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

Les principes de la protection de la vie privée pour les systèmes de courrier électronique

Tom Wright
Commissaire
Février 1994

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

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

This publication is also available in English.

Sommaire

Le courrier électronique est une forme de communication sans papier qui permet l'envoi de messages d'un utilisateur d'ordinateur à l'autre. C'est un outil efficace pour franchir les obstacles à la communication à l'intérieur d'un organisme et entre organismes et pour favoriser l'échange libre de renseignements et d'idées.

En revanche, comme l'a souligné un responsable de sécurité informatique, le courrier électronique présente «le même niveau de sécurité qu'une carte postale[1].» Autrement dit, l'utilisateur du courrier électronique s'expose à des violations du caractère confidentiel de ses communications. En outre, le courrier électronique crée une piste électronique de messages qui se prête à la surveillance des utilisateurs. Il se pose donc des questions juridiques et déontologiques complexes qui touchent la vie privée de ces utilisateurs, surtout en milieu de travail.

La protection de la vie privée des utilisateurs du courrier électronique, en ce qui concerne leurs communications, constitue le thème principal du présent document. Toutefois, on s'est penché également sur la facilité avec laquelle les renseignements personnels peuvent être transmis par ce système, ce qui constitue une menace à la vie privée des particuliers qui font l'objet des messages électroniques.

Le commissaire à l'information et à la protection de la vie privée de l'Ontario a pour mandat, en vertu de 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*) d'examiner les phénomènes qui entravent l'application des objectifs des *lois*. Un des principaux objectifs des *lois* est la protection de la vie privée. Or, l'emploi de la technologie de l'information électronique nouvelle et existante, comme le courrier électronique, au sein des institutions gouvernementales, a des répercussions sur la protection de la vie privée. Afin de sensibiliser le public, le commissaire a mis au point une série de principes en cette matière, destinés aux systèmes de courrier électronique.

Ces principes s'appliquent tout particulièrement aux organismes des administrations provinciales et municipales qui tombent sous le coup des *lois*. Toutefois, ils permettront aussi de guider les autres organismes des secteurs public et privé dans l'élaboration et l'application de leurs propres directives dans ce domaine.

Les principes de protection de la vie privée énoncés à la page suivante se veulent un cadre pour la mise au point de directives précises applicables au courrier électronique. L'élaboration de ces directives entraînera de nombreuses décisions difficiles. Les choix à faire dépendront, dans une certaine mesure, des limites techniques des systèmes de courrier électronique, des raisons pour lesquelles on y fait appel, de la nature des renseignements échangés et des activités de l'organisme. Nous estimons cependant que ces directives doivent reposer sur le souci d'offrir la meilleure protection possible de la vie privée des utilisateurs du courrier électronique au sein de l'organisme et des personnes qui en font l'objet.

Principes

1. Il faut respecter et protéger la vie privée des utilisateurs du courrier électronique.

2. Il faut que chaque organisme élabore des directives précises pour la protection de la vie privée des utilisateurs du courrier électronique.

3. Il faut que chaque organisme communique ses directives en matière de courrier électronique aux utilisateurs et qu'il les informe de leurs droits et obligations en ce qui concerne le caractère confidentiel des messages transmis par le système.

4. Il faut que les utilisateurs reçoivent une formation appropriée au sujet du courrier électronique et des questions de sécurité et de protection de la vie privée qui entourent son utilisation.

5. Il ne faut employer les systèmes de courrier électronique pour recueillir, utiliser et divulguer des renseignements personnels que si des mesures suffisantes pour protéger la vie privée sont en place.

6. Il faut que les fournisseurs de systèmes de courrier électronique examinent des moyens techniques pour protéger la vie privée.

7. Il faut que les organismes élaborent des mesures appropriées pour protéger les messages envoyés par courrier électronique.

Table des matières

Introduction

Le courrier électronique est une forme de communication sans papier. Qu'il s'articule autour d'un réseau local, d'un ordinateur central ou d'un service commercial, le courrier électronique permet la transmission de messages d'un utilisateur d'ordinateur à l'autre. À l'intérieur d'un organisme, il peut remplacer les autres formes de communication, comme les notes de service, les appels téléphoniques et les visites personnelles.

La communication par courrier électronique ne se borne plus à de brefs messages dactylographiés. En effet, grâce à des programmes de plus en plus avancés, certains systèmes de courrier électronique peuvent transmettre des renseignements sous différentes formes : note de service dactylographiée, feuille de calcul, photographie, message vidéo, code à barres et message oral. On peut aussi les lier à un échange de données électroniques qui sert à transmettre des formulaires électroniques structurés, comme les bulletins de commande. En outre, l'uniformisation des normes permet la liaison de systèmes de courrier électronique, permettant à des organismes de communiquer avec le monde extérieur.

La division de l'informatique et des télécommunications du Conseil de gestion du gouvernement estime qu'environ 28 000 employés du gouvernement ontarien utilisent actuellement un système de courrier électronique sous une forme ou une autre. La plupart de ces systèmes sont établis en réseau et peuvent être reliés l'un à l'autre et aux réseaux de courrier électronique publics au moyen d'un système appelé bureau de poste électronique.

Le courrier électronique présente de nombreux avantages possibles. Il contribue à éliminer les «jeux de cache-cache téléphonique» et parfois à réduire la consommation du papier. Utilisé par des employés établis dans des lieux différents, il permet de réduire au minimum l'effet des retards du service postal et du décalage horaire qui peuvent entraver les autres formes de communication. Il favorise également les discussions en groupe et, de façon générale, stimule la communication à l'intérieur de l'organisme.

En revanche, le courrier électronique présente «le même niveau de sécurité qu'une carte postale[2]», selon un responsable de la sécurité informatique. Ainsi, les utilisateurs du courrier électronique s'exposent à des violations du caractère confidentiel de leurs communications. En outre, le système crée une piste électronique de messages qui peut se prêter à la surveillance des utilisateurs. Il se pose donc des questions juridiques et déontologiques complexes qui touchent la vie privée de ces utilisateurs, surtout en milieu de travail.

La protection de la vie privée des utilisateurs du courrier électronique, en ce qui concerne leurs communications, constitue le thème principal du présent document. Toutefois, on s'est penché également sur la facilité avec laquelle la transmission des renseignements personnels se fait par ce système, ce qui constitue une menace à la vie privée des particuliers qui font l'objet des messages électroniques.

Objectif

Le commissaire à l'information et à la protection de la vie privée de l'Ontario a pour mandat, en vertu de 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*) d'examiner les phénomènes qui entravent l'application des objectifs des *lois*. Un des principaux objectifs des *lois* est la protection de la vie privée. Or, l'emploi de la technologie de l'information électronique nouvelle et existante, comme le courrier électronique, au sein des institutions gouvernementales a des répercussions sur la protection de la vie privée. Afin de sensibiliser le public, le commissaire a mis au point une série de principes en cette matière, destinés aux systèmes de courrier électronique.

Les systèmes de courrier électronique varient entre eux sur le plan de leurs caractéristiques techniques, de leur emploi et du genre de renseignements qu'ils transmettent. Il a donc été impossible de dégager une seule série de directives qui soient applicables à tous les organismes. C'est pourquoi nous nous sommes bornés à proposer un certain nombre de principes généraux pour la protection de la vie privée à suivre par l'organisme pour la mise au point de ses propres directives en la matière. Les principes proposés ici se veulent un cadre pour l'élaboration de directives en matière de protection de la vie privée applicables au courrier électronique à l'échelle de l'organisme.

Champ d'application

Ces principes s'adressent expressément aux organismes des administrations provinciales et municipales qui tombent sous le coup des *lois*. Cependant, ils peuvent s'avérer utiles aussi aux autres organismes des secteurs public et privé qui s'attachent à mettre au point leurs propres directives en la matière.

Principes

Principe 1 — Il faut respecter et protéger la vie privée des utilisateurs du courrier électronique

En mars 1989, la Epson Corporation congédie son administrateur du courrier électronique. Epson prétend qu'il s'agit d'un renvoi motivé, mais l'intéressé estime avoir été congédié parce qu'il voulait savoir pourquoi un chef de service lisait les messages électroniques des employés. L'ancien employé intente un procès pour violation du droit à la vie privée à Epson. Le procès laisse sans réponse de nombreuses questions juridiques et déontologiques en matière de courrier électronique, mais fait nettement ressortir un point : les employés s'attendent à ce que la confidentialité du courrier électronique soit protégée.

L'expression «vie privée» a des sens différents, selon le contexte. Il s'agit d'une notion générale qui englobe toute une série d'atteintes à la vie privée, comme la surveillance, les tables d'écoute et l'interception des messages. Les *lois* ne visent qu'un seul domaine : la protection de la vie privée en matière de renseignements. Elles partent du principe que les renseignements personnels appartiennent au particulier auquel ils s'appliquent et que, par conséquent, celui-ci peut prétendre à un certain degré de contrôle ou d'autodétermination sur sa collecte, son emploi et sa divulgation.

La protection de la vie privée prend aussi d'autres formes. Ainsi, la protection territoriale vise le domaine physique dans lequel le particulier bénéficie d'un droit de non-intrusion. Un autre genre, la protection de la personne, fait l'objet des lois qui garantissent la liberté de mouvement et d'expression, interdisent les voies de fait et limitent les fouilles injustifiées. Comme la protection territoriale, la protection de la personne repose sur la notion de l'intrusion physique, mais englobe également les atteintes à la dignité de la personne. Chacun de ces aspects de la vie privée s'applique, dans une certaine mesure, dans le contexte des systèmes de courrier électronique.

Étant donné les caractéristiques inhérentes de la plupart des systèmes de courrier électronique, il est impossible de garantir la protection complète de la vie privée dans ce domaine. Cependant, on peut avancer qu'un organisme a tout intérêt à assurer la plus grande protection de la vie privée possible. À notre avis, la qualité de la vie au travail s'en trouvera améliorée et les employés seront portés à tirer le maximum du courrier électronique.

Le courrier électronique présente l'avantage, notamment, qu'il aplatit la structure hiérarchique traditionnelle de l'organisme grâce à l'élimination des obstacles à la communication entre salariés, patrons et gestionnaires. En un sens, il «démocratise le lieu de travail[3]». Avec une meilleure communication, l'organisme fonctionne mieux. Toutefois, les employés n'ont recours au courrier électronique que s'ils ont la certitude que le caractère confidentiel du message transmis sera, pour une large part, respecté.

Un sondage mené auprès des dirigeants d'entreprise aux États-Unis montre que la fouille des dossiers du courrier électronique constitue l'une des formes de surveillance des employés[4] les plus courantes. Les employeurs prétendent que la surveillance électronique permet d'augmenter la productivité, mais d'après la recherche, elle a plutôt l'effet contraire. Ainsi, on lit dans une étude des employés de société des communications aux États-Unis que la surveillance électronique contribue à aggraver «la tension, l'anxiété, la dépression, la colère et la fatigue[5]». Le sentiment d'impuissance éprouvé par les travailleurs qui font l'objet de surveillance contribue nettement au stress en milieu de travail.

Principe 2 — Il faut que chaque organisme élabore des directives précises pour la protection de la vie privée des utilisateurs du courrier électronique

La nature même du courrier électronique fait ressentir plus profondément le besoin de régler les problèmes de protection de la vie privée qui résultent de l'adaptation des systèmes de courrier électronique, de leur emploi et de leur réglementation. Il est recommandé que chaque organisme élabore des directives officielles pour protéger la vie privée des utilisateurs du courrier électronique. Il faut que chaque personne qui travaille au sein de l'organisme soit informée de ses droits et obligations en vertu de ces directives et s'engage à les respecter[6]. Il faut que les directives permettent aux utilisateurs de protéger non seulement leur propre vie privée, mais aussi celle de leurs collègues qui leur envoient des renseignements et celle d'autres particuliers qui font l'objet de messages électroniques.

Cependant, ces directives ne sauraient être efficaces que si chaque utilisateur du courrier électronique en reconnaît le mérite et s'engage à les suivre. La participation à leur mise au point est donc essentielle. Pour pouvoir bien y participer, les utilisateurs doivent recevoir une bonne formation sur le courrier électronique et sur les problèmes de vie privée et de sécurité qu'il soulève. La mise en application des directives demande aussi une formation.

Pour assurer que l'organisme adapte les directives qui lui conviennent le mieux, il faut que des représentants des salariés, des dirigeants, des services de ressources humaines, des services juridiques et des systèmes informatiques jouent un rôle dans leur élaboration.

Au minimum, les directives doivent porter sur les points suivants :

- objectifs du système de courrier électronique
- accès au courrier électronique de la part de tiers
- conséquences des violations des directives

Objectifs du système de courrier électronique

Dans les directives, on doit désigner les personnes habilitées à se servir du système de courrier électronique et préciser les raisons pour lesquelles on l'emploie. On peut rendre le système accessible aux personnes suivantes :

- employés de l'organisme
- clients et fournisseurs
- experts-conseils
- le grand public

Le risque de sécurité est d'autant plus important que le système est plus accessible aux personnes extérieures à l'organisme. Il y a donc lieu d'imposer aux utilisateurs du courrier électronique des mesures spéciales pour assurer la sécurité des messages envoyés par courrier électronique dans le cas de systèmes de communication inter-réseau. En outre, il faut que les personnes étrangères à l'organisme qui ont le droit d'accéder au système de courrier électronique soient informées des directives de l'organisme à ce sujet et s'engagent à les respecter.

Les systèmes de courrier électronique peuvent servir à différentes fins au sein de l'organisme, notamment :

- envoi de messages et de dossiers se rapportant aux activités de l'organisme
- envoi de messages et de dossiers de nature personnelle
- surveillance à des fins non déterminées (p. ex., par simple curiosité)
- surveillance pour des besoins d'évaluation du personnel
- surveillance pour le dépistage des infractions aux directives ou à la sécurité

Messages administratifs

La protection de la vie privée revêt une importance moindre dans le cas des messages électroniques portant sur des renseignements administratifs à caractère non confidentiel. En effet, les employeurs, dirigeants et autres particuliers au sein de l'organisme doivent avoir accès aux renseignements qui concernent les activités de l'organisme. Les employés ne doivent donc pas s'attendre à la protection absolue du caractère confidentiel des renseignements administratifs et doivent reconnaître le besoin de communiquer ces renseignements librement avec d'autres à l'intérieur de l'organisme.

Toutefois, la question de la protection de la vie privée se pose de façon plus évidente lorsque le message électronique concerne des renseignements administratifs à caractère délicat ou confidentiel. Étant donné le manque de sécurité que représentent la plupart des systèmes de courrier électronique, l'organisme ferait bien d'imposer des restrictions à l'emploi du courrier électronique pour la transmission de renseignements administratifs à caractère délicat ou confidentiel. Il pourrait

mettre en place des procédures de sécurité spéciales ou imposer des restrictions à l'emploi du courrier électronique pour l'échange de documents dont la divulgation est interdite en application des *lois*.

De même, il est recommandé que l'organisme impose des restrictions à l'envoi, à la réception et à l'entreposage des messages administratifs qui renferment des renseignements personnels. Car, une fois les renseignements personnels transmis par courrier électronique, l'expéditeur n'aura que peu de contrôle sur leur conservation, emploi ou divulgation par le destinataire. Ce dernier peut, en effet, les adresser à des tiers, avec ou sans modifications. Pour protéger la vie privée des particuliers qui font l'objet du courrier électronique, il faut que les directives limitent la transmission de renseignements personnels s'il n'existe pas de mesures de protection suffisantes en matière de vie privée. Là, il est toujours mieux d'emprunter d'autres formes de communication.

Parfois, l'organisme se trouve dans l'obligation d'échanger, par courrier électronique, des renseignements sur des particuliers. En effet, lorsque des employés sont établis dans différents lieux, que les renseignements existent déjà dans une forme électronique ou qu'il existe un besoin immédiat de l'information, il n'est peut-être pas pratique d'utiliser d'autres formes de communication. Dans ces cas-là, il faut s'attacher à supprimer tous les points qui permettraient d'identifier des particuliers avant de transmettre les renseignements. Si cela s'avère impossible, il faut faire le nécessaire pour que la collecte, l'emploi et la divulgation des renseignements se fassent conformément aux dispositions de protection de la vie privée visées par les *lois*. Voici des dispositifs de sécurité qui peuvent s'avérer utiles dans la transmission des renseignements de nature délicate.

Messages personnels

Selon un rapport rédigé par l'État de la Californie, plus de 60 pour cent des messages électroniques sont de nature non administrative[7]. Il faut donc que chaque organisme établisse ses propres directives concernant l'utilisation du courrier électronique pour l'envoi des messages de nature personnelle, étant donné les répercussions sur la protection de la vie privée.

On peut avancer plusieurs arguments pour ne pas mettre en place une politique qui limite la transmission électronique des communications non administratives. En premier lieu, on risque de nuire à la communication et de gêner le contact social normal et la libre circulation des idées. Voici un exemple : pour se protéger contre d'éventuelles poursuites judiciaires par ses salariés, Hewlett Packard fait circuler une note de service pour annoncer que les messages électroniques sont surveillés par des chefs de service. Résultat : le courrier électronique de tout genre, administratif et non administratif, a diminué des deux tiers[8].

Autre argument pour permettre l'emploi du courrier électronique à des fins personnelles : les messages sont habituellement brefs et pertinents et accaparent probablement moins de temps de travail que d'autres formes de communication non administrative, comme les appels téléphoniques ou les visites personnelles.

Si l'organisme permet les communications personnelles dans son système de courrier électronique, il doit fixer des directives sur la façon de les protéger. Pour cela il peut, par exemple, adopter des mots de passe entreposés dans des zones protégées d'accès limité.

Surveillance du courrier électronique sans but précis

Il faut que les directives interdisent l'accès au courrier électronique sans but précis, c'est-à-dire par simple curiosité. Le courrier électronique doit être considéré comme une communication privée entre l'expéditeur et le destinataire.

Surveillance du courrier électronique pour des besoins d'évaluation du personnel

Certains organismes surveillent les communications électroniques de leurs employés pour évaluer leur rendement ou leurs activités. Ils désirent s'assurer, par exemple, que les employés font preuve de courtoisie envers leurs clients et qu'ils font un usage efficace des ressources de l'organisme. À moins d'une explication claire de son objectif, de ses procédures et de ses conséquences, ce genre de surveillance secrète risque cependant de saper le moral du personnel.

Même avertis d'avance, les employés risquent de considérer comme une intrusion la surveillance du courrier électronique dans un but d'évaluation. Cette pratique risque non seulement de nuire au moral, mais également de gêner les communications normales et l'échange libre d'idées. Le fait de talonner les employés par des moyens électroniques a peu de chances de favoriser une ambiance productive au travail. Soulignons d'ailleurs que, dans bien des cas, il existe des moyens plus directs et moins envahissants (et aussi plus efficaces) de surveiller le rendement. Il faut donc peser le pour et le contre de la surveillance électronique avant de l'adopter. Et si on décide de l'adopter, une consultation avec le personnel s'impose. Notre bureau a publié des documents[9] qui présentent une étude poussée des répercussions de la surveillance électronique en milieu de travail.

Surveillance du courrier électronique pour infractions aux directives ou à la sécurité

L'organisme décide parfois de surveiller le courrier électronique pour prévenir des infractions aux directives ou à la sécurité, ou pour recueillir des preuves à ce sujet. Parmi les infractions possibles, notons les atteintes à la sécurité, l'activité illégale, l'abus des ressources de l'organisme, la discrimination raciale et le harcèlement sexuel. Dans ces cas-là, il se peut que la surveillance du courrier électronique soit vue comme étant justifiée, surtout s'il existe d'autres preuves établissant l'existence d'infractions possibles.

L'organisme décide parfois de surveiller les messages électroniques pour se faire une idée de l'emploi que l'on fait du système. Les employeurs ont fait valoir, et cela se comprend fort bien, qu'ils ont le droit de déterminer comment sont utilisées les ressources de leur entreprise. Et,

effectivement, la surveillance du courrier électronique a permis de mettre en lumière des incidents d'abus[10]. Toutefois, certains experts ont fait valoir qu'il est possible de prévenir les abus du courrier électronique sans porter atteinte aux droits des travailleurs en matière de vie privée[11]. Ainsi, l'employeur pourrait examiner l'adresse, l'en-tête, le lieu d'expédition et l'importance du dossier pour déterminer s'il y a ou non abus des ressources de l'entreprise, sans lire le contenu du message.

Si l'organisme procède automatiquement, et sans justification valable, à la surveillance du courrier électronique pour détecter les infractions aux directives ou de la sécurité, il se peut que les salariés y voient une intrusion. Pour éviter cette perception, l'organisme aurait intérêt à ne surveiller le courrier électronique que dans la mesure exigée par la loi ou par des obligations légales envers des tiers, ou pour protéger ses intérêts en cas de soupçons justifiés de crime.

Accès au courrier électronique de la part de tiers

Il est parfois nécessaire d'accéder aux messages électroniques d'un employé. Par exemple, si l'intéressé travaille à l'extérieur du bureau, est en vacances ou est absent pour cause de maladie, un autre particulier est parfois obligé d'accéder à ses messages électroniques qui se rapportent au travail.

En outre, il est inévitable, pendant l'exploitation et l'entretien d'un système de courrier électronique, que certains messages soient lus et on ne peut donc jamais garantir la protection de la vie privée. Selon le responsable de la sécurité de l'État de la Californie[12], on attache parfois aux lignes de communication des dispositifs pour enregistrer des erreurs. Dans ces cas-là, les données transmises par ces lignes, y compris les mots de passe, les codes d'identification et les messages, sont affichées dans une forme que le technicien peut lire. C'est pourquoi l'État de la Californie a rapporté dans son projet de directives que l'État ne peut garantir le caractère confidentiel des communications par courrier électronique.

Il incombe à l'organisme de préciser dans ses directives les circonstances où des tiers peuvent avoir accès au courrier électronique de tel ou tel particulier, les restrictions à l'emploi et à la divulgation des renseignements auxquels ont accès des tiers, et les règles spéciales à suivre pour l'approbation d'accès de la part de tiers.

Conditions d'accès

Il faut, suivant la nature des renseignements échangés par courrier électronique, que les directives en matière d'accès par des tiers soient aussi peu envahissantes que possible. Elles doivent stipuler au minimum que la demande d'accès aux messages électroniques soit faite directement à l'employé. Ainsi, on pourrait contacter l'employé chez lui ou lui demander l'accès avant qu'il ne parte en vacances. Lorsqu'il est impossible d'avoir accès au courrier électronique en s'adressant

directement à l'employé, il faut que les directives limitent l'accès de la part des tiers à des fins administratives légitimes, lorsqu'il n'existe aucun autre moyen promptement accessible pour obtenir les renseignements. Nous examinerons ci-après les méthodes précises à suivre pour l'accès au courrier électronique des employés.

Dans la protection de la vie privée, il faut faire la distinction entre les messages non confidentiels se rapportant au travail et les communications confidentielles ou personnelles. Pour protéger la vie privée de l'utilisateur, il convient, autant que possible, d'entreposer séparément les deux genres de communications. On peut ainsi protéger par un mot de passe les communications personnelles et les entreposer dans une zone qui n'est pas facilement accessible par d'autres. Au cas où il faut parcourir des messages administratifs non confidentiels, la menace à la vie privée de l'intéressé sera réduite au minimum.

Lorsque les communications personnelles sont entreposées séparément des communications administratives, on peut rendre plus restrictive la politique d'accès aux communications personnelles. On peut, par exemple, interdire l'accès aux communications personnelles de la part de tiers. Ou bien, on peut limiter l'accès à des circonstances qui soient suffisamment urgentes pour justifier la perte de la protection de la vie privée qui résulte de la lecture des messages électroniques personnels des employés. Une politique restrictive limiterait l'accès aux circonstances où l'on soupçonne des infractions aux directives ou à la sécurité, ou pour des besoins de l'exécution de la loi.

Emploi et divulgation du courrier électronique

Une fois que le message électronique a été envoyé à des tiers ou accédé par ces derniers, l'expéditeur du message n'a que peu de contrôle sur l'emploi subséquent des renseignements ou sur leur divulgation. Il faut donc que les directives renferment des restrictions précises sur l'emploi et la divulgation des renseignements par les destinataires de courrier électronique, ou par des tiers qui peuvent y avoir accès soit intentionnellement, à une fin légitime prévue par la politique de l'organisme, soit par inadvertance, lors du fonctionnement et de l'entretien du système de courrier électronique.

Si l'on ne consulte pas l'expéditeur, il faut que les renseignements obtenus par courrier électronique ne servent qu'à des fins administratives légitimes et qu'ils ne soient divulgués qu'aux tiers qui ont besoin de les connaître. Dans les cas de renseignements particulièrement délicats échangés par courrier électronique, l'organisme a intérêt à limiter davantage la divulgation à des tiers, après avoir obtenu le consentement de l'expéditeur.

Procédures d'accès

Pour les cas où l'on doit accéder au courrier électronique d'un employé qui n'a pas consenti directement à l'accès, il faut avoir en place des procédures spéciales pour obtenir l'approbation appropriée. Il faut qu'un ou plusieurs chefs de service aient le pouvoir d'approuver et de surveiller

l'accès par des tiers, conformément à la politique de l'organisme. Il faut que le processus d'approbation inclue un sommaire de l'emploi et de la divulgation prévus. Autant que possible, il faut avertir d'avance les personnes dont le courrier électronique sera accédé par des tiers. Si cela est impossible, il faut que les intéressés soient informés aussitôt que possible de l'accès, de l'emploi et de la divulgation de leur courrier électronique.

Conséquences des violations des directives en matière de courrier électronique

Des directives ne peuvent être considérées valables que si l'on assure leur application. Sinon, les intéressés sont amenés à conclure qu'ils n'ont pas besoin de les prendre au sérieux. Les directives non appliquées ne sont guère efficaces.

Il faut que la marche à suivre pour déposer une plainte formelle dans le cas d'une infraction, et les conséquences des infractions soient indiquées clairement dans les directives établies par l'organisme en matière de courrier électronique.

De plus, il faut que l'employé soit tenu responsable du caractère confidentiel du courrier électronique, par l'inclusion, dans son contrat de service, de l'obligation de respecter les directives de l'organisme dans ce domaine.

Principe 3 — Il faut que chaque organisme communique ses directives en matière de courrier électronique aux utilisateurs et qu'il les informe de leurs droits et obligations en ce qui concerne le caractère confidentiel des messages transmis par le système

En l'absence de directives connues, la plupart des utilisateurs du courrier électronique supposent que leurs communications sont confidentielles. C'est pourquoi il importe que chaque employé soit expressément informé de ses droits et obligations quant à l'emploi du courrier électronique en milieu de travail.

Il ne suffit pas de reproduire simplement les directives dans le manuel d'opération de l'organisme. Il faut que chaque salarié les lise et accepte de les respecter. Il importe enfin que les chefs de service et employés reçoivent une formation sur la façon de les appliquer.

À son engagement, le nouvel employé reçoit habituellement une sorte d'orientation. Voilà l'occasion par excellence de présenter la question du courrier électronique et de la protection de la vie privée qui en découle. L'organisme a avantage également à faire afficher les directives à l'écran de l'ordinateur chaque fois que l'employé entre dans le système de courrier électronique. Il faut aussi que les modifications aux directives soient portées à la connaissance de tout le personnel (lors de réunions, par des bulletins ou par courrier électronique, et ainsi de suite).

Principe 4 — Il faut que les utilisateurs reçoivent une formation appropriée au sujet du courrier électronique et des questions de sécurité et de protection de la vie privée qui entourent son utilisation

Des problèmes de protection de la vie privée peuvent se poser lorsque l'utilisateur ne comprend pas le fonctionnement du courrier électronique. Souvent, l'utilisateur mal informé suppose que ses communications sont privées. Plus l'utilisateur connaît le système de courrier électronique et mieux il sera en mesure de protéger sa vie privée et celle des autres.

Pour la protection de la vie privée, il faut que l'utilisateur comprenne les caractéristiques suivantes des systèmes de courrier électronique :

Le processus du courrier électronique n'est pas privé en soi.

Par sa nature même, le courrier électronique est vulnérable aux atteintes à la vie privée. Les messages électroniques sont souvent entreposés dans un seul lieu commode, qui permet l'accès et la recherche électronique d'un sujet particulier. À titre d'exemple, un sondage mené auprès des chefs de service aux États-Unis a fait ressortir que près de 22 pour 100 d'entre eux avaient parcouru les dossiers informatiques de leurs employés, leurs messages audios, messages électroniques ou autres communications en réseau. Parmi les employeurs qui avaient pratiqué ce genre de surveillance, 66 pour 100 affirmaient n'avoir donné aucun avertissement préalable[13].

Il y a des organismes qui ont mis en place des directives qui limitent l'accès de la part des tiers, mais souvent ces même directives prévoient des circonstances où ce genre d'accès est jugé nécessaire. Elles permettent, par exemple, l'accès pour des besoins d'exécution de la loi, ou l'accès par des informaticiens pendant le fonctionnement et l'entretien ordinaires du système de courrier.

Le message ne disparaît pas forcément après sa transmission.

Bien des utilisateurs supposent que le courrier électronique est une transmission de l'information qui se fait de clavier à clavier, ou d'écran à écran. Cependant, après la transmission du message électronique, on peut imprimer une copie et la sauvegarder dans des archives personnelles, comme sur disque dur. De plus, selon les mesures de sécurité pratiquées par le destinataire du message, ces copies prêtent le flanc à l'accès non autorisé par des tiers. Après l'expédition du message électronique, l'expéditeur n'aura guère de contrôle sur sa conservation, son accès, son utilisation ou sa divulgation par le destinataire.

La suppression du message dans les fichiers personnels n'entraîne pas forcément la suppression de toutes les copies du message.

Après la suppression du message électronique, il se peut que des copies existent toujours dans les fichiers de sauvegarde automatiquement créés par certains systèmes ou dans les archives personnelles des destinataires du message. Les fichiers de sauvegarde sont parfois conservés pendant longtemps. Les périodes de validité des archives personnelles varient d'une personne à l'autre.

Le transfert des fichiers électroniques est facile.

Après la réception du message électronique, on peut le transmettre sans difficulté à un nombre donné de particuliers, sans le consentement ou la connaissance de l'expéditeur.

Les systèmes de courrier électronique peuvent être reliés par réseau avec d'autres organismes ou particuliers, ou avec des points d'accès publics.

Les systèmes de courrier électronique qui sont accessibles à des personnes étrangères à l'organisme se prêtent davantage à des infractions à la sécurité. Des systèmes de communication inter-réseaux avec d'autres systèmes de courrier électronique peuvent également assurer des liens avec d'autres renseignements entreposés dans le système.

Le destinataire n'est peut-être pas le seul à lire le courrier électronique.

Il se peut que le courrier électronique soit lu par d'autres personnes qui, intentionnellement ou par inadvertance, entrent dans les fichiers informatiques du destinataire ou qui reçoivent des copies du message du destinataire.

Les copies des messages ne sont pas forcément des doubles de l'original.

Après la réception du message, le destinataire peut y apporter des modifications avant de le transmettre à des tiers. Dans certains systèmes de courrier électronique, le destinataire du message transmis n'a aucun moyen de savoir si le message initial a été ou non modifié. Toutefois, la plupart des systèmes de courrier électronique actuellement en usage ont un mécanisme qui empêche le changement du message avant sa retransmission.

Des personnes non autorisées peuvent pénétrer dans les systèmes de courrier électronique.

Il est possible que des pirates informatiques, des employés mécontents, des espions et d'autres, avec ou sans l'intention de nuire, cherchent à avoir accès au courrier électronique.

La technologie du courrier électronique risque de jouer contre la protection de la vie privée.

Il est d'autant plus facile de faire des erreurs que le système du courrier électronique est facile à utiliser. Ainsi, les caractéristiques qui permettent aux utilisateurs d'envoyer un message avec une seule frappe d'une touche facilitent également les erreurs. Les erreurs qui se produisent au moment de l'envoi, de la transmission ou de la réponse du message peuvent entraîner la divulgation, par inadvertance, de renseignements personnels à caractère délicat ou la transmission de renseignements incomplets ou non édités.

Pour éviter des erreurs, il faut sensibiliser les utilisateurs au fonctionnement du système et à ses défauts. Par exemple, pour adresser une réponse à un message électronique, l'utilisateur doit savoir si le système envoie la réponse automatiquement à l'expéditeur du message seulement ou à toutes les personnes qui reçoivent normalement une copie du message initial. Pour éviter les erreurs, il appartient aux utilisateurs de vérifier avec soin, avant la transmission, les noms des destinataires de tous les messages et de toutes les réponses aux messages.

La surveillance du courrier électronique peut se faire à partir d'une région éloignée, à l'insu de l'expéditeur.

À l'intérieur de l'organisme, il peut y avoir des personnes qui désirent surveiller le courrier électronique, et ce, pour différentes raisons : simple curiosité, évaluation, prévention d'infractions éventuelles à la sécurité ou aux directives, ou collecte de renseignements à ce sujet. La surveillance du courrier électronique peut se faire jour et nuit, et à partir d'un lieu éloigné. Dans la plupart des cas, les utilisateurs ne savent absolument pas si leur courrier électronique est surveillé par des tiers.

L'utilisation du courrier électronique à des lieux éloignés peut entraîner la constitution de documents sur lesquels l'organisme a peu de contrôle.

Les utilisateurs qui ont accès aux systèmes de courrier électronique à partir de lieux éloignés, comme leur maison, peuvent imprimer des copies de messages électroniques et les entreposer dans des archives personnelles non protégées qui se trouvent sur ces lieux. En outre, les personnes qui travaillent dans un lieu donné peuvent transmettre des renseignements à imprimer dans un autre lieu. Parfois donc, l'organisme a peu de contrôle sur la conservation des renseignements que renferment ces documents, leur accès, leur utilisation ou leur divulgation par des tiers dans des lieux éloignés.

Les systèmes de courrier électronique n'effectuent pas tous le codage automatique des dossiers et messages.

S'il est vrai que de nombreux systèmes de courrier électronique font le codage automatique des messages et fichiers, il convient de noter que certains ne le font pas. Par exemple, le codage

n'existe pratiquement pas dans les systèmes de courrier électronique publics. De plus, si le système de courrier électronique est lié à un ou plusieurs systèmes différents, dont le codage n'est pas toujours compatible, le message qui quitte un système perd son codage et se prête à l'interception.

Dans certains cas où il n'y a pas de codage automatique, l'utilisateur peut recourir à un logiciel spécial conçu pour coder les communications. Cependant, le système de courrier électronique sera alors moins facile à utiliser.

Les systèmes sans fil sont plus vulnérables que d'autres systèmes à l'interception non autorisée de messages électroniques.

Bien des utilisateurs ne savent pas que certains réseaux locaux font appel à des fréquences radiophoniques et à des transmissions téléphoniques, et que de grands réseaux sont parfois liés par satellite. Les systèmes de courrier électronique qui utilisent des fréquences radiophoniques sont plus vulnérables à l'interception que d'autres systèmes.

Principe 5 — Il ne faut employer les systèmes de courrier électronique pour recueillir, utiliser et divulguer des renseignements personnels que si des mesures suffisantes pour protéger la vie privée sont en place

La protection de la vie privée des utilisateurs du courrier électronique et des personnes qui font l'objet des messages électroniques est une question qui doit être réglée. Les *lois* protègent les renseignements personnels, à savoir les informations consignées au sujet d'un particulier qui peut être identifié, y compris celles qui sont enregistrées par des moyens électroniques.

Afin de protéger la vie privée, les *lois* obligent les organismes à suivre certaines pratiques d'équité en matière de renseignements personnels. De façon générale, ces pratiques empêchent la collecte, l'utilisation ou la divulgation de renseignements personnels sans la connaissance ou le consentement de l'intéressé. Elles font que le particulier conserve un certain contrôle sur les renseignements personnels qui le concernent.

En vertu des *lois*, la collecte des renseignements personnels se limite expressément aux données nécessaires pour réaliser un objectif déterminé. À part quelques exceptions, elles exigent que les renseignements personnels soient obtenus directement de l'intéressé et avec sa connaissance. Aux termes des *lois*, l'utilisation des renseignements personnels se limite à l'objectif auquel ils étaient destinés ou à des fins compatibles, sauf si l'intéressé accepte une autre fin ou s'il existe le pouvoir légal d'utiliser ces renseignements à une autre fin. La divulgation des renseignements personnels se limite à des personnes et circonstances déterminées. Les particuliers ont le droit d'avoir accès à leurs propres renseignements personnels et de demander une rectification si ces renseignements sont inexacts, périmés ou incomplets.

Lorsque des renseignements personnels sont échangés par courrier électronique, plusieurs caractéristiques inhérentes aux systèmes de courrier électronique risquent de contribuer à des infractions aux pratiques d'équité en matière d'information. Par exemple, la facilité avec laquelle on peut échanger des renseignements personnels par courrier électronique, que ce soit intentionnellement ou par inadvertance, peut faciliter la collecte non nécessaire et l'utilisation et la divulgation inappropriées ou non autorisées de ces renseignements.

Même l'expéditeur du message électronique qui respecte scrupuleusement les pratiques d'équité dans sa divulgation des renseignements personnels à des tiers par courrier électronique n'a peut-être pas le contrôle de la façon dont ces renseignements sont utilisés ou divulgués par les destinataires par la suite. Ces derniers peuvent, en effet, modifier les renseignements et les transmettre à des tiers, ou ne pas pratiquer des mesures de sécurité suffisantes pour empêcher de les exposer à l'accès non autorisé ou inapproprié de la part de tiers.

Il est d'autant plus difficile de respecter les pratiques d'équité en matière d'information que les renseignements personnels sont plus éloignés de la source initiale. Il se peut que la collecte des renseignements personnels se fasse sans l'autorisation appropriée et qu'elle ne soit pas obtenue directement de l'intéressé. Étant donné que le destinataire des renseignements personnels ne connaît peut-être pas l'objectif premier pour lequel les renseignements ont été recueillis, il peut, par inadvertance, les utiliser ou les divulguer à des fins incompatibles.

Principe 6 — Il faut que les fournisseurs de systèmes de courrier électronique examinent des moyens techniques pour protéger la vie privée

Nombreux sont ceux qui pensent que le courrier électronique présente le même niveau de protection de la vie privée que les autres types de communications, comme le téléphone et les services postaux. Malheureusement, comme nous l'avons évoqué plus haut, il a «le même niveau de sécurité qu'une carte postale[14]». Néanmoins, on peut incorporer dans les systèmes de courrier électronique des éléments de sécurité pour améliorer la protection de la vie privée des utilisateurs et des personnes qui font l'objet des messages électroniques.

La première ligne de défense contre l'accès non autorisé au courrier électronique est l'identification et l'authentification de l'utilisateur. Pour des besoins d'identification, l'utilisateur peut introduire au clavier un numéro d'identification spécial ou employer une carte à code à barre, un badge d'identification ou une carte à mémoire. L'authentification se fait habituellement au moyen d'un mot de passe. Tant que le mot de passe reste secret, il n'y a que les utilisateurs légitimes qui ont accès à leur courrier électronique. Il faut concevoir le mot de passe avec soin, ne jamais l'afficher, et le changer fréquemment. De plus, la sortie automatique après un nombre précis de tentatives d'introduction du mot de passe contribue à la prévention de l'accès non autorisé.

L'authentification peut également se faire par des moyens biométriques, comme les empreintes manuelles, les enregistrements vocaux ou les images rétiniennes. Cependant, la collecte, la conservation, l'utilisation et la divulgation de ce genre d'information biométrique risquent également d'avoir des répercussions sérieuses sur la protection de la vie privée. Si donc on a recours à des techniques de sécurité biométriques, il faut les appliquer d'une façon qui ne menace pas la vie privée.

Afin d'empêcher l'accès non autorisé, les numéros d'identification, les cartes d'accès, et autres moyens d'authentification doivent être annulés lorsqu'on n'en a plus besoin ou lorsqu'on ne s'en sert pas pendant une période prolongée.

Le codage est un autre moyen technique important de protéger la vie privée. De nombreux systèmes de courrier électronique font le codage automatique des fichiers et des messages selon un code brouillé spécial, au terminal de l'expéditeur, dont le décodage ne peut se faire qu'au moyen du mot de passe au terminal du destinataire. Ainsi, on est certain que le message n'est lu que par l'expéditeur et les destinataires voulus. Malheureusement, la plupart des systèmes publics n'offrent pas de codage, étant donné que de nombreux appareils informatiques n'ont pas la capacité de décoder des messages. Donc, même si un système de courrier électronique local permet le codage, il faut se rappeler que les messages transmis à un système public risquent d'être décodés et restent vulnérables à l'interception.

Parmi les autres moyens de protéger la vie privée, signalons la capacité de cacher le sujet du message et de déclencher l'avertissement qu'un message exigeant une sécurité spéciale a été reçu. La sortie automatique du système, lorsque l'ordinateur reste inactif pendant une période déterminée, est un autre moyen de sécurité permettant de prévenir l'accès non autorisé au courrier électronique.

Sur le plan technique, on peut faire la surveillance électronique des mouvements de courrier électronique grâce à un logiciel de sécurité spécialement conçu. Ce logiciel signale aux responsables du fonctionnement et de l'entretien du système les personnes qui utilisent le système et quand elles l'utilisent. On peut souvent détecter l'accès non autorisé ou inapproprié au courrier électronique par des changements dans le mouvement normal de l'emploi du système.

Certains experts prétendent que l'on peut mettre au point des systèmes de courrier électronique qui offrent une sécurité complète. Cependant, il y a un prix à payer. De façon générale, les systèmes sécuritaires sont plus coûteux, exigent une plus grande capacité de traitement informatique et sont moins commodes que les systèmes non sécuritaires.

Les besoins de sécurité de chaque organisme varient selon le genre de renseignements transmis et reçus par courrier électronique. Il appartient donc à l'organisme d'examiner ses besoins de sécurité et de choisir le système qui garantit le niveau de sécurité approprié. Citons les directives en matière de technologie de la sécurité informatique distribuées par le Conseil de gestion du

gouvernement : «l'importance et le coût des mesures de sécurité doivent correspondre aux risques et aux répercussions éventuels d'une défaillance de la technologie de la sécurité informatique[15]».

Principe 7 — Il faut que les organismes élaborent des mesures de sécurité appropriées pour protéger les messages envoyés par courrier électronique

Les moyens techniques et les directives de protection de la vie privée dans le domaine du courrier électronique ne produisent leurs effets que s'ils sont accompagnés de procédures appropriées pour garantir la sécurité des fichiers et des messages transmis et reçus par courrier électronique.

Par exemple, les mots de passe sont peu efficaces si l'organisme n'applique pas une politique contre la communication des mots de passe. L'organisme doit avertir les intéressés des conséquences à subir lorsqu'ils notent leur mot de passe par écrit ou l'entreposent dans un système informatique qui est accessible par des tiers. Si l'on prête son mot de passe, peut-être en période de crise, la politique doit stipuler qu'il soit changé aussitôt que possible.

En outre, le mot de passe ne sert à rien si l'ordinateur n'est pas verrouillé et reste accessible pendant que l'intéressé s'absente de son bureau. Cela pose un problème surtout si l'ordinateur est en marche et que le mot de passe a déjà été introduit au système. Dans ce cas-là, les fichiers et messages du courrier électronique sont accessibles à quiconque a accès au terminal. Il en est de même des messages électroniques copiés qui sont consignés dans des archives personnelles, comme un disque dur, même si l'ordinateur n'est pas en marche.

Pour protéger la vie privée, il faut que les procédures de sécurité poussent les utilisateurs à maintenir un niveau adéquat de contrôle sur leurs ordinateurs. Il ne faut pas que l'ordinateur soit laissé en marche ou non verrouillé, surtout si l'intéressé ne s'en sert pas pendant une période prolongée. En outre, il faut parfois exiger, selon la nature des messages électroniques au sein de l'organisme, que le message ne soit pas entreposé dans un appareil non protégé par l'emploi d'un mot de passe.

Si le mot de passe secret et le codage contribuent à protéger l'accès au courrier électronique et son emploi, ils font rien pour protéger le courrier électronique contre l'administrateur du système qui veut avoir accès à ces renseignements, ou au chef de service qui tient absolument à le surveiller de près ou qui a des privilèges d'accès semblables. L'administrateur du système a la capacité de changer le mot de passe. Donc, même s'il ne connaît pas le mot de passe, l'informaticien qui jouit des droits d'administrateur de système peut avoir accès aux messages électroniques en changeant le mot de passe.

À cause de la multiplication des systèmes de courrier électronique en réseau local, les occasions de commettre des infractions à la sécurité sont de plus en plus nombreuses[16]. C'est que, dans bien des systèmes, la base de données du message est distribuée parmi plusieurs réseaux locaux. Chaque réseau local a plusieurs administrateurs qui, chacun ont leurs propres pouvoirs de contrôle. Ces pouvoirs leur permettent de créer et de supprimer des utilisateurs, de changer les mots de passe et d'exécuter d'autres tâches. En répartissant cette responsabilité parmi plusieurs personnes au sein de l'organisme, le risque d'accès et d'utilisation non autorisés du courrier électronique monte. Cela pose un problème surtout lorsque le réseau local est lié à d'autres réseaux locaux à l'extérieur de l'organisme. Les séances d'information sur la protection de la vie privée contribuent à minimiser les problèmes, mais l'organisme aura avantage également à examiner la façon dont les changements à l'architecture à base du réseau local, avec un nombre réduit d'administrateurs de système, pourraient réduire les risques de sécurité.

Une autre question de sécurité tient aux copies «sauvegardées» constituées par certains systèmes de courrier électronique. Même après sa suppression, le message électronique est souvent entreposé en permanence sur des bandes magnétiques avec d'autres données tirées du système informatique. À titre d'exemple, l'existence inconnue d'un dossier sur bande dans les archives du système de courrier électronique PROFS de la Maison Blanche a précipité l'enquête sur le comportement d'Oliver North lors des audiences de l'Iran et des Contra. North pensait avoir supprimé tous les messages électroniques à caractère délicat, mais les enquêteurs ont accédé aux copies sauvegardées et les ont introduites comme preuves. Si, dans ce cas, l'atteinte à la vie privée était justifiée à des fins d'exécution de la loi, il n'en est pas toujours ainsi.

Si des fichiers de sauvegarde des messages électroniques sont constitués, il faut que les employés connaissent leur existence et qu'il y ait des politiques et des procédures pour garantir que la conservation et la destruction des fichiers électroniques de sauvegarde ne constituent aucune menace à la vie privée des utilisateurs. À souligner qu'il ne faut pas conserver indéfiniment les fichiers de sauvegarde.

Conclusion

À l'intérieur de l'organisme et entre organismes, le courrier électronique peut constituer un outil efficace pour éliminer les obstacles à la communication et favoriser le libre échange des renseignements et des idées. Mais, sans des directives et des procédures visant à protéger la vie privée, l'utilité du courrier électronique risque d'être réduite. Le souci de protéger le caractère confidentiel du courrier électronique améliore non seulement la communication, mais aussi l'ambiance au travail, du fait que les intéressés savent que leurs droits en milieu de travail sont considérés suffisamment importants pour justifier des mesures de protection. Enfin, l'adoption d'une politique déterminée permet de protéger la vie privée des particuliers dont les renseignements personnels sont transmis par courrier électronique.

Les principes de la protection de la vie privée reproduits à la page suivante se veulent un cadre pour la mise en application de directives précises en matière de courrier électronique. Pour élaborer ces directives, il faut prendre de nombreuses décisions difficiles. Les choix dépendront, dans une certaine mesure, des limites techniques des systèmes de courrier électronique, des objectifs pour lesquels on les utilise, de la nature des renseignements échangés par courrier électronique et des activités de l'organisme. Nous estimons cependant que ces directives doivent s'inspirer du souci d'offrir le plus grand degré de protection de la vie privée possible dans le contexte de l'organisme.

Principes

1. Il faut respecter et protéger la vie privée des utilisateurs du courrier électronique.

2. Il faut que chaque organisme élabore des directives précises pour la protection de la vie privée des utilisateurs du courrier électronique.

3. Il faut que chaque organisme communique ses directives en matière de courrier électronique aux utilisateurs et qu'il les informe de leurs droits et obligations en ce qui concerne le caractère confidentiel des messages transmis par le système.

4. Il faut que les utilisateurs reçoivent une formation appropriée au sujet du courrier électronique et des questions de sécurité et de protection de la vie privée qui entourent son utilisation.

5. Il ne faut employer les systèmes de courrier électronique pour recueillir, utiliser et divulguer des renseignements personnels que si des mesures suffisantes pour protéger la vie privée sont en place.

6. Il faut que les fournisseurs de systèmes de courrier électronique examinent des moyens techniques pour protéger la vie privée.

7. Il faut que les organismes élaborent des mesures appropriées pour protéger les messages envoyés par courrier électronique.

Notes

1. Ronald L. Rivest, communication personnelle d'un professeur en sciences informatiques au MIT et pionnier dans le domaine de la sécurité informatique, rapporté dans *Technology Review*, août/sept. 1992, page 11.

2. Ronald L. Rivest, communication personnelle d'un professeur en sciences informatiques au MIT et pionnier dans le domaine de la sécurité informatique, rapporté dans *Technology Review*, août/sept. 1992, page 11.

3. Michael Crawford, «The New Office Etiquette», *Canadian Business*, mai 1993, page 26.

4. Charles Pillar, «Bosses with X-ray Eyes», *Macworld*, juillet 1993, page 7.

5. L'étude a été menée par des chercheurs de l'University of Wisconsin et des Communications Workers of America. James Pillar, «Bosses with X-ray Eyes», *Macworld*, juillet 1993, page 6.

6. Nombre d'idées pour des sujets traités dans cette section ont été tirées d'un document préparé pour l'Electronic Mail Association par David Johnson et John Podesta, «Access to and Use and Disclosure of Electronic Mail on Company Computer Systems: A Tool Kit for Formulating Your Company's Policy», septembre 1991.

7. Office of Information Technology, Department of Finance, State of California, «Security and Risk Management Guidelines Update», *Calculated Risk: Risk Management, Public Access and Privacy*, avril-mai-juin, 1992, page 4.

8. Jeffrey Rothfeder, *Privacy for Sale: How Computerization has Made Everyone's Private Life an Open Secret*, New York: Simon and Schuster, 1992, page 170.

9. Voir *La vie privée en milieu de travail : Un document de consultation* publié en juin 1992 et *La protection de la vie privée : le besoin d'un filet de sécurité* publié en septembre 1993 par le Bureau du commissaire à l'information et à la protection de la vie privée de l'Ontario.

10. Par exemple, deux employés de Nissan Motor Corporation aux États-Unis ont été congédiés pour «des habitudes de travail non professionnelles, y compris l'abus et l'utilisation personnelle du système de courrier électronique». Les deux personnes appréhendées échangeaient des messages qui dépassaient les bornes de la bonne conduite professionnelle, de l'avis de leurs supérieurs. Jeffrey Rothfeder, *Privacy for Sale: How Computerization has Made Everyone's Private Life an Open Secret*, New York: Simon and Schuster, 1992, page 168.

11. Alice LaPlant, «Perspectives. Is Big Brother Watching?», *Infoworld*, 12:43, 22 octobre, 1990, page 65.

12. Office of Information Technology, Department of Finance, State of California, «Security and Risk Management Guidelines Update», *Calculated Risk: Risk Management, Public Access and Privacy*, avril-mai-juin, 1992, page 4.

13. Charles Pillar, «Bosses with X-ray Eyes», *Macworld*, juillet 1993, page 7.

14. Ronald L. Rivest, communication personnelle d'un professeur en sciences informatiques au MIT et pionnier dans le domaine de la sécurité informatiques rapporté dans *Technology Review*, août/sept. 1992, page 11.

15. Conseil de gestion du gouvernement, Sécurité en matière de technologie d'information, Directive 7-3, février 1991, page 1.

16. James Carroll, «The Increasing Risk of Using E-mail», *The Bottom Line: The News and Information Publication for Financial Professionals*, septembre 1992, page 21.