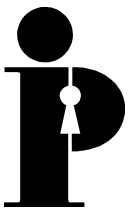
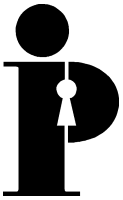
Commissaire à
l'information et à
protection de la
vie privée/Ontario

Lignes directrices sur la protection des renseignements personnels hors de son lieu de travail



Ann Cavoukian, Ph.D.
Commissaire
Juillet 2001



Commissaire à l'information et à la protection de la vie privée/Ontario

2, rue Bloor Est
Bureau 1400
Toronto (Ontario)
M4W 1A8

416-326-3333
1-800-387-0073
Télécopieur : 416-325-9195
ATS (Téléimprimeur) : 416-325-7539
Site Web : www.ipc.on.ca

La commissaire à l'information et à la protection de la vie privée/Ontario souligne la contribution de Colin Bhattacharjee à la préparation du présent document.

Cette publication est aussi disponible sur le site Web du Bureau du commissaire.

This publication is also available in English.

Table des matières

1. Introduction

- Dans l'exercice de leurs fonctions, les fonctionnaires provinciaux et municipaux doivent parfois travailler ailleurs qu'au lieu de travail normal que leur réserve leur employeur. Par exemple, ils transportent des documents en voiture, en autobus, en métro, en train ou en avion, travaillent à la maison, assistent à des réunions dans des hôtels et centres de congrès, comparaissent devant des tribunaux, mènent des enquêtes, visitent des clients ou bénéficiaires de services gouvernementaux et représentent le gouvernement ou l'administration municipale lors de cérémonies ou d'assemblées publiques.

- Les documents qui contiennent des renseignements personnels peuvent être sur support papier ou électronique. Les présentes lignes directrices précisent ce que devraient faire les employés pour assurer la confidentialité de ces documents lorsqu'ils travaillent ailleurs qu'au bureau.

2. Autres renseignements délicats

- Dans certains cas, le personnel qui travaille ailleurs qu'au bureau utilise d'autres documents confidentiels qui ne contiennent pas nécessairement des renseignements personnels, comme des mémoires au conseil des ministres, des documents assujettis au secret professionnel de l'avocat ou des documents qui contiennent des conseils destinés au gouvernement ou à l'administration. Bien que les présentes lignes directrices visent les renseignements personnels, elles s'appliquent tout aussi bien aux documents qui contiennent d'autres types de renseignements délicats.

3. Lois sur l'accès à l'information et la protection de la vie privée

- Que ce soit au bureau ou ailleurs, les fonctionnaires doivent se conformer à la *Loi sur l'accès à l'information et la protection de la vie privée* ou à la *Loi sur l'accès à l'information municipale et la protection de la vie privée* (les « lois »). Ces lois ont notamment pour objet de protéger la vie privée des personnes, et particulièrement des renseignements personnels que le gouvernement ou l'administration détient à leur sujet.

- Dans les lois, les renseignements personnels sont des renseignements consignés sur une personne qui peut être identifiée; il peut s'agir de la race, de l'âge, de la situation familiale, de l'adresse, du numéro de téléphone, des antécédents médicaux ou professionnels ou d'autres renseignements. Les deux lois régissent la collecte, la conservation, l'utilisation, la divulgation et l'élimination des renseignements personnels détenus par le gouvernement. Pour plus de précisions, consultez le texte des lois, qui est accessible au site Web du Bureau du commissaire à l'information et à la protection de la vie privée à www.ipc.on.ca.

4. Sortir des documents de son bureau

- L'employé ne devrait sortir de son bureau des documents contenant des renseignements personnels qu'en cas d'absolue nécessité pour exercer ses fonctions. Dans la mesure du possible, il devrait en faire des copies et laisser les originaux au bureau.

- Selon son poste, l'employé pourrait être tenu d'obtenir l'autorisation de son supérieur avant de sortir des documents contenant des renseignements personnels.

- Les documents contenant des renseignements personnels qui sont sortis du bureau devraient être consignés sur une feuille avec le nom de l'employé, une description des documents, le nom des personnes visées par les renseignements personnels et la date de sortie.

5. Documents sur support papier

- L'employé devrait glisser les documents sur support papier qui contiennent des renseignements personnels dans des chemises, les transporter dans une mallette ou une boîte verrouillée et toujours les garder à portée de la main pendant le transport.

- Lorsqu'il se déplace en voiture, l'employé devrait toujours verrouiller les documents sur support papier dans le coffre arrière. Toutefois, il est déjà arrivé que des fonctionnaires se fassent voler des documents rangés dans le coffre. C'est pourquoi, dans la mesure du possible, l'employé ne devrait jamais laisser sa voiture sans surveillance s'il a mis des documents sur support papier dans le coffre arrière.

- L'employé ne devrait jamais ouvrir ou consulter des documents sur support papier dans les transports en commun : autobus, métro, train ou avion.

- Lorsqu'il travaille à la maison, l'employé devrait ranger les documents sur support papier dans un classeur ou un tiroir verrouillé, qui ne contient que des documents liés à son travail.

- Lorsqu'il travaille ailleurs qu'au bureau, l'employé devrait toujours avoir les documents sur support papier sous surveillance, y compris pendant les repas et les pauses. Si c'est impossible, il devrait les ranger temporairement dans un endroit sûr, comme une pièce ou un tiroir verrouillé.

6. Documents électroniques

- Les documents électroniques qui contiennent des renseignements personnels devraient être chiffrés et sauvegardés sur une disquette ou un disque compact accessible par mot de passe, et non sur le disque rigide d'un ordinateur portatif ou domestique.

- Pour éviter la perte ou le vol, l'employé devrait mettre la disquette ou le disque compact dans une mallette verrouillée qu'il garde toujours sous surveillance pendant le transport.

- Lorsqu'il travaille chez lui, l'employé devrait ranger la disquette ou le disque compact dans un classeur ou un tiroir verrouillé après usage.

- Lorsqu'il travaille ailleurs qu'au bureau, l'employé devrait toujours avoir la disquette ou le disque compact en sa possession, y compris pendant les repas et les pauses. Si c'est impossible, il devrait les ranger temporairement dans un endroit sûr, comme une pièce ou un tiroir verrouillé.

7. Ordinateurs portatifs et domestiques

- L'accès aux ordinateurs portatifs et domestiques devrait être contrôlé par mot de passe, et toutes les données sauvegardées sur le disque rigide devraient être chiffrées. D'autres mesures de sécurité, comme l'installation d'un logiciel antivirus et d'un coupe-feu personnel, devraient être prises. L'employé ne devrait utiliser que des logiciels approuvés par le service d'informatique de son employeur.

- L'employé devrait toujours garder son ordinateur portatif sous surveillance pendant le transport. Lorsqu'il se déplace en voiture, il devrait toujours le ranger dans le coffre arrière. Toutefois, il est déjà arrivé que des fonctionnaires se fassent voler leur ordinateur rangé dans le coffre. C'est pourquoi, dans la mesure du possible, l'employé ne devrait jamais laisser sa voiture sans surveillance s'il a mis un ordinateur portatif dans le coffre arrière.

- L'employé qui doit afficher des renseignements personnels à l'écran d'un ordinateur portatif ailleurs qu'au bureau doit s'assurer que personne d'autre ne peut les lire. Il ne devrait jamais afficher de tels renseignements dans les transports en commun.

- Qu'il soit à la maison ou ailleurs, l'employé devrait fermer son ordinateur portatif ou domestique après usage. Pour plus de protection, l'ordinateur devrait être fixé à une table ou à un autre objet fixe au moyen d'un câble de sécurité. Dans toute la mesure du possible, l'employé devrait garder son ordinateur portatif sous surveillance, surtout lorsqu'il travaille ailleurs qu'au bureau mais pas chez lui. Autrement, il devrait ranger son ordinateur dans un endroit sûr, comme une pièce ou un tiroir verrouillé.

- L'employé ne devrait pas partager un ordinateur portatif utilisé à des fins professionnelles avec d'autres personnes, qu'il s'agisse de membres de sa famille ou d'amis.

8. Technologie sans fil

- Les employés devraient protéger la confidentialité des renseignements personnels sauvegardés dans des appareils sans fil, comme des assistants numériques et des téléphones cellulaires. L'accès à ces appareils devrait être contrôlé par mot de passe, et les données devraient être chiffrées.

- Pour éviter la perte ou le vol, l'appareil sans fil devrait être transporté dans une mallette verrouillée ou un sac à main fermé et demeurer sous la surveillance constante de l'employé. Il ne faut jamais laisser un appareil sans fil sans surveillance dans une voiture. S'il est absolument nécessaire de consulter des renseignements personnels contenus dans un appareil sans fil en public ou dans les transports en commun, l'employé doit s'assurer que personne ne peut lire ce qui est affiché.

- Lorsqu'il travaille ailleurs qu'au bureau, l'employé devrait toujours avoir ses appareils sans fil sous surveillance. Si c'est impossible, il devrait les ranger temporairement dans un endroit sûr, comme une pièce ou un tiroir verrouillé.

- L'employé ne devrait pas partager un appareil sans fil utilisé à des fins professionnelles avec d'autres personnes, qu'il s'agisse de membres de sa famille ou d'amis.

9. Téléphone et boîtes vocales

- Lorsqu'il emprunte les transports en commun ou travaille ailleurs qu'au bureau, l'employé devrait éviter de discuter de renseignements personnels au téléphone cellulaire, car ses voisins pourraient l'entendre ou sa conversation pourrait être interceptée au moyen d'un récepteur à exploration ou d'un autre appareil.

- Une ligne téléphonique distincte avec boîte vocale contrôlée par mot de passe devrait être fournie à l'employé qui travaille régulièrement à la maison. Le mot de passe ne devrait pas être divulgué aux membres de la famille ou aux personnes avec qui il habite.

10. Courriel, télécopieur et photocopies

- Lorsqu'il travaille à la maison ou ailleurs qu'au bureau, l'employé devrait éviter d'envoyer des renseignements personnels par courriel ou par télécopieur. S'il doit le faire absolument, il devrait suivre les directives et conseils énoncés dans les documents suivants du Bureau du commissaire : *Les principes de la vie privée pour les systèmes de courrier électronique*, *Le chiffrement du courrier électronique : Rien de plus simple!* et *Directives concernant la sécurité des transmissions par télécopieur*.

- L'employé devrait de préférence se charger lui-même de la télécopie ou de la photocopie des renseignements personnels. Cependant, il n'est pas toujours facile d'accéder à un télécopieur ou à un photocopieur ailleurs qu'au bureau. S'il doit confier les documents contenant des renseignements personnels à quelqu'un d'autre pour les faire télécopier ou photocopier, il devrait demander à être sur place au moment où ces services seront rendus.

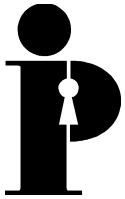
11. Conversations hors du bureau

- Les employés ne devraient pas discuter de renseignements personnels dans des endroits publics comme dans l'autobus, le train de banlieue, le métro, l'avion, un restaurant ou dans la rue. S'il est nécessaire de le faire, ils devraient se rendre à un endroit où personne ne pourra les entendre.

12. Incidents à signaler

- La perte ou le vol de renseignements personnels doit être signalé sans délai au supérieur immédiat, au coordonnateur de l'accès à l'information de l'institution et à la haute direction. Si les renseignements ont été volés, il faut également en informer la police.

- La perte ou le vol de renseignements personnels devrait également être signalé immédiatement au Bureau du commissaire à l'information et à la protection de la vie privée, qui pourrait entreprendre une enquête au besoin. Au début de son enquête, le Bureau du commissaire pourrait recommander que l'institution informe les personnes dont les renseignements personnels ont été perdus et prenne des mesures pour limiter les pertes de renseignements.



Commissaire à l'information et à la protection de la vie privée/Ontario

2, rue Bloor Est
Bureau 1400
Toronto (Ontario)
M4W 1A8

416-326-3333
1-800-387-0073
Télécopieur : 416-325-9195
ATS (Téléimprimeur) : 416-325-7539
Site Web : www.ipc.on.ca