

Mémoire à l'intention du Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique

Au sujet de

l'étude sur l'utilisation par le gouvernement fédéral d'outils technologiques permettant d'extraire des renseignements personnels des appareils mobiles et des ordinateurs

3 mars 2024



Public Service Alliance of Canada
Alliance de la Fonction publique du Canada

Mémoire à l'intention du Comité permanent de l'accès à l'information, de la protection des renseignements personnels et de l'éthique

Au sujet de

l'étude sur l'utilisation par le gouvernement fédéral d'outils technologiques permettant d'extraire des renseignements personnels des appareils mobiles et des ordinateurs

L'Alliance de la Fonction publique du Canada (AFPC) représente près de 230 000 personnes, d'un bout à l'autre du pays et à l'étranger. Nos membres travaillent, entre autres, pour des organismes et ministères fédéraux, des sociétés de la Couronne, des universités, des casinos, des organismes de services communautaires, des collectivités autochtones, des aéroports, ainsi que dans le domaine de la sécurité. En plus de son siège social à Ottawa, l'AFPC compte 23 bureaux régionaux à l'échelle du Canada.

La plupart de ses membres travaillent au quotidien avec des outils technologiques fournis par l'employeur, tant pour le travail en personne que pour le télétravail.

Nous reconnaissons que, dans le cadre de leur travail, bon nombre de nos membres participent à des enquêtes, des recherches, des saisies et d'autres activités liées à l'application de la loi ou à la sécurité, et qu'ils se servent d'outils technologiques pour s'acquitter de ces tâches.

Nous avons plusieurs raisons de craindre l'utilisation d'outils capables d'extraire des données personnelles des appareils en l'absence de processus solides d'encadrement de leur utilisation, de protection des renseignements personnels concernant les employés et d'explication des motifs de leur déploiement.

Le libellé des conventions collectives d'un grand nombre de fonctionnaires fédéraux syndiqués travaillant dans des centres d'appels est sans équivoque :

La surveillance d'appels vise à améliorer le rendement du personnel en offrant des conseils et une rétroaction. La surveillance d'appels ne doit pas servir à imposer des mesures disciplinaires¹.

Les conclusions de la surveillance, recueillies à des fins de perfectionnement professionnel, doivent être pertinentes et transmises rapidement aux employé-e-s.

Notre plus grande préoccupation découle du fait qu'un grand nombre de ministères ont failli à leur responsabilité de mener des évaluations des facteurs relatifs à la vie privée (ÉFVP). Cette attitude passive à l'égard d'un aspect important de la protection des renseignements personnels des fonctionnaires est inacceptable, surtout en contexte de développement rapide de nouvelles technologies toujours plus intrusives. Même si aucun de nos membres n'a encore porté plainte au sujet de logiciels espions, il se peut, compte tenu du caractère secret de tels programmes, que certaines personnes soient actuellement surveillées sans le savoir; cette possibilité appelle la mise en place d'ÉFVP transparentes.

¹ Services des programmes et de l'administration (PA), convention entre le Conseil du Trésor et l'Alliance de la Fonction publique du Canada, <https://psacunion.ca/sites/psac/files/attachments/pdfs/pa-fra.pdf>

Dans l'éventualité où de tels outils seraient utilisés par nos membres ou pour surveiller nos membres, nous exigeons que toutes les ÉFVP soient effectuées préalablement à l'installation de l'outil et passées en revue tout au long du cycle de vie de l'outil, notamment lors des mises à jour, et que toutes les conclusions des ÉFVP soient communiquées de façon proactive aux membres du personnel et au syndicat. De plus, le syndicat devra être tenu informé, de manière proactive, des motifs d'une intrusion dans la vie privée des membres et de sa pertinence relativement au problème à résoudre.

Par exemple, si l'on soupçonne, preuves à l'appui, une personne salariée de commettre des actes criminels, l'installation de logiciels espions sur l'ensemble des ordinateurs de la section ne sera pas une mesure appropriée. Ce genre de méthode soulève des questions : est-ce que les preuves initiales justifient effectivement l'installation d'un logiciel espion ou est-ce qu'un tel logiciel est installé pour trouver des preuves sur la seule base de rumeurs ou de soupçons?

De plus, le manque de mesures correctives visant les hauts fonctionnaires dans la directive du Conseil du Trésor à ce sujet est préoccupant. On semble s'attendre, de façon implicite, à ce que les gestionnaires, les chefs, les directeurs et d'autres personnes occupant de hauts postes décisionnels agissent toujours en conformité avec leur serment ou leur code de valeurs et d'éthique. Or l'omission de procéder à des ÉFVP contredit cette supposition. Nous suggérons au Conseil du Trésor de mettre en place une directive explicite établissant un processus correctif, lequel s'appliquerait dans les cas où hauts fonctionnaires n'effectuent pas les ÉFVP appropriées ou utilisent les outils technologiques de façon inappropriée. Les mesures correctives devraient être assez sévères pour décourager un tel comportement.

Nous espérons que la présente étude du comité et les discussions l'entourant mèneront à l'établissement de mesures solides et proactives pour que les nouvelles technologies facilitent le travail des fonctionnaires sans compromettre leurs droits à la vie privée et à la sécurité.