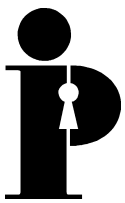
Commissaire à
l'information et à la
protection de la
vie privée/Ontario

Les principes de protection de la vie privée et la messagerie vocale

Tom Wright
Commissaire
Octobre 1995



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

Le commissaire à l'information et à la protection de la vie privée/Ontario tient à remercier Peony Gandolfi pour sa précieuse collaboration à la préparation de ce rapport.

Ce rapport est aussi disponible sur le site Web du CIPVP.

This publication is also available in English. Sur demande, ce document sera fourni sur audio cassette.

Table des matières

Principes de protection de la vie privée **1**

Introduction **2**

Objectif **4**

Principes **6**

Principe 1 — La vie privée des utilisateurs de la messagerie vocale doit être respectée et protégée 6

Principe 2 — Les employés devraient recevoir une formation appropriée en messagerie vocale, et en ce qui a trait aux questions de sécurité/respect de la vie privée 7

Principe 3 — Chaque organisme devrait avoir des règles explicites au sujet du respect de la vie privée des utilisateurs de la messagerie vocale 10

Principe 4 — Chaque organisme devrait faire connaître à ses employés sa politique à l'égard de la messagerie vocale et les informer de leurs droits et obligations relativement à la confidentialité des messages laissés dans les boîtes vocales 14

Principe 5 — Les systèmes de messagerie vocale ne devraient pas être utilisés pour recueillir, utiliser, conserver et divulguer des renseignements personnels sans que des mesures de sécurité adéquates aient été prévues pour protéger la vie privée 14

Principe 6 — Les organismes publics et privés devraient rechercher des moyens technologiques pour protéger la vie privée des utilisateurs de la messagerie vocale 16

Principe 7 — Les organismes publics et privés devraient établir des mesures de sécurité appropriées afin de protéger les messages transmis par les systèmes de messagerie vocale 18

Conclusion **20**

Principes de protection de la vie privée **21**

Notes **22**

Principes de protection de la vie privée

1. La vie privée des utilisateurs de la messagerie vocale doit être respectée et protégée.

2. Les employés devraient recevoir une formation appropriée en messagerie vocale, et en ce qui a trait aux questions de sécurité/respect de la vie privée.

3. Chaque organisme devrait adopter une politique explicite au sujet du respect de la vie privée des utilisateurs de la messagerie vocale.

4. Chaque organisme devrait faire connaître à ses employés sa politique à l'égard de la messagerie vocale et les informer de leurs droits et obligations relativement à la confidentialité des messages laissés dans les boîtes vocales.

5. Les systèmes de messagerie vocale ne devraient pas être utilisés pour recueillir, utiliser, conserver et divulguer des renseignements personnels sans que des mesures de sécurité adéquates aient été prévues pour protéger la vie privée.

6. Les organismes publics et privés devraient rechercher des moyens technologiques pour protéger la vie privée des utilisateurs de la messagerie vocale.

7. Les organismes publics et privés devraient établir des mesures de sécurité appropriées afin de protéger les messages transmis par les systèmes de messagerie vocale.

Introduction

La messagerie vocale est un service de messagerie électronique qui permet la communication en différé entre deux ou plusieurs personnes. Tout comme le répondeur, le système de messagerie vocale prend les messages pour une personne qui est momentanément dans l'impossibilité de répondre au téléphone. Cependant, étant informatisée, la messagerie vocale offre beaucoup plus de possibilités.

Bien que la messagerie vocale ait fait son apparition sur le marché au milieu des années 1970, son utilisation ne s'est répandue qu'au cours de la dernière décennie. La plupart des entreprises privées et un grand nombre d'organismes gouvernementaux utilisent la messagerie vocale.[1] Le gouvernement de l'Ontario compte plus de 40 systèmes de messagerie vocale et environ 25 000 abonnés.* Chaque année, des milliers de nouveaux abonnés viennent grossir les rangs des utilisateurs. Dans la région de Toronto seulement, les employés du gouvernement de l'Ontario reçoivent quotidiennement près de 100 000 messages par messagerie vocale.[2]

La popularité de la messagerie vocale ne cesse de grandir dans le monde entier. En Amérique du Nord, les ventes de systèmes de messagerie vocale totalisent en moyenne plus d'un milliard de dollars par année; bien que le marché européen soit moins important, les revenus provenant de la vente de serveurs vocaux interactifs croissent à un taux de 40 pour cent par année.[3]

La messagerie vocale possède plusieurs avantages virtuels. Ce système peut contribuer à faciliter les communications à l'intérieur des organismes tout comme entre les organismes et les personnes de l'extérieur et à améliorer le service à la clientèle. On estime que plus de 75 pour cent des appels d'affaires sont infructueux la première fois. En traitant ces appels, le système de messagerie vocale peut réduire de plus de 40 pour cent le nombre d'appels infructueux.[4]

La messagerie téléphonique est un moyen efficace d'obtenir et de fournir des renseignements, de réduire le cache-cache téléphonique, le temps d'attente, le temps passé à retourner les appels ou le temps passé au téléphone.[5] La messagerie vocale peut être utilisée en tout temps et n'importe où à l'aide d'un téléphone à clavier. Ce système libère les réceptionnistes qui peuvent ainsi se consacrer à d'autres tâches et permet aux correspondants de laisser des messages détaillés qui peuvent être difficiles à retenir pour la personne qui prend les appels.

*Dans ce document, «abonné» signifie une personne qui possède une boîte vocale à l'intérieur de la messagerie vocale d'un organisme. La messagerie vocale permet aux abonnés d'envoyer des messages à d'autres abonnés et de recevoir des messages de leurs différents correspondants, abonnés ou pas.

La messagerie vocale peut même contribuer à protéger davantage la vie privée étant donné que les messages personnels sont communiqués directement à l'abonné plutôt qu'à un intermédiaire qui note le message.

Toutefois, une mauvaise installation ou un système non muni d'un dispositif de sécurité (incluant une attitude laxiste à l'égard de la sécurité) peuvent porter atteinte à la vie privée et diminuer la qualité du service à la clientèle. La sécurité de la messagerie vocale deviendra de plus en plus importante au fur et à mesure que les systèmes informatiques seront intégrés aux systèmes téléphoniques. Grâce à ces systèmes intégrés, l'employé pourra avoir accès sur demande, depuis son bureau, à des services de messagerie vocale, de courrier électronique, de télécopieur, de réponse vocale interactive ainsi qu'à d'autres technologies.[6]

Plus les systèmes de communication sont regroupés, plus les chances de piratage de ces technologies sont nombreuses. Par exemple, le fait de pouvoir accéder à une boîte vocale, à un télécopieur, au courrier électronique et à d'autres service du genre au moyen d'un seul appel téléphonique rend encore plus nécessaire l'utilisation des mots de passe comme mesure de sécurité. La sécurité des systèmes incorporés équivaut à celle du point d'accès le plus vulnérable du système.[7]

D'autres technologies apparentées à la messagerie vocale et ayant des répercussions sur la vie privée font leur apparition sur le marché. Parmi celles-ci, le courrier vidéo. Le courrier vidéo est semblable à la messagerie vocale et au courrier électronique si ce n'est que le message peut inclure une photo vidéo de l'expéditeur. Ainsi, le but même des systèmes technologiques de communication est de recueillir, utiliser et divulguer des renseignements personnels, tout cela automatiquement. Ce qui a des répercussions sur la façon dont ces renseignements peuvent être utilisés ultérieurement, transmis, conservés ou détruits.

Objectif

Le commissaire à l'information et à la protection de la vie privée/Ontario a, en vertu de la *Loi sur l'accès à l'information et la protection de la vie privée* et de la *Loi sur l'accès à l'information municipale et la protection de la vie privée* (les lois) le mandat d'effectuer des recherches et de faire des recommandations sur des questions qui font l'objet de ces lois. Un des principaux objectifs des lois est de protéger la vie privée. L'utilisation de technologies de l'information existantes et nouvelles, comme la messagerie vocale, dans les organismes du gouvernement, a des conséquences pour la protection de la vie privée. Bien qu'il soit possible, en vertu des clauses sur l'accès à l'information, de demander l'accès à des messages enregistrés dans une boîte vocale, ce document porte surtout sur les questions de protection de la vie privée associées à la messagerie vocale.

Le bureau du commissaire a établi un ensemble de règles relatives à la protection de la vie privée à l'intention des organismes qui utilisent les systèmes de messagerie vocale afin de les sensibiliser davantage à l'importance de cette question.[8] Bien que ces règles s'adressent surtout aux organismes gouvernementaux visés par les lois, elles peuvent également être utiles aux institutions du secteur public ou privé qui peuvent s'en inspirer pour adopter une politique à l'égard de la messagerie vocale dans leur entreprise.

La messagerie vocale soulève des questions relatives à la protection de la vie privée pour les expéditeurs, les destinataires et les personnes qui font l'objet de ces messages. Bien que ce document porte surtout sur le respect de la vie privée des personnes[9] qui communiquent par messagerie vocale, la facilité avec laquelle les renseignements personnels peuvent être échangés par le biais de ce système est une autre préoccupation importante, car elle peut constituer une menace pour la vie privée des personnes qui font l'objet de ces messages. Les utilisateurs doivent en tenir compte chaque fois qu'ils utilisent la messagerie vocale.

L'utilisation et les sortes de systèmes de messagerie vocale sont très variées; il n'existe donc pas de lignes directrices applicables à tous les organismes. Le bureau du commissaire a, par conséquent, établi un certain nombre de règles générales afin de fournir aux organismes un plan d'ensemble leur permettant d'élaborer et de définir leur propre politique à l'égard du respect de la vie privée lors de l'utilisation de la messagerie vocale. Les organismes voudront peut-être illustrer les règles établies par des exemples pour faciliter la compréhension des employés. Il ne faut pas oublier que les règles sont interdépendantes et ne doivent pas être considérées isolément.

Lorsqu'on élabore une politique, il faut prendre plusieurs décisions (ex. : le niveau de sécurité requis, fonctions du responsable de la messagerie, etc.) Ces décisions seront, dans une certaine mesure, influencées par les limitations technologiques du système de messagerie vocale, l'utilisation qui en est faite, la nature des renseignements échangés et le type

d'entreprise. Le bureau du commissaire croit que la politique adoptée par l'entreprise doit reposer sur l'engagement de l'organisme à offrir le maximum de protection possible aux utilisateurs de la messagerie vocale ainsi qu'à ceux qui font l'objet des messages.

Principes

Principe 1 — La vie privée des utilisateurs de la messagerie vocale doit être respectée et protégée

En général, la messagerie vocale devrait être considérée comme une communication privée entre l'expéditeur et le destinataire. La plupart des gens s'attendent à ce que leur vie privée soit protégée lorsqu'ils utilisent le téléphone. Pour eux, la messagerie vocale est souvent le prolongement de l'appareil téléphonique. Ainsi, les utilisateurs croient souvent à tort que la communication par boîte vocale est aussi privée qu'une conversation téléphonique ordinaire.

L'expression «vie privée» a des significations variées selon différents contextes. C'est un concept large qui recouvre un ensemble de préoccupations au sujet de divers types d'ingérence dans la vie privée d'un citoyen comme la surveillance, l'écoute clandestine et la divulgation de renseignements personnels inexacts. Les lois portent surtout sur la protection des renseignements personnels et partent du principe que la personne est propriétaire des renseignements qui la concernent. Par conséquent, chaque citoyen devrait avoir un certain droit de regard sur la collecte, l'utilisation et la divulgation de renseignements qui le concernent.

La vie privée signifie également le respect du territoire d'une personne, c'est-à-dire l'espace physique qui l'entoure et qu'elle considère comme privé. Ces deux significations s'appliquent, dans une certaine mesure, aux systèmes de messagerie vocale. Par exemple, lorsqu'un saboteur accède à une boîte vocale et détraque le système, l'abonné peut avoir l'impression qu'on a empiété sur son territoire. La question de la protection des renseignements entrerait également en jeu si, en plus, le saboteur écoutait les messages contenant des renseignements personnels.

Il n'est pas possible de garantir le respect total de la vie privée à cause des caractéristiques inhérentes à la plupart des systèmes de messagerie vocale. Toutefois, le degré de protection et de sécurité d'un système repose en grande partie sur la façon dont un organisme configure et exploite ce système. La messagerie vocale, et c'est là un de ses principaux avantages, contribue à améliorer l'efficacité d'un organisme en accroissant les communications. Mais à moins que les entreprises ne fassent des efforts pour offrir le maximum de protection possible, les employés hésiteront peut-être à explorer toutes les possibilités de la messagerie vocale.

Dans un sondage effectué auprès d'entreprises américaines, près de vingt-deux pour cent des personnes interrogées (et trente pour cent des grandes entreprises qui ont participé au sondage) ont admis avoir fouillé les fichiers informatiques des employés, écouté les messages

transmis dans les boîtes vocales, lu les messages du courrier électronique ou exercé une surveillance électronique dans les autres systèmes de communication en réseau.[10] Dans une autre étude américaine, plus de vingt-sept pour cent des directeurs ont avoué qu'ils vérifiaient régulièrement les boîtes vocales des employés.[11]

Bien que des employeurs soutiennent que la surveillance électronique contribue à augmenter la productivité, les recherches semblent indiquer le contraire. Ainsi, une autre étude menée aux États-Unis révèle que les travailleurs qui font l'objet d'une surveillance électronique sont plus tendus, inquiets, déprimés, agressifs, blasés, fatigués et stressés physiquement que les travailleurs qui ne sont pas surveillés.[12] Le sentiment d'impuissance qui est souvent associé à la surveillance de l'employé peut être une grande source de tension dans le milieu de travail.

Principe 2 — Les employés devraient recevoir une formation appropriée en messagerie vocale, et en ce qui a trait aux questions de sécurité/respect de la vie privée

Beaucoup de problèmes d'atteinte à la vie privée surviennent parce que les utilisateurs ne savent pas comment fonctionne la messagerie vocale. Souvent, par exemple, cette ignorance amène les utilisateurs à croire que leurs communications seront toujours privées.

Plus les utilisateurs connaîtront le fonctionnement de la messagerie vocale, plus ils seront en mesure de protéger à la fois leur vie privée et celle de leurs correspondants. Bien qu'il ne soit pas possible pour un organisme d'offrir une formation à chaque personne utilisant la messagerie vocale, elle devrait au moins former ses propres employés. Il est important que les employés reçoivent une formation adéquate sur le fonctionnement de la messagerie vocale ainsi que des renseignements sur les questions liées à la sécurité et au respect de la vie privée pour pouvoir participer efficacement à l'élaboration d'une politique à cet égard.

Voici ce que les utilisateurs doivent savoir au sujet des systèmes de messagerie vocale afin de protéger la vie privée et la confidentialité des renseignements :

Le traitement de la messagerie vocale n'est pas complètement privé

Tout le monde a accès à la messagerie vocale, ce qui peut donner lieu à des atteintes à la vie privée et au non-respect de la confidentialité. De même, certains systèmes peuvent être en réseau, ce qui permet à des abonnés de serveurs différents d'envoyer et de recevoir des messages sur les deux serveurs.[13] Si les deux systèmes ont des niveaux de sécurité et de protection différents, cela peut porter atteinte à la vie privée et à la confidentialité.

Les tiers peuvent avoir accès aux messages, volontairement ou involontairement, de plusieurs façons. Les messages écoutés sur un téléphone à haut-parleur peuvent être entendus facilement. Les destinataires peuvent transmettre une copie des messages à un certain nombre de personnes. Un organisme peut, dans certains cas, accorder à des tiers l'accès aux boîtes vocales. Les saboteurs, les employeurs ou d'autres personnes peuvent également accéder sans autorisation aux boîtes vocales. Les messages peuvent également être entendus par hasard par des personnes chargées de la surveillance et du fonctionnement du système.

Enfin, même si les utilisateurs, les administrateurs et les fabricants ont pris toutes les mesures de protection nécessaires, les systèmes informatiques peuvent toujours effectuer un traitement et, par inadvertance, faire entendre les messages à la mauvaise personne. Ainsi, une abonnée qui essayait d'accéder à ses propres messages a entendu un message qui ne lui était pas destiné. Dans un autre cas, une avocate du Manitoba qui tentait de rejoindre un employé du gouvernement par téléphone a accédé sans trop savoir comment à un message incontestablement passionné en provenant de l'amie de coeur de l'employé.[14]

Pour toutes ces raisons, il est préférable de ne pas laisser de renseignements personnels ou confidentiels dans la boîte vocale.

Un message qui a été envoyé ou effacé peut se trouver encore dans le système

Après qu'il a été envoyé, le message restera dans le système jusqu'à ce qu'il ait été reçu et écouté. Le message est écouté puis sauvegardé («archivé») et il pourra être conservé tant qu'il y aura suffisamment de place dans le système. Les messages effacés sont conservés jusqu'à ce que de nouveaux messages soient enregistrés par-dessus.

On peut forcer l'accès aux systèmes de messagerie vocale

On a tous entendu parler de saboteurs, de concurrents et d'employés mécontents ayant accédé illégalement à des boîtes vocales pour faire de l'espionnage ou du sabotage. [15] Ces personnes peuvent s'ingérer dans la vie privée des expéditeurs et des destinataires en écoutant leurs messages et en utilisant ces renseignements au préjudice et à l'insu des deux parties ou sans leur consentement.

On sait que les saboteurs effacent les messages ou empêchent les abonnés de récupérer leurs messages en changeant leurs mots de passe. Ils peuvent effacer les messages d'accueil ou les remplacer par des messages obscènes. De telles méthodes peuvent ternir la réputation d'un organisme ou entraîner de grosses pertes de revenus.

Aux États-Unis, une fleuriste a découvert que quelqu'un avait remplacé son message d'accueil par un message qui nuisait à son commerce. On a fini par retrouver le saboteur. Il s'agissait d'un ex-employeur de la fleuriste qui avait réussi à obtenir le mot de passe auprès du responsable du système en fournissant le numéro de sécurité sociale de son ex-employée. Apparemment, le responsable du système utilisait les numéros de sécurité sociale comme code d'accès.[16]

Les mots de passe faciles à deviner représentent une autre tentation pour les saboteurs. Plusieurs systèmes sont configurés de façon à ce que le mot de passe initial pour une nouvelle boîte vocale corresponde au numéro du poste de téléphone de l'abonné. Les saboteurs peuvent utiliser un ordinateur pour composer le numéro de chaque poste dans une entreprise et avoir ainsi facilement accès aux messages personnels des abonnés qui n'ont pas changé leur mot de passe initial. [17]

La technologie de la messagerie vocale peut aller à l'encontre du respect de la vie privée

Il est facile d'envoyer ou de retransmettre des messages accidentellement ou à la mauvaise personne. Il faut faire preuve de vigilance lorsqu'on envoie ou retransmet des messages à un groupe de personnes. La liste de diffusion peut contenir des noms de personnes qui ne devraient pas recevoir le message.[18] Une fois qu'un message est envoyé, l'expéditeur renonce à toute responsabilité sur la façon dont le message sera conservé, utilisé ou divulgué par les destinataires. Un destinataire peut retransmettre le message à d'autres ou même y annexer un message personnel avant de l'expédier de nouveau. La note peut, selon sa nature, influencer l'interprétation du message par le destinataire suivant — et ce, à l'insu de l'expéditeur initial.

Les utilisateurs devraient écouter attentivement le message d'accueil avant de laisser un message, sinon, ils risquent de se tromper de boîte vocale. Les erreurs qui surviennent dans l'envoi, la retransmission ou la réponse à un message peuvent aboutir à la divulgation involontaire de renseignements personnels de nature délicate ou de renseignements incomplets ou inopportuns.

Avec certains modèles de téléphone, il est également important de se débrancher complètement de la boîte vocale d'un correspondant avant de faire un autre appel. Sans quoi, le second appel pourrait être intercepté par la boîte vocale du premier correspondant. Et la conversation du second appel pourrait être enregistrée dans la boîte vocale du premier correspondant à l'insu des abonnés.[19] Il est donc très important que les employés se familiarisent avec les fonctions et les possibilités de leurs téléphones.

Principe 3 — Chaque organisme devrait avoir des règles explicites au sujet du respect de la vie privée des utilisateurs de la messagerie vocale.

Chaque organisme devrait adopter une politique officielle au sujet de la protection des communications qui s'effectuent par l'intermédiaire de la boîte vocale. Une politique claire définit les attentes des employés et favorise la confiance entre les employés et la direction. Elle peut même contribuer à prévenir des litiges, des poursuites donnant lieu à des renvois injustifiés et la mauvaise publicité.

Chaque employé devrait connaître ses droits et obligations en vertu de la politique de son organisme et accepter de s'y conformer.[20] Les règles établies par l'entreprise devraient permettre aux abonnés de protéger non seulement leur vie privée mais également celle des autres utilisateurs et des personnes qui font l'objet de messages dans les boîtes vocales. Les correspondants externes sont particulièrement vulnérables, car souvent, ils ne connaissent pas les répercussions que l'utilisation de la messagerie vocale peut avoir sur la vie privée, comme par exemple, la possibilité pour des tiers d'avoir accès aux messages qu'ils ont laissés dans la boîte vocale.

Pour que la politique adoptée par l'entreprise soit efficace, il faut que le personnel en reconnaisse le bien-fondé et s'engage à en respecter les principes. La participation du personnel à l'élaboration et à la mise en place de la politique est essentielle au maintien de cette dernière. Les représentants des employés, les directeurs, des spécialistes des systèmes informatiques et des ressources humaines, des conseillers juridiques devraient tous prendre part à l'élaboration de la politique.

Voici un aperçu des questions qui devraient faire l'objet d'une politique de l'entreprise :

- les utilisations approuvées du système de messagerie vocale;
- l'accès des tiers aux boîtes vocales; et
- les conséquences de la violation de la politique.

Utilisations approuvées du système de messagerie vocale

La politique d'une entreprise devrait fournir des renseignements sur les utilisations possibles de la messagerie vocale.

Messages d'affaires ou messages personnels

Les messages déposés dans la boîte vocale peuvent être personnels ou liés au travail. La politique à l'égard de la messagerie vocale devrait préciser le niveau de protection prévu pour les deux types de messages. Bien que l'accès des tiers aux messages personnels devrait être interdit, certains employeurs peuvent avoir une opinion différente en ce qui a trait aux messages d'affaires.[21] La politique de l'entreprise devrait définir clairement dans quelles circonstances l'accès aux messages d'affaires est autorisé ou interdit aux directeurs et aux autres membres du personnel.

La question du respect de la vie privée se pose d'une façon plus manifeste lorsqu'il s'agit de messages d'affaires contenant des renseignements de nature délicate ou confidentielle. Si le niveau de sécurité du système de messagerie vocale n'est pas adéquat, un organisme peut interdire aux employés d'utiliser le système pour la transmission des renseignements de cette nature. Par exemple, des organismes peuvent mettre en place des règles de sécurité spéciales ou interdire l'utilisation du système pour la transmission de renseignements que les lois obligent à garder confidentiels.[22] Les entreprises devraient également imposer des restrictions relativement à l'envoi, la retransmission et la sauvegarde des messages d'affaires qui contiennent des renseignements personnels (Voir principe n^{o} 5.)

Surveillance électronique : violations des règles de sécurité ou de la politique établie

La surveillance des boîtes vocales ne devrait pas être considérée par les employeurs comme un moyen de prévenir la violation des règles de sécurité ou de réunir des preuves relativement au non-respect de la politique de l'entreprise et des règles de sécurité (ex. : violations de la sécurité, activités illégales, fuite à propos de renseignements d'affaires confidentiels ou discrimination). Il faudrait d'abord penser à utiliser d'autres méthodes d'enquêtes. Par exemple, le responsable de l'administration de la messagerie est capable de savoir si un employé n'écoute pas ses messages, s'il reçoit quotidiennement un nombre exceptionnellement élevé de messages et d'où proviennent ses messages. Ces indications peuvent permettre de déceler des activités illégales sans qu'il soit nécessaire d'avoir recours à l'écoute des messages de l'employé.

Évaluation du personnel

L'utilisation de la messagerie vocale pour évaluer le rendement ou les activités des membres du personnel pourrait constituer une atteinte à la vie privée, nuire au moral des employés, aux communications normales et à l'échange spontané des idées. L'utilité, l'à-propos et la fiabilité de la surveillance électronique devraient être étudiés à fond. Les messages électroniques ne présentent qu'un côté de la médaille; il ne faut donc pas présumer qu'ils

peuvent fournir un tableau exact et complet du rendement d'un employé. Il existe des façons plus directes, moins indiscrètes et plus efficaces de surveiller le rendement des employés.

Un employeur qui envisage d'utiliser la surveillance électronique devrait prendre soin de peser le pour et le contre avant d'utiliser une telle méthode. S'il décide de passer à l'action, il devra consulter les membres du personnel. La surveillance électronique ne devrait jamais être utilisée à l'insu des employés et sans leur consentement. L'accès clandestin aux boîtes vocales ou la surveillance électronique est non seulement contraire à l'éthique mais elle est également illégale et pourrait entraîner des poursuites en justice.[23]

Satisfaction de la curiosité

L'accès à la boîte vocale d'un autre abonné sans raison sérieuse et uniquement par curiosité devrait être formellement interdit. Un employé d'un restaurant McDonald aux États-Unis a poursuivi son employeur pour un montant de 1 million de dollars. L'employeur avait écouté les messages laissés dans la boîte vocale de l'employé marié et avait découvert que ce dernier avait une liaison; il avait par la suite fait écouter ces messages à la femme de l'employé et à d'autres personnes. [24]

Accès d'une tierce personne à la boîte vocale

Les organismes devraient toujours essayer de trouver d'autres moyens d'obtenir les renseignements dont elles ont besoin avant d'effectuer des recherches dans les boîtes vocales des employés. La politique à l'égard de la messagerie vocale devrait préciser les circonstances où une tierce personne peut avoir accès à la boîte vocale d'un employé; les restrictions relativement à l'utilisation et à la divulgation de ces renseignements; et, enfin, la marche à suivre pour obtenir l'autorisation d'accéder à la boîte vocale d'une tierce personne. Les abonnés devraient connaître les noms des personnes qui ont l'autorisation d'accéder à leur boîte vocale. Ils devraient également être avisés chaque fois que ces personnes tentent d'accéder à leur boîte vocale.

L'abonné qui doit s'absenter pendant une longue période (ex. : vacances) devrait enregistrer un message d'accueil spécial avisant ses correspondants de ne pas laisser de messages, surtout des messages confidentiels ou personnels, pendant son absence. L'abonné devrait également indiquer le nom d'une autre personne avec laquelle le correspondant peut communiquer. Certains systèmes peuvent être configurés pour empêcher automatiquement la boîte vocale de l'abonné de recevoir des messages pendant une absence prolongée. L'employé qui est au bureau ou qui s'absente temporairement tout en ayant accès à sa boîte vocale, devrait écouter ses messages au moins une fois par jour.

Conditions d'accès

Les conditions d'accès à la boîte vocale par une tierce personne devraient être définies afin de limiter au minimum l'ingérence dans la vie de l'abonné. L'accès devrait être accordé pour les messages d'affaires non confidentiels et pour des raisons valables uniquement. Dans la politique établie par l'entreprise, il faudrait exiger qu'une demande d'autorisation soit faite directement à l'abonné toutes les fois que c'est possible. Par exemple, l'autorisation d'accès pourrait être demandée à l'abonné avant le départ de ce dernier en vacances.

Procédures d'accès

Lorsque l'autorisation d'accéder à une boîte vocale est requise mais ne peut être accordée directement par l'abonné, il faudrait établir des procédures pour obtenir cette autorisation. La politique de l'entreprise devrait préciser qui a l'autorité d'approuver et de surveiller l'accès à une boîte vocale par une tierce personne conformément aux règles adoptées. Avant d'accorder l'autorisation, il faudrait connaître et évaluer l'utilisation que la tierce personne prévoit faire de la boîte vocale et des renseignements obtenus. Toutes les fois que c'est possible, l'abonné devrait être avisé avant que la tierce partie n'utilise sa boîte vocale. Autrement, il faudrait prévenir l'abonné aussitôt que possible de l'utilisation qui a été faite de sa boîte vocale et des renseignements qui s'y trouvaient.

Si la politique de l'entreprise autorise les tiers à accéder aux boîtes vocales, l'entreprise doit le faire savoir aux correspondants internes et externes. Par exemple, un grand nombre de systèmes peuvent être programmés pour faire jouer un message d'accueil de l'entreprise avant qu'une personne de l'extérieur ne dépose un message dans la boîte vocale d'un abonné. Le message d'accueil préviendra les correspondants que des tiers peuvent avoir accès aux messages laissés dans le système.

Conséquences de la violation de la politique

Il est nécessaire d'offrir aux membres du personnel et de la direction une formation et des renseignements pour s'assurer que la politique sera bien comprise et mise en place adéquatement. La formation pourrait avoir lieu en même temps que le cours d'initiation à la messagerie vocale. Il faudra profiter de l'occasion pour informer les membres du personnel et de la direction des conséquences de la violation de la politique.

Pour qu'une politique soit efficace, les organismes doivent prévoir des mesures afin de s'assurer qu'elle sera respectée. Si on ne prend pas les moyens de faire respecter la politique, on croira que ce n'est pas sérieux. Une clause pourrait être incluse dans le contrat de rendement de l'employé lui demandant de donner son adhésion à la politique. Les conséquences du non-respect de la politique et la marche à suivre pour déposer une plainte devraient être clairement précisées dans la politique de l'entreprise.

Principe 4 — Chaque organisme devrait faire connaître à ses employés sa politique à l'égard de la messagerie vocale et les informer de leurs droits et obligations relativement à la confidentialité des messages laissés dans les boîtes vocales.

Tous les membres du personnel devraient être informés de leurs droits relativement à leur vie privée et de leurs obligations relativement à l'utilisation de la messagerie vocale sur les lieux de travail. Une politique et des règles claires, comprises et acceptées par chacun, permettront aux utilisateurs de connaître exactement tous les aspects de la confidentialité des messages sur le système. La politique de l'entreprise peut également traiter de questions comme la propriété des renseignements enregistrés dans les boîtes vocales et les droits de l'abonné.

Il ne suffit pas de consigner la politique de l'entreprise et les règles dans un manuel. Il faut également que chaque employé en prenne connaissance et accepte de s'y conformer. Les nouveaux employés pourraient, au cours de la séance d'orientation, être informés de la politique de l'entreprise à l'égard de la messagerie vocale et être sensibilisés aux questions de protection de la vie privée associées à l'utilisation du système. Les entreprises doivent veiller à ce que chaque membre du personnel soit mis au courant de toute mise à jour apportée à la politique. Les employés pourront être informés par des communiqués, des réunions ou par le biais du courrier électronique. Le système de messagerie vocale peut être également programmé pour fournir des renseignements aux utilisateurs lorsqu'ils accèdent à leur boîte vocale.

Principe 5 — Les systèmes de messagerie vocale ne devraient pas être utilisés pour recueillir, utiliser, conserver et divulguer des renseignements personnels sans que des mesures de sécurité adéquates aient été prévues pour protéger la vie privée.

Les abonnés des boîtes vocales ne sont pas les seuls à avoir besoin de protection. Les personnes qui font l'objet de messages ont également besoin d'être protégées. La messagerie vocale étant considérée comme un moyen de communication plus privé que le courrier électronique, les messages laissés dans la boîte vocale peuvent également contenir des renseignements plus personnels. De plus, les abonnés qui donnent le numéro de téléphone de leur résidence dans leur boîte vocale du bureau peuvent inciter leurs correspondants à laisser plus de messages personnels qu'ils n'auraient tendance à le faire.

En vertu des lois ontariennes, la confidentialité des renseignements personnels détenus par le gouvernement doit être protégée. Les renseignements personnels comprennent les renseignements consignés au sujet d'une personne identifiable, y compris les renseignements enregistrés par des systèmes électroniques. Pour protéger la vie privée, les organismes devraient adhérer à des règles de protection de la confidentialité des renseignements personnels.[25]

Certaines caractéristiques inhérentes aux systèmes de messagerie vocale peuvent aller à l'encontre de la protection de la confidentialité des renseignements. Par exemple, la facilité avec laquelle les renseignements peuvent être volontairement ou involontairement envoyés ou retransmis et l'absence de mesures de sécurité adéquates peuvent faciliter la collecte de renseignements par des tiers non autorisés, à l'insu de la personne à qui ces renseignements appartiennent. Cela peut également faciliter la divulgation ou une mauvaise utilisation des renseignements.

Plus les renseignements personnels sont en dehors de leur contexte original, plus il est difficile de respecter les règles de protection de la confidentialité. Les personnes qui reçoivent les renseignements personnels ne savent peut-être pas dans quel but ces renseignements ont été fournis à l'origine; elles peuvent donc, par inadvertance, utiliser ou divulguer ces renseignements d'une manière intempestive. Pour toutes ces raisons, les messages d'accueil devraient inciter les correspondants à ne pas laisser de messages contenant des renseignements personnels ou de nature délicate. Sur certains systèmes, les correspondants peuvent vérifier le contenu de leur message ou enregistrer de nouveau leur message avant de l'envoyer, ce qui est utile si les correspondants ont l'impression que leur message original contenait trop de renseignements personnels ou confidentiels.

Il est parfois nécessaire de fournir des renseignements personnels par messagerie vocale même si cela est déconseillé. Par exemple, lorsqu'il faut transmettre de toute urgence de l'information à des employés se trouvant dans des endroits différents, la messagerie vocale est sans doute le moyen de communication le plus efficace. Lorsqu'on fournit des renseignements personnels au sujet d'une autre personne, il faudrait faire en sorte que le message ne contienne aucun indice pouvant permettre d'identifier la personne en question. Sinon, il faudrait prendre des mesures pour s'assurer que la collecte, la conservation, l'utilisation, la divulgation et la destruction des renseignements personnels soient conformes aux lois sur la protection de la confidentialité. Cette règle est obligatoire pour toutes les organismes visés par les lois.

Principe 6 — Les organismes publics et privés devraient rechercher des moyens technologiques pour protéger la vie privée des utilisateurs de la messagerie vocale.

Les entreprises de messagerie vocale devraient mettre au point des dispositifs technologiques de protection de la vie privée et promouvoir leur utilisation. Ces entreprises sont souvent en mesure d'expliquer les faiblesses d'un système et les fonctions de sécurité et de protection offertes à leurs clients. Un grand nombre de ces entreprises donnent maintenant des cours de formation en sécurité aux administrateurs des systèmes. De plus, il y a désormais des experts en sécurité qui s'occupent d'inspecter les systèmes de messagerie vocale des entreprises.[26] Les entreprises devraient évaluer les répercussions que peuvent avoir sur la vie privée les systèmes existants ou proposés afin de déterminer quand et comment la vie privée peut être menacée et corriger les points faibles avant que les problèmes ne surgissent.

Les besoins en sécurité de chaque organisme varient selon le type de renseignements qui sont transmis par la messagerie vocale et le niveau d'intégration du système au réseau informatique du bureau. Par conséquent, chaque organisme devrait évaluer ses besoins en sécurité et choisir un système qui lui convient. Bien qu'aucun système ne puisse garantir une sécurité complète, certains peuvent offrir une très bonne protection. Cependant, les systèmes munis de très bons dispositifs de sécurité coûtent généralement plus cher et ils peuvent être moins pratiques que les systèmes moins perfectionnés.

Il y a plusieurs moyens technologiques d'accroître la sécurité et la protection de la vie privée des utilisateurs de la messagerie vocale et des personnes qui font l'objet des messages. C'est aux organismes de déterminer quelles sont les fonctions de sécurité sur leur système et d'ajouter d'autres fonctions qui leur semblent appropriées.

Mesures de sécurité que peuvent prendre les abonnés

Le premier moyen d'empêcher une personne d'accéder sans autorisation à une boîte vocale est l'identification et l'authentification de l'utilisateur. Pour accéder à leur boîte vocale, les abonnés doivent normalement entrer un numéro d'identification (numéro de la boîte vocale) sur un téléphone à clavier. Le mot de passe permet l'authentification de l'abonné. Normalement, puisque les mots de passe sont gardés secrets, seuls les utilisateurs autorisés devraient pouvoir accéder à leur boîte vocale.[27] Lorsqu'ils composent leur mot de passe, les assurés devraient s'assurer que personne ne les observe. Il faudrait éviter d'utiliser les téléphones qui affichent le numéro d'identification et le mot de passe de l'abonné.

Le mot de passe devrait comprendre au moins six chiffres, être complexe et difficile à deviner. Par exemple, il ne faudrait jamais utiliser le numéro de son poste, sa date de naissance, son numéro d'assurance sociale, le nom d'un enfant, etc. Les employeurs

pourraient par exemple dresser une liste des mots de passe incorrects et demander aux abonnés de ne pas les utiliser. Certains systèmes peuvent être programmés pour accepter seulement les mots de passe comportant un nombre minimal de chiffres et pour rejeter les mots de passe faciles à deviner ou trop simples (comme «22222»). Les chances de deviner correctement un mot de passe diminuent avec chaque chiffre additionnel. Selon le niveau de sécurité requis, on peut utiliser entre 10 et 20 chiffres. Un grand nombre de chiffres permet d'accroître la sécurité, par exemple, lorsqu'il s'agit d'effectuer des tâches spéciales comme la programmation et la surveillance du système. Des niveaux d'accès multiples avec des mots de passe à chaque niveau d'accès pourraient également être établis pour les abonnés, les programmeurs et les administrateurs du système. Les mots de passe devraient être mémorisés, gardés secrets, changés régulièrement, ne jamais être notés par écrit ni mis en mémoire sur les touches de composition abrégée.

En plus des mots de passe, il existe un certain nombre d'autres moyens permettant d'accroître la protection de la vie privée. Par exemple, sur certains systèmes, il est possible d'attribuer à un message la mention «privé» avant de l'envoyer si on ne veut pas que le message soit retransmis par les destinataires. Il existe même une fonction permettant à un abonné de vérifier si quelqu'un a tenté d'accéder à sa boîte vocale.[28]

Mesures de sécurité que peuvent prendre les administrateurs

Pour protéger les abonnés contre l'accès non autorisé, certains systèmes de messagerie vocale peuvent être configurés, pour aviser automatiquement les abonnés de changer leur mot de passe, au moins tous les six mois ou selon les besoins de l'organisme. D'autres systèmes peuvent être configurés pour couper la communication après un certain nombre de tentatives infructueuses de la part d'un correspondant d'entrer un mot de passe.

Des vérifications régulières peuvent permettre d'exposer au grand jour les nombreuses tentatives infructueuses d'accéder à un système et ainsi d'éveiller l'attention de l'employeur sur la possibilité d'un problème de sécurité.[29] Il est très important de surveiller et de vérifier l'accès au fichier où sont emmagasinés les numéros d'identification et les mots de passe ainsi que sa sécurité.

D'autres voies d'accès dans un système de messagerie vocale peuvent être utilisées pour des activités suspectes et, par conséquent, elles devraient faire l'objet d'une surveillance spéciale. Il existe un logiciel qui permet à l'administrateur d'un système de savoir qui utilise la messagerie vocale et quand le système est libre. Des changements dans les modes d'utilisation normaux de la boîte vocale sont souvent un moyen de déceler qu'il y a eu violation. Dans certains cas, l'administrateur du système peut même bloquer l'accès à un saboteur en changeant le mot de passe de la boîte vocale qui a été visitée sans autorisation.

Une autre façon de prévenir l'accès non autorisé, c'est de désactiver les numéros de téléphone/poste, les numéros d'identification et les mots de passe lorsqu'ils ne servent plus ou qu'ils ne seront pas utilisés pendant une période prolongée (ex.: lorsqu'un employé a quitté la compagnie ou est en congé). Pour plus de sécurité, les documents contenant des renseignements sur le responsable du système, sur les numéros de téléphone ou de poste des employés devraient être déchiquetés avant d'être jetés. Cela empêchera les pêcheurs de poubelles de récupérer les renseignements afin d'obtenir illégalement l'accès au système.[30]

Dans des cas exceptionnels, les organismes qui attachent une grande importance à la sécurité, peuvent désactiver certaines fonctions du système téléphonique pendant la nuit (où il y a souvent des tentatives d'accéder illégalement aux boîtes vocales). Toutefois, cette mesure pourrait également réduire les avantages du système de messagerie vocale.

Fonctions de sécurité automatiques

Certains systèmes sont munis de fonctions de sécurité intégrées qui n'ont pas à être activées comme des messages sur des lecteurs de disques qui ne peuvent pas être téléchargés et le cryptage ou chiffrement automatique des messages. Le cryptage ou chiffrement est un moyen technologique important qui consiste à protéger les renseignements en brouillant les messages. Les messages qui seront interceptés seront ainsi inintelligibles. Pour déchiffrer le message, le correspondant devra entrer le bon mot de passe. Dans plusieurs systèmes, y compris certains systèmes publics de messagerie, les messages sont fragmentés et sauvegardés automatiquement sous une forme encodée sur un certain nombre de lecteurs de disques. D'autres systèmes utilisent également le chiffrement pour les mots de passe ou ne permettent pas de les copier ou de les lire à partir du lecteur.

Principe 7 — Les organismes publics et privés devraient établir des mesures de sécurité appropriées afin de protéger les messages transmis par les systèmes de messagerie vocale.

Les politiques de protection de la vie privée et les fonctions de sécurité automatiques seront efficaces seulement si des mesures appropriées sont prises pour promouvoir et maintenir la protection des renseignements personnels, la confidentialité et la sécurité. Par exemple, les mots de passe ne serviront à rien s'il n'existe pas des règles interdisant de dévoiler ou de partager son mot de passe. Les employés devraient être avertis de ne pas noter leur mot de passe par écrit et de ne pas le conserver dans un endroit facilement accessible aux autres.

Bien que les mots de passe et le chiffrement puissent contribuer à la sécurité de la messagerie vocale, ils n'empêchent pas les spécialistes du système d'accéder aux boîtes vocales. Les employés responsables de la messagerie vocale détiennent l'autorisation d'accéder en tout temps aux boîtes vocales, sans connaître les mots de passe, simplement en changeant le mot de passe. Si cela se produit, dans une situation d'urgence par exemple, il faudrait demander à l'abonné d'entrer un nouveau mot de passe dès que possible.[31]

Les responsables du système sont également capables de créer ou d'éliminer des boîtes vocales et d'effectuer d'autres tâches sur le système. Ces responsabilités devraient être assumées par le plus petit nombre de personnes possible. Pour réduire encore davantage les risques de violation de la sécurité, les organismes devraient mettre en place des procédures bien réglementées pour annuler les mots de passe et adopter un code de conduite définissant clairement les rôles et responsabilités des administrateurs des systèmes. La responsabilité de protéger les renseignements personnels devrait faire partie des tâches des responsables des systèmes et être incluse dans l'évaluation de leur rendement.

Il arrive parfois que des saboteurs potentiels (prétendant être des spécialistes de la sécurité) ou d'autres personnes communiquent avec les administrateurs des systèmes pour obtenir des renseignements au sujet de la messagerie vocale. Avant de donner un renseignement, l'administrateur devra faire toutes les démarches raisonnables et appropriées pour vérifier l'identité du correspondant et connaître les raisons exactes de la demande de renseignements.

Certains systèmes de messagerie vocale peuvent créer des copies de secours des messages effacés, ce qui peut aussi poser un problème de sécurité.[32] Si cela se produit, les employés devraient être informés. Des lignes directrices et des procédures devraient également être mises en place afin de s'assurer que la conservation et l'élimination de ces messages ne constituent pas une atteinte à la vie privée des utilisateurs.

L'équipement devrait également faire l'objet de mesures de sécurité. Ainsi, le système de messagerie vocale devrait être situé dans une pièce fermée à clef et l'accès devrait être limité aux membres du personnel autorisés.[33]

Conclusion

La messagerie vocale peut être un outil efficace qui facilite la communication et l'échange de renseignements à la fois à l'intérieur des organismes et entre les organismes et le monde extérieur. Mais s'il n'y a pas de politique ni de procédures pour protéger la vie privée et la confidentialité des renseignements, les avantages de la messagerie vocale pourraient être très coûteux. L'engagement à protéger la vie privée et la confidentialité des messages peut non seulement favoriser des communications efficaces mais avoir un effet positif sur le climat de travail. Les employés verront que leurs droits ont suffisamment d'importance aux yeux de leur employeur pour faire l'objet d'une protection spéciale. En outre, la mise en place d'une politique permettra de protéger la vie privée des personnes dont les renseignements personnels sont transmis par messagerie vocale.

Les principes de protection de la vie privée résumés à la page suivante constituent un ensemble d'idées générales qui peuvent servir de fondement à l'élaboration et à la mise en place de politiques précises pour accroître le respect de la vie privée lors de l'utilisation de la messagerie vocale. Plusieurs décisions doivent être prises lorsqu'on élabore ces politiques. Ces décisions seront, dans une certaine mesure, influencées par les limitations technologiques des systèmes de messagerie vocale, l'objectif visé, la nature des renseignements qui seront communiqués et le type d'entreprise. Toutefois, le commissaire croit que ces politiques devraient être guidées par un engagement à offrir le degré le plus élevé possible de protection de la vie privée en milieu de travail.

Principes de protection de la vie privée

1. La vie privée des utilisateurs de la messagerie vocale doit être respectée et protégée.

2. Les employés devraient recevoir une formation appropriée en messagerie vocale, et en ce qui a trait aux questions de sécurité/respect de la vie privée.

3. Chaque organisme devrait adopter une politique explicite au sujet du respect de la vie privée des utilisateurs de la messagerie vocale.

4. Chaque organisme devrait faire connaître à ses employés sa politique à l'égard de la messagerie vocale et les informer de leurs droits et obligations relativement à la confidentialité des messages laissés dans les boîtes vocales.

5. Les systèmes de messagerie vocale ne devraient pas être utilisés pour recueillir, utiliser, conserver et divulguer des renseignements personnels sans que des mesures de sécurité adéquates aient été prévues pour protéger la vie privée.

6. Les organismes publics et privés devraient rechercher des moyens technologiques pour protéger la vie privée des utilisateurs de la messagerie vocale.

7. Les organismes publics et privés devraient établir des mesures de sécurité appropriées afin de protéger les messages transmis par les systèmes de messagerie vocale.

Notes

1. BRENT, Paul. «Voice mail can do more than just answer phone», Telecommunications Special Report, *Financial Post*, 1er avril 1995, p. 28.

2. Renseignements fournis par la Direction des services informatiques du gouvernement, Secrétariat du Conseil de gestion.

3. O'LOUGHLIN, Mary Ann. «The European markets for voice processing and computer telephony», *The 1995 International VoicePower Directory & Buyers Guide*, janvier 1995, p. 7 et 8.

4. BRENT, Paul. «Voice mail can do more than just answer phone», Telecommunications Special Report, *Financial Post*, 1er avril 1995, p. 28.

5. Selon un sondage Gallup sur la productivité, trente-six pour cent des directeurs de télécommunications à l'emploi d'entreprises figurant dans le magazine Fortune 500 considèrent que la messagerie vocale a fait plus qu'aucun autre moyen de télécommunication pour améliorer la productivité sur les lieux du travail au cours des trois dernières années.

   Source : BRENT, Paul. «Voice mail can do more than just answer phone», Telecommunications Special Report, *Financial Post*, 1er avril 1995, p. 28.

6. NORTON, Margaret. «Messaging: the next step beyond voice mail», *The 1995 International VoicePower Directory & Buyers Guide*, janvier 1995, pages 63 à 65.

7. SURTEES, Lawrence. «Security stifles voice mail attacks», *Globe and Mail*, 1er mai 1991, p. B4.

8. Consulter également deux autres documents rédigés par le Commissaire à l'information et à la protection de la vie privée : *Les principes de la vie privée pour les systèmes de courrier électronique* (février 1994) et *Mise à jour des directives concernant la sécurité de transmission par télécopieur* (juin 1990).

9. Dans ce document, «utilisateur» signifie un correspondant interne ou externe qui transmet un message par la boîte vocale. Le correspondant peut être ou ne pas être un abonné.

10. PILLAR, Charles. «Bosses with x-ray eyes», *Macworld*, juillet 1993, p. 4.

11. FOULSHAM, Dom. «Who else is listening in to your voicemail», *The Times*, 16 juin 1995.

12. WORSNOP, Richard L. «Privacy in the workplace», *CQ Researcher*, vol. 3 numéro 43, 19 novembre 1993, p. 1014.

13. «Octel Voice Information Processing — Intelligent systems That Meet Changing Communication Needs», Version 6, 12/94. Brochure sur les serveurs vocaux interactifs.

14. «Racy voice mail message raises concern over privacy», *North Bay Nugget*, 16 décembre 1994, p. C5.

15. Voir l'article de FLANAGAN, William G. et GUTNER, Toddi, «The perils of voice mail», *Forbes*, 17 janvier 1994, p. 106 et 107. L'article recommande également que lorsqu'un employé détenant un poste clé quitte la compagnie pour aller travailler chez un concurrent, les membres du personnel devraient aussitôt changer leurs mots de passe.

16. *Second Annual Report of the Privacy Rights Clearinghouse* (octobre 1993 — septembre 1994), Center for Public Interest Law, Université de San Diego, janvier 1995, p. 43.

17. Afin de réduire ce risque au minimum, les responsables de l'administration du système peuvent attribuer des numéros au hasard comme mot de passe initial et temporaire lorsque de nouvelles boîtes vocales sont créées. L'administrateur peut également bloquer l'accès à des boîtes non utilisées. Cela pourrait empêcher l'enregistrement de renseignements de nature délicate dans ces boîtes auxquelles pourraient avoir accès des personnes non autorisées. Les administrateurs devraient également vérifier régulièrement les boîtes vocales qui sont inutilisées depuis longtemps.

    Une activité excessive sur le système (particulièrement après les heures de bureau), des tonalités occupées ou des raccrochages répétés dans la boîte vocale d'un abonné peuvent être des indices que quelqu'un a pénétré dans le système frauduleusement. Si le personnel ou le responsable du système soupçonnent quelque chose de louche, ils devraient utiliser la note de service pour faire part du problème et non la messagerie vocale. De plus, les mots de passe des boîtes vocales faisant l'objet de ce type d'activités clandestines devraient être changés immédiatement.

    «The great voice-mail robbery», *The Economist*, 13 août 1994, p. 56.

18. Certains systèmes permettent à un abonné d'envoyer un message à plusieurs personnes en même temps à l'aide d'une liste de diffusion. Cela élimine la nécessité de rejoindre chaque personne pour lui retransmettre les mêmes renseignements.

19. Exposé de Ross Tennant, Directeur du marketing, Octel Communications Canada, juin 1995.

20. Un grand nombre d'idées exprimées dans cette partie proviennent d'un document rédigé par David Johnson et John Podesta pour l'*Electronic Mail Association* et intitulé :«Access to and Use and Disclosure of Electronic Mail on Company Computer Systems : A Tool Kit for Formulating Your Company's Policy», septembre 1991.

21. Pour accroître la protection de la vie privée, les messages d'affaires non confidentiels et les messages personnels/confidentiels devraient être archivés séparément toutes les fois que c'est possible. De cette façon, il sera possible, au besoin, d'avoir accès aux messages d'affaires non confidentiels d'un membre du personnel et les messages personnels/confidentiels resteront privés. Une boîte vocale «résidence» protégée par un mot de passe pourrait par exemple servir de fichier pour les messages personnels. Sur certains systèmes, une partie de la boîte vocale de l'employé peut être utilisée par la famille de l'abonné comme boîte vocale «résidence». Cela permet aux abonnés d'envoyer et de recevoir des messages des membres de leur famille.

22. Les abonnés doivent également savoir que le fait de laisser le numéro de téléphone d'affaires sur le répondeur de la résidence peut permettre à des tiers d'avoir accès à des renseignements d'affaires confidentiels.

23. Voir également les documents rédigés par le Commissaire à l'information et à la protection de la vie privée intitulés : *Workplace Privacy : A Consultation Paper* (juin 1992) et *La protection de la vie privée en milieu de travail : le besoin d'un filet de sécurité* (septembre 1993). L'extrait suivant du document *Workplace Privacy : A Consultation Paper* peut s'appliquer aux communications par messagerie vocale :

> En Ontario, la *Loi sur le téléphone* interdit à un tiers de divulguer une conversation téléphonique qui ne lui est pas destinée. L'article 112 de la loi stipule en effet que :*
>
> > **112**. Sauf s'il y est autorisé par la loi ou s'il en a reçu l'ordre, quiconque, ayant pris connaissance d'une conversation ou d'un message transmis par une ligne téléphonique et qui ne lui est pas adressé ou destiné, en divulgue la signification ou la substance est coupable d'une infraction.
>
> Selon les conclusions d'un tribunal dans une cause où l'article 112 fut invoqué, le but de l'article est de protéger le caractère privé des conversations téléphoniques. Le *Code criminel* interdit également l'interception des conversations privées comme les conversations téléphoniques (p.39).*
>
> * Il n'existe pas de version française du document *Workplace Privacy : A Consultation Paper*. L'extrait ci-dessus est donc une traduction libre sauf pour ce qui est de l'article 112 de la *Loi sur le téléphone*.

24. «McDonald's snooping too», *Privacy Journal*, Vol. 21, N° 3, janvier 1995, p.5.

25. Des règles relatives à la protection des renseignements sont décrites dans le document intitulé «Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère général», Organisation de coopération et de développement économiques, Paris, 1980.

26. Dans le document *Information Technology Security Directive* (février 1991) préparé à l'intention du Secrétariat du Conseil de gestion, il est précisé que« les ministères et les agences doivent s'occuper de vérifier périodiquement la sécurité de leurs systèmes informatiques afin de s'assurer qu'elle est conforme aux exigences requises... » (p.7-3-2)*. En outre :

> Les ministères et les agences doivent s'assurer que les contrats établis avec des spécialistes des systèmes informatiques doivent inclure :
>
> - une description des moyens qui seront pris pour répondre aux exigences de sécurité du ministère ou de l'agence;
>
> - une clause exigeant des vérifications périodiques de la sécurité des systèmes informatiques. (p.7-3-3).*
>
> *Ce document n'a jamais été traduit. Les extraits ci-dessus sont une traduction libre.

27. Certains organismes ont fait ajouter la fonction «remise à l'état initial», ce qui permet à l'abonné qui a oublié son mot de passe d'accéder à ses messages. Toutefois, cette fonction permet également à ceux qui remettent le système à l'état initial d'accéder aux messages de l'abonné.

28. Fonction contrôle des accès : le système demande à l'abonné son nom et l'heure chaque fois que ce dernier demande d'accéder à sa boîte vocale. Puis, il fait entendre l'enregistrement réalisé la fois précédente. Ex. : Dernière demande d'accès de la part de (nom) à (indication de l'heure). Si aucune information n'a été communiquée à la messagerie lors de la dernière demande, il y a lieu de soupçonner qu'il y a eu violation.

29. Le document *Information Technology Security Directive* préparé à l'intention du Secrétariat du Conseil de gestion recommande que des vérificateurs internes ou externes vérifient périodiquement si les systèmes technologiques externes utilisés par le ministère ou l'agence satisfont aux normes de sécurité. Le document suggère également que des vérificateurs internes inspectent régulièrement les systèmes informatiques internes pour s'assurer que les normes de sécurité sont respectées.

30. ST-ONGE, Stéphane. «Lack of voice-mail security can let hackers into system», Telecommunications Special Report, *Financial Post*, 1er avril 1995, p. 37.

31. Après avoir annulé le mot de passe, l'administrateur créera un nouveau mot de passe temporaire que l'abonné devrait immédiatement changer. Si le responsable de la messagerie vocale n'a pas attribué un mot de passe temporaire à l'abonné, ce dernier n'aura pas accès à sa boîte vocale. Si on peut accéder à la boîte vocale dans ces conditions, il peut s'agir d'une violation de la sécurité et il faudra par conséquent aviser immédiatement le responsable du système.

32. Voir le *Second Annual Report of the Privacy Rights Claringhouse* (octobre 1993 — septembre 1994), Center for Public Interest Law, Université de San Diego, janvier 1995, p. 42.

33. Lorsque le système de messagerie vocale et le terminal de l'administrateur sont tous deux dans une pièce fermée à clef, l'équipement et l'accès au système (mot de passe) se trouvent protégés. Toutefois, les risques d'accès non autorisés sont plus élevés si les deux appareils sont dans des locaux différents et reliés par un modem.

    En pareil cas, il est possible d'accroître la protection en utilisant un dispositif de sécurité pour le modem sur le port du terminal de l'administrateur. Ce dispositif permet d'intercepter les appels et demande au correspondant un code d'utilisateur et un mot de passe. Si les codes entrés sont valides, la communication est interrompue et l'administrateur reçoit un appel à un numéro de téléphone déterminé au préalable. Lorsque l'administrateur répond à cet appel, l'accès au système est autorisé. Enfin, le système demandera d'entrer un mot de passe pour accéder au terminal avant que les menus ne soient affichés.

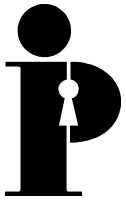
    L'administrateur ne devra pas divulguer systématiquement ce mot de passe aux personnes prétendant être chargées de l'entretien du système. L'administrateur prendra soin de vérifier l'identité des employés et les rappellera.

    Sources : «Security on Octel Voice Processing Systems», Octel Product Note, avril 1995, p.11. Également : Octel Security Presentation Training Video, TRT :26:35.

    Les systèmes qui sont configurés pour permettre aux personnes chargées de l'entretien de l'équipement de se relier par un port devraient être protégés contre l'accès non autorisé au téléphone ou au modem. Le port est une série de numéros ou une carte de communication auquel se relie le modem. Le modem devrait être débranché lorsqu'il n'est pas utilisé. On pourrait également utiliser un modem muni d'un dispositif de sécurité ou protégé par un mot de passe comme celui qui est décrit ci-dessus. Un port qui n'est pas utilisé devrait être enlevé.

Source : SMITH, Jan. «Call of the dialed», *Compuserve Magazine*, juin 1995, p. 35.

La protection de l'équipement est une question infiniment plus préoccupante lorsqu'il s'agit des répondeurs. Un grand nombre de répondeurs dans les bureaux sont situés dans des endroits facilement accessibles où quiconque a soit la possibilité de voler la bande, soit de l'écouter en appuyant sur un bouton. Les messages ne sont pas protégés par cryptage ou chiffrement et aucun mot de passe n'est requis pour avoir accès au répondeur. Le volume de l'appareil est souvent élevé, ce qui permet aux passants d'entendre les messages. Toute politique relative à l'utilisation des systèmes de répondeurs automatiques incluant les répondeurs devra aborder ces problèmes.



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