier doivent être minimisés si la Société veut rester concurrentielle. Pour y parvenir, les mesures de sécurité doivent être resserrées, de façon à ce que son département puisse convaincre les clients que les effets qu'ils confient à la Société sont en sécurité.

14

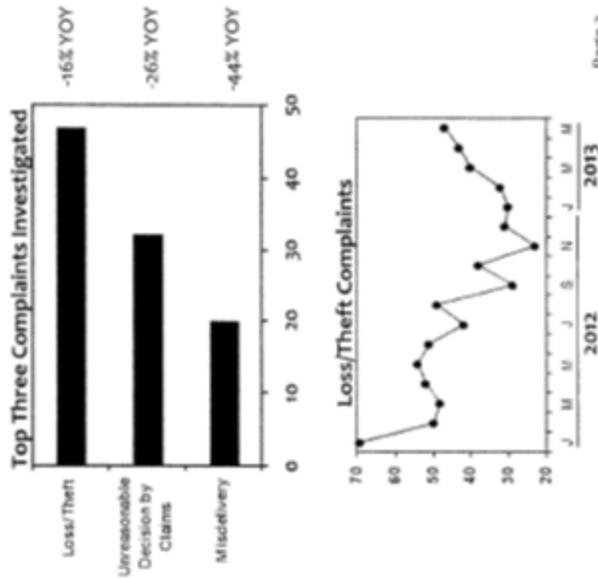
PROTECTED B

Appeals to the Ombudsman – May 2013 Snapshot

- Overall appeals in May were down 34% over last year and 19% fewer cases required investigation:
 - 456 appeals received resulting in 235 investigations.
 - 56% of appeals investigated required corrective action by Canada Post mainly in the form of improved compliance to procedures.
- Loss/Theft complaints continue to be the top issue and the upward trend continues:
 - 30% of these cases involved high value goods (cash/cashier's cheques, gift cards, jewellery, etc.);
 - 28% involved identity papers; and
 - 13% involved electronic goods, mainly cell phones.
- Unreasonable decisions by Claims typically reflect customers' discontent with policies regarding insurance coverage particularly pertaining to compensation for the loss of identity papers.
- Misdelivery cases dropped after the sudden increase in April but remain higher than the trend over the previous months.



- Discontinued (attempt to bypass Customer Service, dissatisfied with turnaround time, appeal withdrawn, etc.)
 - Appeal Denied (CPC complied with policies)
 - Corrective Action Required/Taken by Canada Post



Page 2

[45] Dans son C.V., Monsieur Tom Baltzer décrit son poste actuel comme ceci :

«Director, Product Management, Consumer Products and Services. »

[46] C'est en cette qualité qu'il a entrepris des démarches en vue de nouveaux débouchés d'affaires pour la Société, dont

- U.K.B.A. (United Kingdom Border Agency), de pair avec les Services d'immigration, en vue de l'authentification des visas, par exemple dans le cas d'une extension du visa d'un résident britannique. Il existe cinq centres de service dans le moment, et le projet est d'en mettre dix autres sur pied. Cette initiative a débuté en 2011, sous la forme de rencontres avec des représentants de U.K.B.A. et des Services d'immigration, mais il n'y a pas eu de consensus, vu le facteur de la sécurité. En mars 2013, l'entreprise V.F.S. Global a proposé à la Société de s'impliquer dans le processus, mais là encore le projet a dû être abandonné à cause de l'incapacité de la Société de satisfaire aux exigences en matière de sécurité.
- Driver Examination Services, pour la province d'Ontario. Pour ce projet, la Société a fait équipe avec deux partenaires. Là encore, certaines exigences n'ont pas pu être satisfaites, celles-ci incluant la prise des empreintes digitales et des vérifications aux trois ans. La Société a dû se retirer du projet.

[47] Certains autres débouchés étaient plutôt des perspectives d'affaires :

- B.C.I.D. (British Columbia Services Card Pass code program)
- Backcheck (Biometrer Criminal record check)
- Data Card Group.

[48] On trouvera à la page qui suit un aperçu des programmes existants, de ces débouchés d'affaires et de ces perspectives, ceci pour l'année 2013. C'est le document E-25. Les ententes en vigueur pour la même année sont mentionnées au document E-26, également reproduit ci-après.

[49] Monsieur Baltzer a reconnu que les évaluations de revenus dans les cinq mentionnés sous la rubrique «*Opportunities*» dans le document E-25 étaient essentiellement spéculatives.

[50] En sa qualité de «*general manager of strategic accounts*», Monsieur Don Bougie a, entre autres, la responsabilité de maintenir les contrats en vigueur et de les ajuster en fonction des nouveaux produits.

[51] De tels contrats ont été conclus, entre autres, avec l'Agence du revenu du Canada, le service des passeports du Canada, le bureau des achats (division du programme canadien de prêts aux étudiants et du recensement et division du transport du matériel)...

[52] A titre d'exemple, le contrat entre la Société et le service des passeports stipule, à son paragraphe 8.2, que «*Canada Post has an agreement with Treasury Board Secretariat whereby Canada Post has adopted and applies the requirements of the Security Policy of the Government of Canada (GSP), including the security screening of its employees. Canada Post will apply these procedures to employees acting as Receiving agents...*».

[53] C'est ce qui a poussé Monsieur Bougie à déclarer que vu que, dans l'état actuel des choses, la vérification de sécurité n'était faite qu'au moment de l'embauche et non de façon périodique tel que prévu à la Politique sur la sécurité du gouvernement fédéral, un tel manquement pourrait constituer un motif de bris de contrat. Cependant, en contre-interrogatoire, Monsieur Bougie a reconnu que ces contrats étaient des renouvellements d'ententes en vigueur depuis plusieurs années, et que ce manquement n'avait jamais été soulevé.

E-25

Retail, Consumer Products and Services
Business Overview
December 2013

Existing programs

1. Passport – Receiving agent program — *vide E-27a*
 - Revenue \$600K/yr (2012)
 - SRP \$20/ transaction
 - Approximately 30K transactions (2012)
2. HRSDC (Human Resources Skills Development Canada) – Student loan program — *vide E-28*
 - Revenue \$4 M (2012)
 - SRP \$6.46 to \$8.03 / transaction
 - Approximately 612K transactions (2012)

Opportunities

1. UKBA – United Kingdom Border Agency Visa Application Centre program
 - Estimated Revenue of \$1.85 Million/yr
 - SRP \$92/ transaction (\$42 counter + \$50 shipping) *E 94 .30*
 - Approximately 20K transactions
2. Driver Examination Services (DES) – Administering driver exams and tests on behalf of the Ontario Ministry of Transportation
 - Estimated Revenue of \$2.3 Million/yr
 - SRP \$8/ transaction (vision and knowledge testing) *) speculative*
 - Estimated approximately 287K transactions
3. Backcheck – Biometric Criminal record check via RCMP Live Scan RTID
 - Estimated Revenue of \$40 Million/yr
 - SRP \$40/ transaction
 - Estimated 1 Million transactions/yr*speculative vide E-32*
4. BCID – British Columbia Services Card pass code program
 - Estimated Revenue of \$3.6 Million/yr
 - SRP \$4 / transaction
 - Average 900K /yr (then 300K /yr after initial volume)*vide E-31*
5. Card Issuance – Printing of replacement cards and ID cards (Data Card Group / Census Canada)
 - Market volume (estimate 2 Million /yr)
 - CPC share 5%
 - \$10 - \$15 / transaction
 - Estimated Potential revenue \$1M to \$1.5M /yr*(speculative)*

E-26

Strategic Accounts – Public Sector
Business Overview
December 2013

Existing Agreements

- Passport Cda – Transportation and Distribution of Passports (Protected B)
- Transportation and Distribution of Passport related documents with RFID
- Revenue \$33 M/yr (2012)
 - Approximately 3 M transactions (2012)
 - Total estimated value of agreement over 3 years – \$99 M

> Vide E-34

HRSDC (Human Resources Skills Development Canada) – Student loan program

- Revenue \$4 M (2012)
- SRP \$6.46 to \$8.03 / transaction
- Total value of agreement over 3 years - \$8.1 M

CRA (Canada Revenue Agency) – Courier Services with RFID (Protected B)

- Revenue \$4.9 M (2012)
- Total value of agreement over 4 years plus 3 option yrs - \$35 M

> Vide E-33

Government of Canada Standing Offer Agreement (PWGSC) – Courier Services with Protected B Security Checklist

- Revenue \$23.4 M (2012)
- Total value of the Standing Offer agreement 1 year plus 1 option yr - \$48 M

[54] Selon Monsieur Bougie, les banques et les compagnies de téléphone manifestent de plus en plus des préoccupations en matière de sécurité. Pour illustrer ce propos, le témoin a déposé en preuve un projet de contrat proposé par Apple Inc., où on peut lire le passage qui suit :

Paragraphe 3.2: «... *Supplier will, subject to applicable national employment, data protection and privacy laws, screen all employees and contractors at its own expense, using background checks and drug tests at least as stringent as those Apple uses in connection with its own employees...*»

et un autre projet de contrat, cette fois avec la compagnie Pitney Bowes:

Paragraphe 8.2: «*Services Provider agrees to conduct on all its employees... background checks for the previous seven year period covering criminal convictions and employment verification...*»

(A noter qu'un contrat a été signé entre la Société et Pitney Bowes le 6 juin 2014. La clause ci-dessus ne s'y retrouve pas.)

[55] (Il importe de souligner que la preuve a été beaucoup plus poussée en ce qui a trait aux contrats existants, ainsi qu'aux discussions en cours avec les clients potentiels. Néanmoins, vu la conclusion à laquelle le tribunal en est venu, il n'est pas nécessaire d'élaborer.)

La Position du Syndicat

[56] Avant *cette «pratique»* que la Société se proposait de mettre en vigueur le 29 avril 2013, les vérifications relatives à la sécurité se faisaient strictement au moment de l'embauche. Avec cette directive, tous les salariés à l'emploi de la Société devraient se soumettre à ces vérifications d'une façon régulière, comme on peut le lire à la page 5 du document reproduit plus haut à la suite du paragraphe (6) :

«Afin d'assurer le maintien de fiabilité des personnes, une mise à jour régulière des enquêtes de sécurité doit être effectuée.»

Tel qu'indiqué à la page 9 du même document, cette mise à jour serait effectuée *«... une fois tous les dix ans ou plus souvent (selon les modifications apportées aux autres tâches, aux ententes contractuelles, aux lois ou autres obligations...)»*. Ce qui a fait dire au procureur du syndicat que ce serait *«au gré du vent...»*

[57] A l'occasion d'une telle mise à jour de la cote de fiabilité, la vérification des empreintes digitales peut s'avérer nécessaire *«si la personne déclare avoir eu une condamnation pour (une) infraction criminelle pour laquelle elle n'a pas obtenu un pardon»*, ou encore, si *«la GRC en fait la demande afin de mener à bien la vérification du dossier judiciaire...»* (page 10 du document reproduit). En cas de refus de l'employé, celui-ci est *«susceptible d'être suspendu... jusqu'à ce que toutes les exigences de cette pratique soient atteintes et (il) peut même être congédié»*. (page 12)

[58] La politique proposée va un peu plus loin quant aux circonstances où un employé peut être requis de fournir ses empreintes digitales :

Page 13 : 4. *«La Société peut exiger des empreintes digitales en cas de modifications aux fonctions de l'employé, aux ententes contractuelles ou à la loi, ou encore pour satisfaire à d'autres obligations ».*

(Ce sont les mêmes termes qui sont utilisés en ce qui a trait aux mises à jour.)

[59] Après avoir passé en revue les témoignages au soutien des motifs invoqués par la Société pour justifier la politique proposée, le procureur du syndicat en est venu à préciser ce qu'était *«le droit applicable»*, soit la convention collective et les dispositions législatives relatives à la protection de la vie privée et des renseignements personnels.

[60] Voici comment Maître Philion a résumé la position du syndicat en ce qui a trait aux dispositions de la convention collective, au paragraphe 265 de son argumentaire :

«Le Syndicat soumet que les dispositions de la convention collective en vigueur ne permettent pas à la Société de requérir des employés qu'ils se soumettent, après leur embauche ou en cours d'emploi, à un processus de vérification de sécurité. A plus forte raison, la Société ne peut requérir de vérification récurrente de sécurité comme elle envisage de le faire par sa politique.»

[61] Il a alors cité l'article 2.01 de la convention collective :

«Il est reconnu que la Société exerce les droits et les responsabilités de la direction sous réserve des dispositions de la présente convention collective.»

[62] L'arbitre Richard B. Bird avait fait état de cet article dans sa décision du 3 mai 1988 (Canada Post Corporation and Canadian Union of Postal Workers, grievance no : 730-85-00037, 34 L.A.C. (32) 392), indiquant que cette disposition était celle que la Société invoquait pour justifier la demande aux salariés qu'ils soumettent leurs empreintes digitales (paragraphe 11 de la décision).

[63] L'arbitre Bird a également référé à l'article 9.06 (maintenant 9.08) et à l'article 9.07 (b) (maintenant 9.09 (b)) :

9.06: *«An authorized representative of the Union may present a grievance if he believes that an employee, a group of employees the employees as a whole or the Union have been aggrieved or treated in an unjust or unfair manner. »*

9.07: *«An authorized representative of the Union may present a policy grievance in order to obtain a declaratory decision. Without restricting the generality of the above, a policy grievance may be presented in the following cases:*

(b) *where the Union is of the opinion that a policy, directive, regulation, instruction or communication of the Corporation has or will have the effect of contravening any provision of the collective agreement, of causing prejudice to employees or the Union or of being unjust or unfair to them. »*

[64] Cette décision de l'arbitre Bird mérite qu'on s'y arrête, vu que la question dont il avait été saisi est essentiellement la même que celle qui est soumise au tribunal dans la présente affaire :

Paragraphe 27: *«There is a contest here between the individual employee's right to privacy and the employer's need for reliable employees in handling the mail...*

...Are the special needs of the employer so important that the Corporation can properly claim that its management rights include the right to require employees to give fingerprints so that the reliability checks may be completed ?»

[65] Aux paragraphes 280 et suivants de son argumentaire, le procureur du syndicat traite de *«la protection de la vie privée et des renseignements personnels»*; voici les dispositions législatives sur lesquelles il s'appuie :

- La Charte canadienne des droits et libertés :

Article 1 : *« La Charte canadienne des droits et libertés garantit les droits et libertés qui y sont énoncés. Ils ne peuvent être restreints que par une règle de droit, dans des limites qui soient raisonnables et dont la justification puisse se démontrer dans le cadre d'une société libre et démocratique,»*

Article 7 : *«Chacun a droit à la vie, à la liberté et à la sécurité de sa personne; il ne peut être porté atteinte à ce droit qu'en conformité avec les principes de justice fondamentale.»*

Article 8 : *«Chacun a droit à la protection contre les fouilles, les perquisitions ou les saisies abusives»*

- La Loi sur la protection des renseignements personnels, L.R.C. (1985) ch. P-21 :

Article 3 (Définition) : *«Renseignements personnels – Les renseignements quels que soient leur forme et leur support, concernant un individu identifiable, notamment :*

... b) les renseignements relatifs à son éducation, à son dossier médical, à son casier judiciaire, à ses antécédents professionnels ou à des opérations financières auxquelles il a participé

Article 8 (1) : *«Les renseignements personnels qui relèvent d'une institution fédérale ne peuvent être communiqués, à défaut du consentement de l'individu qu'ils concernent, que conformément au présent article,*

Article 8 (2) : *«Sous réserve d'autres lois fédérales, la communication des renseignements personnels qui relèvent d'une institution fédérale est autorisée dans les cas suivants :*

m) communication à toute autre fin dans les cas où, de l'avis du responsable de l'institution :

(2) des raisons d'intérêt public justifieraient nettement une éventuelle violation de la vie privée...»

[66] Le procureur du syndicat souligne ensuite qu'il *«importe de distinguer, parmi la jurisprudence applicable à des vérifications de sécurité, celle qui porte sur l'application de normes de vérification de sécurité imposées par des lois et des règlements, de celles découlant de politiques adoptées par des employeurs...»* (sic) (paragraphe 310 de l'argumentaire syndical) Plus loin, au paragraphe 318, on peut lire ce qui suit :

« En l'espèce, les motifs invoqués par la Société sont plutôt de l'ordre de ses intérêts commerciaux et ne visent nullement à protéger la santé ou la sécurité du public, de ses clients ou de ses employés. »

[67] Il existe, en effet, des situations où les vérifications de sécurité sont imposées aux termes d'une loi, par exemple lorsqu'il s'agit de transport maritime ou aérien, ou lorsque les employés visés sont en contact régulier avec des mineurs ou des personnes de âgées. Dans le cas sous étude, il s'agit simplement d'une règle d'entreprise qui n'est soutenue par aucune disposition législative, et qui n'est justifiée que par des intérêts commerciaux. Au surplus, s'il s'agit d'une exigence imposée par un tiers, celle-ci ne peut être invoquée pour modifier de quelque façon les obligations des parties aux termes de la convention collective ou des lois applicables.

[68] Parlant de *«la proportionnalité ou la mise en balance des intérêts»*, le procureur du syndicat a proposé ce qui suit au paragraphe 370 de son argumentaire :

«Les intérêts en cause sont les suivants : les employés ont le droit de préserver leur vie privée et leurs informations personnelles, la Société invoque son obligation de protéger le courrier et vise à satisfaire sa clientèle actuelle ou éventuelle.»

La Position de la Société

[69] Le procureur de la Société a d'abord résumé la situation actuelle en regard de celle qui est envisagée par la Politique contestée. Dans le moment, on procède à la vérification de sécurité lors de l'embauche d'un salarié et lors d'une mutation à un poste commandant une

cote de sécurité plus élevée. La seule différence importante, sous le régime proposé, consiste dans une vérification en cours d'emploi pour les salariés qui possèdent déjà la cote de fiabilité.

[70] Une telle mise à jour est prévue dans la Politique sur la sécurité du gouvernement (Gouvernement du Canada). Depuis plus de vingt-cinq années, la Société s'est engagée à adopter les exigences de cette Politique et à les appliquer à son organisation. La preuve a démontré que la Société avait conclu avec le gouvernement du Canada, au fil des années, «*plusieurs ententes de grande importance en terme de revenu*» (sic) (paragraphe 26 de l'argumentaire patronal). A ce sujet, Maître Forget a écrit, un peu plus loin :

Paragraphe 28 : *«De fait, la perte ou le non-renouvellement de contrats avec le gouvernement du Canada et l'impossibilité de continuer les efforts pour obtenir de nouveaux contrats, au motif d'impossibilité de rencontrer les normes de vérification de sécurité, auraient un impact négatif considérable sur les revenus générés par la S.C.P.» (mon souligné)*

[71] Ce thème a été repris dans un commentaire que le procureur de la Société a formulé en regard d'un extrait d'un rapport du vérificateur général au printemps 2013, soit une recommandation au Conseil du trésor :

«... Nous soumettons que dans un tel contexte, il est probable qu'un audit ait lieu concernant les différents contrats entre la S.C.P. et le gouvernement du Canada, que l'absence de vérification en cours d'emploi entraîne la perte ou le non-renouvellement de nombreux contrats à moins que la S.C.P. puisse appliquer en totalité sa politique intitulée Pratique relative à l'enquête de sécurité du personnel». (Argumentaire patronal, paragraphe 62)

[72] Le défaut d'une telle vérification en cours d'emploi porte aussi atteinte aux diverses possibilités d'affaires que les représentants de la Société ont explorées dans le but de générer des revenus pour compenser les pertes considérables du courrier ordinaire depuis 2007.

Comme en a témoigné Madame Rita Estwick, les clients, actuels ou éventuels, se sont montrés préoccupés par cette absence de vérification en cours d'emploi des employés de la Société, le tout tel qu'illustré par le rapport de 2012 de la GRC, dont la conclusion se lisait comme suit :

«This assessment confirmed that the Canadian postal system, more specifically Canada Post, is utilized by criminals to transport various contraband both domestically and internationally. »

(Au stade des représentations, Maître Forget a qualifié ce rapport de «*troublant*».)

[73] Le procureur de la Société a soumis qu'il n'existait *«aucune disposition de la convention collective limitant le droit de la S.C.P. de mettre en place des politiques concernant la sécurité des biens et des employés, et, notamment, d'exiger l'obtention d'une cote de sécurité.»* (paragraphe 65 a) de l'argumentaire patronal) Il a continué en soumettant que ce droit était en opposition avec celui des employés quant au respect de leur vie privée, tel que reconnu par la Charte; ce droit n'est pas absolu, de sorte que le tribunal doit *«dans chaque situation, équilibrer les droits opposés et déterminer, à la lumière de la preuve présentée et des critères développés par les tribunaux, s'il y a ingérence indue.»* (sous-paragraphe c) du même paragraphe 65)

[74] Ces principes ont été acceptés par l'arbitre Bird dans sa décision de 1988 :

Paragraphe 23: *«It is the Corporation's position that there is no implied term in the collective agreement which restricts the exercise of management rights under Article 2.01 so that such rights must be exercised justly and fairly. I accept that position as correct...»*

L'arbitre Bird écrit, un peu plus loin:

Paragraphe 27: *«There is a contest here between the individual employee's right to privacy and the employer's need for reliable employees in handling the mail... Are the special needs of the employer so important that the Corporation can properly claim that its management rights include the right to require employees to give fingerprints so that the reliability checks may be completed ? »*

[75] Au paragraphe 29 de sa décision, l'arbitre Bird, continuant dans son analyse des intérêts en présence, a conclu, relativement aux empreintes digitales, que

«No doubt many probationary employees are embarrassed by having their fingerprints taken regardless of their criminal records, if any. I take it from authorities that the taking of fingerprints is regarded as a serious invasion of privacy which, as a matter of (the) general law, can be justified in a particular situation only by specific statutory authority. »

Il a ensuite statué que *«la prise d'empreintes durant l'emploi constitue une intrusion significative dans les droits civils des employés»*, tel que rapporté par le procureur de la Société au paragraphe 70 de son argumentaire.

[76] Quant à l'applicabilité de l'article 9.103 de la convention collective par rapport à cette décision de l'arbitre Bird, voici ce qu'a proposé le procureur patronal dans son argumentaire :

Paragraphe 72 : *«Une décision sur le sujet de l'intrusion dans la vie privée doit être rendue à la lumière des faits de chaque cas et des principes établis par les tribunaux et, notamment, la Cour suprême du Canada; principes qui ont été en constante évolution au cours des années, ainsi que de la preuve factuelle présentée et, partant, l'article 9.103 de la convention collective n'a aucune application dans le présent cas.» (sic)*

(C'est là en quelque sorte une autre façon d'exprimer la position prise par les représentants de la Société lorsque le syndicat avait fait état de cette décision de l'arbitre Bird lors de la rencontre du 25 janvier 2013 :

«La S.C.P. répond qu'en 1988, le monde était très différent de ce qu'il est aujourd'hui et que les attentes du marché en matière de sécurité ont considérablement changé depuis.» (Voir le paragraphe 14 ci-dessus)

[77] Maître Forget y est ensuite allé de commentaires sur la jurisprudence relative à cet équilibre à établir entre les droits en présence, plus particulièrement quant aux restrictions raisonnables qui peuvent être apportées aux droits et libertés protégés par la Charte, ceci *«dans le cadre d'une société libre et démocratique»* :

- Sa Majesté la Reine c. Walter Tessling et al, [2004] 3 R.C.S. 432;
- Sa Majesté la Reine c. Daniel James Gombor et al, [2010] 3 R.C.S. 211;
- R. c. Oakes, [1986] 1 R.C.S. 103;
- Renvoi relatif au Règlement sur la sûreté du transport maritime (CA), 2009 CAF 234 (Can LII);
- R. c. Beare [1988] 2 R.C.S. 387.

[78] Après avoir cité un certain nombre d'autres décisions où la prise d'empreintes digitales avait été jugée raisonnable dans le contexte de la mise en œuvre d'une loi ou d'une réglementation d'ordre public (transport aéroportuaire ou maritime, transport scolaire, résidence privée pour aînés, installations nucléaires, etc.) le procureur de la Société y est allé de l'affirmation suivante :

Paragraphe 95 : *«En ce qui concerne la S.C.P., la preuve démontre une problématique similaire à la problématique portuaire et aéroportuaire en matière de contrebande, crime organisé et de menace à la sécurité nationale...»*

(Le seul fondement pour cette affirmation étant le rapport de la GRC dont il a été question plus haut.)

[79] Voici deux des conclusions de l'argumentaire de la Société :

Paragraphe 99 : *«Il est également essentiel que la S.C.P. puisse maintenir ses contrats avec les grands expéditeurs de courrier tel que le gouvernement et les entreprises qui demandent à la S.C.P. de recevoir, traiter et distribuer des documents de haute valeur et de haut niveau de confidentialité, et soit en mesure de développer de nouveaux services qui demandent un haut niveau de sécurité.»*

Paragraphe 100 : *«Si la S.C.P. ne peut vérifier les antécédents judiciaires de ses employés, elle ne pourra soumissionner sur ce type de contrat et ne pourra compenser ses pertes importantes en matière de poste-lettres par de nouveaux revenus.»*

Décision

[80] Il convient de reproduire ici le texte de l'article 9,103 de la convention collective :

«Cas à venir :

La décision finale rendue par un arbitre lie la Société, le Syndicat et les employées, et employés dans tous les cas comportant des circonstances identiques et (ou) substantiellement identiques.»

et dans la version anglaise :

«Future Cases :

The final decision rendered by an arbitrator binds the Corporation, the Union and the employees in all cases involving identical and/or substantially identical circumstances. »

[81] Il n'y a pas de litige entre les parties quant à la nature de la décision rendue par l'arbitre Bird en 1988 : il s'agit bien d'une «*décision finale*» quant à un grief (numéro 730-85-00037) entre les parties en présence «*in the matter of fingerprinting*».

[82] A la lecture de cette décision, et, en particulier, à la lumière du passage qui suit, il ne fait pas de doute que les «*circonstances*» du cas dont l'arbitre Bird était saisi étaient «*substantiellement identiques*» à celle de l'affaire sous étude :

Paragraphe 34 : «*...The right of privacy, including the right if an employee to refuse to permit an employer to take fingerprints, is fundamental to any free society and should not be infringed upon by an employer in the absence of clear and unequivocal statutory authority, clear and unequivocal contractual language or by a clear and compelling inference to be drawn from contractual language. None of these is present in the grievance before me. »*

[83] Un des changements majeurs dans la Pratique proposée par la Société consiste dans la «*mise à jour régulière des enquêtes de sécurité*». On peut lire ceci dans le document reproduit à la suite du paragraphe 6 ci-dessus :

Page 2, article 3 : «*... Pour toutes les enquêtes de sécurité, une vérification du casier judiciaire est requise et, dans certains cas, une vérification des empreintes digitales, une vérification de solvabilité et une entrevue sont requises.*»

[84] Plus loin, dans le même document, à la page 6, paragraphe 6 intitulé «*non-conformité*», il est écrit :

«Il incombe à tous les employés de Postes Canada, à tous les niveaux, de se conformer à cette pratique. Le refus de coopérer au cours du procédé de vérification ou le non-respect de cette pratique pourrait entraîner l'application des mesures disciplinaires suivantes :

... Un employé actuel qui ne coopère pas au cours de la mise à jour ou de la révision du processus de vérification de sécurité visant à trouver une cause ou qui ne se conforme pas à cette pratique est susceptible d'être suspendu... jusqu'à ce que toutes les exigences de cette pratique soient atteintes et peut même être congédié.»

(La mise à jour de la cote de fiabilité doit se faire à tous les 10 ans ou plus souvent, comme on peut le lire à la page 9 du document, *«selon les modifications apportées aux tâches, aux ententes contractuelles, aux lois ou aux autres obligations...»* (mon souligné) Le même texte se retrouve à la page 12 de la Pratique.)

[85] Ce que la Société se propose de faire avec cette Pratique, aux termes de l'article 2.01 de la convention collective (droits de la Direction), se rapproche donc substantiellement de ce qu'elle avait entrepris en 1988, comme l'a indiqué l'arbitre Kenneth P. Swan dans sa décision préliminaire du 26 avril 2013 :

Page 12: *«Arbitrator Bird decided that, while the Corporation relied on the management rights provision, Article 2, there were limitations on the exercise of rights under that article. In the absence of real consent by the employees, or the agreement of the Union, the arbitrator found that privacy interests of individual employees out-weighed the interests of the Corporation in pursuing criminal record background checks. In short, Arbitrator Bird found a violation of Article 2 and, at least potentially, of clause 10.01 if discipline should be invoked to compel the production of fingerprints...»*

(et un peu plus loin, à la même page :)

«To do what is proposed, the Corporation will have to act in contravention of the collective agreement as interpreted by an arbitrator in a formal arbitration hearing. Whatever arguments may be made in respect of applying the Fingerprinting award in the future, there is a clear prima facie case of contravention as long as that award continues to apply. »

[86] Bien que le principe de la res judicata soit moins rigide dans le domaine arbitral que dans celui des tribunaux de droit commun, surtout en common law, il n'en demeure pas moins que ce principe s'applique en matière de relations de travail, mais avec le bémol apporté par le professeur Bora Laskin dans la décision de *Brewers Warehousing*, (1954) 5 L.A.C. 1797 :

«It is not good policy for one Board of Arbitration to refuse to follow the award of another Board in a similar dispute between the same parties arising out of the same Agreement where the dispute involves the interpretation of the Agreement. Nonetheless, if the second Board has the clear conviction that the first award is wrong, it is its duty to determine the case before it on principles that it believes are applicable. »

[87] Cette décision a été citée avec approbation par l'arbitre Michel G. Picher dans une affaire mûre entre les parties en présence, décision du 12 février 2012 (*Technological Change – Vancouver MPP National Policy grievance number N00-07-00030*), où il cite également les auteurs Palmer et Palmer, *Collective Agreement Arbitration in Canada*, 3rd Edition at pp. 153-154 :

«It is clear that res judicata applies not only during the life of the collective agreement in force at the time of the first award, but also until the wording is changed or the parties mutually agree on a new interpretation. »

[88] Voici comment l'arbitre Picher s'est exprimé, en regard de ces principes, à la page 33 de sa décision du 12 février 2012 :

«In my view the rationale for the above principles is easily understood. In the Canadian system of collective bargaining, following the certification of a trade union as the bargaining agent for a group of employees, the employer and the union enter into an ongoing bargaining relationship which is anticipated to continue over a number of years, through successive collective agreements. As common sense would suggest, through the years of a bargaining relationship and the resolution of grievances, whether by settlement or through binding arbitration, the parties refine their understanding of their collective agreement and stabilize their mutual expectations as to the scope and interpretation of their agreement accordingly. So understood, the principle whereby parties are bound to respect the rulings of boards of arbitration under a given collective agreement and to continue to respect those rulings under a subsequent collective agreement where no change in language has been made with respect to the relevant provisions of the collective agreement, assures the very stability of collective agreements and collective bargaining relationships. »

[89] Et l'arbitre Picher de continuer en ces termes, à la page 34 :

«In my view the parties to the instant dispute have mutually imported the principles developed in the jurisprudence discussed above into the text of their collective agreement. That is evident from the language of article 9.103 of the collective agreement. »

[90] Finalement, à la page 36 de sa décision, l'arbitre Picher s'exprime comme suit:

«...in keeping with long established Canadian jurisprudence, I am satisfied that by the language of article 9.103 the parties intended that matters fought out between them over the years and ultimately resolved by final and binding

arbitration under prior collective agreements of identical language must be considered as settled and binding upon them. To conclude otherwise is to conclude that the parties consciously intended to sweep away the effect and value of all previous arbitration awards with the renewal of each collective agreement effectively inviting the mischief of forum shopping and the relitigation of long settled arguments. I cannot accept, as a matter of responsible collective bargaining, that is what the parties intended. »

Je ne saurais dire mieux.

[91] Tel que rapporté au paragraphe (82) ci-dessus, l'arbitre Bird a décidé que le droit à la vie privée des employés ne doit pas subir d'empiètement par leur employeur, sauf si celui-ci peut invoquer un texte de la loi ou une disposition non équivoque dans la convention collective donnant ouverture à un tel empiètement.

[92] Ici la Société n'a pas fondé la pratique proposée sur une telle disposition de la convention collective, autre que celle consacrant ses droits de gérance (article 2.01), tout comme ce fut le cas devant l'arbitre Bird.

[93] Dans la grande majorité des décisions citées par le procureur de la Société où cette exigence des empreintes digitales avait été jugée raisonnable, il y avait un texte de loi (« *clear and unequivocal statutory authority*») justifiant que l'on puisse déroger à la restriction posée par les articles 7 et 8 de la Charte et par la Loi sur la protection des renseignements personnels, L.R.C. (1985), ch. P-21.

[94] Voici quelques-unes de ces décisions en regard de la Loi ou du règlement invoqués pour justifier une telle dérogation :

- Renvoi relatif au Règlement sur la sûreté du transport maritime(CA), 2009 CAF 234 (Can L II), où la Cour fédérale d'appel avait à analyser le Règlement sur la sûreté du transport maritime, DORS/2004-144; et pour arriver à cette fin, la

Cour devait mettre «*en balance l'intérêt des employés en ce qui a trait à leur vie privée avec les intérêts publics visés par le «régime législatif.»*» (Paragraphe 49) (mon souligné)

(Il convient de citer un autre extrait de cette décision de la Cour fédérale d'appel.

Paragraphe 11 : «*Le programme fédéral fait partie d'un processus d'examen de la sécurité mis sur pied par Transports Canada en 2002, en partie en réaction à l'attentat du 11 septembre 2001 contre World Trade Center à New York.»*)

- Les Autobus Transco (1988) inc. Et Le Syndicat des travailleurs de Transco, Maître François Hamelin, 18 juin 2010000. La Loi de l'instruction publique, RLRQ, c. I-13.3

Paragraphe 87 : «*...Pour conserver leur emploi, ils doivent donc divulguer leurs antécédents, puisque l'obligation de protéger les élèves mineurs prime sur le respect de la vie privée des conducteurs.»*

- Syndicat du transport scolaire de la Mauricie et Autobus la Mauricie inc. D.T.E. 2011T-600 La Loi de l'instruction publique et La Loi sur l'enseignement privé RLRQ, c. E-9.1.
- Greater Toronto Airports Authority v. P.S.A.C., Local 0004, L.A.C. (4TH) 179, C.L.A.S. 494 – Le Programme d'habilitation de sécurité en matière de transport.

[95] Les situations envisagées dans ces décisions, et dans quelques autres citées par le procureur de la Société, portaient sur des circonstances tout à fait particulières, comme l'a résumé Maître Forget au paragraphe 90 de son argumentaire :

«Il est manifeste que les gouvernements portent une attention de plus en plus grande en matière de sécurité et d'antécédents judiciaires visant notamment à prévenir le terrorisme, la contrebande et le crime organisé (voir règlements en matière portuaire et aéroportuaire) et protéger des clientèles à risque, notamment les mineurs et les personnes âgées ainsi que pour viser des employés qui acceptent des postes de confiance tel que pompier et policier.»

[96] Ces considérations nous emmènent loin de notre débat, surtout tel que restreint par la décision de l'arbitre Bird, qui, comme on l'a vu plus haut, a statué que

«...the taking of fingerprints is regarded as a serious invasion of privacy which... can be justified in a particular situation only by specific statutory authority. »
(paragraphe 29 de la décision).

[97] Il est exact, comme l'a représenté le procureur de la Société, que les conditions, de même que le droit applicable, ont évolué depuis 1988. Néanmoins, elles n'ont pas changé au point de justifier une dérogation à la décision Bird, d'autant moins que les dispositions de la convention collective sont restées les mêmes au fil des années, en particulier les articles 2.01 et 9.103.

[98] Le présent débat est substantiellement le même que celui dont l'arbitre Bird était saisi, du moins en ce qui a trait aux passages importants de la Pratique qui ont été contestés par le grief du 11 avril 2013. Il s'en suit que les parties sont liées par la décision Bird, et qu'il est du devoir de l'arbitre de reconnaître l'obligation que leur impose l'article 9.103.

Dispositif

[99] En conséquence, le tribunal conclut que la Pratique relative à l'enquête de sécurité sur le personnel porte atteinte à la liberté et à la vie privée des employés, qu'elle viole les dispositions de la convention collective et de la Charte canadienne des droits et libertés, et

qu'elle va à l'encontre de la décision de l'arbitre Richard B. Bird rendue le 3 mai 1988, ceci en contravention de l'article 9.103 de la convention collective.

[100] Il est ordonné à la Société de cesser d'exiger que les employés autorisent la vérification de leurs antécédents criminels, leur dossier de crédit et autres informations personnelles, et soient tenus de fournir leurs empreintes digitales à la Société ou à ses représentants.

[101] Il est ordonné à la Société de cesser d'imposer des mesures de représailles aux employés qui ont refusé d'autoriser la vérification de leurs informations personnelles.

[102] Le tribunal garde compétence au cas de mésentente entre les parties dans la mise en œuvre de la présente décision.

Montréal, ce 19 novembre 2014

CLAUDE LAUZON, Arbitre