(TRADUCTION)

SURVEILLANCE DES ORDINATEURS ET DU COURRIER ÉLECTRONIQUE EN MILIEU DE TRAVAIL AU CANADA : DE L'ATTENTE RAISONNABLE EN MATIÈRE DE RESPECT DE LA VIE PRIVÉE À LA SURVEILLANCE RAISONNABLE

Professeur Michael Geist*
Université d'Ottawa, Faculté de droit
Directeur des questions juridiques afférentes
au commerce électronique, Goodmans LLP

Mars 2002

Document préparé pour le Conseil canadien de la magistrature

Table des matières

[TRADUCTION]

> « La technologie de surveillance n'est ni mauvaise ni bonne en soi, mais [...] il y a à la fois de la bonne et de la mauvaise surveillance. »
>
> - David Flaherty, commissaire à l'information et à la protection de la vie privée pour la province de Colombie-Britannique, enquête P98-012[1]

Il n'y a rien de nouveau à la question de la surveillance de la société. Par le passé, les images orwelliennes de caméras vidéo à chaque coin de rue et de dispositifs d'écoute clandestine sur tous les téléphones ont fait craindre à plusieurs un monde sans protection de la vie privée. Bien que les préoccupations en matière de surveillance audio et vidéo n'aient pas disparu, l'ubiquité de l'informatique et des communications par Internet a propulsé la surveillance des ordinateurs et du courrier électronique sur le devant de la scène publique. On y porte surtout attention dans le milieu du travail, là où des millions d'employés disposant d'un ordinateur et connaissant bien leurs applications de traitement de texte et de courrier électronique peuvent en savoir très peu sur les technologies de surveillance qui enregistrent silencieusement leurs activités sur le réseau ou, pire encore, chacune de leurs frappes.

Les entreprises de toutes tailles ont commencé à installer des technologies de surveillance informatique qui ciblent plus particulièrement l'utilisation des ressources de l'information par les employés. Jusqu'à 14 millions de travailleurs aux États-Unis sont soumis à une surveillance de l'utilisation qu'ils font d'Internet et du courrier électronique[2]. Un sondage mené en 2001 par l'American Management Association (AMA) a révélé que presque 80 pour cent des grandes compagnies américaines surveillaient l'utilisation du courrier électronique et d'Internet par leurs employés, soit une augmentation spectaculaire par rapport au chiffre de 35 pour cent obtenu en 1997[3]. Le fait suivant est particulièrement étonnant : [TRADUCTION] « [p]ar le passé, la croissance de la surveillance allait de pair avec l'accroissement de la proportion d'employés obtenant l'accès au courrier électronique et à Internet. Toutefois, cette année, la proportion moyenne d'employés disposant d'une connexion Internet au bureau est demeurée presque la même, tandis que la surveillance des activités Internet s'est accrue de

presque 10 pour cent[4]». Dans le même ordre d'idées, une étude de la Society for Human Resource Management a révélé que 74 pour cent des 722 entreprises recensées surveillaient l'utilisation d'Internet par les travailleurs et que 72 pour cent vérifiaient le courrier électronique des employés[5].

Par ailleurs, la surveillance informatique ne se limite pas qu'au milieu de travail ordinaire. En 2001, la Judicial Conference of the United States, l'organisme qui détermine la façon dont la magistrature américaine veille à sa propre administration, a suscité la controverse après avoir recommandé la surveillance généralisée de tous les ordinateurs utilisés par la magistrature et son personnel[6]. La recommandation a déclenché de nombreuses protestations de la part des principaux magistrats du pays; au printemps, les juges du 9e circuit ont voté à l'unanimité en faveur de la désactivation du logiciel de surveillance[7]. La question a été réglée plusieurs mois plus tard, par suite de l'adoption d'une proposition modifiée[8].

Des préoccupations similaires se sont manifestées en Nouvelle-Zélande au début de 2002, après la publication de rapports indiquant que plusieurs juges avaient accédé à des sites Web pornographiques à partir de leurs ordinateurs au bureau[9]. Les renseignements sont apparus à la suite d'une vérification régulière des dossiers d'accès Internet, une pratique prévue par la politique d'utilisation des ordinateurs du New Zealand Department of Courts[10]. Bien qu'aucun des sites visités ne fût illégal, les révélations ont fait les manchettes nationales, lesquelles étaient accompagnées de demandes réclamant la démission des juges visés[11]. Une enquête immédiate a révélé que tous les juges, sauf un, avaient accédé aux sites par accident ou à des fins professionnelles[12]. Le seul juge à ne pas l'avoir fait a par la suite été innocenté de toute activité illégale, bien que les demandes réclamant sa démission eussent subsisté après le scandale[13].

Alors que la surveillance informatique de la magistrature soulève des considérations particulièrement complexes, les questions de droit liées à la surveillance informatique dans le milieu du travail ordinaire sont souvent mal comprises. Nombreux sont ceux qui tiennent pour acquis que le droit de propriété des employeurs sur l'équipement informatique et le droit

d'établir des règles en milieu de travail confèrent aux employeurs le droit absolu de surveiller l'utilisation des ordinateurs par les employés, en autant qu'ils divulguent une telle pratique. Toutefois, un examen soigneux des lois, de la jurisprudence et des énoncés de politique des principaux organismes de protection de la vie privée révèle que la question est sujette à débat, surtout lorsque l'on compare les approches américaine et canadienne. Selon plusieurs décisions et commentaires, bien que l'émission d'un avis soit en effet une condition préalable nécessaire à l'adoption de la plupart des formes de surveillance informatique, elle est rarement suffisante pour justifier une telle pratique.

Le présent document se penche sur la question de la surveillance des ordinateurs et du courrier électronique du point de vue du droit canadien et met l'accent sur la surveillance au sein de la magistrature. La partie un offre un aperçu des pratiques actuelles de surveillance des ordinateurs et du courrier électronique. Elle traite des principaux motifs invoqués par les entreprises à l'appui de l'installation des technologies de surveillance et effectue un survol des principales technologies actuellement disponibles sur le marché.

La partie deux se penche sur le cadre juridique de la surveillance informatique au Canada. Après un bref examen des principaux arrêts américains, le document présente les nombreuses lois canadiennes qui mettent en valeur la protection de la vie privée. La jurisprudence des tribunaux judiciaires et administratifs canadiens est également étudiée, de même que la position de principe du Commissaire à la protection de la vie privée du Canada, lequel est responsable de l'application des deux principales lois canadiennes en matière de protection de la vie privée. Dans la partie deux du document, nous concluons que l'évaluation de la légalité de la surveillance informatique au Canada s'éloigne graduellement d'une analyse de l'attente raisonnable de la cible en matière de respect de la vie privée pour se fonder davantage sur une évaluation du caractère raisonnable de la surveillance informatique. Une telle évaluation fait son apparition alors que les tribunaux et décideurs cherchent à trouver un équilibre entre, d'une part, les préoccupations légitimes des employeurs en milieu de travail qui soutiennent les initiatives de surveillance et, d'autre part, le droit à la vie privée des employés.

Puisque la détermination du caractère raisonnable de la surveillance peut constituer un exercice très subjectif, la partie trois propose six facteurs à considérer lors de l'évaluation. Les six facteurs, dont l'importance peut varier selon les circonstances, comprennent notamment (i) la cible de la surveillance, (ii) l'objet de la surveillance, (iii) l'utilisation préalable de solutions de rechange à la surveillance informatique, (iv) le type de technologie utilisé aux fins de la surveillance, (v) la suffisance de l'avis donné à la cible de la surveillance et (vi) la protection des autres normes relatives à la vie privée, telles que celles se rapportant à l'administration, la sécurité et la conservation des renseignements personnels, une fois ces derniers obtenus par surveillance.

La partie quatre applique le critère du caractère raisonnable à la surveillance informatique éventuelle de la magistrature. La controverse qu'a suscitée la surveillance informatique de la magistrature aux États-Unis et en Nouvelle-Zélande a fait ressortir la possibilité que la surveillance compromette les protections conférées à la magistrature en vue de garantir son indépendance judiciaire. La jurisprudence canadienne appuie l'immunité judiciaire en tant que condition préalable nécessaire à la liberté; certaines formes de surveillance informatique au sein de la magistrature canadienne pourraient compromettre une telle immunité.

Partie un – Surveillance informatique en milieu de travail : pourquoi et comment?

a. Pourquoi les entreprises se servent-elles de la technologie de surveillance informatique?

Puisque presque 80 pour cent des grandes entreprises américaines surveillent désormais l'utilisation du courrier électronique et des ordinateurs par leurs employés[14], il importe de savoir pourquoi tant d'organisations sont disposées à se procurer des technologies de surveillance. Bien que le coût relativement peu élevé des technologies de surveillance (notamment calculé en tant que pourcentage des dépenses totales en technologie de l'information) explique sans

aucun doute l'installation de systèmes de surveillance en milieu de travail[15], les entreprises invoquent d'autres motifs, dont plusieurs sont de nature juridiq ue.

i. Productivité des employés

Tandis que les entreprises installent des ordinateurs personnels de plus en plus rapides sur les bureaux de millions d'employés, d'importantes préoccupations apparaissent au niveau de l'utilisation personnelle de ressources informatiques par les employés. En fait, au cours d'une étude récente, plus de 75 pour cent des entreprises ont précisé que la surveillance des employés les avait aidées à lutter contre l'utilisation d'Internet à des fins personnelles pendant les heures de bureau[16]. Un autre sondage a révélé que [TRADUCTION] « la majorité des employés passent entre 10 minutes et une heure à chaque jour ouvrable à visiter des sites ne se rapportant aucunement à leur emploi -- en utilisant l'ordinateur au travail pour lire des journaux virtuels, acheter des vêtements, ou regarder des femmes nues[17] ». Toujours selon le sondage, 25 pour cent des employés ont déclaré qu'ils passaient entre 10 et 30 minutes par jour à visiter des sites à des fins non professionnelles. Vingt-deux pour cent des employés ont précisé qu'ils y passaient entre 30 minutes et une heure, 12 pour cent ont déclaré qu'ils y passaient entre une et deux heures, tandis que 13 pour cent ont admis qu'ils passaient plus de deux heures par jour en ligne sur des sites ne se rapportant aucunement à leur emploi[18].

Les données canadiennes ont affiché des tendances similaires. Un sondage mené par le groupe Angus Reid en 2000 a révélé que les employés canadiens gaspillaient presque 800 millions d'heures de travail à chaque année à surfer sur Internet à des fins personnelles[19]. Le sondage a également révélé que les Canadiens disposant de l'accès Internet au travail passaient en moyenne huit heures par semaine en ligne, dont au moins deux à des fins personnelles[20].

ii. Rendement du réseau

La question du rendement du réseau, qui se rapporte à l'efficacité du réseau informatique, est étroitement liée à la productivité des employés. Les gestionnaires de technologies de l'information éprouvent des difficultés au niveau du ralentissement du trafic sur la largeur de bande causé par les employés qui téléchargent de grands fichiers audio et vidéo d'Internet[21]. Plutôt que de se procurer une plus grande largeur de bande pour améliorer la performance d'Internet, certaines entreprises ont décidé que la surveillance informatique et les technologies de filtrage pouvaient constituer une solution plus économique. Par exemple, une entreprise a adopté un programme de surveillance informatique après s'être rendu compte que l'accès à certaines pages Web prenait plus de temps et que son système ne pouvait plus envoyer ou recevoir des courriels contenant des pièces jointes volumineuses. D'après le gestionnaire des technologies de l'information de l'entreprise, [TRADUCTION] « lorsque nous avons annoncé que nous adoptions un système de surveillance d'Internet, les employés ont commencé à y penser deux fois avant de visiter des sites Web[22] ». Les clients de SurfControl, un fabricant de technologies de surveillance informatique, ont remarqué que les diverses utilisations de l'ordinateur personnel variaient selon les employés et comprenaient notamment le visionnement de séquences vidéo ou l'exploitation de sites Web à partir des serveurs de l'entreprise -- des pratiques qui s'accaparent une grande partie des ressources du réseau[23]. Selon le directeur des études de gestion de l'AMA, [TRADUCTION] « [i]l ne s'agit pas seulement de la curiosité de l'entreprise; il y a également de réelles préoccupations en matière de productivité et de responsabilité qui sous-tendent de telles politiques [...] Le courrier électronique personnel peut obstruer le système de télécommunications d'une entreprise[24] ».

iii. Responsabilité légale

On cite souvent à titre de préoccupation la responsabilité légale pouvant résulter de l'utilisation malveillance des ordinateurs par les employés, surtout lorsque ceux-ci se servent d'Internet pour accéder à du contenu inopportun ou envoient un tel contenu à d'autres employés par l'entremise du système de courrier électronique de l'entreprise. Par exemple, la maison de courtage Morgan Stanley a fait l'objet d'une poursuite de 70 millions de dollars relativement à des blagues racistes qui étaient apparues sur le système de courrier électronique de l'entreprise[25]. Les préoccupations en matière de responsabilité légale résultent également des poursuites pour harcèlement sexuel liées à l'exploration de sites Web pornographiques ou aux courriels à caractère sexuel. En fait, [TRADUCTION] « [m]algré les efforts généralisés de sensibilisation des travailleurs ayant avisé la plupart des employés des pièges juridiques de la pornographie en milieu de travail, quatre pour cent des employés recensés dans le sondage de Vault.com admettent qu'ils utilisent encore leur ordinateur au bureau pour accéder à des sites pornographiques. Par ailleurs, 25 pour cent des employés déclarent recevoir à l'occasion des « courriels inopportuns »[26] ».

Les grandes entreprises ont congédié certains employés pour utilisation inopportune d'Internet ou du courrier électronique, à savoir l'accès à du contenu inopportun ou les atteintes au droit d'auteur résultant de l'installation et de l'utilisation de logiciels non autorisés. De telles pratiques sont souvent détectées grâce aux technologies de surveillance informatique[27]. Par exemple, en se servant de la surveillance informatique, Dow Chemical a découvert que 50 employés utilisaient les ordinateurs de l'entreprise pour mettre en mémoire et envoyer des images sexuelles ou violentes. Les 50 employés ont tous été éventuellement congédiés[28].

Au Canada, plusieurs cas d'arbitrage se sont penchés sur le congédiement des employés fondé sur l'utilisation inopportune des ordinateurs. Dans l'affaire *Syndicat canadien des communications, de l'énergie et du papier, section locale 552 c. CAE Electronique Ltée (Grief du Petruzzi)*[29], un employé québécois a été congédié après qu'une vérification régulière de ses activités informatiques effectuée par son employeur ait révélé qu'il avait passé plus de 50 pour cent de ses heures de travail à surfer sur Internet, au cours d'une période de quatre mois. Il avait passé la plus grande partie de son temps en ligne sur des sites Web pornographiques. La décision de l'employeur de congédier l'employé a été confirmée par un groupe d'arbitrage du Québec.

Dans le même ordre d'idées, dans l'arrêt *Di Vito and Mathers v. Macdonald Dettwiler & Associates*[30], une décision rendue par la Cour suprême de la Colombie-Britannique en 1996, celle-ci a confirmé le congédiement de deux employés pour leur rôle dans la diffusion d'un courriel contenant des commentaires de nature à discréditer au sujet d'un employé faisant de l'embonpoint. La décision du tribunal s'est en partie fondée sur le fait que les actions entreprises par les employés avaient nui à leur collègue et au milieu de travail.

iv. <u>Préoccupations en matière de confidentialité et de secrets commerciaux</u>

Les technologies de surveillance informatique sont également souvent utilisées pour s'assurer de la confidentialité des renseignements commerciaux. D'après une étude menée par l'American Society for Industrial Security et PricewaterhouseCoopers, [TRADUCTION] « les sociétés Fortune 1000 ont subi des pertes de plus de 45 milliards de dollars en 1999, en raison du vol de renseignements exclusifs -- soit une augmentation par rapport aux estimations du FBI du milieu des années 1990, lesquelles chiffraient les pertes à quelque 24

milliards de dollars par année[31] ». Un porte-parole d'Intel a précisé que [TRADUCTION] « [s]elon notre politique, tout ce qui fait partie de l'actif d'Intel au sein de la compagnie appartient à celle-ci. L'actif comprend notamment le réseau [...] [l]es renseignements qui se déplacent à travers ce réseau ne sont pas considérés privés[32] ».

Des préoccupations concernant l'utilisation des réseaux de l'entreprise pour envoyer des secrets commerciaux ou des renseignements confidentiels de la société sont également apparues au Canada. Par exemple, dans l'arrêt *Nesbitt Burns Inc. v. Lange*,[33] une décision rendue en 2000 par la Cour supérieure de l'Ontario, Nesbitt Burns a demandé une injonction interlocutoire afin d'empêcher un ancien vice-président d'utiliser ses renseignements confidentiels. À l'appui de sa demande d'injonction, l'entreprise a présenté des éléments de preuve selon lesquels l'ancien vice-président avait abusé du système de courrier électronique de l'entreprise pour solliciter des clients, en leur envoyant des renseignements confidentiels et exclusifs par courrier électronique.

v. Délits informatiques

À la lumière des événements du 11 septembre et de la montée rapide du piratage informatique, on peut aussi avoir recours à la surveillance des réseaux pour aider à mettre au jour des crimes tels que le détournement et la fraude[34]. Tel qu'un auteur le souligne, [TRADUCTION] « après le 11 septembre, les employeurs veulent plus que jamais s'assurer que leurs employés ne se livrent à aucune activité criminelle en milieu de travail[35] ». Dans la jurisprudence canadienne, on s'est servi de l'utilisation du courriel comme preuve démontrant les activités frauduleuses d'un employé. Dans l'arrêt *Lovelock v. DuPont Canada Inc.*, un cas de congédiement injustifié sur lequel a statué la Cour de justice de l'Ontario (Division générale) en 1998[36], M.

Lovelock a contesté son congédiement par DuPont Canada. L'entreprise a passé ses dossiers de courrier électronique au peigne fin et a découvert un courriel envoyé par l'employé. Le courriel a en bout de ligne convaincu le juge de l'invraisemblance du récit, donné par l'employé, des événements ayant mené à son congédiement.

vi. Obligation juridique

Dans certaines circonstances, le droit positif impose aux employeurs l'obligation de surveiller l'utilisation des ordinateurs. Par exemple, la *Health Insurance Portability and Accountability Act* (HIPPA)[37] des États-Unis exige des compagnies médicales qu'elles surveillent les données informatiques afin de protéger les renseignements personnels des patients. Des étiquettes sont jointes aux renseignements des patients et identifient tous ceux qui consultent de tels renseignements. Tel qu'un auteur le fait valoir, [TRADUCTION] « [i]l va sans dire que de tels individus sont des employés surveillés. Par conséquent, le respect de la vie privée (d'un groupe donné, tel que les patients ou consommateurs) s'obtient aux dépens du respect de la vie privée (d'un autre groupe, à savoir les employés)[38] ».

b. Comment fonctionnent les technologies de surveillance informatique?

Étant donné les préoccupations généralisées des employeurs concernant l'utilisation des ordinateurs par les employés, il n'est pas étonnant de constater l'apparition rapide sur le marché de douzaines de produits différents offrant aux employeurs la possibilité de surveiller avec aisance les activités informatiques de leurs employés[39]. Les divers produits de surveillance partagent plusieurs caractéristiques similaires. Premièrement, chacun d'entre eux peut générer des rapports personnalisés sur l'utilisation de l'ordinateur par les membres du personnel. Par exemple, la plupart des produits surveilleront les activités sur

Internet, notamment la fréquence des visites effectuées sur le Web par les employés, de même que l'identité des sites qu'ils visitent. La plupart des produits peuvent également fournir des rapports détaillés au sujet du courrier électronique, y compris la fréquence du courrier départ et arrivée[40], de même que les ébauches rédigées par les employés mais effacées par ces derniers. Deuxièmement, plusieurs programmes permettent également à l'employeur de mieux contrôler les ordinateurs de ses employés, en les empêchant d'utiliser leurs programmes informatiques de certaines façons, par exemple en éliminant les sites Web offensants ou en empêchant l'envoi ou la réception de certains courriels.

Étant donné la grande variété de produits, les entreprises peuvent habituellement trouver un programme de surveillance qui réponde à leurs besoins particuliers. Voici ce qu'un auteur a souligné :

> [TRADUCTION]
>
> Par exemple, l'employeur qui s'intéresse principalement à la surveillance de la productivité des employés peut préférer un dispositif de surveillance très différent de celui favorisé par l'employeur dont la principale préoccupation est d'empêcher (ou, à tout le moins, de détecter) le harcèlement sexuel en milieu de travail. La détection des fuites de secrets commerciaux peut nécessiter une technologie qui se distingue de celle servant à empêcher l'accès à des sites Web se spécialisant dans la pornographie ou les jeux de hasard[41].

Les programmes de surveillance informatique peuvent être classés en deux groupes généraux : les programmes axés sur les serveurs, installés sur le réseau de l'employeur, et les programmes axés sur les clients, installés directement sur les ordinateurs des employés.

i. Programmes axés sur les serveurs

Les programmes de surveillance informatique axés sur les serveurs sont installés directement sur le réseau informatique de l'employeur. Il n'est pas étonnant que les programmes

mettent surtout l'accent sur l'utilisation du réseau, laquelle comprend l'utilisation du courrier électronique et d'Internet. La plupart des programmes axés sur les serveurs limitent l'accès au contenu sur le Web en fonction des adresses Internet (URL)[42]. D'autres programmes empêchent les employés de télécharger certains fichiers, tels que les fichiers de films, les fichiers graphiques, les fichiers pornographiques ou les fichiers musicaux MP3[43].

Certains programmes axées sur les serveurs possèdent également un logiciel renifleur de paquets qui peut capter, étudier et archiver toutes les communications sur un réseau donné, telles que le courrier électronique, les séances de bavardage, le partage de fichiers et l'exploration d'Internet[44]. Puisque de tels programmes sont placés sur le serveur de l'entreprise, les employés qui utilisent leurs propres comptes de courrier électronique sur le Web, tels que Hotmail ou Yahoo!, ne bénéficient pas d'une meilleure sécurité que s'ils utilisaient le programme de courrier électronique de leur employeur. Par ailleurs, les messageries instantanées, qui utilisent des programmes comme ICQ, MSN Messenger ou l'Instant Messenger (AIM) d'America Online, risquent également de faire l'objet d'une surveillance de la part de l'employeur[45].

Les technologies de surveillance informatique axées sur les serveurs sont particulièrement utiles si l'employeur désire surveiller de façon simultanée les activités d'un important groupe d'utilisateurs[46]. Elles sont conçues afin de conserver les journaux et créer des rapports détaillés pouvant identifier les employés individuels, en cas de non-respect de la politique d'utilisation des ordinateurs de l'entreprise[47].

Certains programmes confèrent même des pouvoirs de surveillance aux employés. Par exemple, FastTracker permet aux employés de surveiller les activités Internet de leurs collègues, dans l'espoir qu'une telle forme de contrôle par les pairs dissuadera les utilisateurs d'accéder à des sites Web interdits. FastTracker se distingue également des technologies traditionnelles axées sur les serveurs, en ce sens qu'elle ne comprend aucun logiciel. L'entreprise achemine

plutôt tout son trafic Internet au site de FastTracker, qui tient un journal du trafic des employés et bloque l'accès aux sites indésirables[48].

ii. Programmes axés sur les clients

Bien que les programmes axés sur les serveurs soient efficaces à des fins de détection ou pour empêcher les employés d'accéder à certains sites Web, ils ne peuvent surveiller les activités qui ne se passent pas sur le réseau. Pour surveiller les programmes utilisés par les employés sur leur ordinateur personnel sans l'aide d'une connexion réseau, l'employeur doit installer directement sur les ordinateurs des employés des programmes de surveillance axés sur les clients et pouvant être utilisés pour « signaler » les activités à l'employeur[49].

Les technologies de surveillance informatique axées sur les clients génèrent des journaux qui enregistrent toutes les activités des employés dans un fichier ou une base de données en vue d'un examen futur. En surveillant les activités de l'employé sur le réseau ou hors réseau, l'employeur peut accumuler un plus grand nombre de données, lesquelles englobent un éventail d'utilisations informatiques beaucoup plus vaste[50].

Le programme WinWhatWhere Investigator illustre bien la façon dont fonctionne un programme axé sur les clients. Le programme est installé directement sur l'ordinateur d'un employé. Lorsque l'employé utilise l'ordinateur pendant la journée, le programme crée des journaux qui enregistrent certains renseignements. Dans la plupart des cas, le programme enregistre le nom des applications logicielles utilisées, le titre des fenêtres ouvertes sur l'écran, ainsi que les frappes au clavier de l'employé, y compris celles qui sont éventuellement effacées[51].

Certains programmes fournissent des images graphiques de ce qui apparaît à l'écran à n'importe quel moment. Les instantanés d'écran peuvent ensuite être envoyés à l'employeur par courrier électronique à des fins d'enquête. Par exemple, le programme Webroot WinGuardian

permet à l'employeur d'examiner les activités de l'employé à tout moment pendant son quart de travail[52]. D'autres produits permettent à l'employeur de savoir pendant combien de temps l'employé ne travaille pas à son ordinateur ou pendant combien de temps l'ordinateur est inactif[53]. Les employeurs peuvent également surveiller leurs employés grâce à des logiciels qui enregistrent les frappes. Les employeurs peuvent connaître le nombre de frappes à l'heure de chaque employé et les comparer ensuite aux moyennes de l'entreprise ou aux niveaux de performance désirés[54].

Il est important de souligner que l'employé ne sait pas toujours qu'il est surveillé, même si le logiciel axé sur les clients est installé directement sur son ordinateur. Par exemple, le programme pcAnywhere de Symantec permet aux employeurs de brancher les ordinateurs personnels à leurs réseaux, à l'insu de leurs employés. Une fois les ordinateurs branchés, les employeurs peuvent surveiller les activités de leurs employés en temps réel. De plus, tout en surveillant secrètement l'utilisation de l'ordinateur par l'employé, l'employeur peut générer et conserver des instantanés d'écran pour analyse ultérieure[55]. En fait, le programme WinWhatWhere possède un « mode invisible » qui dissimule le programme en arrière-plan. Aucune icône sur la barre d'outils ni aucun écran fugitif n'indiquent que le programme est en fonction. En outre, le programme n'est pas affiché dans la liste Fermeture de programmes de Windows ni dans la fenêtre Ajout/Suppression de programmes, de sorte qu'il est encore plus difficile de savoir s'il est en fonction ou non[56].

Partie deux - Cadre juridique de la surveillance informatique en milieu de travail

a. Perceptions générales (erronées) du droit de la surveillance en milieu de travail

Malgré la carence relative de jurisprudence canadienne sur le sujet, la plupart des discussions portant sur la surveillance des ordinateurs et du courrier électronique en milieu de travail se fondent sur l'hypothèse selon laquelle les employés n'ont pas ou presque pas d'attente en matière de respect de la vie

privée en milieu de travail. Voici ce que soulignent MacIsaac *et al.* dans *The Law of Privacy in Canada* :

[TRADUCTION]

> Plusieurs employeurs considèrent que le courrier électronique envoyé et reçu en utilisant l'équipement informatique de l'entreprise et gardé en mémoire sur les réseaux informatiques de l'entreprise appartient à l'employeur. Du point de vue de l'employeur, il s'agit là d'une ressource professionnelle acquise par l'employeur et qui ne doit être utilisée qu'à des fins professionnelles. Par conséquent, les courriels et conversations téléphoniques générés au nom de l'employé dans le cours des activités d'une entreprise devraient être disponibles à des fins d'examen pour des motifs professionnels et de sécurité légitimes. Ainsi, un employé agissant au nom de son employeur ne devrait avoir aucune attente raisonnable en matière de respect de la vie privée[57].

Une telle perspective du respect de la vie privée en milieu de travail n'est pas unique en son genre. Lors de son examen d'un cas d'arbitrage de la Colombie-Britannique en droit du travail, dans lequel un grief avait été porté par un technicien de laboratoire après son congédiement pour avoir affiché sur un babillard électronique à l'échelle du campus des allégations injustifiées contre d'autres employés, le cabinet d'avocats Emond Harnden a résumé les conclusions du tribunal de la façon suivante : [TRADUCTION] « courrier électronique au bureau : aucune attente raisonnable en matière de respect de la vie privée[58] ». Bien que certains auteurs, notamment Charles Morgan, aient commencé à faire valoir que les employés pourraient disposer de quelques protections de la vie privée en milieu de travail, un tel point de vue s'est heurté à une certaine opposition[59].

i. Droit de la surveillance en milieu de travail aux États-Unis

La perspective canadienne en matière de surveillance informatique en milieu de travail est beaucoup influencée par la jurisprudence américaine, dans laquelle les tribunaux et législateurs ont abordé la question de façon beaucoup plus active[60]. Dans *Smyth v. Pillsbury Co.*, une décision très souvent citée qui a été rendue en 1996 par la Cour de District de Pennsylvanie, un employé de la société Pillsbury a été congédié pour avoir échangé des courriels avec son superviseur sur le système de courrier électronique de la société[61]. Les

courriels ont été jugés non professionnels et l'employé a été congédié. Le tribunal a confirmé le congédiement, en faisant remarquer que, puisque la communication était volontaire et qu'il n'existait aucune attente raisonnable en matière de respect de la vie privée sur le système de courrier électronique d'une entreprise, [TRADUCTION] « l'intérêt qu'a la société à empêcher, sur son système de courrier électronique, la tenue de commentaires inopportuns et non professionnels ou même, d'activités illégales, l'emporte sur tout intérêt en matière de respect de la vie privée que peut avoir l'employé dans ces commentaires[62] ». Il est intéressant de remarquer que le tribunal en est arrivé à une telle décision malgré la preuve selon laquelle la société avait promis aux employés que les communications par courrier électronique ne seraient pas interceptées par la direction[63].

Dans le même ordre d'idées, dans *Bourke* v. *Nissan Motor Corp.*, une décision non publiée rendue en 1993 par la Cour d'appel de Californie, celle-ci a traité de la question de l'attente raisonnable en matière du respect de la vie privée dans le domaine des communications par courrier électronique en milieu de travail, en concluant qu'il n'existait aucune attente de la sorte[64]. En l'espèce, M. Bourke a été congédié après qu'un courriel au contenu inopportun ait été identifié au hasard lors d'une séance de formation en informatique. Le tribunal a confirmé le congédiement, en faisant remarquer que, d'une part, l'employé avait signé une entente concernant l'utilisation des ordinateurs qui limitait à des fins professionnelles l'utilisation de l'équipement et du logiciel informatiques appartenant à la société et, d'autre part, qu'il savait que les courriels pouvaient être lus de temps à autre par des tiers autres que le destinataire visé.

Dans *United States v. Simons*, une décision rendue en 1998 par la Cour fédérale de Virginie et dans laquelle la surveillance par l'employeur a été contestée, le tribunal a également conclu à l'absence d'une attente raisonnable en matière de respect de la vie privée. En l'espèce, un gestionnaire de systèmes avait retracé l'accès à des sites pornographiques jusqu'à l'ordinateur du défendeur[65]. Le tribunal a conclu que la fouille du lecteur de disque dur de l'ordinateur du défendeur, où plus de mille fichiers pornographiques avaient été retrouvés, n'enfreignait pas ses droits constitutionnels garantis par le Quatrième amendement. Le tribunal a

conclu qu'il n'existait aucune attente raisonnable en matière de respect de la vie privée, puisque l'entreprise avait une politique d'accès à Internet, ainsi qu'un intérêt commercial légitime à empêcher l'utilisation non autorisée d'Internet par les employés.

Parmi les lois américaines, l'*Electronic Communications Privacy Act* (ECPA) est particulièrement pertinente[66]. Selon l'article 2511, commet un acte illégal quiconque [TRADUCTION] « intercepte, tente d'intercepter, ou permet de façon intentionnelle à toute autre personne d'intercepter ou de tenter d'intercepter toute [...] communication électronique[67] ». L'ECPA définit la « communication électronique » comme [TRADUCTION] « tout transfert de signes, de signaux, d'écritures, d'images, de sons, de données ou de renseignements de quelque nature que ce soit, transmis en tout ou en partie par fil, liaison radio, ou système magnétoélectrique, photoélectronique ou photo-optique[68] » mais prévoit qu'elle « ne comprend pas [...] les communications par fil ou orales[69] ». Ainsi, l'ECPA ne traite pas des courriels gardés en mémoire sur un ordinateur personnel, puisqu'elle ne s'applique qu'au transfert de données.

Bien que l'EPCA semble interdire l'interception de courriels ou d'autres communications transmises par réseau, deux exceptions prévues par la loi s'appliquent au milieu du travail. Premièrement, l'article 2511(2)(d) prévoit une exception relative au consentement, selon laquelle l'interception d'une communication électronique n'est pas illégale lorsque la partie qui intercepte la communication a obtenu le consentement de l'une des parties à la communication[70]. Deuxièmement, l'article 2511(2)(a)(i) prévoit une exception relative à l'usage professionnel, qui s'applique lorsqu'un membre, employé ou agent d'un fournisseur de services de communication électronique, par fil ou par fil électrique, intercepte, divulgue ou utilise la communication dans le cadre de son emploi et dans le cours normal d'une activité reliée à la prestation de ses services ou à la protection des droits ou de la propriété du fournisseur de services[71].

Les tribunaux américains ont interprété les exceptions d'une manière qui favorise tant les partisans que les détracteurs de la surveillance par l'entreprise. L'arrêt de principe sur la portée du consentement est *Watkins* v. *L.M. Berry & Co*, une décision traitant de l'écoute électronique et rendue en 1983 par la Cour d'appel du 11e circuit[72]. En l'espèce, Mme Watkins a reçu un appel téléphonique personnel pendant les heures de bureau. L'appel a fait l'objet d'une écoute téléphonique de la part de son superviseur, bien que Mme Watkins ne fût pas au courant d'une telle écoute. L.M. Berry, son employeur, avait fait parvenir à tous les employés sa politique de surveillance en matière d'appels personnels. La politique autorisait de tels appels; par ailleurs, on avait assuré aux employés que les appels personnels ne feraient pas l'objet d'une écoute, sauf dans la mesure nécessaire pour déterminer la nature de l'appel.

Le tribunal a conclu que Mme Watkins n'avait pas consenti à une politique de surveillance générale et que, lorsque l'interception du superviseur est allée au-delà de ce qui était nécessaire pour déterminer la nature de l'appel, elle a dépassé la portée du consentement donné par Mme Watkins. Le tribunal a rejeté l'argument selon lequel la simple connaissance d'une capacité de surveillance constituait un consentement tacite, en soulignant qu'[TRADUCTION] « il ne faut pas conclure d'une façon cavalière à l'existence d'un consentement tacite[73] ». Les partisans de la surveillance se sont servis de la décision pour affirmer qu'un consentement clairement obtenu assurerait la légalité de la surveillance des employés, tandis que les détracteurs de la surveillance ont souligné la réticence du tribunal à donner effet à un consentement rédigé en termes généraux.

L'exception relative à l'usage professionnel a également été interprétée de manière à favoriser les deux camps. Bien que celle-ci semble viser principalement les exploitants de systèmes de télécommunication, les tribunaux américains ont conclu que l'exception s'appliquait à tout employeur offrant un service de courrier électronique[74]. Par ailleurs, les tribunaux ont accordé une marge de manoeuvre aux employeurs en concluant que la surveillance des employés satisfaisait à la partie de l'exception relative à l'intérêt commercial[75]. Toutefois, tel que mentionné ci-haut, dans l'affaire *Watkins*, le tribunal a conclu que la surveillance du contenu de

la communication dépassait la portée de l'exception, laquelle ne s'appliquait qu'à la détection de la nature (personnelle ou commerciale) et de la fréquence de la communication. Dans une affaire ne portant pas sur la surveillance en milieu de travail, un tribunal américain s'est récemment penché sur l'admissibilité de la preuve obtenue au moyen d'un programme de surveillance « enregistreur de frappes» similaire à celui décrit dans la section ci-haut traitant des programmes de surveillance axés sur les clients. Tel que l'a souligné le juge dans l'affaire *United States v. Scarfo*, celle-ci soulevait [TRADUCTION] « une question intéressante de première impression se rapportant aux tensions sans cesse présentes entre, d'une part, les droits des individus à la vie privée et la liberté et, d'autre part, l'utilisation de nouvelles technologies avancées par les autorités chargées de l'application de la loi pour faire activement enquête sur les activités criminelles[76] ». La question en litige portait sur le droit des autorités américaines chargées de l'application de la loi d'utiliser des éléments de preuve obtenus grâce à un programme qui avait enregistré les frappes du suspect sur le clavier de son ordinateur personnel. Les autorités chargées de l'application de la loi se sont servies du programme pour obtenir les mots de passe de M. Scarfo donnant accès à des fichiers codés autrement inaccessibles.

M. Scarfo a contesté l'utilisation de la preuve en se fondant sur l'ECPA. Le tribunal a rejeté la contestation, en concluant que le programme enregistreur de frappes était conçu pour n'enregistrer des renseignements que lorsque l'ordinateur n'était pas branché à un réseau. Le juge a évalué la technologie sous-jacente et conclu ce qui suit :

> [TRADUCTION]
>
> Tout en sachant que l'ordinateur de M. Sarfo était doté d'un modem et donc capable de transmettre des communications électroniques par l'entremise du modem, le F.B.I. a configuré le [système enregistreur de frappes] KLS pour éviter d'intercepter les communications électroniques tapées sur le clavier et transmises de façon simultanée en temps réel par le biais des ports de communication. Pour ce faire, le F.B.I. a conçu la composante « afin que chaque frappe soit évaluée individuellement ». Tel que l'a expliqué M. Murch, le statut par défaut de la composante de frappe avait pour effet de ne pas enregistrer automatiquement toutes les frappes. Lors d'une frappe au clavier par un utilisateur, le KLS vérifiait le statut de chaque port de communication installé sur l'ordinateur et, si tous les ports de communication étaient inactifs, ce qui voulait dire que le modem n'utilisait aucun

> port à ce moment-là, la frappe visée était enregistrée. Ainsi, lorsque le modem fonctionnait, le KLS n'enregistrait pas les frappes. Il était conçu pour empêcher l'enregistrement de frappes lorsque le modem fonctionnait. Puisqu'à l'exception du modem, l'ordinateur de M. Scarfo n'était doté d'aucun autre moyen de communication avec un autre ordinateur, le KLS n'a intercepté aucune communication par fil[77].

ii. Droit de la surveillance en milieu de travail au Canada

Bien que le Canada ne dispose pas d'une loi en tous points semblable à l'ECPA, le *Code criminel* traite de l'interception des communications d'une manière similaire. Selon le paragraphe 184(1), « [e]st coupable d'un acte criminel et passible d'un emprisonnement maximal de cinq ans quiconque, au moyen d'un dispositif électromagnétique, acoustique, mécanique ou autre, intercepte volontairement une communication privée[78] ». L'article 183 du *Code criminel* définit tant « intercepter » que « communication privée ». « Intercepter » s'entend notamment « du fait d'écouter, d'enregistrer ou de prendre volontairement connaissance d'une communication ou de sa substance, son sens ou son objet[79] », tandis qu'une « communication privée » s'entend d'une « [c]ommunication orale ou télécommunication [...] qui est faite dans des circonstances telles que son auteur peut raisonnablement s'attendre à ce qu'elle ne soit pas interceptée par un tiers[80] ».

La définition de « communication privée » est particulièrement pertinente puisqu'elle exige une attente raisonnable en matière de respect de la vie privée. Aucun tribunal canadien n'a abordé de façon concluante la question de l'attente raisonnable en matière de respect de la vie privée, bien que plusieurs cas d'arbitrage en droit du travail se soient penchés sur la question[81]. Celle-ci est apparue en dehors du contexte du milieu du travail, comme dans *R. v. Weir*, une décision rendue en 1998 par la Cour du banc de la Reine de l'Alberta et traitant de l'attente raisonnable en matière de respect de la vie privée dans le domaine du courrier électronique, en ce qui concerne les fournisseurs d'accès Internet[82]. En l'espèce, le tribunal a conclu que les internautes avait une telle attente, bien que celle-ci fût inférieure à celle qui s'appliquait au

courrier de première classe. La Cour d'appel de l'Alberta a confirmé la décision en 2001, sans toutefois aborder dans ses motifs la question du respect de la vie privée[83].

Tout comme l'ECPA, le *Code criminel* prévoit lui aussi des exceptions relatives au consentement et à l'usage professionnel. L'alinéa 184(2)*a)* prévoit que l'interdiction relative à l'interception des communications ne s'applique pas à « une personne qui a obtenu, de l'auteur de la communication privée ou de la personne à laquelle son auteur la destine, son consentement exprès ou tacite à l'interception[84] ». Étant donné les similitudes qui existent entre le *Code criminel* et l'ECPA, la jurisprudence américaine en la matière, telle que l'affaire *Watkins*, pourrait aider les tribunaux canadiens à interpréter la disposition ci-haut[85].

Au Canada, l'exception relative à l'usage professionnel a une portée plus restreinte que celle prévue par l'ECPA et ne semble s'appliquer qu'aux fournisseurs de services de communication. L'alinéa 184(2)*c)* prévoit que l'interdiction relative à l'interception des communications ne s'applique pas à

> une personne qui fournit au public un service de communications téléphoniques, télégraphiques ou autres et qui intercepte une communication privée dans l'un ou l'autre des cas suivants :
>
> (i) cette interception est nécessaire pour la fourniture de ce service,
> (ii) à l'occasion de la surveillance du service ou d'un contrôle au hasard nécessaire pour les vérifications mécaniques ou la vérification de la qualité du service,
> (iii) cette interception est nécessaire pour protéger ses droits ou biens directement liés à la fourniture d'un service de communications téléphoniques, télégraphiques ou autres[86].

La disposition anti-piratage du *Code criminel* pourrait aussi s'appliquer au présent contexte. En vertu de l'al. 342.1(1)*b)*, quiconque, frauduleusement et sans apparence de droit, intercepte une fonction d'ordinateur au moyen d'un dispositif quelconque, est coupable d'un acte criminel ou d'une infraction. Bien que la disposition soit susceptible de s'appliquer à la surveillance informatique en milieu de travail, les employeurs qui agissent de bonne foi tout en

croyant qu'ils ont le droit de surveiller leurs employés (et n'agissent donc pas sans apparence de droit) ne seraient pas visés par la loi[87].

b. La transition vers une attente raisonnable en matière de respect de la vie privée en milieu de travail

Bien que la jurisprudence américaine puisse être responsable de la perception générale selon laquelle les employés n'ont pas d'attente raisonnable en matière de respect de la vie privée en milieu de travail, un examen plus soigneux de la nouvelle jurisprudence et des nouvelles lois et politiques, notamment au Canada, donne à penser qu'une perspective plus équilibrée est rapidement en voie d'apparaître. Aux États-Unis, l'affaire *Watkins* démontre que les tribunaux ne sont pas disposés à donner *carte blanche* aux employeurs pour que ceux-ci surveillent les employés en milieu de travail.

Par ailleurs, la jurisprudence récente donne à penser que les intérêts en matière de respect de la vie privée sont encore plus importants. Dans *Konop v. Hawaiian Airlines*, une décision rendue en 2001 par la Cour d'appel du 9e circuit, le tribunal s'est penché sur la question de l'utilisation, par un employeur, d'un mot de passe obtenu d'un employé pour accéder à un site Web interdit[88]. En traitant la transmission vers un site Web comme une communication avec un tiers, le tribunal a conclu que l'accès par l'employeur constituait une interception illégale. Bien que la décision ait été retirée pour des motifs encore inconnus, elle démontre que les tribunaux pourraient être de plus en plus disposés à interpréter l'ECPA de façon plus générale, dans l'intérêt de la protection de la vie privée[89].

La National Labor Relations Board met encore davantage l'accent sur la nécessité d'obtenir un équilibre entre le droit de l'employeur d'effectuer une surveillance en milieu de travail et la vie privée des employés. Le rapport annuel 2000 de l'avocat général de la NLRB contient plusieurs décisions traitant du

> respect de la vie privée en milieu de travail[90]. Les décisions appuient à l'unanimité le droit à la vie privée en milieu de travail, la NLRB concluant à plusieurs reprises que [TRADUCTION] « l'imposition, par l'employeur, d'une interdiction complète visant tout courrier électronique ne se rapportant pas à l'emploi [...] était trop générale et à première vue illégale[91] ».

Quant à elles, les législatures de plusieurs États ont commencé à étudier l'adoption de protections législatives en matière de vie privée à l'intention des employés en milieu de travail. Par exemple, en 2001 la législature de la Californie a adopté la loi SB 147, laquelle aurait empêché les employeurs de lire les communications de leurs employés sur le système de courrier électronique fourni par l'entreprise. La loi n'aurait pas défendu à une entreprise de surveiller ses employés; elle aurait plutôt exigé que l'employeur fournisse un avis suffisant aux employés avant que ces derniers n'entrent dans le système informatique[92]. En bout de ligne, le gouverneur de la Californie, Gray Davis, a opposé son veto à la loi, en soutenant que [TRADUCTION] « les employés au sein de l'économie électronique d'aujourd'hui comprennent que les ordinateurs fournis à des fins professionnelles appartiennent à l'entreprise et que leur utilisation peut être surveillée et contrôlée[93] ».

Le Canada a connu plus de succès sur le plan législatif, si bien que plusieurs employés canadiens reconnaissent qu'une surveillance en milieu de travail est possible, tout en sachant que les protections législatives imposent des limites à la surveillance et leur confèrent un certain droit à la vie privée en milieu de travail.

Au Canada, la source la plus importante de droits à la vie privée dans le secteur privé est la nouvelle *Loi sur la protection des renseignements personnels et les documents électroniques* (LPRPDE)[94], laquelle crée à l'échelle nationale des protections qui s'appliquent au secteur privé. Bien que la loi n'entre pleinement en vigueur que le 1er janvier 2004, ses principes fondamentaux ont déjà un effet sur des milliers d'organisations canadiennes.

Dans le domaine de la surveillance en milieu de travail, la LPRPDE reproduit l'équilibre entre les droits de l'employeur et ceux de l'employé en traitant de la double préoccupation concernant la protection de la vie privée ainsi que la collecte et l'utilisation raisonnables de renseignements personnels. La disposition de déclaration d'objet de la loi mentionne expressément un tel équilibre, de la façon suivante :

> La présente partie [Protection des renseignements personnels dans le secteur privé] a pour objet de fixer, dans une ère où la technologie facilite de plus en plus la circulation et l'échange de renseignements, des règles régissant la collecte, l'utilisation et la communication de renseignements personnels d'une manière qui tient compte du droit des individus à la vie privée à l'égard des renseignements personnels qui les concernent et du besoin des organisations de recueillir, d'utiliser ou de communiquer des renseignements personnels à des fins qu'une personne raisonnable estimerait acceptables dans les circonstances[95].

Bien qu'un examen exhaustif de la LPRPDE dépasse la portée du présent document, plusieurs dispositions de la loi méritent une attention toute particulière. D'abord et avant tout, la loi comprend une disposition prévoyant que « l'organisation ne peut recueillir, utiliser ou communiquer des renseignements personnels qu'à des fins qu'une personne raisonnable estimerait acceptables dans les circonstances[96] ». Une telle disposition impose des limites importantes à la surveillance en milieu de travail, puisque le simple consentement de l'employé à la surveillance n'est plus suffisant pour justifier des activités de surveillance illimitées. La disposition impose d'importantes restrictions à la surveillance, en limitant de telles activités à des fins qu'une personne raisonnable considérerait appropriées. Par exemple, la surveillance informatique généralisée en milieu de travail, sous prétexte de prévenir toute forme de harcèlement, pourrait bien s'avérer illégale en l'absence de preuve démontrant clairement que les mesures de surveillance répondent à un véritable problème.

Deuxièmement, la LPRPDE exige la désignation d'une personne qui doit s'assurer que l'organisation respecte les principes relatifs à la protection des renseignements personnels[97]. La création d'un poste d'agent du service de la protection de la vie privée dans toutes les organisations a d'importantes conséquences sur la surveillance en milieu de travail. Elle donne à penser que la collecte de renseignements personnels en milieu de travail ne doit pas demeurer du ressort exclusif du personnel en technologie de l'information d'une organisation donnée, mais

qu'elle doit également être examinée par son service de la protection de la vie privée. En outre, l'accès non autorisé aux renseignements personnels pourrait être restreint de la même façon pour éviter d'enfreindre les obligations en matière de respect de la vie privée prévues par la loi.

Troisièmement, la loi prévoit plusieurs dispositions dont il faut tenir compte au moment d'aviser les employés des pratiques de surveillance en milieu de travail. La loi exige que l'organisation détermine les fins de la collecte de renseignements[98], obtienne le consentement de la personne concernée avant de recueillir les renseignements[99] et ne recueille que les renseignements personnels nécessaires aux fins déterminées[100]. Dans leur ensemble, de telles dispositions limitent la portée de la collecte par les employeurs et obligent clairement ces derniers à donner à leurs employés un avis adéquat concernant les pratiques de surveillance.

Toutefois, la loi prévoit une exception importante qui semble conférer aux employeurs le droit d'effectuer sans avis une surveillance raisonnable de leurs employés, dans des circonstances très limitées. L'alinéa 7(1)*b)* de la Loi prévoit ce qui suit :

> [...] l'organisation ne peut recueillir de renseignement personnel à l'insu de l'intéressé et sans son consentement que [s']il est raisonnable de s'attendre à ce que la collecte effectuée au su ou avec le consentement de l'intéressé puisse compromettre l'exactitude du renseignement ou l'accès à celui-ci, et la collecte est raisonnable à des fins liées à une enquête sur la violation d'un accord ou la contravention du droit fédéral ou provincial[101].

Bien que l'effet d'une telle exception n'ait pas encore été ressenti, les termes employés incorporent la notion du caractère raisonnable de deux façons importantes. Premièrement, la collecte de renseignements personnels sans consentement ne peut avoir lieu que lorsqu'il est raisonnable de s'attendre à ce que la collecte effectuée au su ou avec le consentement de l'intéressé puisse compromettre l'exactitude des renseignements. On constate souvent la remise, à l'échelle de l'entreprise, d'un avis concernant les politiques de surveillance, puisque les employeurs se servent de l'avis pour limiter l'attente raisonnable en matière de respect de la vie privée qu'ont les employés. En conséquence, la disposition ci-haut ne s'applique que lorsque l'employeur craint qu'un avis particulier puisse compromettre une enquête. Bien qu'une telle

situation doive en théorie être rare dans le cadre de la plupart des activités de surveillance informatique, il est possible d'envisager un scénario dans lequel l'entreprise a des motifs de croire qu'un employé se livre à des activités criminelles et désire mettre en oeuvre des mesures de surveillance uniques dans le cadre de l'enquête, sans toutefois nuire à celle-ci.

Un tel scénario incorpore la notion du caractère raisonnable d'une deuxième façon. Selon la loi, non seulement doit-il être raisonnable de s'attendre à ce que le consentement puisse compromettre l'exactitude des renseignements obtenus, mais la collecte elle-même doit être raisonnable à des fins liées à une enquête sur la violation d'un accord. Ainsi, la notion du caractère raisonnable est incorporée à la surveillance, en ce sens que seules des mesures de surveillance raisonnables peuvent être utilisées. Tel que précisé ci-dessous, une telle exigence donne à penser que des méthodes de surveillance portant atteinte à la vie privée peuvent être illégales lorsqu'il existe une solution tout aussi efficace et respectant davantage la vie privée.

Quatrièmement, la loi exige que l'organisation protège les renseignements personnels au moyen de mesures de sécurité correspondant à leur degré de sensibilité[102] et établit des limites relatives à la conservation de renseignements. Elle prévoit qu'« [o]n ne doit conserver les renseignements personnels qu'aussi longtemps que nécessaire pour la réalisation des fins déterminées[103] ». De telles dispositions imposent des limites à ce que peuvent faire les employeurs après avoir effectué la collecte des renseignements, en veillant à ce que les renseignements ne puissent être conservés pendant une période illimitée tout en établissant une obligation pour s'assurer que le personnel non autorisé ne puisse avoir accès aux renseignements.

Bien que la LPRPDE offre sans doute aux citoyens canadiens la plus vaste gamme de protections de la vie privée, elle n'est qu'une parmi plusieurs lois illustrant l'engagement du Canada envers les droits à la vie privée. La *Loi sur la protection des renseignements personnels*[104], qui applique des règles similaires à la collecte de renseignements personnels par les institutions fédérales, favorise le respect de la vie privée. La disposition de déclaration

d'objet de la *Loi* prévoit que celle-ci vise à « compléter la législation canadienne en matière de protection des renseignements personnels relevant des institutions fédérales et de droit d'accès des individus aux renseignements personnels qui les concernent[105] ».

Plusieurs lois fédérales en matière de communications traitent également de questions liées au respect de la vie privée. Par exemple, la *Loi sur la radiocommunication*[106] prévoit que « [s]auf exception réglementaire, il est interdit d'intercepter et soit d'utiliser, soit de communiquer toute radiocommunication sans l'autorisation de l'émetteur ou du destinataire[107] ». Quant à elle, la *Loi sur les télécommunications*[108] prévoit ce qui suit : « La présente loi affirme le caractère essentiel des télécommunications pour l'identité et la souveraineté canadiennes; la politique canadienne de télécommunication vise à [...] contribuer à la protection de la vie privée des personnes[109] ». Les lois commerciales telles que la *Loi sur les banques*[110], laquelle comporte des dispositions relatives au respect de la vie privée qui imposent des limites quant à la collecte, l'utilisation et la communication de renseignements sur la clientèle, de même que la *Loi sur la Société canadienne des postes*[111], laquelle prévoit que nul ne peut ouvrir une lettre scellée depuis son dépôt jusqu'à sa livraison à moins d'avoir des motifs de croire que la lettre est utilisée pour commettre une infraction ou d'obtenir le consentement de son auteur ou du destinataire, illustrent elles aussi l'orientation de la législation fédérale axée sur le respect de la vie privée.

Le tribunaux canadiens ont également démontré à maintes reprises leur engagement envers la protection de la vie privée. Outre l'affaire *Weir,* dans laquelle un tribunal de l'Alberta a conclu que le courrier électronique bénéficiait d'une attente raisonnable en matière de respect de la vie privée, l'arrêt *Pacific Northwest Herb Corp. v. Thompson*, rendu en 1999 par la Cour suprême de la Colombie-Britannique, se distingue du fait que le tribunal a conclu qu'un intérêt en matière de respect de la vie privée applicable à l'utilisation d'un ordinateur pouvait exister en milieu de travail[112]. En l'espèce, un ancien employé de Pacific Northwest avait utilisé chez lui un ordinateur de l'entreprise, à des fins tant professionnelles que personnelles. Après avoir été congédié, l'employé a continué à se servir de l'ordinateur à des fins personnelles,

notamment pour documenter les renseignements se rapportant à la poursuite pour congédiement injustifié qu'il comptait intenter contre son ancien employeur. Avant de remettre l'ordinateur à son ancien employeur, l'employé a retenu les services d'une société de conseils en informatique pour effacer tous les renseignements se trouvant sur le lecteur de disque dur de l'ordinateur, y compris les fichiers professionnels et personnels. Malgré la tentative visant à effacer le contenu de l'ordinateur, l'employeur a réussi à récupérer les renseignements lorsque l'ordinateur lui a été remis.

L'ancien employé a voulu empêcher l'entreprise de se servir des renseignements récupérés, en invoquant tant le secret professionnel (par rapport aux documents concernant le congédiement injustifié) que le droit à la vie privée, relativement aux renseignements se trouvant sur le lecteur de disque dur. Le juge a accepté l'argument de l'employé, en concluant que [TRADUCTION] « le défendeur peut avoir une attente raisonnable en matière de respect de la vie privée en ce qui concerne les documents créés à des fins familiales ou personnelles[113] ». Fait intéressant, le juge en est arrivé à sa décision en dépit du fait que l'employeur était le propriétaire du système informatique.

On constate également la volonté d'établir une approche équilibrée en matière de respect de la vie privée en milieu de travail dans plusieurs cas d'arbitrage canadiens en droit du travail qui traitent de la surveillance vidéo. Bien que la surveillance informatique se compare mieux à la surveillance téléphonique, en raison du rôle essentiel que jouent désormais les ordinateurs et le courrier électronique dans les communications de tous les jours, l'analyse des droits à la vie privée en milieu de travail qui se retrouve dans plusieurs cas de surveillance vidéo nous renseigne sur l'importance croissante accordée de façon générale aux droits à la vie privée des employés.

Parmi les premiers cas d'arbitrage en droit du travail à s'être penchés sur de telles questions, on compte *Re Doman Forest Products Ltd*, une décision de la Colombie-Britannique rendue en 1990[114]. Plus d'une décennie avant l'arrivée des lois en matière de

respect de la vie privée, telles que la LPRPDE, l'arbitre s'est fondé sur les principes fondamentaux de la *Charte*, notamment sur la confirmation de l'importance de la protection des renseignements personnels dans l'arrêt *R. c. Duarte*, une décision rendue en 1990 par la Cour suprême du Canada[115], pour conclure que [TRADUCTION] « la surveillance électronique par l'État enfreint le droit à la vie privée de l'individu et ne sera tolérée que si la norme du caractère raisonnable est appliquée[116] ». En appliquant de tels principes à la relation employeur privé-employé, l'arbitre a conclu que, bien que le droit à la vie privée ne fût pas absolu, il devait être [TRADUCTION] « évalué selon ce qui est « raisonnable dans les circonstances » et, entre autres choses, dépendait d'intérêts opposés tels que « la relation entre les parties »[117] ». Pour déterminer ce qui était raisonnable dans les circonstances, l'arbitre a souligné trois facteurs à considérer : (i) la demande de surveillance était-elle raisonnable? (ii) La surveillance a-t-elle été effectuée d'une manière raisonnable? (iii) L'employeur disposait-il de solutions de rechange à la surveillance?[118]

L'affaire *Doman* a depuis été citée et approuvée dans plusieurs décisions[119], y compris dans l'arrêt *St. Mary's Hospital and H.E.U.*[120], une décision arbitrale de la Colombie-Britannique rendue en 1997. En l'espèce, un électricien effectuant une vérification périodique des fils dans un hôpital a découvert un câble qu'il ne connaissait pas. Il a retracé le câble jusque dans le bureau d'un gestionnaire, où il a découvert une caméra vidéo cachée derrière un carreau de plafond, au milieu de la salle. Lorsque le syndicat local a eu vent de la surveillance clandestine, il s'est dit indigné de ce qu'il considérait comme une grave atteinte aux droits à la vie privée des employés. Bien que la caméra ait par la suite été démontée, le syndicat a déposé un grief.

L'arbitre a examiné un vaste éventail de décisions canadiennes, dans lesquelles plusieurs tribunaux ont conclu que le droit à la vie privée des employés n'était pas absolu et devait être évalué à la lumière de ce qui était raisonnable dans les circonstances, avant de résumer l'état du droit sur la surveillance en milieu de travail en plusieurs principes. Premièrement, l'arbitre a conclu que la surveillance pouvait être divisée en trois catégories. La *surveillance anodine*, qui

est utilisée lors de séances de formation du personnel ou d'autres situations similaires, profite aux employés et n'a donc guère besoin d'être justifiée par l'employeur. La *surveillance de sécurité*, qui nécessite habituellement des caméras visibles conçues pour assurer la sécurité des employés et de l'employeur, est adoptée avec le consentement tacite des employés et est visible aux yeux de tous. La *surveillance clandestine* est la plus problématique, puisqu'elle porte le plus atteinte à la vie privée des employés. L'arbitre a souligné qu'une telle forme de surveillance devait faire l'objet d'une justification stricte par l'employeur, notamment si la surveillance, plutôt que de cibler un individu, avait une portée générale. L'arbitre a ajouté ce qui suit :

> [TRADUCTION]
>
> Après la détermination du type, de l'objet, du lieu et de la fréquence de la surveillance clandestine, l'équilibrage des intérêts nécessite l'application de critères particuliers. L'employeur a le fardeau de justifier l'atteinte au droit à la vie privée de l'employé en démontrant qu'un problème important existe et que la surveillance est fortement susceptible d'aider à résoudre le problème. L'employeur doit démontrer non seulement qu'il existe des motifs d'effectuer une surveillance, mais aussi que la surveillance ne contrevient aucunement à la convention collective; il doit démontrer qu'il a épuisé toutes les solutions de rechange disponibles et qu'il n'existe aucune autre solution raisonnable et portant moins atteinte à la vie privée; en dernier lieu, l'employeur doit s'assurer que la surveillance est effectuée de manière systématique et non discriminatoire[121].

La décision ci-haut illustre comment les intérêts opposés sont soupesés dans les cas d'arbitrage canadiens en droit du travail – une surveillance est autorisée, mais seulement si un problème important a été identifié, la surveillance est susceptible de résoudre le problème, on a tenté, mais sans succès, de trouver des solutions de rechange, et la surveillance est mise en oeuvre de façon juste et impartiale.

Bien que certains se soient demandé si l'affaire *Doman* et les décisions qui ont suivi ont force de jurisprudence à l'extérieur de la Colombie-Britannique, plusieurs décisions donnent à penser que tel est le cas. Par exemple, dans *Re Toronto Transit Commission and A.T.U., Loc. 113 (Belsito)*[122], une décision arbitrale ontarienne de 1999 en droit du travail, l'arbitre a conclu qu'[TRADUCTION] « [e]u égard à toutes ces décisions, les cas d'arbitrage tranchés en Ontario appuient largement la proposition selon laquelle la surveillance effectuée par un

employeur peut, dans certaines circonstances, porter atteinte au droit à la vie privée d'un employé de façon déraisonnable[123] ». Dans le même ordre d'idées, dans *New Flyer Industries Ltd. and C.A.W.-Canada, Loc. 3003 (Mogg)*[124], une décision manitobaine rendue en 2000, l'arbitre a conclu que l'affaire *Doman* avait force de jurisprudence au Manitoba.

Le Commissaire à la protection de la vie privée du Canada a également exprimé des préoccupations quant à la surveillance et au respect de la vie privée en milieu de travail. De telles préoccupations ont pris une importance accrue depuis l'adoption de la LPRPDE, puisque le Commissaire est le premier arbitre des plaintes déposées aux termes de cette loi[125]. Le rapport annuel 2000-2001 du Commissaire, publié à la fin décembre 2001, énonce clairement sa position quant à la surveillance, la protection du courrier électronique et l'attente raisonnable en matière de respect de la vie privée en milieu de travail[126].

Le Commissaire a fait état d'une situation dans laquelle on lui a demandé de traiter une plainte déposée par un employé du ministère de la Défense nationale aux termes de la *Loi sur la protection des renseignements personnels*. La plainte se rapportait à la question de savoir si l'employeur avait le droit d'utiliser et de divulguer les courriels privés de l'employé dans le cadre de l'enquête sur une plainte de harcèlement[127]. Le Commissaire a entamé son analyse de la surveillance du courrier électronique en milieu de travail en soulignant que les employeurs justifiaient souvent les pratiques de surveillance en invoquant la nécessité de protéger les employés contre le harcèlement en milieu de travail. Bien que le Commissaire ait reconnu qu'une telle protection était nécessaire, il a déclaré ce qui suit : « je ne crois pas que cette protection se traduise nécessairement par la surveillance générale des communications électroniques ou de l'utilisation des ordinateurs. Il faut accepter qu'il y a des limites contraignantes au droit d'un employeur de lire le courrier des employés ou d'écouter leurs conversations téléphoniques ou vider leurs tiroirs. Je crois qu'il faut regarder de près les communications électroniques afin de déterminer les principes à appliquer à leur sujet[128] ».

En l'espèce, la politique du MDN sur la gestion du courrier électronique précisait que

les employés ne pouvaient s'attendre au respect de leur vie privée lorsqu'ils utilisaient les systèmes de courrier électronique. Le Commissaire a précisé qu'il trouvait une telle politique particulièrement déplorable, en ajoutant ce qui suit:

> La loi en matière de la protection de la vie privée a été élaborée en se fondant sur la notion d'« attentes raisonnables de respect de la vie privée », et l'une des façons dont les tribunaux déterminent s'il y a eu violation de la vie privée est d'établir tout d'abord si une personne peut raisonnablement s'attendre à ce que sa vie privée soit respectée à un endroit et à un moment donnés. Mais je ne suis pas d'accord qu'en raison de ce principe on porte atteinte à la vie privée d'un employé ou de quiconque en lui disant simplement qu'il ne peut s'attendre au respect de celle-ci. Bien que la direction ait le droit et la responsabilité de gérer, elle doit toutefois le faire en tenant compte de certaines contraintes, y compris le respect des droits fondamentaux. Il ne revient pas à la direction seulement de déterminer si l'attente en matière de respect de la vie privée est raisonnable[129].

Le Commissaire a exprimé un point de vue similaire lors d'un discours sur le respect de la vie privée en milieu de travail dans la foulée des événements du 11 septembre[130]. Le Commissaire a souligné l'opinion sans cesse plus répandue selon laquelle les communications Internet devaient être surveillées, en citant la productivité des employés, la protection des renseignements confidentiels, la sécurité et la responsabilité légale comme principaux motifs invoqués à l'appui de l'installation de systèmes de surveillance. Bien qu'il ait reconnu qu'une certaine surveillance était inévitable, il a fait valoir que « [l]'enquête dirigée, fondée sur des soupçons, est préférable à la surveillance et à la violation à grande échelle du droit à la vie privée. Une enquête ciblée, partant de soupçons raisonnables, non seulement porte moins atteinte à la vie privée, mais encore est plus efficace[131] ».

Partie trois – Vers un équilibre surveillance-respect de la vie privée fondé sur le caractère raisonnable

La discussion ci-haut donne à penser que deux tendances sociétales s'affrontent. Alors que l'utilisation des ordinateurs et d'Internet continue de croître, la popularité des systèmes de surveillance des ordinateurs et du courrier électronique en milieu de travail semble susceptible d'accompagner et même de dépasser une telle croissance. Tout en reconnaissant les avantages et gains de rendement créés par les nouvelles technologies, les entreprises craignent clairement

que la productivité, la sécurité et la responsabilité légale ne soient des sous-produits potentiels de l'habilitation des employés disposant d'ordinateurs et de connexions Internet.

Entre-temps, il semble tout aussi vrai que le respect de la vie privée demeurera une valeur sociétale prisée à laquelle la population ne renoncera pas sans justification adéquate. L'opinion selon laquelle les employés renoncent à toute protection de la vie privée en milieu de travail semble aussi désuète que les ordinateurs centraux d'antan. Le droit canadien consacré dans la législation, la jurisprudence, les cas d'arbitrage en droit du travail et la politique publique ont peu à peu accepté l'argument selon lequel un simple avis ne peut servir de justification à la surveillance en milieu de travail – que celle-ci soit effectuée au moyen de caméras vidéo ou de programmes informatiques axés sur les serveurs ou sur les clients. Les activités de surveillance doivent plutôt satisfaire à un critère de caractère raisonnable qui vise l'équilibre entre les préoccupations des employeurs et les intérêts en matière de respect de la vie privée des employés.

De tels développements indiquent qu'une transition importante s'opère au niveau de l'analyse. Alors que les décisions antérieures se penchaient principalement sur la question de savoir si un employé avait une attente raisonnable en matière de respect de la vie privée (et que, dans plusieurs cas, un avis indiquant aux employés qu'ils ne disposaient pas d'un droit à la vie privée était considéré suffisant pour supprimer une telle attente)[132], la nouvelle analyse met plutôt l'accent sur le caractère raisonnable de la surveillance.

Au fur et à mesure qu'augmente l'affrontement entre la surveillance informatique et le respect de la vie privée se rapprochent, il devient de plus en plus nécessaire d'établir des critères précis servant à évaluer le caractère raisonnable de la surveillance. À la lumière des développements dans les domaines du droit et de la technologie, nous faisons valoir que six facteurs doivent être examinés au moment d'évaluer le caractère raisonnable de la surveillance des ordinateurs et du courrier électronique : (i) la cible de la surveillance, (ii) son objet, (iii) les solutions de rechange à la surveillance, (iv) la technologie de surveillance, (v) la suffisance de

l'avis et (vi) la mise en oeuvre des activités de surveillance.

Ce qui précède ne signifie pas qu'un facteur puisse être considéré déterminant à lui seul. Dans certains cas, un facteur peut être suffisamment important pour réduire l'importance des autres facteurs. Par exemple, si la loi impose à un employeur l'obligation de mettre en oeuvre un système de surveillance, comme dans le cas de certains fournisseurs de soins de santé aux États-Unis, un tel objet légitime est susceptible de l'emporter sur les autres facteurs. Dans le même ordre d'idées, si l'objet de la surveillance effectuée par un employeur n'est pas clairement défini, et si celui-ci se sert de la surveillance principalement parce qu'il en est capable, un examen soigneux des autres facteurs sera nécessaire pour s'assurer de la réalisation d'un équilibre surveillance-respect de la vie privée fondé sur le caractère raisonnable.

a. Les six facteurs

i. Cible de la surveillance

La cible de la surveillance soulève deux questions distinctes. Premièrement, il faut se demander si la surveillance informatique est effectuée à l'échelle de l'entreprise de manière à viser tous les employés de façon égale, ou si seulement certains employés font l'objet d'une surveillance. Si l'on suppose qu'elle n'est pas mise en oeuvre de façon discriminatoire, la surveillance étroite est préférable du point de vue du respect de la vie privée. Par exemple, si un cabinet d'avocats s'inquiète de la productivité des employés, il peut être inutile de surveiller les avocats et le personnel de soutien de la même manière, puisque les avocats font habituellement état de leur emploi du temps en présentant des registres de temps hebdomadaires. Dans le même ordre d'idées, si une entreprise spécialisée dans la technologie craint que ses ingénieurs tentent de transmettre des renseignements confidentiels à des sources externes, il peut être inutile de surveiller les employés n'ayant pas accès à de tels renseignements, tels que le personnel des ressources humaines et des finances.

Le Commissaire à la protection de la vie privée du Canada appuie la surveillance ciblée et soutient qu'une telle approche porte moins atteinte aux droits à la vie privée, en plus d'être plus efficace. Bien que la LPRPDE ne traite pas expressément d'une telle question, plusieurs dispositions s'appliquent au présent contexte. Premièrement, le critère général de caractère raisonnable peut être utile au moment d'examiner s'il est ou non raisonnable d'effectuer la collecte de renseignements personnels auprès d'une personne dont les activités ne sont pas visées par la surveillance. Deuxièmement, puisque la collecte de renseignements personnels doit se limiter à ce qui est nécessaire pour les fins identifiées par l'organisation, une surveillance dont la portée est trop générale pourrait contrevenir à la disposition importante qui établit une telle condition.

Outre la question de la surveillance générale ou particulière, le facteur de la cible de la surveillance se rapporte également aux types de personnes qui ne peuvent faire l'objet d'une surveillance que dans des circonstances limitées, en raison de leurs fonctions. Tel que nous le verrons en détail dans la partie quatre, la magistrature illustre bien une telle question, puisque la surveillance de la magistrature soulève non seulement des préoccupations quant au respect de la vie privée, mais aussi des considérations fondamentales d'indépendance judiciaire qui peuvent s'opposer à certaines formes de surveillance.

ii. Objet de la surveillance

Bien que certaines organisations puissent installer de nouvelles technologies de surveillance sans motif clairement défini, la jurisprudence et les nouvelles politiques en matière de respect de la vie privée indiquent qu'un objet bien défini est essentiel pour satisfaire au critère de caractère raisonnable. Du point de vue législatif, la disposition générale de la LPRPDE, laquelle prévoit que la collecte, l'utilisation et la communication de renseignements personnels ne peuvent avoir lieu qu'à des fins acceptables, présume que la collecte de renseignements a bel et bien un objet. De la même manière, dans la décision arbitrale rendue

dans *St. Mary's Hospital and H.E.U.*, l'arbitre s'est tout d'abord penché sur l'identification de l'objet avant de passer à la partie plus difficile de l'analyse fondée sur le caractère raisonnable.

La partie un du présent rapport a identifié certains des motifs les plus souvent invoqués par les organisations à l'appui de l'utilisation de technologies de surveillance. Parmi ceux-ci, on compte le rendement des employés et du réseau, la responsabilité de l'employeur, les préoccupations en matière de confidentialité et de secrets commerciaux, les délits informatiques, l'obligation juridique, de même que la surveillance exigée par la loi. L'utilisation de technologies de surveillance en milieu de travail peut être légitime – il revient à l'employeur d'énoncer un objet clairement défini qui corresponde à la cible de la surveillance et à la technologie utilisée.

iii. Solutions de rechange à la surveillance

Bien que les technologies de surveillance puissent constituer un moyen efficace de détecter l'utilisation malveillante des ordinateurs ou des réseaux, leurs effets sur le respect de la vie privée et leurs répercussions potentiellement nuisibles sur le moral des employés[133] en ont poussé plusieurs à réclamer l'exploration de méthodes portant moins atteinte à la vie privée avant de recourir à des activités de surveillance. La discussion dans *St. Mary's Hospital and H.E.U.* est riche en enseignements; l'arbitre y a conclu que [TRADUCTION] « l'employeur doit démontrer non seulement qu'il existe des motifs d'effectuer une surveillance, mais aussi que la surveillance ne contrevient aucunement à la convention collective; il doit démontrer qu'il a épuisé toutes les solutions de rechange disponibles et qu'il n'existe aucune autre solution raisonnable et portant moins atteinte à la vie privée[134] ».

Dans le même ordre d'idées, dans *Brewers Retail Inc. and United Brewers' Warehousing Workers' Provincial Board (Merson)*[135], une décision arbitrale ontarienne de 1999 en droit du travail, l'arbitre a examiné plus d'une douzaine de décisions en matière de surveillance et remarqué qu'un accent répété avait été mis sur l'exploration de solutions de rechange. Tout en reconnaissant que la surveillance ne serait pas toujours la solution de dernier ressort, il a conclu que [TRADUCTION] « lorsque l'activité visée a lieu au travail, il se peut

que d'autres solutions soient plus facilement à la disposition de l'employeur, puisque celui-ci est responsable du milieu de travail et en mesure de gérer et d'administrer le milieu de travail et les employés. En effet, dans certaines circonstances, le fait que la surveillance a lieu au travail pourrait la rendre moins susceptible d'être admissible[136] ».

La nécessité de trouver des solutions portant moins atteinte à la vie privée a également été soulevée par plusieurs magistrats lors de la controverse entourant la surveillance informatique de la magistrature aux États-Unis en 2001. Dans une note de service adressée à tous les juges en chef des tribunaux américains, la juge en chef du 9e circuit, Mary M. Schroeder, a fait valoir ce qui suit :

> [TRADUCTION]
>
> [p]lusieurs juges croient que des méthodes visant l'administration d'une politique Internet qui portent moins atteinte à la vie privée devraient être adoptées avant de passer à la surveillance des activités menées par les employés sur Internet. La plupart des tribunaux ont à peine commencé à sensibiliser et renseigner leur personnel au sujet des préoccupations en matière d'Internet, notamment l'utilisation de la largeur de bande [...] [c]ertains juges sont d'avis que nous devrions donner aux tribunaux l'occasion d'aborder la question avant de passer à la surveillance[137].

De tels arguments ont été repris dans une lettre de la juge Edith Jones du 5e circuit. En ce qui concerne les plans visant l'installation de systèmes de surveillance au sein de la magistrature américaine, la juge Jones a précisé ce qui suit :

> [TRADUCTION]
>
> [...] le rapport du Comité n'explique pas pourquoi des mesures de rechange visant à décourager l'utilisation malveillante d'Internet ou des ordinateurs au sein de la magistrature et portant moins atteinte à la vie privée ne sont pas réalisables. Par exemple, [...] après que le programme de surveillance ait été annoncé, le Comité exécutif a distribué à l'ensemble de la magistrature un communiqué concernant l'utilisation acceptable. On nous a dit que l'utilisation de la largeur de bande avait chuté de façon immédiate et spectaculaire par suite du communiqué. Si des incitations sont suffisantes pour décourager l'usage inacceptable, pourquoi recourir à une surveillance aléatoire?[138]

Les technologies de surveillance peuvent certainement jouer un rôle en fournissant aux organisations l'assurance qu'elles limitent leur responsabilité légale en milieu de travail et maximisent la productivité des employés. Toutefois, dans le cadre d'un équilibre surveillance-

respect de la vie privée fondé sur le caractère raisonnable, d'autres solutions portant moins atteinte à la vie privée en milieu de travail pourraient s'avérer tout aussi efficaces et devraient être examinées avant que ne soit adoptée la solution qui respecte le moins la vie privée.

iv. Technologie de surveillance

En raison de la disponibilité de douzaines de technologies de surveillance, le choix de la technologie doit aussi faire partie de l'analyse fondée sur le caractère raisonnable. À certains égards, un tel facteur reprend les mêmes objectifs que ceux du troisième facteur consistant à trouver la solution de rechange qui porte le moins atteinte à la vie privée. Une fois prise la décision d'adopter des technologies de surveillance, les organisations devraient alors choisir celle qui satisfait le mieux à leurs objectifs tout en portant le moins possible atteinte à la vie privée des employés.

On retrouve dans l'opinion 8/2001 du groupe de travail de l'Union européenne traitant de la protection des données à caractère personnel dans le contexte professionnel l'exigence de technologies de surveillance appropriées.[139] Aux termes de cet avis, « [t]out contrôle doit être une réponse proportionnée de l'employeur aux risques qu'il encourt tout en veillant aux intérêts légitimes des membres de son personnel en matière de vie privée et autre. […] [l]e contrôle doit être le moins intrusif possible[140] ».

Au moment de choisir une technologie de surveillance, les organisations devraient garder à l'esprit les différences qui existent entre la surveillance axée sur les serveurs et celle axée sur les clients. Bien que des programmes de surveillance axés sur les clients puissent être nécessaires pour s'attaquer au problème du délit informatique, tel que dans l'affaire *Scarfo*, les préoccupations relatives au rendement des réseaux ne nécessitent pas de telles technologies, puisque qu'elles visent les réseaux et non pas le contenu créé ou visionné par l'employé. En conséquence, les programmes de surveillance axés sur les serveurs, lesquels, portant moins atteinte à la vie privée, constituent une meilleure forme de contrôle du rendement des réseaux.

v. Suffisance de l'avis

Étant donné les exceptions relatives au consentement prévues par le *Code criminel*, un consentement pleinement éclairé est nécessaire pour s'assurer que la surveillance en milieu de travail ne viole pas le droit criminel. En outre, les protections de la vie privée prévues par la LPRPDE exigent également que les organisations obtiennent un consentement dans la grande majorité des cas avant que la collecte, l'utilisation et la communication de renseignements personnels ne puissent avoir lieu.

Afin de fournir un consentement valable, les employés doivent recevoir une description précise des pratiques de surveillance. Le Commissariat à la protection de la vie privée de l'Australie a prévu certaines directives utiles pour s'assurer que les employés comprennent bien la position de leur employeur[141]. Le Commissariat recommande que les six lignes directrices suivantes soient incorporées dans la politique de l'entreprise :

[TRADUCTION]

1. La politique devrait être émise au personnel et à la direction afin d'être bien connue et comprise par le personnel. Idéalement, la politique devrait être accessible à partir de l'écran que voit l'utilisateur lorsqu'il se branche au réseau.
2. La politique devrait expressément prévoir les activités autorisées et interdites.
3. La politique devrait clairement identifier les renseignements enregistrés et les personnes qui, au sein de l'organisation, ont le droit d'accéder aux journaux et au contenu des activités de courrier électronique et d'exploration d'Internet menées par le personnel.
4. La politique devrait mentionner la politique de l'organisation en matière de sécurité informatique. L'utilisation inacceptable du courrier électronique risque de compromettre le système de sécurité, la vie privée du personnel et d'autres personnes et la responsabilité légale de l'organisation.
5. La politique devrait souligner, en langage clair, la façon dont l'organisation entend contrôler ou vérifier l'observation, par le personnel, des règles relatives à l'utilisation acceptable du courrier électronique et d'Internet.
6. La politique devrait être révisée de façon régulière afin de tenir compte des développements rapides dans les domaines d'Internet et de la technologie de l'information. La politique devrait être émise de nouveau en cas de modification importante. Le message serait ainsi mieux reçu par le personnel.

Les recommandations du Commissaire visent à ce que les employés connaissent et comprennent la politique de surveillance de l'entreprise, et qu'il y ait divulgation expresse de la collecte, de l'utilisation et de la dissémination que prévoit faire l'entreprise des renseignements colligés.

La suffisance de l'avis dépend non seulement de son existence et de sa perceptibilité, mais aussi de son contenu. Les décisions rendues par le directeur général du contentieux de la NLRB, qui a conclu qu'une interdiction complète de tout courrier électronique non relié à l'emploi était trop générale et à première vue illégale, de même que par le Commissaire à la protection de la vie privée du Canada, lequel est d'avis que les entreprises ne peuvent outrepasser le droit à la vie privée des employés par la simple remise d'un avis, démontrent que les organisations ne peuvent incorporer des droits de surveillance illimités dans leurs politiques. Celles-ci doivent plutôt respecter les normes relatives à la vie privée et tenter d'atteindre un équilibre acceptable entre les besoins en matière de surveillance et le respect de la vie privée.

vi. Mise en oeuvre des technologies de surveillance

L'installation d'une technologie de suveillance appropriée et la remise d'un avis suffisant aux employés ne mettent pas fin à l'analyse fondée sur le caractère raisonnable. Bien qu'ils soient souvent ignorés, il faut aussi examiner les divers processus et protections mis en oeuvre une fois entamées la surveillance et l'accumulation de renseignements. Une telle obligation se retrouve plus particulièrement dans la LPRPDE, laquelle exige la désignation, au sein de l'organisation, d'une personne chargée des questions relatives à la vie privée, de la sécurité adéquate des renseignements et des politiques de conservation de renseignements appropriées.

Au cours de la controverse entourant la surveillance de l'appareil judiciaire, les magistrats du 9e circuit se sont dits particulièrement préoccupés par l'identité des personnes ayant accès aux renseignements obtenus par surveillance. Dans sa note de service adressée à tous les juges en chef américains, la juge en chef Mary M. Schroeder a souligné que [TRADUCTION] « [p]lusieurs

juges craignaient que l'enregistrement et le contrôle des renseignements conservés par le Bureau administratif ne fassent obligatoirement partie de tout processus de confirmation par le Sénat[142] ». L'incident survenu au sein de la magistrature néo-zélandaise, au cours duquel une fuite de renseignements concernant l'utilisation légale mais potentiellement gênante des ordinateurs a immédiatement mené à des demandes réclamant la démission des juges visés, illustre le mieux la posssibilité d'un tel scénario..

Compte tenu des nouvelles obligations prévues par la LPRPDE, il appert de plus en plus que la surveillance en milieu de travail ne peut être considérée comme une simple question technique relevant des professionnels de la technologie de l'information de l'organisation. Le directeur de la protection de la vie privée de l'organisation ou son équivalent doit plutôt jouer un rôle essentiel dans l'établissement d'une politique en matière d'accès, de sécurité et de conservation de renseignements.

b. Conclusions – Surveillance informatique en milieu de travail

Dans le cadre de l'élaboration d'une approche convenable en matière de surveillance informatique en milieu de travail, il importe de se rappeler que ni le droit à la vie privée ni le droit à la surveillance ne sont absolus. Dans une ère où l'informatique et les communications Internet se retrouvent presque partout, les droits à la vie privée prennent de plus en plus d'importance au sein de notre tissu juridique. Cependant, que ce soit au travail ou à la maison, notre droit à la vie privée est limité par d'autres objectifs sociétaux, tels que l'application efficace du *Code criminel*.

Dans le même ordre d'idées, les employeurs ont souvent des motifs légitimes d'effectuer une surveillance informatique en milieu de travail. Au fur et à mesure que l'informatique et les communications Internet prennent de plus en plus d'importance au sein du milieu de travail, les employeurs ont des motifs valables de recourir à des technologies de surveillance, pour s'assurer que le milieu demeure libre de harcèlement et d'actes illégaux, de même que pour favoriser l'utilisation efficace de la technologie.

Le droit canadien cherche à équilibrer les intérêts en jeu en évaluant le caractère raisonnable de la surveillance. Par le passé, l'attente raisonnable d'un employé en matière de respect de la vie privée était déterminante à elle seule. Tel n'est plus le cas aujourd'hui. L'émergence des principes de respect de la vie privée prévus par la *Charte*, des lois nationales en matière de protection de la vie privée, des normes internationales relatives à la vie privée et de la jurisprudence en droit du travail, souligne une transition vers une plus grande protection de la vie privée en milieu de travail.

L'auteur croit que dans l'appréciation des intérêts opposés des employeurs et des employés, il est nécessaire de procéder à l'examen d'une série de facteurs pour déterminer l'opportunité d'une mesure de surveillance en milieu de travail, ou pour établir une politique appropriée en la matière. Ces facteurs, dont aucun n'est déterminant à lui seul, comprennent notamment (i) la cible de la surveillance, (ii) son objet, (iii) les solutions de rechange à la surveillance, (iv) la technologie de surveillance, (v) la suffisance de l'avis et (vi) la mise en oeuvre des activités de surveillance.

Tel que souligné au début du présent document, David Flaherty, l'ancien commissaire à l'information et à la protection de la vie privée pour la province de Colombie-Britannique, fait remarquer que « [l]a technologie de surveillance n'est ni mauvaise ni bonne en soi, mais [...] il y a à la fois de la bonne et de la mauvaise surveillance[143] ». Le nouveau cadre juridique canadien de la surveillance informatique en milieu de travail incorpore un tel point de vue en offrant la flexibilité nécessaire pour établir des systèmes appropriés, tout en respectant l'importance qu'accorde notre société au respect de la vie privée.

Partie quatre – Surveillance informatique de la magistrature au Canada

a. Les ordinateurs au sein de la magistrature canadienne

L'apparition des ordinateurs au sein de la magistrature canadienne remonte au moins au début des années 1980[144]. Il n'est pas étonnant que les questions de surveillance et de respect de la vie privée qui nous préoccupent aujourd'hui n'aient pas constitué le centre d'intérêt de l'époque. On cherchait plutôt à démystifier les ordinateurs et à sensibiliser la magistrature à l'égard de leurs applications éventuelles[145]. À l'époque, l'informatique était surtout considérée comme l'outil des administrateurs judiciaires, lesquels pouvaient améliorer leur rendement par un rassemblement des données. En fait, l'un des premiers commentaires concernant les ordinateurs écartait toute préoccupation en matière de respect de la vie privée : « [l]a plupart des données créées par ordinateur sont des données d'ensemble et des statistiques brutes (totaux, moyennes) qui ne portent pas atteinte à la vie privée d'un individu en particulier[146] ».

Tandis qu'en 1986, le Conseil canadien de la magistrature (CCM) prévoyait que [TRADUCTION] « chacun des juges de la Cour [suprême] disposerait éventuellement d'un ordinateur[147] », il est bientôt devenu évident que les ordinateurs faisaient leur apparition au sein de la magistrature beaucoup plus rapidement que ne l'avaient prévu plusieurs observateurs. Une étude du CCM menée en 1988 et portant sur l'utilisation des ordinateurs par les juges nommés par le fédéral a indiqué qu'onze pour cent des sujets interrogés s'étaient servis d'un ordinateur et qu'un autre 15 pour cent avaient accès à un ordinateur[148]. Bien qu'il restât beaucoup de travail à faire (41 pour cent des sujets interrogés n'ayant pas d'accès à un ordinateur souhaitaient le contraire), le rapport a conclu ce qui suit : [TRADUCTION] « le message est clair en l'espèce : les juges commencent à se servir des ordinateurs[149] ».

De nos jours, l'ordinateur est un outil indispensable pour la grande majorité des juges. Dans plusieurs provinces, dont l'Alberta, la Colombie-Britannique, le Manitoba, le Nouveau-Brunswick, Terre-Neuve et l'Ontario, presque tous les juges ont leur propre ordinateur personnel, qu'ils utilisent à des fins diverses, notamment le travail se rapportant aux jugements, la communication et la recherche juridique[150]. Le travail informatique se rapportant aux jugements comprend la sauvegarde des notes prises au procès, la rédaction et révision de mémoires de recherche, ainsi que la rédaction de jugements. Lorsque plusieurs membres de la formation participent conjointement à

la rédaction d'un seul jugement, les capacités de traitement de texte en collaboration ainsi qu'une fonctionnalité de comparaison de documents s'avèrent d'une très grande valeur.

Les ordinateurs jouent également un rôle critique au sein des communications entre magistrats, puisque plusieurs juges se servent du courrier électronique pour communiquer avec les collègues, les clercs et les membres du personnel. Bien que certaines communications puissent être de moindre importance, les juges ont parfois recours à la communication par voie électronique dans le cadre de discussions hautement confidentielles. En outre, étant donné que plusieurs juges voyagent régulièrement pour instruire des procès dans différentes parties de leur province, la communication par voie électronique est souvent le principal moyen de communication entre les membres de la magistrature et leurs familles.

Comme le confirmeraient la plupart des juristes et étudiants en droit, la recherche juridique informatisée est devenue un élément essentiel du processus de recherche juridique. La magistrature utilise régulièrement les bases de données juridiques informatisées telles que Quicklaw, de même que les nouveaux services juridiques sur Internet, tels que l'Institut canadien d'information juridique. De plus, la recherche juridique peut englober une vaste série de documents non traditionnels, Internet donnant accès à des ressources de l'information illimitées.

b. Surveillance informatique de la magistrature au Canada

Étant donné le rôle essentiel des ordinateurs au sein de la magistrature canadienne contemporaine, les préoccupations des années 1980 semblent quelque peu banales par rapport aux questions d'aujourd'hui. Les controverses entourant la surveillance informatique des magistratures américaine et néo-zélandaise ont mieux fait connaître les répercussions de la surveillance des ordinateurs et du courrier électronique sur le respect de la vie privée, ainsi que la mesure dans laquelle les ordinateurs sont devenus un outil de travail et de communication essentiel au sein de la magistrature.

Au Canada, des préoccupations similaires sont apparues à la suite d'un sondage national confidentiel au sujet de la sécurité de la technologie judiciaire, effectué par le Comité consultatif sur l'utilisation des nouvelles technologies par les juges du CCM en novembre 2001[151]. Le sondage a été distribué à 37 juges en chef et à 35 gestionnaires des technologies de l'information au sein du système judiciaire canadien. Dans le sondage, auquel ont participé 55 répondants - soit un taux de participation élevé - on demandait au personnel de technologie de l'information de répondre à 208 questions, tandis que les juges en chef devaient répondre à 41 questions[152].

Bien que l'étude se soit surtout penchée sur les préoccupations en matière de sécurité, la question de la surveillance informatique de la magistrature a également été soulevée. Les réponses ont donné à penser qu'une telle surveillance n'était pas tout à fait absente au sein de l'appareil judiciaire canadien :

> 62 pour cent des répondants ont indiqué que les activités d'entrée et de compte des juges ou du personnel judiciaire faisaient l'objet d'une surveillance;
> 29 pour cent des répondants ont indiqué que les activités d'accès et l'utilisation du courrier électronique des juges ou du personnel judiciaire faisaient l'objet d'une surveillance;
> 33 pour cent des répondants ont indiqué que l'utilisation d'Internet par les juges ou le personnel judiciaire faisait l'objet d'une surveillance[153].

Les données se sont avérées particulièrement inquiétantes à la lumière des réponses concernant la suffisance de l'avis et la mise en oeuvre de la surveillance des ordinateurs et du courrier électronique. Seulement 50 pour cent des répondants ont indiqué qu'ils avaient été avisés de la possibilité que leurs activités informatiques fassent l'objet d'une surveillance. Par ailleurs, seulement 33 pour cent des utilisateurs ont été tenus de signer une entente d'utilisation acceptable avant d'obtenir l'accès au système informatique[154], tandis qu'un maigre cinq pour cent des répondants ont indiqué que leur écran d'accès au système apportait des précisions au sujet de l'utilisation de l'équipement informatique à laquelle on s'attendait de la part des juges et du personnel judiciaire[155]. En outre, puisque seulement 14 pour cent des répondants ont précisé que les juges ou le personnel judiciaire participaient aux activités de surveillance, il est devenu évident que la magistrature ne participait pas à la mise en oeuvre de telles activités[156].

À la lumière des conclusions du Comité consultatif sur l'utilisation des nouvelles technologies, il est essentiel que l'on examine comment mettre en place des politiques de surveillance informatique à l'endroit de la magistrature canadienne, à supposer même qu'une telle surveillance soit indiquée. L'analyse du caractère raisonnable de la surveillance des ordinateurs et du courrier électronique doit comprendre l'examen des six facteurs identifiés dans la partie trois. La plupart de ces facteurs servent à orienter l'examen des systèmes existants et la mise en oeuvre de nouveaux systèmes. On ne peut évaluer, dans l'abstrait, des facteurs tels que la suffisance de l'avis, l'identité des personnes ayant accès aux renseignements obtenus par les activités de surveillance, la technologie ayant été adoptée, les solutions de rechange ayant été étudiées, ou l'objet de la surveillance. Chaque facteur doit être examiné à la lumière des faits. Le caractère raisonnable de la politique de surveillance dépendra largement du résultat d'une telle évaluation.

Or, la magistrature accorde une importance toute particulière à l'analyse du premier des six facteurs - la cible de la surveillance. Étant donné l'importance conférée à l'indépendance judiciaire au sein d'une société libre et démocratique, il faut accorder une attention particulière à la pertinence de toute surveillance informatique des membres de la magistrature. Par ailleurs, si l'on conclut que la surveillance informatique de la magistrature peut s'avérer raisonnable dans certaines circonstances, un tel facteur aura un effet direct sur l'analyse des cinq autres facteurs, y compris sur la question de savoir si la politique de surveillance informatique devrait s'appliquer de façon égale à tous les membres de l'appareil judiciaire, ou si des distinctions devraient être établies entre les juges, les greffiers et autres membres du personnel judiciaire.

i. Indépendance judiciaire

Plusieurs sources, dont les traités internationaux et les lois canadiennes, soulignent l'importance de l'indépendance judiciaire et les répercussions potentielles de la surveillance informatique sur une telle valeur. Sur le plan international, l'art. 1.17 *b)* de la Déclaration universelle sur l'indépendance de la justice, adoptée en 1983 à la Première conférence mondiale sur

l'indépendance de la justice, prévoit que [TRADUCTION] « [l]es États et autres autorités externes respectent et protègent la confidentialité des délibérations des tribunaux, à toutes les étapes de celles-ci[157] ». Une telle disposition pourrait éventuellement s'appliquer à la surveillance informatique de la magistrature, si une telle surveillance permettait de capter des renseignements se rapportant aux délibérations des tribunaux, notamment par l'enregistrement de projets de jugement et de communications entre juges portant sur des questions liées aux délibérations. En outre, la mention des autorités externes par la disposition renforce la nécessité de limiter l'accès aux renseignements obtenus par voie de surveillance.

La Cour suprême du Canada a eu l'occasion d'étudier la question de l'indépendance judiciaire à maintes reprises. Dans l'arrêt *Valente c. La Reine*[158], le juge LeDain, s'exprimant au nom de la Cour, a souligné que la notion canadienne d'indépendance judiciaire comportait des éléments tant individuels qu'institutionnels. Il a précisé ce qui suit :

> On admet généralement que l'indépendance judiciaire fait intervenir des rapports tant individuels qu'institutionnels: l'indépendance individuelle d'un juge, qui se manifeste dans certains de ses attributs, telle l'inamovibilité, et l'indépendance institutionnelle de la cour ou du tribunal qu'il préside, qui ressort de ses rapports institutionnels ou administratifs avec les organes exécutif et législatif du gouvernement[159].

Les commentaires du juge LeDain ont été repris par la juge McLachlin dans l'arrêt *MacKeigan c. Hickman*[160], dans lequel la Cour suprême s'est penchée sur l'importance de la confidentialité des délibérations dans le cadre d'une enquête provinciale sur la condamnation injustifiée de Donald Marshall. La juge McLachlin a résumé l'état du droit canadien en réaffirmant les éléments individuels et institutionnels de l'indépendance judiciaire et en précisant que « [l]es actes des autres organes du gouvernement qui minent l'indépendance du pouvoir judiciaire nuisent donc à l'intégrité de notre Constitution. En tant que protecteurs de notre Constitution, les tribunaux ne prendront pas ces empiétements à la légère[161] ».

Il convient également de souligner l'opinion dissidente du juge Cory dans l'arrêt *MacKeigan*, dans laquelle il a traité de la question du privilège judiciaire relatif aux questions administratives. L'opinion du juge Cory démontre que l'immunité judiciaire s'étend au-delà des

activités judiciaires rattachées à l'adjudication et s'applique aux fonctions administratives telles que les conversations avec le personnel, les collègues et les clercs :

> [...] une large exemption de l'obligation de témoigner de la part des juges à l'égard de l'administration des travaux des tribunaux constitue un facteur important et nécessaire dans le fonctionnement du système judiciaire. Par exemple, il serait impensable qu'un organisme extérieur, fût-il un ministère ou un organisme gouvernemental ou encore un barreau, puisse dire quel juge entendra une affaire en particulier ou quels membres d'une cour d'appel siégeront dans un appel. Il est important que les juges jouissent d'une exemption relativement à leurs conversations avec le personnel administratif tout autant qu'avec leurs collègues et leurs clercs[162].

Les tribunaux canadiens ont appliqué l'analyse de la Cour suprême au moment d'examiner la confidentialité rattachée aux notes prises par un juge au cours d'une audience et à d'autres documents. Dans *Canada (Commissaire à la vie privée) c. Canada (Conseil des relations du travail)*[163], la Section de première instance de la Cour fédérale a examiné une demande réclamant la divulgation des notes prises par un arbitre au cours d'une audience du Conseil des relations du travail. En citant à l'appui les arrêts *Valente* et *MacKeigan*, le tribunal a précisé ce qui suit :

> [u]n juge doit pouvoir prendre des notes, libre de toute ingérence, et notamment libre de toute crainte que ces notes auront par la suite à être divulguées à des fins qui ne sont pas celles de leur auteur. Un juge doit avoir l'entière liberté de décider de ce qu'il convient de noter ou non, et être certain que personne ne pourra par la suite venir mettre en doute la sagesse de ses résolutions. [...] Or, la liberté complète de trancher ne peut exister que si le juge est complètement libre de toute immixtion par des personnes de l'extérieur, dans la manière dont il mène le procès et prend sa décision[164].

En ce qui a trait à la question de la surveillance informatique de la magistrature, la jurisprudence indique que le contenu obtenu par voie de surveillance, y compris le contenu des courriels et des documents créés par traitement de texte, doit obligatoirement bénéficier d'une confidentialité absolue. Puisque la surveillance informatique exige que les données soient d'abord captées avant qu'on puisse en déterminer la confidentialité, toute surveillance du contenu judiciaire risque d'enfreindre l'immunité judiciaire.

Ce qui précède ne signifie pas qu'aucune surveillance informatique de la magistrature n'est

possible. Bien que les programmes axés sur les clients semblent être hors de question, il se peut que les programmes axés sur les serveurs, lesquels ne font que contrôler l'utilisation du réseau, sans égard au contenu, ne portent pas atteinte à la confidentialité conférée à la magistrature. Pour que de tels programmes soient jugés acceptables, il serait nécessaire d'effectuer une analyse plus poussée des objectifs et de la mise en oeuvre de la surveillance, des solutions de rechange et de la suffisance de l'avis.

ii. Impartialité judiciaire

La question de l'indépendance judiciaire n'est pas la seule question de surveillance informatique qui préoccupe la magistrature. Puisque les juges peuvent aussi être appelés à déterminer la légalité des pratiques de surveillance informatique, la capacité des juges surveillés de trancher cette légalité de façon impartiale risque d'être remise en question, surtout lorsque les juges ont à se prononcer sur une politique de surveillance à laquelle ils sont eux-mêmes assujettis.

Fait intéressant, la Commission des relations de travail de l'Ontario (CRTO) a récemment eu l'occasion de se pencher sur les questions de l'indépendance et l'impartialité judiciaires. L'arrêt *Re Ontario (Management Board of Cabinet)*[165], une décision rendue en octobre 2001, illustre la complexité de l'adoption de politiques de surveillance permettant d'accéder aux notes privées, au courrier électronique et aux projets de jugement des arbitres. En l'espèce, l'Association des employées et employés gestionnaires, administratifs et professionnels de la couronne de l'Ontario (AEEGAPCO) alléguait que la politique en matière de technologie de l'information de l'Ontario, qui consistait à bloquer le courrier électronique entre l'AEEGAPCO et ses membres, constituait une pratique de travail injuste. Une requête présentée par l'AEEGAPCO et soutenant que la CRTO, l'organisme chargé de trancher le litige, était incapable de le faire de façon équitable, est venue compliquer l'affaire. L'AEEGAPCO a tout d'abord fait remarquer que les membres de la CRTO étaient assujettis aux politiques mêmes faisant l'objet du litige. Ensuite, fait encore plus important, l'AEEGAPCO a souligné que [TRADUCTION] « la couronne a la capacité technique [...] et revendique le droit de surveiller les notes privées, le courrier électronique et les projets de

jugement des arbitres de la Commission et d'y accéder[166] ». Ainsi, selon l'AEEGAPCO, la Commission [TRADUCTION] « ne contrôlait pas les décisions administratives ayant un effet important sur ses délibérations et, par conséquent, n'était pas suffisamment indépendante de la couronne[167] ».

La couronne s'est opposée à la requête en soutenant que, bien qu'elle disposât de la capacité technique d'accéder aux notes, à la correspondance et aux projets de jugement, une telle surveillance serait répréhensible et contraire à ses pratiques en matière de technologie de l'information[168]. La couronne a présenté une lettre de son conseil donnant plus de détails au sujet de sa capacité technique et de sa politique de surveillance officielle. Dans la lettre, la couronne a reconnu qu'elle avait la capacité technique d'examiner les projets de jugement et notes informatisés, de même que la correspondance interne et externe. Toutefois, elle a soutenu qu'une telle surveillance n'était ni envisagée ni autorisée par les politiques du ministère. Dans la lettre, la couronne a également cherché à assurer la Commission que la vérification potentielle de l'utilisation des réseaux informatiques ne s'appliquerait pas aux fichiers texte et nécessiterait une double approbation afin que le personnel de la Commission puisse participer au processus[169].

La Commission a tranché en faveur de la couronne et rejeté les deux allégations de l'AEEGAPCO, mais seulement après s'être engagée dans un débat intéressant, notamment sur la question de savoir si la capacité de surveillance de la couronne entravait la capacité de la Commission de fonctionner de façon suffisamment indépendante. Quant aux préoccupations relatives à l'impartialité découlant du fait qu'elle était assujettie à la même politique en matière de technologie de l'information de l'Ontario, la Commission a conclu que [TRADUCTION] « les décideurs créent une jurisprudence ayant un certain effet durable sur le paysage juridique. En tant que citoyens de la province, il se peut que les arbitres soient un jour visés par les changements au paysage juridique qu'ils ont aidé à façonner. Cependant, la possibilité d'être visé par une décision n'empêche pas les juges d'instruire une affaire[170] ».

Les répercussions de la surveillance informatique sur l'indépendance institutionnelle ont

présenté un défi plus épineux. Bien que la Commission ait conclu que les données susceptibles d'être obtenues par voie de surveillance faisaient partie intégrante de la confidentialité des délibérations, elle a en bout de ligne été rassurée par la politique déclarée de la couronne, selon laquelle celle-ci s'engageait à ne pas effectuer de surveillance ou à ne se livrer à de telles activités qu'à condition d'y faire participer la haute direction de la Commission. Toutefois, la Commission a tenu compte de l'arrêt *Ocean Port Hotel Ltd. c. Colombie-Britannique (General Manager, Liquor Control and Licensing Branch)*[171], une décision récente de la Cour suprême du Canada dans laquelle celle-ci a établi une distinction entre le degré d'indépendance accordé aux tribunaux administratifs et celui dont jouissent les tribunaux judiciaires.

Dans l'affaire *Ocean Port Hotel*, l'indépendance d'une commission d'appel des permis d'alcool provinciale a été contestée. La Cour d'appel de la Colombie-Britannique a conclu que les commissaires n'avaient pas les garanties d'indépendance requises pour des décideurs habilités à prononcer des peines et a annulé la décision de la commission. La Cour suprême a infirmé la décision, en précisant que la loi habilitante définissait clairement les paramètres relatifs à la nomination des commissaires et qu'il n'y avait donc pas lieu d'importer les théories de common law en matière d'indépendance. La Cour suprême a fondé sa décision sur la distinction entre, d'une part, les commissions et tribunaux administratifs et, d'autre part, les tribunaux judiciaires. Dans des motifs unanimes, la juge en chef McLachlin a souligné ce qui suit:

> Du fait de leur compétence inhérente, les cours supérieures sont constitutionnellement tenues d'offrir des garanties objectives d'indépendance institutionnelle et individuelle. Le même impératif constitutionnel s'applique aux tribunaux provinciaux. Par contre, les tribunaux administratifs ne sont pas constitutionnellement séparés de l'exécutif. Ils sont en fait créés précisément en vue de la mise en oeuvre de la politique gouvernementale. Pour remplir cette fonction, ils peuvent être appelés à rendre des décisions quasi judiciaires. Toutefois, vu que leur fonction première est d'appliquer des politiques, il appartient à bon droit au Parlement et aux législatures de déterminer la composition et l'organisation qui permettront aux tribunaux administratifs de s'acquitter des attributions qui leur sont dévolues. Même si certains tribunaux administratifs peuvent parfois être assujettis aux exigences de la *Charte* relatives à l'indépendance, ce n'est généralement pas le cas.[172]

À la lumière de l'affaire *Ocean Port Hotel*, la décision de la Commission a laissé entendre qu'une politique de surveillance bien conçue pourrait offrir une protection adéquate aux tribunaux,

mais non aux cours. En outre, la décision de la Commission a laissé sous-entendre qu'en l'absence de protections adéquates, la surveillance informatique d'un organisme ayant un pouvoir décisionnel, qu'il s'agisse d'un tribunal ou d'une cour, porterait atteinte à la confidentialité des délibérations et minerait l'indépendance institutionnelle de l'organisme.

iii. Secret judiciaire

Outre les facteurs relatifs à l'indépendance et l'impartialité judiciaires, les facteurs se rapportant au secret judiciaire doivent également faire partie de

l'analyse. Bien que la confidentialité des délibérations et des communications judiciaires soit essentielle à l'indépendance de la magistrature, les membres du personnel judiciaire obtiennent souvent accès à des renseignements que la loi considère strictement confidentiels.

Par exemple, la *Loi sur les jeunes contrevenants* du Canada[173] prévoit une série de dispositions exigeant la confidentialité presque absolue en ce qui a trait à l'identité d'une personne accusée aux termes de la *Loi*[174]. La *Loi* prévoit des dispositions particulières imposant des restrictions à la communication de renseignements[175], établissant des limites relativement à l'accès aux renseignements[176] et exigeant même la destruction des renseignements dès qu'ils ne sont plus nécessaires aux fins auxquelles ils ont été communiqués[177].

Dans le même ordre d'idées, les dispositions du *Code criminel* relatives à la surveillance électronique prévoient elles aussi de strictes exigences en matière de confidentialité[178]. La législation canadienne anti-terrorisme récemment adoptée impose à la magistrature plusieurs nouvelles exigences en matière de confidentialité. La législation modifie la *Loi sur la preuve* du Canada[179] en créant de nouvelles restrictions qui s'appliquent à la communication de renseignements lors d'une procédure judiciaire[180].

Étant donné que la magistrature se voit souvent confier des renseignements de nature hautement délicate, les exigences en matière de confidentialité ci-haut pourraient restreindre encore davantage la capacité juridique de surveiller l'utilisation des ordinateurs par la magistrature et de procéder à la collecte de tels renseignements. Par exemple, si un gestionnaire des systèmes accédait à des renseignements assujettis à la *Loi sur les jeunes contrevenants*, il risquerait d'enfreindre les limites relatives à l'accès prévues par la loi. Bien que les exigences en matière de confidentialité n'interdisent pas de façon absolue la surveillance informatique de la magistrature, elles rendent encore plus complexe une question déjà difficile.

iv. Recommandations

D'après les conventions internationales et la jurisprudence canadienne, la surveillance des ordinateurs et du courrier électronique de la magistrature n'est autorisée par la loi que dans des circonstances très limitées. Toute surveillance portant atteinte à la confidentialité des délibérations serait intrinsèquement illégale. Y serait incluse l'utilisation de programmes de surveillance axés sur les clients, tels que les programmes enregistreurs de frappes pouvant capter tous les renseignements entrés dans un ordinateur personnel, dont la correspondance, les projets de jugement et d'autres documents protégés. Les programmes de surveillance axés sur les serveurs pourraient être autorisés par la loi, sous réserve de limites très rigoureuses. Tel que constaté dans l'arrêt *Re Ontario (Management Board of Cabinet)*, la mise en oeuvre de tels programmes de surveillance nécessiterait des protections rigoureuses, y compris des limites relatives à l'accès aux renseignements obtenus par voie de surveillance, un système de notification clair et efficace, l'examen de solutions de rechange moins intrusives, ainsi qu'un objectif valable qui ne viole pas les protections visant à garantir l'indépendance judiciaire.

Dans le nouveau cadre législatif canadien de la surveillance en milieu de travail, les limites imposées à la surveillance de la magistrature sont renforcées par une évaluation des six facteurs se rapportant au caractère raisonnable. Puisque le facteur de la cible exclut la plupart

des formes de surveillance informatique, les possibilités de surveillance raisonnable sont limitées, les cinq autres facteurs étant évalués à la lumière d'un seuil élevé au-delà duquel la surveillance est jugée raisonnable. Parmi les limites rigoureuses susceptibles de s'appliquer à la surveillance informatique de la magistrature, on compte notamment celles qui suivent :

> La surveillance licite de la magistrature devrait avoir un objectif bien défini excluant la surveillance du contenu, sous risque de porter atteinte à la confidentialité des délibérations. Étant donné l'utilisation répandue des ordinateurs par la magistrature, les objectifs acceptables se limiteraient aux questions reliées au rendement du réseau, lesquelles peuvent englober les menaces externes à la sécurité du réseau. Puisque l'examen du rendement du réseau se fonde sur des renseignements cumulatifs se rapportant aux tendances générales en matière d'utilisation du réseau, il ne nécessite ni l'identification d'utilisateurs particuliers ni la surveillance de renseignements confidentiels ou de nature délicate.
>
> Les administrateurs devraient avant tout chercher à identifier des solutions de rechange à la surveillance informatique. Les questions liées au rendement du réseau devraient tout d'abord être abordées par le biais de programmes de sensibilisation, afin que les juges et leur personnel soient convenablement sensibilisés à l'égard des questions qui préoccupent le personnel de technologie de l'information.
>
> Si la surveillance doit se limiter au rendement du réseau, les systèmes de surveillance axés sur les clients sont susceptibles de porter atteinte à l'indépendance judiciaire. L'installation de systèmes de surveillance axés sur les serveurs semble donc être la seule solution possible à l'heure actuelle.
>
> En règle générale, la surveillance de la magistrature visant le contenu devrait être évitée en raison des préoccupations relatives à la confidentialité des délibérations. Toutefois, une exception pourrait être faite s'il existait des motifs raisonnables de croire qu'un acte criminel était en voie d'être commis.
>
> Les juges et le personnel judiciaire devraient être informés des pratiques de surveillance par voie d'avis précis, évidents et cohérents. Sont nécessaires la notification des politiques d'utilisation des ordinateurs, au moment d'entrer dans le système informatique du système judiciaire, de même que des rappels réguliers, pendant les sessions, au sujet des politiques existantes et de leurs répercussions sur l'utilisation des ordinateurs au sein de la magistrature.
>
> Les juges et leur personnel doivent également participer activement à

l'administration d'un système de surveillance offrant un accès externe limité aux renseignements. L'expérience néo-zélandaise illustre l'impact que peuvent avoir les renseignements de nature délicate portant sur la conduite des juges au niveau de la confiance du public dans le système judiciaire.

Les juges et le personnel judiciaire doivent participer à l'élaboration et à la mise en place de tout programme de surveillance, en collaboration avec le personnel de technologie de l'information, lequel administre le programme et fait rapport directement au juge en chef.

∗ Les vues exprimées dans le présent document sont celles de l'auteur et ne correspondent pas nécessairement à celles de l'Université d'Ottawa ou de Goodmans LLP.

[1] Information and Privacy Commissioner for British Columbia, Investigation P98-012, Video Surveillance by Public Bodies: A Discussion (31 mars 1998).

[2] S. Shankland, « Study: Web, e-mail monitoring spreads », *CNet* (8 juillet 2001), en ligne : http://news.com.com/2100-1001-269584.html (date d'accès : 20 janvier 2002).

[3] American Management Association, communiqué de presse, « More Companies Watching Employees, American Management Association Annual Survey Reports » (18 avril 2001), en ligne : http://www.amanet.org/press/amanews/ems2001.htm (date d'accès : 19 janvier 2002) [ci-après « communiqué de presse de l'AMA »].

[4] *Ibid.*

[5] L. Keller, « Monitoring employees: Eyes in the workplace », *CNN.com* (2 janvier 2001), en ligne : http://www.cnn.com/2001/CAREER/trends/01/02/surveillence/ (date d'accès : 20 janvier 2002).

[6] N. A. Lewis, « Monitoring of Judiciary Computers is Backed », *New York Times* (14 août 2001).

[7] M. Dolan, « Defiant Judges Bar Monitoring of Staff Net Use », *Los Angeles Times* (9 août 2001).

[8] N. A. Lewis, « Plan for Web Monitoring in Courts Dropped », *New York Times* (9 septembre 2001).

[9] V. Small, « Four Judges Logged on to Sex Sites », *New Zealand Herald* (19 février 2002), en ligne : <http://nzherald.co.nz/storydisplay.cfm?storyID=940048> (date d'accès : 22 février 2002).

[10] *Ibid.*

[11] « Cabinet to Discuss Sex-Site Judge », *New Zealand Herald* (18 février 2002), en ligne : <http://www.nzherald.co.nz/storydisplay.cfm?storyID=939890> (date d'accès : 22 février 2002).

[12] « District Court Judges Innocent in Visiting Sex Sites, says Minister », *New Zealand Herald* (19 février 2002), en ligne : <http://www.nzherald.co.nz/storydisplay.cfm?storyID=940107> (date d'accès : 22 février 2002).

[13] V. Small, « Porn Inquiry Clears Judge », *New Zealand Herald* (20 février 2002), en ligne : <http://www.nzherald.co.nz/storydisplay.cfm?storyID=940245> (date d'accès : 22 février 2002).

[14] Communiqué de presse de l'AMA, précité, note 3.

[15] En fait, les programmes de surveillance pourraient être les moins coûteux d'un système informatique. Par exemple, Surf Control, un programme qui surveille l'utilisation des ordinateurs par les employés, se vend à 39,95 $. R. Konrad et S. Ames, « Web-based e-mail services offer employees little privacy », *CNet* (3 octobre 2000), en ligne : http://news.cnet.com/news/0-1007-200-2924978.html (date d'accès : 19 janvier 2002).

[16] E. J. Sinrod, « Electronic surveillance in the workplace », *USAToday.com* (18 octobre 2001), en

ligne : http://www.usatoday.com/life/cyber/ccarch/2001/10/18/sinrod.htm (date d'accès : 19 janvier 2002).

[17] H. Chen, « Internet Use Survey 2000 -- Trends and Surprises in Workplace Web Use », *Vault.com* (1er septembre 2000), en ligne : http://vault.com/nr/main_article_detail.jsp?article_id=19331 (date d'accès : 19 janvier 2002).

[18] *Ibid.*

[19] S. Chu, « Workers Waste 800 Million Hours on Web », *The Globe and Mail* (6 juillet 2000).

[20] *Ibid.*

[21] M. Seminerio, « Content filters don't just spy risqué surfing », *ZDNet* (29 novembre 1999), en ligne : <http://techupdate.zdnet.com/techupdate/stories/main/0,14179,2398149,00.html> (date d'accès : 19 janvier 2002).

[22] M. Street, « Filtering speeds up traffic », *IT Week* (15 octobre 2001), en ligne : <http://www.surfcontrol.com/general/articles/Virginairship_IT_Week_Reprint_1001.pdf> (date d'accès : 19 janvier 2002).

[23] H. Harreld, « And forgive us our trespasses », *Federal Computer Week* (5 février 2001), en ligne : http://www.fcw.com/fcw/articles/2001/0205/mgt-filter-02-05-01.asp (date d'accès : 19 janvier 2002).

[24] Communiqué de presse de l'AMA, précité, note 3.

[25] D. Hawkins, « Who's watching now? Hassled by lawsuits, firms probe workers' privacy », *USNews.com* (15 septembre 1997), en ligne : http://www.usnews.com/usnews/nycu/tech/articles/970915/15priv.htm (date d'accès : 19 janvier 2002).

[26] Chen, précité, note 17.

[27] B. Wallace et J. Fenton, « Analysis: Your PC could be watching you », *CNN.com* (15 novembre 2000), en ligne : http://www.cnn.com/2000/TECH/computing/11/15/desktop.tracker.idg/index.html (date d'accès : 19 janvier 2002).

[28] « Dow Chemical Fires 50 Over E-mail Abuse », *USA Today* (28 juillet 2000), en ligne : http://www.usatoday.com/life/cyber/tech/cti298.htm . Parmi les autres grandes sociétés ayant congédié des employés pour utilisation inopportune des ordinateurs au travail, on compte notamment Xerox, qui a congédié 40 employés pour utilisation inappropriée d'Internet au travail, ainsi que le New York Times, qui a congédié 23 employés pour avoir envoyé des courriels potentiellement offensants sur les ordinateurs de la société. Voir W. Blitzer, « More employers taking advantage of new cyber-surveillance software », *CNN.com* (10 juillet 2000), en ligne : http://www.cnn.com/2000/US/07/10/workplace.eprivacy/ (date d'accès : 19 janvier 2002).

[29] [2000] D.A.T.C. no 15.

[30] (1996), 21 C.C.E.L. (2d) 137 (C.S. C.-B.).

[31] R. Konrad, « Leaks and geeks: International espionage goes high-tech », *CNet* (21 septembre 2000), en ligne : http://news.com.com/2100-1001-242620.html (date d'accès : 20 janvier 2002).

[32] R. Konrad et S. Ames, précité, note 15.

[33] [2000] O.J. no 842.

[34] Wallace et Fenton, précité, note 27.

[35] Sinrod, précité, note 16.

[36] [1998] O.J. no 4971.

[37] Public Law 104-191.

[38] A. Schulman, « Computer And Internet Surveillance in the Workplace: Rough Notes », en ligne : http://www.sonic.net/~undoc/survtech.htm (dernière modification : 12 juillet 2001) (date d'accès : 4 mars 2002).

[39] *Ibid.*
[40] *Ibid.*
[41] *Ibid.*
[42] C. E. Dalton, « Special Report -- Preventing Corporate Network Abuse Gets Personal », *Network Magazine* (5 février 2001), en ligne : http://www.networkmagazine.com/article/NMG20010126S0003/1 (date d'accès : 13 janvier 2002).
[43] Harreld, précité, note 23.
[44] Electronic Privacy Information Center, « EPIC Workplace Privacy Page », en ligne : http://epic.org/privacy/workplace/default.html (dernière modification : 8 janvier 2002) (date d'accès : 4 mars 2002).
[45] Konrad et Ames, précité, note 15.
[46] Schulman, précité, note 38.
[47] A. Schulman, « Fatline & AltaVista: "Peer Pressure" Employee Monitoring? », *Privacy Foundation: Workplace Surveillance Project* (18 juin 2001), en ligne : http://www.privacyfoundation.org/workplace/technology/tech_show.asp?id=69&action=0 (date d'accès : 19 janvier 2002).
[48] *Ibid.*
[49] Schulman, précité, note 38.
[50] *Ibid.*
[51] *Ibid.*
[52] *Ibid.*
[53] B. W. Gall, « Company E-mail and Internet Policies », *GigaLaw.com* (janvier 2000), en ligne : http://www.gigalaw.com/articles/gall-2000-01-p1.html (date d'accès : 19 janvier 2002).
[54] S. King, « Digital Workplace Privacy - Protect Yourself », *Emergit.com* (19 février 2001), en ligne : http://www.emergit.com/html/content_cur/profiles/02-19-2001_privacy.jsp (date d'accès : 19 janvier 2002).
[55] Dalton, précité, note 42.
[56] Wallace et Fenton, précité, note 27.
[57] B. MacIssac, R. Shields et K. Klein, *The Law of Privacy in Canada*, Butterworths, 2000 aux pp. 2-82.
[58] Emond Harnden, « Office E-mail: No Reasonable Expectation of Privacy » (2000), 4(3) *FOCUS: Employment Law* à la p. 7, en ligne : http://www.emond-harnden.com/apr00/camo.html .
[59] C. Morgan, « Employer Monitoring of Employee Electronic Mail and Internet Use » (1999), 44 *McGill L.J.* 849.
[60] A. Rogers, « You Got Mail But Your Employer Does Too: Electronic Communication and Privacy in the 21st Century Workplace » (2000), 5 *Journal of Technology Law and Policy* 1.
[61] 914 F.Supp. 97 (E.D. Pa. 1996).
[62] *Ibid.* à la p. 101.
[63] *Ibid.* aux pp. 100 et 101.
[64] *Bourke v. Nissan Motor Corp.*, No. B068705 (Cal. Ct. App.) (26 juillet 1993).
[65] 29 F.Supp.2d 324 (E.D. Va. 1998).
[66] Pub. L. 89-508 (1996).
[67] *Ibid.*, art. 2511(1).
[68] *Ibid.*, art. 2510(12).
[69] *Ibid.*, art. 2510(12)(a).
[70] *Ibid.*, art. 2511(2)(d).
[71] *Ibid.*, art. 2511(2)(a)(i).

[72] 704 F.2d 577 (11th Cir. 1983).
[73] *Ibid*. à la p. 581.
[74] *Bohach v. City of Reno*, 932 F. Supp. 1232 (D. Nev. 1996).
[75] Watkins, précité aux pp. 582-585.
[76] Criminal Action No. 00-404 (NHP) (D. N.J. 2001), en ligne : <http://lawlibrary.rutgers.edu/fed/html/scarfo2.html-1.html>.
[77] *Ibid.*
[78] L.R.C. 1985, ch. C-46, par. 184(1).
[79] *Ibid.*, art. 183.
[80] *Ibid.*
[81] Voir la partie deux *b)* ci-dessous.
[82] (1998), 213 A.R. 285; [1998] 8 W.W.R. 228.
[83] 50 W.C.B. (2d) 463.
[84] L.R.C. 1985, ch. C-46, par. 184(2).
[85] Morgan, précité, note 59 au par. 79.
[86] L.R.C. 1985, ch. C-46, al. 184(2)*c)*.
[87] Morgan, précité, note 59 au par. 87.
[88] 236 F. Supp. 1035 (9th Cir. 2001).
[89] McCutchen Update: Electronic Communications Monitoring in the Spotlight, en ligne : <http://www.mccutchen.com/are/ecomm/konop_hawaiian_airlines_update.htm> (date d'accès : 10 février 2001).
[90] Report of the General Counsel: September 1999 – September 2000, NLRB Office of the General Counsel, en ligne : <http://www.lawmemo.com/emp/nlrb/gc2000.htm> (date d'accès : 13 décembre 2001).
[91] *Ibid.*
[92] California Legislative Summary 2001, en ligne : <http://www.dir.ca.gov/OD_pub/2001Summary.htm#sb147> (date d'accès : 10 février 2002).
[93] *Ibid.*
[94] L.C. 2000, ch. 5.
[95] *Ibid.*, art. 3.
[96] *Ibid.*, par. 5(3).
[97] *Ibid.*, annexe 1, principe 4.1.
[98] *Ibid.*, annexe 1, principe 4.2.
[99] *Ibid.*, annexe 1, principe 4.3.
[100] *Ibid.*, annexe 1, principe 4.4.
[101] *Ibid.*, al. 7(1)*b)*.
[102] *Ibid.*, annexe 1, principe 4.7.
[103] *Ibid.*, annexe 1, principe 4.5.
[104] L.R.C. 1985, ch. P-21.
[105] *Ibid.*, art. 2.
[106] L.R.C. 1985, ch. R-2.
[107] *Ibid.*, par. 9(2).
[108] L.C. 1993, ch. 38.
[109] *Ibid.*, art. 7(i).
[110] L.C. 1991, ch. 46.
[111] L.C. 1993, ch. C-10.
[112] [1999] B.C.J. n° 2772.
[113] *Ibid.*, par. 26.

[114] 13 L.A.C. (4th) 275.
[115] [1990] 1 R.C.S. 945.
[116] *Ibid.* à la p. 279.
[117] *Ibid.* à la p. 280.
[118] *Ibid.* à la p. 282.
[119] Voir, par ex., *Re Alberta Wheat Pool and G.W.U., Loc. 333 (Gould)* (1995), 48 L.A.C. (4th) 332 (Williams); *Re Pacific Press Ltd. and Vancouver Printing Pressmen, Assistants and Offset Workers' Union, Loc. 25 (Dales)* (1997), 64 L.A.C. (4th) 1 (Devine); *Re Toronto Transit Commission and A.T.U., Loc. 113 (Adams)* (1997), 61 L.A.C. (4th) 218 (Saltman); *Re Labatt Ontario Breweries (Toronto Brewery) and Brewery, General and Professional Workers' Union, Loc. 304* (1994), 42 L.A.C. (4th) 151 (Brandt) et *Re Toronto Star Newspapers Ltd. and Southern Ontario Newspaper Guild, Loc. 87* (1992), 30 L.A.C. (4th) 306 (Springate).
[120] 64 L.A.C. (4th) 382.
[121] *Ibid*. à la p. 399.
[122] 95 L.A.C. (4th) 402.
[123] *Ibid.* à la p. 426.
[124] 85 L.A.C. (4th) 304.
[125] L.C. 2000, ch. 5, par. 11(1).
[126] Rapport annuel 2000-2001 du Commissaire à la protection de la vie privée du Canada, en ligne : <http://www.privcom.gc.ca/information/ar/02_04_09_f.asp> (date d'accès : 4 janvier 2002).
[127] *Ibid.* aux pp. 38 et 39.
[128] *Ibid.*
[129] *Ibid.*
[130] G. Radwanski, « Le respect de la vie privée à l'ère d'Internet "Workplace Privacy in the Age of the Internet », Centre des relations industrielles de l'Université de Toronto et Lancaster House Publishing, 5e Conférence annuelle sur l'arbitrage en relations de travail, Toronto (2 novembre 2001), en ligne : <http://www.privcom.gc.ca/speech/02_05_a_01102_f.asp>.
[131] *Ibid.*
[132] Voir, par ex., *Smyth v. Pillsbury Co.*, précité, note 61.
[133] M. O'Donoghue, « Reasonableness in the Context of Workplace Privacy », allocution prononcée à la conférence Infonex sur la protection de la vie privée en milieu de travail, Toronto (25 juin 2001).
[134] 64 L.A.C. (4th) 382 à la p. 399.

[135] 78 L.A.C. (4th) 394.
[136] *Ibid.*, par. 36.
[137] Chief Judge Mary M. Schroeder, « Clarification of AO Correspondence on Intrusion Detection System Shutdown », note de service du 11 juillet 2001 à la p. 4 (copie chez l'auteur).
[138] Lettre du juge Edith Jones adressée à l'honorable Edwin L. Nelson, président du comité CAT (18 août 2001) à la p. 3 (copie chez l'auteur).
[139] Avis du groupe de travail « article 29 » sur le traitement des données à caractère personnel dans le contexte professionnel, 5062/01/EN/Final, WP 48, adopté le 13 septembre 2001, en ligne : <http://europa.eu.int/comm/internal_market/en/dataprot/wpdocs/wp48fr.pdf>.
[140] *Ibid.* à la p. 4.
[141] Australian Office of the Privacy Commissioner, Guidelines on Workplace E-mail, Web Browsing and Privacy (30 mars 2000), en ligne : <http://www.privacy.gov.au/internet/email/index.html>.
[142] Schroeder, précité, note 137.
[143] Flaherty, précité, note 1.
[144] P. S. Millar et C. Baar, *Judicial Administration in Canada*, McGill – Queen's University Press,

1981.
[145] M. Felsky, *Computers and Law for Judges*, 1986 Canadian Judicial Council Superior Court Judges Seminar (30 avril 1986) à la p. 1.
[146] Millar et Baar, précité, note 143 à la p. 286.
[147] Felsky, précité, note 144 à la p. 18.
[148] B. Franson, « The Use of Computers By Federally Appointed Judges, 1988 », *Computer News for Judges*, vol. 1 (automne 1988) à la p. 2.
[149] *Ibid.*
[150] Sondage informel mené par J. Jordan (mars 2002) (copie chez l'auteur).
[151] Court Technology Security: A Report of the Judges Technology Advisory Committee to the Canadian Judicial Council (30 novembre 2001) (copie chez l'auteur).
[152] *Ibid.* à la p. 2.
[153] *Ibid.*, tableaux 2-27.
[154] *Ibid.*, tableaux 2-18.
[155] *Ibid.*, tableaux 2-27.
[156] *Ibid.*
[157] *Judicial Independence: The Contemporary Debate* dans S. Shetreet et J. Deschenes, éd., Martinus Nijhoff Publishers, Dordrecht, 1985, p.449.
[158] [1985] 2 R.C.S. 673.
[159] *Ibid*. à la p. 687.
[160] [1989] 2 R.C.S. 796.
[161] *Ibid.* à la p. 829.
[162] *Ibid.*, par. 91 et 94.
[163] [1996] 3 C.F. 609.
[164] *Ibid.*, par. 68 et 69.
[165] [2001] O.L.R.D. n^{o} 3934.
[166] *Ibid.*, par. 2.
[167] *Ibid.*
[168] *Ibid.*, par. 5.
[169] *Ibid.*
[170] *Ibid.*, par. 29.
[171] [2001] A.C.S. n^{o} 17.
[172] *Ibid*., par. 23 et 24.
[173] L.R.C. 1985, ch. Y-1.
[174] *Ibid*., art. 38.
[175] *Ibid*., art. 38 (1.14).
[176] *Ibid*., art. 38 (1.15*b)*).
[177] *Ibid*., art. 38 (1.15*c)*).
[178] L.R.C. 1985, ch. C-46, art. 187.
[179] L.R.C. 1985, ch. C-5.
[180] Projet de loi C-36, art. 37.