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

Directives concernant la sécurité des transmissions par télécopieur

Ann Cavoukian, Ph. D.
Commissaire
Modifié en janvier 2003

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 tient à souligner la participation de Mark Ratner à la préparation du présent rapport.

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

This publication is also available in English.

Table des matières

Introduction

Envoyer une télécopie consiste à produire une copie exacte d'un document par balayage électronique et à transmettre les données ainsi produites. Les télécopies sont transmises par ligne téléphonique ordinaire au moyen d'un télécopieur.

Normalement, l'utilisateur place le document à télécopier dans l'alimentateur de documents du télécopieur et compose le numéro de téléphone du télécopieur destinataire. Ce dernier reçoit rapidement une copie du document. Documents écrits, les télécopies contiennent souvent des renseignements personnels ou confidentiels.

Malheureusement, comme c'est le cas pour d'autres médias, la télécopie comme forme de communication a ses défauts. Parfois, les télécopies ne parviennent pas à leur destinataire, que ce soit en raison d'une erreur de composition du numéro de télécopieur ou d'un problème technique.

Conscient des risques que pose la transmission de télécopies, le Bureau du commissaire à l'information et à la protection de la vie privée (CIPVP) a publié en juin 1989 le document *Directives concernant la sécurité des transmissions par télécopieur*. Les organismes gouvernementaux ont été invités à consulter ces directives aux fins de l'élaboration de systèmes et de procédés visant à protéger l'intégrité et la confidentialité des renseignements transmis par télécopieur.

En février 1990, le Secrétariat du Conseil de gestion du gouvernement de l'Ontario a publié une directive concernant la gestion des mesures de sécurité informatiques, qui avait notamment pour but de veiller à ce que les ministères protègent la confidentialité, l'intégrité et la disponibilité des données créées, stockées, traitées ou communiquées par voie informatique, y compris par télécopieur.

Parmi les principes énoncés dans ce document figurait la nécessité de faire conformer la sécurité informatique aux exigences de la *Loi sur l'accès à l'information et la protection de la vie privée* en matière de vie privée et de confidentialité. Cette importance accordée à la vie privée témoigne du fait que le gouvernement reconnaît le rôle crucial de la protection des renseignements personnels dans l'élaboration de mesures de sécurité technologique dans le secteur public, conformément aux directives du CIPVP concernant les transmissions par télécopieur.

Depuis le début des années 1990, la popularité des télécopieurs ne cesse de croître, de même que leur variété et leur complexité. Les réseaux, Internet et le courriel se sont également répercutés sur l'utilisation des télécopieurs. Pour toutes ces raisons, le CIPVP a préparé cette nouvelle édition de ses directives.

Obligations en vertu des *Lois*

La *Loi sur l'accès à l'information et la protection de la vie privée* et la *Loi sur l'accès à l'information municipale et la protection de la vie privée* (les *Lois*) régissent les organismes gouvernementaux concernant l'utilisation, la collecte, la divulgation, la conservation et la disposition des renseignements personnels.

La protection de la vie privée est l'un des deux objets des *Lois* en vertu de leur alinéa 1 b) :

> [...] protéger la vie privée des particuliers que concernent les renseignements personnels détenus par une institution et accorder à ces particuliers un droit d'accès à ces renseignements.

L'article 42 de la *Loi* provinciale (qui correspond à l'article 32 de la *Loi* municipale) énonce un certain nombre de circonstances dans lesquelles une institution est autorisée à divulguer des renseignements personnels. Comme une télécopie envoyée au mauvais destinataire ne figure pas parmi ces circonstances, sa divulgation est de toute évidence interdite en vertu des *Lois*.

Il importe de souligner que les dispositions des *Lois* concernant la protection de la vie privée ne s'appliquent pas à tous les organismes, mais bien à ceux qui sont considérés comme étant des « institutions ». D'après l'article 2 des deux *Lois*, une institution est un ministère du gouvernement de l'Ontario ou un organisme, un conseil, une commission, une personne morale ou une autre entité désigné comme institution dans les règlements.

Les organismes du secteur privé ne sont pas tenus de protéger les renseignements personnels au même titre que les institutions gouvernementales; cependant, ils peuvent consulter le présent document au moment d'élaborer leurs propres politiques en matière de protection des renseignements personnels.

Objet

Le CIPVP recommande aux institutions d'utiliser les présentes lignes directrices aux fins de l'élaboration de leurs propres politiques concernant les transmissions par télécopieur.

Ces directives visent à assurer l'adoption de pratiques acceptables en matière de vie privée (p. ex., en veillant à ce que les renseignements délicats et personnels ne soient accessibles qu'aux personnes autorisées) et à éviter le recours à des pratiques indésirables (p. ex., problèmes de protection de la vie privée, de sécurité ou de confidentialité)

Le présent document aborde brièvement des technologies de protection de la vie privée telles que le chiffrement, mais n'a pas pour objet de recenser la totalité des technologies ou produits de pointe en télécopie ni de recommander de produit, de marque ou de fournisseur particulier. Comme la technologie évolue constamment, les techniques nouvelles au moment de rédiger ces lignes risqueront d'être déjà périmées au moment de la publication. Les lecteurs sont donc invités à se renseigner sur les nouvelles tendances qui pourraient se répercuter sur la sécurité des communications par télécopieur.

Directives

Un processus permanent devrait être établi pour sécuriser le bureau où l'on envoie et reçoit des télécopies. Les politiques et procédures du bureau devraient être examinées régulièrement pour assurer la sécurité des documents télécopiés. Pour faciliter l'adoption de procédures appropriées, le CIPVP recommande plusieurs méthodes, qui sont divisées en trois catégories générales : vue d'ensemble, procédures de transmission et procédures de réception.

Vue d'ensemble

Établir des politiques écrites

La sécurité des transmissions par télécopieur repose en grande partie sur l'existence de politiques et procédures adéquates du côté de l'expéditeur et du destinataire. En rédigeant des politiques et procédures officielles, l'institution démontre son souci de la sécurité des transmissions par télécopieur. Le personnel pourra consulter ces documents de référence au besoin.

Toutes les institutions gouvernementales devraient élaborer des politiques écrites concernant l'usage du télécopieur. Ces politiques devraient comprendre les éléments mentionnés dans les présentes directives. En effet, il est essentiel qu'elles tiennent compte de tous les aspects soulevés ci-dessous.

Désigner une personne responsable

Le traitement sûr et efficace des télécopies repose notamment sur l'élaboration de procédures normalisées, qui consiste avant tout à désigner une personne comme responsable du traitement de tous les documents à télécopier ainsi que des télécopies reçues. Cette personne joue plusieurs rôles importants en ce qui concerne le traitement des documents avant leur transmission et celui des télécopies reçues. Un substitut devrait également être désigné au cas où cette personne ne pourrait remplir ses fonctions normales.

Sur réception d'une télécopie, la personne désignée devrait vérifier le nombre de pages pour s'assurer qu'il correspond au nombre indiqué sur le bordereau de transmission. Elle devrait ensuite agrafer les pages et acheminer le document au destinataire.

Installer le télécopieur dans une pièce sécurisée

Il est difficile d'assurer la sécurité des télécopies reçues dans un bureau où tout le personnel peut accéder facilement au télécopieur. Contrairement au courrier, qui parvient généralement dans des enveloppes scellées qui ne seront ouvertes que par leur destinataire ou une personne autorisée, il arrive souvent que toutes les télécopies destinées à un bureau arrivent au même télécopieur. Il est donc possible pour le personnel qui passe à côté du télécopieur de lire les télécopies, de sorte que les renseignements qu'elles contiennent sont mal protégés.

Compte tenu de ce risque, il faut choisir avec soin l'emplacement du télécopieur. Idéalement, il devrait s'agir d'un endroit qui n'est pas accessible à tout le monde. Ainsi, seul le personnel autorisé pourra lire les télécopies contenant des renseignements personnels ou confidentiels.

En outre, il arrive que des télécopies arrivent après les heures de travail, à un moment où les mesures de sécurité sont peut-être moins strictes et où seuls des employés de certains services sont au travail. Dans ce cas, il est prudent de désigner un télécopieur particulier auquel doivent être acheminés les messages après la fermeture des bureaux; chaque télécopieur secondaire est alors programmé pour faire suivre les télécopies vers un appareil central après les heures de travail. Si cet appareil est employé pour recevoir des renseignements personnels ou délicats, seules les personnes autorisées devraient pouvoir s'en servir.

Procédures de transmission

Utiliser un bordereau de transmission

Toutes les télécopies qu'envoient les institutions devraient comprendre un bordereau de transmission normalisé précisant le nom, le titre et l'organisme de l'expéditeur et du destinataire, ainsi que le nombre de pages transmises.

Comme mesure de sécurité supplémentaire, le bordereau devrait comprendre une case que l'expéditeur pourrait cocher s'il désire que le destinataire confirme la réception du document.

Le bordereau devrait également mentionner que la télécopie est confidentielle et pourrait comprendre des renseignements personnels visés par les dispositions de la *Loi sur l'accès à l'information et la protection de la vie privée* ou de la *Loi sur l'accès à l'information municipale et la protection de la vie privée* en matière de vie privée. Cet avis devrait préciser que la télécopie ne doit pas être copiée et distribuée ou divulguée à des personnes non autorisées, et donner au destinataire des directives à suivre si la télécopie lui a été envoyée par erreur.

Diviser les renseignements en catégories

Il faut veiller à protéger tous les documents transmis par télécopieur, mais tous les renseignements ne nécessitent pas le même degré de protection. Si le document contient des renseignements consignés sur un particulier qui peut être identifié, ces renseignements sont considérés comme étant des « renseignements personnels », qui sont assujettis aux dispositions des *Lois* en matière de protection de la vie privée.

La définition de « renseignements personnels » est large. En règle générale, des documents comme des formules de demande, des contrats, de la correspondance ou des bases de données sur la clientèle peuvent contenir des renseignements personnels. Dans ses ordonnances, le CIPVP a confirmé que des renseignements sur un particulier sont considérés comme étant « personnels » dans tous les cas où il s'agit d'un particulier identifiable agissant à titre personnel.

Généralement, il faut éviter de télécopier des renseignements personnels. Dans la mesure du possible, les institutions devraient plutôt envoyer des copies papier des documents en question. Le courrier électronique chiffré représente également une solution de rechange valable.

Dans les cas ou des contraintes de temps ou autres obligent l'envoi de renseignements personnels par télécopieur, les institutions devraient envisager d'utiliser des technologies de protection de la vie privée comme un dispositif de chiffrement, ou encore tenter d'éliminer des documents à télécopier tous les renseignements qui permettraient d'identifier le particulier.

Lorsqu'il est absolument nécessaire de télécopier des renseignements personnels et qu'il est impossible de les extraire des documents ou de les chiffrer, l'expéditeur devrait avertir le destinataire par téléphone de l'arrivée imminente de la télécopie. La responsabilité de donner un avis téléphonique est abordée en détail plus loin.

Les documents qui ne contiennent pas de renseignements personnels pourraient quand même nécessiter des mesures de protection strictes en raison de leur nature confidentielle. Mentionnons comme exemples des documents faisant l'objet d'une exception en vertu des *Lois*, comme des documents du Conseil des ministres, qui concernent l'application de la *Loi* ou qui sont assujettis au secret professionnel de l'avocat. Selon leur contenu, ces documents pourraient nécessiter une protection semblable à celle que l'on réserve aux documents contenant des renseignements personnels.

Confirmer le numéro avant de composer

Souvent, les listes de numéros de télécopieur des institutions sont périmées ou inexactes. Il faut vérifier régulièrement leur exactitude avant de s'en servir. Il en va de même des numéros préprogrammés dans les télécopieurs.

En cas de doute concernant le numéro de télécopieur, la personne responsable des transmissions devrait appeler le bureau du destinataire pour le confirmer, afin de s'assurer que la télécopie parviendra au destinataire prévu.

Vérifier l'exactitude des numéros composés

Après que l'exactitude du numéro de télécopieur a été confirmée, il importe de le composer correctement. Sur la plupart des télécopieurs, le numéro composé est affiché. Avant de transmettre le document, il faut donc s'assurer que le numéro affiché est le bon.

Appeler le destinataire pour l'informer de l'arrivée imminente d'une télécopie

Comme nous l'avons déjà mentionné, il est préférable de ne pas télécopier des documents qui contiennent des renseignements personnels. Cependant, lorsqu'il est impossible de retirer ces renseignements d'un document qui doit être télécopié, l'expéditeur doit appeler le destinataire pour l'informer de l'arrivée imminente d'une télécopie contenant des renseignements personnels.

Ainsi, le destinataire sera conscient de la nature délicate du document. S'il ne le reçoit pas après avoir été informé de son arrivée, il devrait en aviser l'expéditeur pour que ce dernier puisse régler le problème de transmission.

Vérifier les confirmations et les rapports d'activité

La plupart des télécopieurs peuvent imprimer une confirmation après chaque usage. Ce rapport confirme que le document a été transmis correctement, et indique le numéro de télécopieur du destinataire et le nombre de pages transmises. L'expéditeur devrait confirmer ainsi chaque transmission.

De même, le destinataire devrait vérifier que le nombre de pages reçues correspond à celui qui est indiqué sur le bordereau de transmission ou, à défaut, dans la confirmation. S'il y a des pages manquantes, le destinataire devrait demander à l'expéditeur de les lui envoyer. La section « Procédures de réception » ci-dessous contient d'autres précisions sur les tâches du destinataire.

La plupart des télécopieurs peuvent également imprimer des rapports d'activité après une période ou un nombre d'opérations donné, par exemple, toutes les 40 opérations. Ce rapport permet de contrôler l'utilisation du télécopieur. Cependant, sur la plupart des appareils, il ne peut être imprimé qu'une seule fois.

Il est donc possible pour une personne non autorisée de commander l'impression d'un rapport d'activité pour le détruire, afin d'éliminer toute trace d'une utilisation non autorisée. Cette personne pourrait donc s'emparer d'une télécopie qui ne lui est pas destinée puis éliminer toute mention de son arrivée en imprimant puis en détruisant le rapport d'activité. La personne responsable du télécopieur devrait donc passer en revue régulièrement les rapports d'activité pour déterminer s'il y a eu des utilisations non autorisées.

Procédures de réception

Informer l'expéditeur après réception d'une télécopie transmise au mauvais numéro

Même après avoir établi des politiques et procédures conformes aux présentes directives, il arrive qu'une institution reçoive des télécopies qui ne lui sont pas destinées. Il faut donc prévoir dans les procédures la marche à suivre dans ce cas.

Avant tout, il faut informer l'expéditeur de la télécopie, qui pourra déterminer si l'erreur est de nature technique ou humaine et prendre des mesures pour qu'elle ne se reproduise pas.

Le destinataire devrait également demander à l'expéditeur s'il veut récupérer la télécopie (qui lui serait renvoyée par un moyen autre que le télécopieur) ou s'il veut que celle-ci soit détruite. Le destinataire ne devrait pas acheminer la télécopie à la personne qui était censée la recevoir.

Photocopier les télécopies assujetties à une période de conservation

Certains vieux modèles de télécopieurs impriment les télécopies sur du papier thermique spécial. Comme ces télécopies s'estompent après un certain temps, les institutions devraient les photocopier après réception afin de respecter les périodes de conservation établies. Dans le cas des renseignements personnels, les *Lois* prévoient une période de conservation d'un an.

Une fois photocopiés, les documents imprimés sur papier thermique devraient être détruits de façon sécurisée. Les télécopies reçues au moyen d'appareils à jet d'encre ou au laser ne s'estompent pas.

Se renseigner sur les technologies de protection de la vie privée

L'évolution technologique a soulevé une foule de questions concernant la sécurité des télécopies. Un grand nombre de ces changements ont amélioré l'efficacité des télécopieurs, mais ont également suscité de nombreuses préoccupations. Les institutions devraient donc se familiariser avec les technologies de protection de la vie privée (TPVP). En général, les TPVPs s'agissent de technologies qui visent à protéger la vie privée des particuliers.

En ce qui concerne les télécopies, le chiffrement compte parmi les TPVP utiles. En termes simples, le chiffrement consiste à coder des données numériques afin que seule la personne qui possède la « clé » puisse les déchiffrer. Le chiffrement s'utilise plus couramment dans les communications par courriel, mais il est possible de relier le télécopieur à un dispositif qui chiffre les documents télécopiés.

L'utilité du chiffrement procède du fait que les télécopies sont transmises par ligne téléphonique ordinaire ou par l'entremise des réseaux cellulaires. Comme les conversations, les télécopies peuvent être interceptées en cours de transmission par des personnes non autorisées. En effet, il suffit pour ce faire d'obtenir du matériel facile d'accès et d'assemblage, au coût étonnamment bas.

Grâce à un chiffreur, les documents transmis par télécopieur peuvent être chiffrés afin de réduire le risque d'interception. Utilisé correctement, le chiffreur modifie les données numériques transmises afin qu'elles ne puissent être interprétées que par le télécopieur du destinataire. Une personne qui intercepte la transmission obtiendra non pas le document d'origine, mais un code illisible. Les institutions pourraient donc envisager d'utiliser cette technologie pour télécopier des renseignements personnels ou confidentiels.

Mentionnons toutefois que le chiffrement ne permet pas de contrer toutes les atteintes à la sécurité. En raison des limites de la technologie des télécopieurs, il est possible pour une personne déterminée d'intercepter une télécopie chiffrée et de la déchiffrer manuellement.

En outre, le chiffrement des télécopies est d'une utilité limitée car il n'est pas encore répandu au sein du gouvernement. Comme il ne fonctionne que lorsque l'appareil transmetteur et l'appareil récepteur sont tous deux munis d'un chiffreur, le chiffrement est impossible dans bien des cas.

En raison des problèmes de sécurité que pose le chiffrement des télécopies et du fait que les chiffreurs ne sont pas d'usage courant, le CIPVP recommande la prudence au moment de transmettre des documents délicats au moyen de cette technologie. Si l'on craint

l'interception de la télécopie, il ne faut pas utiliser le chiffrement, mais plutôt livrer les documents en personne ou peut-être par courriel chiffré, technique plus sûre que les télécopies chiffrées.

Pour chiffrer les télécopies, il faut que l'expéditeur et le destinataire soient équipés du même type de chiffreur. Cet appareil pourrait se révéler utile au sein d'un groupe « fermé » d'utilisateurs, notamment au sein d'un même service.

A l'échelon de l'organisme, chaque groupe d'utilisateurs se trouvant dans un même édifice pourrait envisager de consacrer un télécopieur aux transmissions chiffrées. Tous ceux qui communiquent avec ce groupe devraient alors utiliser le même type de chiffreur. Ainsi, une télécopie envoyée par erreur à un télécopieur qui n'est pas muni d'un chiffreur compatible sera illisible.

Comme autres exemples de TPVP pour les télécopieurs, mentionnons les dispositifs de verrouillage et les boîtes de réception confidentielles. Ces dispositifs réduisent le risque d'utilisation non autorisée des télécopieurs. Dans certains cas, une institution peut avoir à télécopier des renseignements qui nécessitent une protection supplémentaire. Le télécopieur peut être équipé d'un dispositif de verrouillage qui, lorsqu'il est utilisé, empêche la transmission et la réception de télécopies. En installant un tel dispositif, l'organisme peut réserver l'usage du télécopieur à des personnes désignées.

Certains télécopieurs sont munis d'une boîte de réception confidentielle, c'est-à-dire d'une mémoire qui emmagasine les documents reçus. Pour imprimer ces documents, il faut entrer un mot de passe. Ainsi, seule une personne désignée peut recevoir la télécopie. En outre, l'appareil de l'envoyeur doit être en mesure de transmettre le document à un télécopieur muni d'une telle boîte de réception.

Certains télécopieurs sont équipés d'un dispositif de stockage permanent, comme un disque dur, pour protéger le contenu de la boîte de réception confidentielle en cas de panne de courant. Les données sauvegardées sur disque sont ainsi préservées.

Envoi de télécopies par ordinateur

Au milieu des années 1990, les « modems télécopieurs » ont gagné en popularité. Ces appareils permettent à l'utilisateur d'envoyer et de recevoir des télécopies au moyen de son ordinateur. Les modems télécopieurs ne sont plus d'usage courant, ayant été remplacés par le courrier électronique. Cependant, comme cette technologie existe toujours, il faut soulever les questions de sécurité et de protection de la vie privée qu'elle pose dans les présentes directives.

Les avantages des modems télécopieurs sont les suivants :

- Il est possible de créer des bases de données comptant un grand nombre de numéros de télécopieur afin de transmettre des documents à des groupes de destinataires;
- La taille des documents à télécopier n'a plus d'importance, et ces documents ne sont plus seulement sur papier;
- Presque toutes les données sauvegardées dans un ordinateur (p. ex., lettres, rapports, tableurs financiers, photos) peuvent être télécopiées;
- Le document à télécopier peut être constitué à partir de plusieurs sources de renseignements contenues dans l'ordinateur;
- Contrairement aux télécopies imprimées, les télécopies sauvegardées dans un ordinateur sont très faciles à modifier (avant la transmission ou après la réception);
- Quiconque est muni d'un ordinateur ainsi que du matériel et du logiciel nécessaires peut envoyer ou recevoir une télécopie.

Plusieurs de ces avantages soulèvent toutefois des préoccupations en matière de vie privée. Par exemple, comme toute personne ayant accès à un ordinateur peut transmettre et recevoir des télécopies, il pourrait être nécessaire de resserrer les mesures prises pour améliorer la sécurité et la protection de la vie privée.

Par ailleurs, les progrès réalisés dans l'informatique mobile et les communications sans fil suscitent d'autres inquiétudes au sujet de la sécurité des transmissions par télécopieur. Par exemple, un ordinateur portable équipé du matériel et du logiciel nécessaires peut être employé pour envoyer ou recevoir des télécopies au moyen d'un téléphone cellulaire. En outre, les télécopieurs portatifs peuvent être utilisés presque n'importe où.

En raison des problèmes particuliers que posent ces technologies, les institutions devraient déterminer si leur personnel est en mesure d'envoyer et de recevoir des télécopies par ordinateur, et prendre des mesures pour limiter cette pratique conformément aux présentes directives.

Conclusion

Les institutions devraient se servir des présentes directives comme outil de référence aux fins de la formulation de leurs propres politiques et procédures sur les communications par télécopieur. Nous espérons qu'elles sauront sécuriser ces communications en tenant compte de leur situation particulière.

Sources et lectures suggérées

Office of the British Columbia Information and Privacy Commissioner. *Guidelines for the Secure Transmission of Personal Information by Fax*, août 1996. Internet : www.oipcbc.org/advice/faxguide.php.

Office of the Information and Privacy Commissioner (Alberta). *Guidelines on Fax Transmission* (modifiées en octobre 2002). Internet : www.oipc.ab.ca/ims/client/upload/Guidelines_on_Facsimile_Transmission.pdf.

Organisation de coopération et de développement économiques. *Lignes directrices de l'OCDE régissant la sécurité des systèmes et réseaux d'information : vers une culture de la sécurité*, l'Organisation, 2002. Internet : www.ftc.gov/bcp/conline/edcams/infosecurity/popups/OECD_guidelines.pdf.