

L'INTERNET EN MILIEU DE TRAVAIL ET LES POLITIQUES ET DIRECTIVES RELATIVES À L'UTILISATION DES NOUVELLES TECHNOLOGIES

Karl Delwaide*

INTRODUCTION

Selon une étude d'Ispos-Reid publiée en juin 2001¹, 400 millions de personnes utilisent l'Internet dans le monde. Sur ces 400 millions d'internautes, près de 70% se trouvent en Amérique du nord.

L'accès à l'Internet et l'utilisation du courrier électronique («courriel») constituent désormais des moyens de communication communément utilisés en milieu de travail. Un sondage mené en 1998 par Forrester Research inc. a fait ressortir que 98% des compagnies qui emploient plus de 1000 employés fournissent des accès Internet à leurs employés tandis que cette proportion est de 45% dans les entreprises qui emploient de 20 à 99 employés². Ce réseau possède plusieurs avantages, qu'ils soient de nature à augmenter l'efficacité des entreprises en reliant rapidement entre eux les divers intervenants du marché ou encore par l'ouverture aux entreprises d'un immense réservoir de données de toutes sortes. D'ailleurs, selon Statistiques Canada, la valeur du commerce électronique au Canada en 1999 s'est élevée à 4,4 milliards de dollars.³

Mais l'introduction des nouvelles technologies en milieu de travail a aussi soulevé plusieurs questions d'ordre juridique relativement à la responsabilité civile de l'entreprise, au maintien de la qualité de l'environnement de travail, à la protection des informations de l'entreprise de même qu'au maintien de son «image» dans la communauté, cette image étant souvent garante de succès commerciaux.

La protection des intérêts de l'employeur sous ces divers aspects soulève plusieurs questions quant à son droit de contrôler et de surveiller l'utilisation d'Internet et du courriel par ses employés et quant à son droit d'accès à cette correspondance électronique.

Il est donc d'une importance primordiale pour les entreprises de connaître, en plus des moyens technologiques leur permettant de contrôler l'utilisation des outils de travail, leurs droits face aux situations qui peuvent survenir dans le cadre de cette utilisation. Les nouvelles technologies de l'information n'évoluent pas dans un vide juridique. L'arrivée de ces nouvelles technologies n'a

* Associé principal chez Fasken Martineau DuMoulin, s.r.l., LL.B et M.C.L. (1982), University of San Diego. L'auteur remercie très sincèrement M. Jean-François de Rico et Mme Isabelle Durand pour leur collaboration à la préparation et à la rédaction de ce texte.

¹ Citée dans le numéro d'octobre 2001 de Québec Science, dans l'article *Internet, génération X*, p. 36, à la p. 38, les résultats de cette étude se retrouvent sur le site internet : http://www.angusreid.com/us/services/little_net_book.cfm

² <http://www.mlb.com/le0699.htm>.

³ Statistiques Canada, 10 août 2000; <http://www.statcan.ca>.

pas transformé du tout au tout les principes juridiques déjà établis. À titre d'exemple, pour expliquer sa position à l'effet qu'il ne réglementerait pas (pour l'instant) les services des nouveaux médias sur Internet, le *Conseil de la Radiodiffusion et des Télécommunications Canadiennes* («CRTC») a souligné ce qui suit :

«Il existe des outils plus adéquats que la réglementation du Conseil pour régler les problèmes de contenu offensant ou illégal sur Internet, comme par exemple Le Code criminel canadien, la Charte des droits et libertés, l'autoréglementation de l'industrie, divers logiciels de filtrage du contenu et une sensibilisation accrue aux médias⁴.»

En principe, l'utilisation d'Internet est soumise aux lois d'application générale. Nul besoin de réinventer la roue, il s'agit plutôt d'adapter les principes généraux connus en droit à la réalité des nouvelles technologies. Les principes généraux du droit commun, que ce soit en matière de responsabilité civile ou en matière de contrats d'emploi ou de services, devront être appliqués à l'utilisation des technologies de l'information. De plus, l'application de ces principes devra être modulée pour tenir compte de la *Loi concernant le cadre juridique des technologies de l'information*⁵ lorsqu'elle entrera en vigueur.

Par notre analyse, nous ferons ressortir que les tribunaux tentent généralement d'établir, à la lumière des faits en cause, un équilibre entre les droits de l'entreprise et ceux de ses employés. Cet équilibre se dégagera des intérêts sérieux et légitimes qui s'affrontent de même que de la manière dont une partie entend les exercer.

C'est ainsi qu'en regard de l'utilisation d'Internet et du courriel, nous examinerons, dans un premier temps, les principes du pouvoir de gérance d'un employeur et ce, à la lumière des intérêts légitimes que celui-ci possède sur les différentes facettes de la gestion et de l'exploitation de son entreprise. À ce chapitre, nous étudierons plus particulièrement les questions relatives aux intérêts légitimes de l'employeur à obtenir une prestation de travail adéquate, à se protéger contre des recours ou réclamations en matière de diffamation, de harcèlement, d'utilisation non autorisée de documents ou informations protégés par des droits d'auteur et, aussi, ces questions relatives à la protection que toute entreprise désire accorder aux informations financières ou commerciales la concernant. D'un autre côté, ces intérêts légitimes à la protection de l'entreprise seront contrebalancés par les intérêts légitimes des employés au chapitre de l'interdiction d'intercepter une communication privée, des attentes raisonnables de protection d'une sphère de vie privée (même en milieu de travail), au maintien de la protection de la dignité des employés, de même qu'au maintien de conditions raisonnables d'emploi.

⁴ Conseil de la Radiodiffusion et des Télécommunications Canadiennes, Communiqué du 17 mai 1999.

⁵ P.L. 161; sanctionné le 21 juin 2001, mais pas encore en vigueur. Les dispositions de cette loi entreront en vigueur à la date ou aux dates fixées par le gouvernement (art. 105).

Nous terminerons avec ce qui semble faire consensus chez les auteurs qui se sont penchés sur cette problématique : la nécessité pour l'entreprise de se doter d'une politique et de directives claires quant aux paramètres d'utilisation d'Internet et du courriel par ses employés. Nous dégagerons d'une façon générale les paramètres idéaux de telles politiques et directives, lesquelles viendront encadrer d'une façon claire et transparente le droit de l'employeur d'accéder légalement et sans reproche au courriel de ses employés.

1. Le droit de l'employeur de contrôler et surveiller l'utilisation d'Internet et du courriel au sein de son entreprise

L'édition du 8 mai 1999 du *Philadelphia Inquirer* rapportait qu'un employé de la *FCC* (Federal Communication Commission) avait malencontreusement fait parvenir une blague à connotation sexuelle aux 6000 destinataires de la «mailing list» de l'organisme au lieu de l'envoyer à un ami. Cet incident met en relief l'ampleur des risques reliés à l'introduction d'Internet et du courriel en milieu de travail. L'employeur voudra donc encadrer l'utilisation de ces outils de travail. Il voudra ainsi éviter que ses employés utilisent ces instruments pour des motifs qui seraient contraires au contrat de travail, à la convention collective ou à la loi.

Le contexte de l'emploi se caractérise par une relation de subordination d'un salarié face à un employeur. L'article 2085 du *Code civil du Québec* («C.c.Q.») est explicite à cet effet :

«2085. Le contrat de travail est celui par lequel une personne, le salarié, s'oblige pour un temps limité et moyennant rémunération, à effectuer un travail sous la direction ou le contrôle d'une autre personne, l'employeur.»

L'employeur a donc généralement le droit de gérer et d'administrer son entreprise comme bon lui semble. Il peut également, de ce fait, exercer un contrôle sur le travail de ses employés. Ces pouvoirs doivent toutefois s'exercer en tenant compte des limites imposées par la loi.

L'employeur exercera ce pouvoir de contrôle pour s'assurer de la qualité et de la quantité de la prestation de travail qu'il reçoit de ses employés. Il pourra aussi se prévaloir de ce droit pour protéger son entreprise de l'utilisation illégitime, illégale et dommageable d'Internet et du courriel par ses employés.

(1.1) Se prémunir contre une baisse de productivité

L'implantation des nouvelles technologies en milieu de travail vise certainement, au premier chef, à doter l'entreprise et ses employés de ressources toujours plus adéquates et puissantes pour améliorer la performance globale de l'entreprise. En principe, l'implantation des nouvelles technologies et l'accès à Internet viseraient à obtenir une hausse tant qualitative que quantitative de la productivité résultant de l'utilisation efficiente de ces outils. Mais, à ce chapitre, comme le

souligne Karen L. Casser dans *The Internet and Business: A Lawyer's Guide to the Emerging Legal Issues*⁶ :

«Three issues arise. First, are employees surfing the Net instead of doing assigned work? Second are these activities clogging the corporate networks, blocking access and using computing power needed for corporate activities? Third, even if computing is not interfering with work, are resources being used at a significant cost to the company for personal gain?»

Le droit d'un employeur de contrôler et de surveiller la qualité et la quantité de la prestation de travail réside au cœur de ses prérogatives. Les employés ont le devoir de fournir une prestation de travail adéquate dans des temps raisonnables :

«Organizations usually have standards and job descriptions that an employee must meet. If Internet surfing is affecting job performance then the employer should proceed with its usual procedures⁷.»

Dans cette perspective, nous ne saurions être étonnés que les politiques et directives d'une entreprise incluent le fait que l'employeur entend vérifier périodiquement (en adoptant et en adaptant les mesures déjà appliquées en cette matière) la qualité et la quantité du travail effectué par les employés. L'employeur visera donc à effectuer un resserrement des moyens de contrôle et de surveillance des outils informatiques.

(1.2) Contrer les utilisations diffamatoires d'Internet

Le contexte d'Internet impose un examen de la responsabilité qui doit être assumée par les différents intervenants dans la transmission du message ou dans la mise à disposition d'un environnement rendant possibles les communications⁸. L'entreprise propriétaire d'installations informatiques et qui fournit un accès à l'Internet ou qui est l'hôte d'un babillard accessible à des tiers, devient un intervenant dans la transmission de messages. Ces messages pourraient contenir des informations fausses ou même publiées dans le but de nuire à autrui, donc diffamatoires, et qui pourraient ainsi entraîner la responsabilité non seulement de leur auteur, mais aussi de son employeur. Mme le juge Carole Cohen de la Cour supérieure s'exprimait d'ailleurs ainsi dans une récente décision par laquelle elle émettait une ordonnance de sauvegarde visant à faire cesser la diffusion sur des sites Web (exploités par un «serveur» situé hors du Canada) de propos diffamatoires tenus contre son ancien employeur par un employé congédié :

⁶ Au chapitre 6 intitulé «Employers, Employees, E-mail and The Internet», aux pages 6 et 7, *The Computer Law Association Inc.*, 1996.

⁷ K.L. Casser, précité, note 6, à la page 7.

⁸ M. Racicot, M.S. Hayes, A.R. Szibbo, P. Trudel, *Étude de la responsabilité relative au contenu circulant sur Internet*, Industrie Canada, 1997, <http://strategis.ic.gc.ca>.

«...he has described his ongoing litigation with Investors on his two websites in a manner which is clearly critical of Investors Group and

alleged to be defamatory. (...) The Internet can be considered by analogy to other means of communication, such as newspapers⁹.»

Plus récemment, M. le juge Michel Simard de la Cour du Québec a constaté qu'il y avait diffamation là où un courriel d'insultes avait été expédié à plus de 1000 personnes par l'ex-trésorière du syndicat concerné en guise de réponse aux préoccupations exprimées (par courriel) par une candidate au poste de trésorière du syndicat. Reconnaisant qu'on avait ainsi porté atteinte à la réputation de la personne visée par les injures, le juge soulignait :

«L'intimée connaît ou doit connaître l'ampleur possible de telle diffusion par ce moyen [le courrier électronique] moderne, il est vrai, mais combien dangereux lorsqu'on l'utilise sans une certaine réserve qui s'impose alors.¹⁰»

Certains se rappelleront aussi l'affaire *Rindos c. Hardwick* où la «Supreme Court of Western Australia» a condamné à des dommages intérêts de 40 000 \$ l'auteur d'un message comportant des propos qui portaient atteinte à l'honneur et à la réputation d'un professeur d'anthropologie, message qui avait été envoyé à un groupe de discussion auquel étaient abonnés 23,000 étudiants et chercheurs du même domaine¹¹.

Les principes généraux relatifs à la diffamation seront donc applicables aux cas où le message est publié ou diffusé sur Internet. Mais à cet égard il ne faut pas oublier la réalité suivante :

«(...), tenter un recours contre l'auteur peut présenter des inconvénients importants. En premier lieu, il peut-être extrêmement difficile sinon carrément impossible de le retracer. En second lieu, même s'il peut être retracé, l'auteur peut être insolvable. Finalement, il est possible qu'il soit situé dans un ressort étranger, ce qui peut rendre passablement complexe l'exécution d'un jugement contre lui. Pour ces raisons, une victime peut

⁹ *Investors Group Inc. c. Hudson*, J.E. 99-499 (C.S.), aux pages 1 et 3. Pour un exemple d'une sanction disciplinaire imposée à un employé suite à la diffusion à l'ensemble du personnel, par courriel, d'un message «médissant sur autrui», voir *Organisation catholique canadienne pour le développement et la paix et Syndicat des employés de Développement et paix*, D.T.E. 97T-702 (Me Charles Turmel, arbitre).

¹⁰ *Jouvet c. Lévesque*, REJB 2001-23963, 1er mai 2001 (C.Q.), par. 20.

¹¹ Supreme Court of Western Australia, 31 mars 1994.

décider d'intenter son recours non pas contre l'auteur de l'acte, mais contre un ou plusieurs acteurs télématiques¹².»

C'est pourquoi l'entreprise, qui aura mis à la disposition de son personnel les outils de travail informatiques par lesquels un acte dommageable (ce qui inclut la diffamation) aura été commis, pourra voir sa responsabilité recherchée, soit par sa faute propre (art. 1457 C.c.Q.) ou soit par le biais de l'article 1463 C.c.Q. (la responsabilité des commettants).

À n'en pas douter, la nature de l'entreprise et des fonctions de l'employé au sein de celle-ci devra être considérée. D'abord, si l'entreprise elle-même œuvre dans le domaine de la fourniture de services de communication par Internet, il y a tout lieu de croire que sa responsabilité devra être analysée en tenant compte du rôle joué par celle-ci dans la diffusion du message incriminé. L'entreprise doit-elle être considérée comme un éditeur, un diffuseur, un rediffuseur, un bibliothécaire, un retransmetteur, un propriétaire des locaux ou un transporteur public ?¹³ À titre d'exemple, nous soulignerons que l'auteur Stephen D. Imparl¹⁴ a émis le commentaire suivant sur l'affaire *Blumenthal c. Drudge and America Online Inc.*¹⁵:

«It is also important to remember that Drudge was not AOL's employee. If it had been the case, the Court might have allowed the Blumenthals to present a case holding AOL's liable for Drudge's actions committed within the scope of his employment. In that case, the CDA would not provide a defence to liability for the interactive computer service.»

Se pose alors la question de la responsabilité extra-contractuelle directe; par exemple, pour avoir omis d'adopter des politiques ou directives appropriées pour encadrer suffisamment la diffusion d'information sur Internet par les employés ou encore, d'avoir omis de prendre les moyens raisonnables pour en assurer l'application.

Dans *Stratton Oakmont Inc. c. Prodigy Services Co*¹⁶, une entreprise exploitant un babillard électronique et un de ses abonnés ont été poursuivis en diffamation par une firme d'investissement bancaire, Stratton Oakmont, et son président, après que l'abonné eût fait paraître un message dans lequel il accusait la compagnie et son président d'avoir agi de façon criminelle lors d'une émission d'actions. Parce que Prodigy avait adopté une politique de contrôle éditorial, le tribunal jugea son rôle assimilable à celui d'un éditeur et sa responsabilité

¹² F. Thémens, *Internet et la responsabilité civile*, coll. Minerve, Cowansville, Éditions Yvon Blais, 1998, à la page 25.

¹³ P. Trudel, *Technologies de l'information et des communications*, Strategis 1997, au chapitre 3, «Les acteurs et la responsabilité».

¹⁴ Stephen D. Imparl, *Internet Law The Complete Guide*, STP Specialty Technical Publishers, Inc., North Vancouver, 1998, à la page 8-24a.

¹⁵ *Sidney Blumenthal and Jacqueline Jordan Blumenthal vs. Matt Drudge and America Online, Inc.*, Civil Action No. 97-1968 (PLF), April 22, 1998, in America Online, Online Defamation;

¹⁶ 1995 WL 323710 (N.Y. Sup. Ct. 24 mai 1995).

fut retenue. Par contre, un autre gestionnaire de réseau, qui n'effectuait aucun contrôle éditorial, fut plutôt considéré comme un distributeur ou comme un «kiosque à journaux» et ne fut pas jugé responsable des propos diffamatoires¹⁷.

Suite à la décision dans *Stratton*, le Congrès américain a adopté une loi qui prévoit une immunité pour les fournisseurs de services Internet :

«Section 230 of (Communication Decency Act of 1996) (“CDA”), officially titled, “Protection for private blocking and screening of offensive material,” was Congress’s attempt to balance the interests of free speech, commercial competition on the Internet, and to encourage self-regulation of the Internet by allowing individuals and companies to block certain offensive content from being published on the Internet. Specifically, Congress stated :

- (b) Policy. — It is the policy of the United States —
 - (1) to promote the continued development of the Internet and other interactive computer services and other interactive media;
 - (2) to preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services, unfettered by Federal or State regulation;
 - (3) to encourage the development of technologies which maximize user control over what information is received by individuals, families, and schools, who use the Internet and other interactive computer services;
 - (4) to remove disincentives for the development and utilization of blocking and filtering technologies that empower parents to restrict their children’s access to objectionable or inappropriate online material; and
 - (5) to ensure vigorous enforcement of Federal criminal laws to deter and punish trafficking in obscenity, stalking, and harassment by means of computer.

To protect online services from being held liable as distributors or publishers of defamatory information and to encourage those services to block and screen offensive material, Congress provided that providers and users of online services would not be treated as publishers of any information that was provided by another person. Further, Congress proscribed civil liability for online services or their users who exercise editorial control over offensive materials online. Specifically, CDA states:

- (c) Protection for “Good Samaritan” Blocking and Screening of Offensive Material.—
 - (1) Treatment of publisher or speaker, —No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.

¹⁷ *Cubby c. Compuserve*, 776 F. Supp. 135 (1991).

- (2) Civil liability.—No provider or user of an interactive computer service shall be held liable on account of—
- (A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent, harassing, or otherwise objectionable, whether or not such material is constitutionally protected; or
- (B) any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in paragraph (1).

Finally, regarding online services, Congress preempted any state law tort causes of action that were inconsistent with CDA; however, Congress left intact any state laws that are consistent with this section. Section 230(d)(3) of CDA provides:

- (d) Effect on Other Laws.—
- (3) State law.—Nothing in this section shall be construed to prevent any State from enforcing any State law that is consistent with this section. No cause of action may be brought and no liability may be imposed under any State or local law that is inconsistent with this section.

This preemption is crucial because tort law, generally, is a matter of the common law of the several states. While federal law does provide some civil remedies, the tort of defamation is exclusively a matter of state common law. The following case demonstrates one use of Section 230 as a defense to liability for conduct posted to an online service by another person¹⁸.»

L'adoption de ces dispositions législatives semble avoir été particulièrement efficace et a permis aux tribunaux de rejeter, même sur procédures sommaires, des poursuites en diffamation intentées contre des entreprises exploitant des serveurs Internet, tels America Online et même Prodigy Service Company¹⁹.

¹⁸ *Internet Law The Complete Guide*, précité note 14, aux pages 8-17 et 8-18. Le *Communications Decency Act* («CDA») a été déclaré (en grande partie) inconstitutionnel par la Cour Suprême des États-Unis. Il a été remplacé par le *Child Online Protection Act of 1998*, lequel maintient en faveur des entreprises exploitant des serveurs Internet l'exception du «common carrier» applicable aux compagnies de télécommunications. De la sorte, ces entreprises voient leur responsabilité écartée sur le contenu des propos véhiculés par le biais de leurs services.

¹⁹ *Ben Ezra, Weinstein, and Company, Inc. vs. America Online, Inc.*, No. CIV 97-485 LH/LFG, April 23, 1998, in America Online, Online Defamation; *Sidney Blumenthal and Jacqueline Jordan Blumenthal vs. Matt Drudge and America Online, Inc.*, précité, note 15; *Jane Dow vs. America Online, Inc.* Case No. 97-25 87, October 14, 1998, in America Online, Online Defamation; *Zeran vs. America Online*, in America Online, Online Defamation; *Alexander G. Lunney vs. Prodigy Services Company*, 97-07342, 98-00842, in America Online, Online Defamation; *Thomas Kempf vs. Time, Inc. et al.*, Case No. BC 184799, June 11, 1998, in America Online, Online Defamation; *Gerald Nicosia vs. Diane De Rooy*, No. C98-3029 MMC, July 7, 1999, in America Online, Online Defamation; *Alan J. Truelove vs. Mensa International, Ltd. et al.*, Civil No. PJM 97-3463, February 10, 1999, in America Online, Online Defamation.

Le lecteur sera intéressé par les quatre principes développés par le tribunal dans l'affaire *Lunney c. Prodigy Services Company*, à la page 6.

De la même manière, au Québec, la nouvelle *Loi concernant le cadre juridique des technologies de l'information*²⁰ semble exonérer les fournisseurs de services Internet de toute responsabilité relativement au contenu des documents technologiques transigeant sur leurs réseaux. En effet, l'article 27 de cette loi se lit ainsi :

27. Le prestataire de services qui agit à titre d'intermédiaire pour fournir des services sur un réseau de communications ou qui y conserve ou y transporte des documents technologiques n'est pas tenu d'en surveiller l'information, ni de rechercher des circonstances indiquant que les documents permettent la réalisation d'activités à caractère illicite.

Toutefois, il ne doit prendre aucun moyen pour empêcher la personne responsable de l'accès aux documents d'exercer ses fonctions, notamment en ce qui a trait à la confidentialité, ou pour empêcher les autorités responsables d'exercer leurs fonctions, conformément à la loi, relativement à la sécurité publique ou à la prévention, à la détection, à la preuve ou à la poursuite d'infractions.

À ce sujet, Jean-François Codère écrivait, dans un article daté du 22 juin 2001, le commentaire suivant :

« Le cadre juridique déterminé par la loi 161 ne touche pas seulement que les documents. Les fournisseurs d'accès Internet seront par exemple probablement heureux d'en lire l'article 27 [texte de l'article]... »

Le Québec semble donc se rapprocher, par l'adoption de telles dispositions, de la position américaine, et modifie par le fait même son régime de responsabilité civile. À ce sujet, le Barreau du Québec, dans son mémoire sur l'avant projet de loi, faisait remarquer que le C.c.Q. contient déjà un régime de responsabilité civile, lequel est d'application générale. Dans cette perspective, le Barreau proposait de modifier plutôt le Code pour y inclure des dispositions précises visant les intermédiaires, ce qui aurait eu l'avantage de respecter l'objectif d'harmonisation et les principes fondamentaux de responsabilité civile, selon lesquels une personne est responsable des dommages subis par une autre personne en raison de sa faute ou de la faute des personnes qu'elle a sous sa garde²¹.

²⁰ Précité note 5.

²¹ *Mémoire du Barreau du Québec sur la nouvelle Loi sur la normalisation juridique des nouvelles technologies de l'information (Avant-projet de loi)*, 3e trimestre 2000, commentaires sur l'article 25 de l'avant-projet de loi. Voir aussi l'article 36 de la loi.

À noter qu'en parallèle, en droit français, la Cour de cassation (la plus haute instance du pays) a ordonné à Yahoo, le 20 novembre 2000, de retirer de son site de vente aux enchères tous les liens qui pourraient permettre d'accéder à la vente aux enchères d'objets nazis.

Voici un extrait de l'ordonnance de la Cour :
[Ordonne]

Un auteur²² faisait remarquer que la situation des entreprises découlant des quelques décisions existantes avant l'adoption par le Congrès américain du *Communications Decency Act* plaçait une entreprise exploitant des serveurs informatiques (et, selon nous, même les entreprises «propriétaires» d'un site Web ou exploitant un tel site) dans une position délicate : si elles intervenaient en adoptant une politique et des directives quant au type de messages acceptables sur Internet, elles devaient alors effectuer un suivi et un contrôle adéquats de ceux-ci, à défaut de quoi elle devenait responsable, à titre d'éditeur ou de diffuseur, du contenu des messages diffusés. C'est d'ailleurs ce qui a amené la firme Prodigy Services Company à cesser tout effort de contrôle éditorial du contenu des propos diffusés sur Internet par son intermédiaire après la décision de *Stratton Oakmont* :

«Second, the evidence in the record in *Stratton Oakmont* describes the efforts at editorial control which, according to the evidence in the present record, Prodigy in fact abandoned in January 1994, prior to the events underlying the present complaint. Thus, the decision in *Stratton Oakmont* was made in an entirely different factual context²³.»

D'un autre côté, si l'entreprise n'adopte pas de politiques ou de directives relatives à l'utilisation d'Internet et du courriel, s'expose-t-elle à être poursuivie pour négligence, c'est-à-dire pour avoir omis de prendre les moyens raisonnables appropriés pour éviter qu'un dommage à autrui ne soit causé par ses employés? Si l'entreprise avait déjà été avisée que des membres de son personnel utilisaient de façon «incorrecte» l'Internet mis à leur disposition et qu'aucun encadrement raisonnable n'est mis en place malgré cet avis, il apparaît que l'entreprise engagera sa responsabilité : l'«aveuglement volontaire» ne peut constituer une défense valable²⁴. Si l'acte dommageable est commis hors la connaissance de l'employeur, les circonstances détermineront s'il y a eu faute autonome de l'employeur : ce dernier aurait-il pu ou dû savoir qu'une utilisation fautive d'Internet avait cours ou pouvait survenir?

1/ à **Yahoo Inc** : de prendre toutes les mesures de nature à dissuader et à rendre impossible toute consultation sur *yahoo.com* du service de vente aux enchères d'objets nazis et de tout autre site ou service qui constituent une apologie du nazisme ou une contestation des crimes nazis ;

2/ à **Yahoo France** : de délivrer à toute internaute, dès avant même que celui-ci fasse usage du lien lui permettant de poursuivre ses recherches sur *yahoo.com*, un message l'informant des risques qu'il prenait en poursuivant la consultation de tels sites ;

3/ la poursuite de l'instance afin de permettre à Yahoo Inc de soumettre au débat contradictoire les mesures qu'elle entendait prendre pour mettre un terme au trouble et au dommage subi et pour prévenir tout nouveau trouble. (Sur le site : http://www.legalis.net/cgi-iddn/french/affiche-jnet.cgi?droite=decisions/responsabilite/ord_tgi-paris_201100.htm. Voir également le commentaire de Maître Valérie Sédallian sur l'affaire, disponible sur le site : <http://juriscom.net/chr/2/fr20010112.htm>).

En droit français, donc, il semble que la responsabilité des fournisseurs de services Internet puisse être retenue.

²² David Potts, *Liability for Liable on the Internet*, à la page 6.

²³ *Lunney vs. Prodigy Services Company*, précité, note 19, à la page 6.

²⁴ Par analogie, voir *1267623 Ontario inc. c. Nexx Online inc.*, Cour supérieure d'Ontario, 14 juin 1999.

La faute civile d'un employé peut donner ouverture au régime de la responsabilité des commettants de l'article 1463 C.c.Q. En fait, cet article fixe une responsabilité pour autrui au sens strict du terme puisque la faute du commettant lui-même n'est pas nécessaire pour engager

sa responsabilité²⁵. L'employeur ne pourra s'exonérer que si l'auteur du préjudice n'est pas son préposé, que son préposé n'a commis aucune faute ou encore que, si faute il y a, elle s'inscrit

hors du cadre d'exécution des fonctions de l'employé. D'ailleurs, la diffamation constitue un cas d'application de ces principes relatifs à la responsabilité extra-contractuelle en droit civil²⁶.

À titre d'exemple, il y a fort à parier qu'en présence d'un geste fautif d'un employé, l'employeur voudra faire valoir que ce geste diffamatoire s'inscrit hors du cadre d'exécution des fonctions de son employé; autrement dit, que l'employeur n'a jamais autorisé l'employé à tenir des propos diffamatoires. Ce moyen de défense, bien que recevable sur un strict plan théorique, devra être examiné à la lumière des cas dans lesquels il se soulève.

Encore ici, la nature de l'entreprise et des fonctions de l'employé au sein de celle-ci devrait être prise en compte. Si les propos diffamatoires ont été tenus dans le cadre des activités qui sont au cœur de l'exploitation de l'entreprise (par exemple, si un employé d'une firme d'analyse financière émet des commentaires erronés, même de bonne foi, sur la santé financière d'une autre entreprise), il y a tout lieu de croire que la défense relative aux gestes posés hors du cadre d'exécution des fonctions de l'employé ne pourrait bénéficier à l'employeur.

Par contre, si les propos diffamatoires étaient tenus par un employé sur un sujet totalement étranger au cadre d'activités habituelles de l'entreprise, une telle défense serait probablement envisageable, surtout si l'employeur n'a eu aucune connaissance préalable des propos diffusés sur Internet par son employé et que l'employeur est totalement étranger à ces propos.

Enfin, sur cet aspect de la responsabilité du fait d'autrui, il nous apparaît qu'un message émanant d'une personne détentrice d'un certificat d'attribut au sens de l'article 47 de la *Loi concernant le cadre juridique des technologies de l'information*²⁷ établira, à toutes fins pratiques, un lien entre cette personne et l'entreprise au point d'entraîner la responsabilité de cette dernière.

²⁵ A. Soldevila, «La responsabilité pour le fait ou la faute d'autrui et pour le fait des biens», dans *La responsabilité*, Collection de droit, vol. 4, Cowansville, Les Éditions Yvon Blais, 1996, à la page 53.

²⁶ J.L. Baudouin et P. Deslauriers, *La responsabilité civile*, 5e éd., Cowansville, Les Éditions Yvon Blais inc., 1998, à la page 301.

²⁷ Précitée, note 5

L'employeur sera donc bien avisé de porter une attention particulière au choix de ces personnes puisqu'un tel certificat pourra servir à établir, notamment, les droits et pouvoirs de cette personne au sein de l'entreprise.

En définitive, en autant que les relations employeur-employé sont concernées, il n'y a aucun doute que l'existence d'une responsabilité potentielle pour l'employeur sur les propos diffusés sur Internet par ses employés constitue une préoccupation véritable qui pourrait, dans certaines circonstances, constituer un fondement juridique valable quant au droit de l'entreprise de contrôler et de surveiller l'utilisation d'Internet et du courriel par ses employés. L'employeur voudra déterminer les limites qu'il entend poser à ses employés dans l'utilisation des nouveaux

moyens de communication. L'employeur voudra informer ses employés des mesures de contrôle et de surveillance qu'il entend prendre à ce sujet. À ce stade du développement des autorités doctrinales et jurisprudentielles, il nous semble plutôt hasardeux de choisir la route de l'«attentisme» pour ne pas intervenir et ne pas fixer de balises sur le contrôle et la surveillance des propos diffusés sur Internet par les employés d'une entreprise pour tenter d'invoquer par la suite l'ignorance que de tels propos auraient été tenus. Nous suggérons d'emblée que les entreprises choisissent la voie de la prévention en adoptant les politiques et directives appropriées et en informant leurs employés.

(1.3) Éviter le harcèlement (sexuel ou autre) en milieu de travail

La loi, que ce soit par le biais des dispositions relatives à la responsabilité pour le fait d'autrui énoncées à l'article 1463 C.c.Q. ou par le biais des dispositions relatives au maintien d'un milieu de travail où la santé, la sécurité et la dignité du salarié forment la base des conditions raisonnables d'un emploi (art. 2087 C.c.Q. et 46 *Charte québécoise des droits et libertés de la personne*), établit qu'un employeur est également tenu d'offrir à ses employés un environnement exempt de harcèlement.

Dans *Di Vito and Mathers c. Macdonald Dettwiler*²⁸, la Cour suprême de Colombie-Britannique s'est penchée sur une affaire de congédiement motivé par l'utilisation abusive du courrier électronique.

Les événements ayant mené au congédiement des plaignants ont tiré leur origine de la réception d'un courriel à connotation sexuelle intitulé "sexuel acts with an obese woman". L'expéditeur du message avait altéré le message afin qu'on puisse y reconnaître une co-employée qui souffrait d'obésité. Le message a circulé et a ensuite été imprimé. La femme qui était visée dans le message a en trouvé une copie et s'en est plainte à l'employeur. Le juge conclut que les actes des plaignants relatifs à la circulation du courriel étaient suffisants pour justifier une suspension, mais non un congédiement (qui a tout de même été maintenu pour d'autres motifs). De même,

²⁸ Vancouver Registry, n° C944198, 27 juin 1996, <http://www.courts.gov.bc.ca>.

dans une affaire ontarienne²⁹, un congédiement pour usage abusif et personnel du système de courrier électronique pour faire circuler certains messages à caractère sexiste et raciste fut maintenu. La compagnie avait adopté une politique stricte qui restreignait l'usage du système à des fins professionnelles.

C'est dans l'arrêt *Robichaud c. Canada (Conseil du trésor)*³⁰ que la Cour suprême du Canada a établi les paramètres de la responsabilité de l'employeur pour les actes discriminatoires accomplis sans autorisation par ses employés «dans le cadre» de leur emploi. Mme Robichaud alléguait avoir été victime de harcèlement sexuel de la part de son surveillant et de discrimination et d'intimidation de la part de son employeur, le ministère de la Défense nationale. La question qui occupait la Cour était de savoir si les actes fautifs d'un employé

commis en cours d'emploi, mais certes non autorisés ou approuvés par l'employeur, pouvaient être imputés à ce dernier. Bien que la décision ait été rendue suite à un recours pris en vertu de la *Loi canadienne sur les droits de la personne*, l'obligation qu'elle impose est assimilable à celle énoncée dans la législation québécoise de procurer un environnement de travail sain et exempt de toute discrimination.

Dans l'arrêt *Robichaud*, la Cour suprême du Canada affirme que les lois interdisant le harcèlement sexuel ou la discrimination fondée sur le sexe en milieu de travail posent la responsabilité de l'employeur selon des principes différents de ceux traditionnellement reconnus en matière de responsabilité pour le fait d'autrui. La Cour est unanime à reconnaître que le régime de responsabilité applicable est le régime propre aux lois sur les droits de la personne, c'est-à-dire un régime qui permet d'atteindre les objectifs de ces lois, soit la suppression des actes prohibés.

Ainsi, il appartient à l'employeur de démontrer qu'il a pris les mesures nécessaires pour prévenir le harcèlement ou qu'il est intervenu pour supprimer les actes prohibés. L'employeur doit agir. Il ne peut se contenter de réagir. Bref, s'il n'agit pas en temps opportun et avec l'efficacité requise, l'enseignement de la Cour suprême est clair : peu importe la nature et la portée des gestes posés, la responsabilité de l'employeur sera engagée dès lors que ces gestes sont posés à l'occasion de l'emploi³¹.

Une firme de courtage new-yorkaise a été poursuivie pour 60 millions \$ après qu'un courriel à connotation raciale ait circulé entre des employés. Les parties ont conclu un règlement hors cour d'un montant non dévoilé. De même, un auteur rapporte qu'une filiale de Chevron a récemment réglé une poursuite pour un montant 2.2 millions de dollars suite à la distribution sur courrier électronique d'un texte intitulé «why beer is better than women»³².

²⁹ *In the matter of a claim by Prasad A. Bhamre*, décision rendue par E.J. Houston, arbitre, Ottawa, 2 octobre 1998.

³⁰ [1987] 2 R.C.S. 84.

³¹ *CDPDJ (Lippé) c. P.g. Québec*, J.E. 98-2370 (T.D.P.), à la page 21.

³² <http://www.gahtan.com/alan/articles/monitor.htm>.

L'employeur a donc grandement avantage à adopter une politique d'utilisation claire qui proscrie les comportements qui peuvent créer un environnement de travail offensant ou hostile... et à la faire respecter.

(1.4) Assurer le contrôle de l'information privilégiée

Est-il besoin d'insister longuement sur la nécessité pour une entreprise de se prémunir contre toute divulgation non autorisée des informations commerciales sensibles la concernant : listes de prix, listes de clients, structures financières et commerciales d'un contrat, etc. Sans entrer dans le débat de déterminer si l'entreprise peut être qualifiée de «propriétaire» de ces informations, il importe de souligner que les tribunaux ont généralement reconnu aux entreprises le droit de contrôler selon leur bon vouloir la dissémination de ce type d'informations³³.

L'utilisation des nouvelles technologies ne change pas l'obligation de loyauté et de confidentialité qui lie un employé à son employeur et qui est énoncée à l'article 2088 du *Code Civil du Québec* :

«2088. Le salarié, outre qu'il est tenu d'exécuter son travail avec prudence et diligence, doit agir avec loyauté et ne pas faire usage de l'information à caractère confidentiel qu'il obtient dans l'exécution ou à l'occasion de son travail.

Ces obligations survivent pendant un délai raisonnable après cessation du contrat, et survivent en tout temps lorsque l'information réfère à la réputation et à la vie privée d'autrui.»

L'article 2088 C.c.Q. établit l'obligation pour l'employé d'accomplir le travail pour lequel il est rémunéré en plus de l'obligation de ne pas divulguer l'information confidentielle avec laquelle il vient en contact au cours de son travail. Un employé (et même un ancien employé dans certaines circonstances) ne peut faire un usage non autorisé de l'information à caractère confidentiel qu'il a obtenue durant son emploi dans l'entreprise. S'il fait défaut de respecter cette obligation, il s'expose à ce que son employeur prenne des sanctions disciplinaires contre lui et le poursuive en dommages, voire en injonction. Ces obligations de l'employé sont à la base du pouvoir général de l'employeur de diriger et de contrôler son entreprise, droit qui inclut celui de surveiller le travail de ses employés et qui est étudié au paragraphe (2.3) ci-après³⁴.

³³ *R. c. Stewart*, (1988) 1 R.C.S. 963, à la page 975 et *Lac Minerals c. International Corona Resources*, (1989) 2 R.C.S. 574, aux pages 638-639.

³⁴ À cet égard, nous sommes aussi d'avis que les informations financières ou commerciales privées d'une entreprise font partie de ce que nous pourrions appeler une «sphère de protection de la vie privée» de l'entreprise. À ce sujet, voir K. Delwaide, «La protection de la vie privée et les nouvelles technologies : L'accès au courrier électronique des employés par un employeur», in *Congrès annuel du Barreau du*

Un employé peut, par exemple, avoir accès à de l'information privilégiée par le biais de son ordinateur et la transmettre par courrier électronique, sans autorisation, à des tiers. Une telle situation a donné lieu à une poursuite aux États-Unis lorsque suite à l'embauche par Symantec d'un employé haut placé de la compagnie Borland, cette dernière a allégué que l'employé avait transmis par courriel, avant de quitter, des informations confidentielles, «propriété» de Borland, à Symantec et à son président. L'enquête conduite a donné lieu à la saisie des fichiers des ordinateurs de Symantec et de son président. En plus de voir sa responsabilité civile et criminelle retenue, la compagnie Symantec a souffert de la couverture médiatique du litige³⁵.

Au Québec, la décision rendue dans l'affaire *L.N.S. Systems Inc. c. Allard*³⁶ a vu la Cour supérieure s'appuyer notamment sur la preuve de documents informatiques reconstitués par un expert en «computer forensic consulting and investigations» pour appuyer les conclusions d'une violation de l'obligation de loyauté et de non-concurrence de deux employés de l'entreprise concernée et congédiés pour cause, de même qu'au maintien de la justification du congédiement.

Différentes lois québécoises³⁷ créent aussi l'obligation pour les organismes ou entreprises de maintenir et de protéger la confidentialité des renseignements personnels détenus par eux. De son côté, le gouvernement fédéral a adopté une loi de même nature applicable au secteur privé, la *Loi sur la protection des renseignements personnels et les documents électroniques*³⁸, afin d'assurer la protection des renseignements personnels et, ainsi, améliorer la perception du public sur l'intégrité dans la conduite du commerce électronique.

La protection des renseignements personnels et, au premier chef, le maintien de leur confidentialité, sont devenus des enjeux majeurs. Un tribunal d'arbitrage a eu à examiner le cas d'un programmeur en informatique qui avait utilisé ses compétences pour avoir accès à des

Québec (1997), Service de la formation permanente, Barreau du Québec, 627, aux pages 633-636. Voir aussi *Barrou c. Micro-Boutique Éducative inc.*, J.E. 99-1951 (C.S.), à la page 19; *SOQUIA C. Libman*, J.E. 98-1648 (C.Q.), aux pages 9-10 et *Régie intermunicipale des déchets de la Mauricie c. Service spécial de vidanges inc.*, J.E. 97-730 (C.Q.), aux pages 14-15 (maintenu en appel, mais sans se prononcer sur la question de la protection de la vie privée d'une entreprise, J.E. 97-1258).

³⁵ *Borland International Inc. v. Eubanks*, Santa Cruz, CA, County Sup. Ct. Civ. Case no. 123059; *People v. Eubanks*, Santa Cruz, CA, County Sup. Ct. Crim., Case no. 67483.

³⁶ J.E. 2001-1277 (C.S.) (en appel).

³⁷ *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels*, L.R.Q., c. A-2.1. et la *Loi sur la protection des renseignements personnels dans le secteur privé*, L.R.Q., c. P-39.1. L'article 1 de cette dernière énonce ce qui suit :

1. La présente loi a pour objet d'établir, pour l'exercice des droits conférés par les articles 35 à 40 du Code civil du Québec en matière de protection des renseignements personnels, des règles particulières à l'égard des renseignements personnels sur autrui qu'une personne recueille, détient, utilise ou communique à des tiers à l'occasion de l'exploitation d'une entreprise au sens de l'article 1525 du Code civil du Québec.

³⁸ L.C. 2000, c. 5.

informations confidentielles sans autorisation de l'employeur. Dans cette affaire³⁹, l'arbitre a conclu, malgré l'absence de preuve quant à la mauvaise foi de l'employé, que les agissements de l'employé étaient prémédités dans la mesure où il savait parfaitement ce qu'il faisait et qu'il tentait d'accéder à des informations auxquelles il n'avait pas droit. Étant donné la nature confidentielle de l'information (échantillons-dossiers médicaux), les fonctions de l'employé exigeaient un très haut niveau de loyauté envers son employeur et l'arbitre a conclu que le comportement de l'employé avait brisé le lien de confiance qu'il avait avec son employeur. Le congédiement de l'employé était donc nécessaire.

Dans *Canadian Pacific Ltd. c. Transportation Communication Union*⁴⁰, l'arbitre a réduit une sanction contre un employé qui avait utilisé le courriel pour émettre des commentaires dérogatoires sur d'autres employés et obtenir l'accès non autorisé à des fichiers personnels appartenant à des collègues. Les communications de l'employé incluaient des conversations à caractère intime, quelquefois des conversations de potinage incluant des insultes et des commentaires négatifs à l'endroit de collègues. L'arbitre justifie la réduction de la sanction de la façon suivante :

«The arbitrator is inclined to give some weight to the submission that in the instant case the Company has not established that it developed and properly communicated a clear policy or system of rules for employees in relation to the use of Merlin e-mail (le logiciel de courrier électronique) for sending personal messages(...) While the sending of a general e-mail, addressed over the Company's entire system, may have certain efficiencies from the standpoint of broad communication, it is less than perfect for confirming the receipt of a given message by any individual employee. There is no evidence that employees were required to give any acknowledgment of the communication, or to sign a policy booklet or document, as is sometimes done in the communication of policies and rules⁴¹.»

Curieusement, la *Loi concernant le cadre juridique des technologies de l'information*⁴², alors qu'elle semble exonérer de responsabilité les fournisseurs de services Internet dans certaines circonstances⁴³, semble par contre accroître le fardeau des entreprises en leur imposant l'adoption de mesures de protection des renseignements confidentiels encore plus poussées. En effet, les articles 25 et 34 de cette loi se lisent ainsi :

³⁹ *Laboratoire de santé publique c. Syndicat de la fonction publique, section locale 2667*, [1992] T.A. 23. Voir aussi *Frezza et Réseau CP Rail, St-Jean-sur-Richelieu*, 24 juillet 1997, Claude Lauzon, arbitre et *Syndicat des fonctionnaires municipaux de Québec c. Québec (Ville de)*, (1995) T.A. 997, DTE 95T-1337.

⁴⁰ Canadian Railway Office of Arbitration, Case no. 2731, Calgary, 14 mai 1996.

⁴¹ *Idem*, à la page 6.

⁴² Précitée, note 5.

⁴³ Voir les articles 27 et 36 de la loi et notre texte à ce sujet au paragraphe (1.2) ci-haut.

«25. La personne qui est responsable de l'accès à un document technologique qui porte un renseignement confidentiel doit prendre les mesures de sécurité propres à en assurer la confidentialité, notamment par un contrôle d'accès effectué au moyen d'un procédé de visibilité réduite ou d'un procédé qui empêche une personne non autorisée de prendre connaissance du renseignement ou, selon le cas, d'avoir accès autrement au document ou aux composantes qui permettent d'y accéder.

34. Lorsque la loi déclare confidentiels des renseignements que comporte un document, leur confidentialité doit être protégée par un moyen approprié au mode de transmission, y compris sur des réseaux de communication.

La documentation expliquant le mode de transmission convenu, incluant les moyens pris pour assurer la confidentialité du document transmis, doit être disponible pour production en preuve, le cas échéant.»

De telles dispositions imposent des obligations importantes aux entreprises. À titre d'exemple, le lecteur notera que l'obligation faite de protéger la confidentialité de l'article 34 ne se limite pas aux documents technologiques. De plus, une telle obligation pourra signifier qu'en matière de transmission informatique, les échanges d'information confidentiels devront être faits en utilisant des systèmes de cryptographie (codage). Que l'on pense aux communications assujetties au secret professionnel ou à la transmission de renseignements personnels, ces nouvelles dispositions législatives devront être prises en compte. Elles auront certainement pour effet de resserrer la surveillance des employeurs envers l'utilisation que font leurs employés ou des tiers des informations contenues sur le réseau de leur entreprise.

L'employeur doit donc être en mesure de limiter les risques relatifs à l'accès et à l'utilisation d'informations confidentielles concernant son entreprise, ses clients et ses employés. Dans l'éventualité de telles violations, l'employeur doit pouvoir imposer des sanctions afin de limiter la possibilité qu'il y ait d'autres violations dans l'avenir. D'où l'importance d'adopter une politique explicite et même, lorsque possible, d'obtenir un engagement exprès de la part des employés de ne pas accéder ni utiliser et communiquer les informations détenues par l'entreprise autrement qu'aux fins de l'exécution des fonctions pour lesquelles ils sont dûment autorisés.

L'entreprise voudra aussi protéger l'information et la documentation qu'elle détient et qui bénéficient de «droits d'auteur». L'employeur voudra éviter que même involontairement ses employés ne viennent copier des informations d'une autre entreprise qui elles aussi sont protégées par des droits d'auteur.

L'employé qui utilise l'autoroute de l'information ou le courrier électronique pour copier et distribuer l'œuvre originale et licenciée d'une tierce personne, sans le consentement de cette

dernière peut voir la responsabilité de son employeur retenue pour atteinte aux droits d'auteur. Des auteurs s'expriment ainsi sur l'impact de l'essor des communications sur les droits d'auteur :

«Le droit d'auteur est un concept juridique fondamental à la création, à la croissance et à l'exploitation des produits artistiques et de divertissement qui enrichissent nos vies. En outre, avec l'expansion des ordinateurs et des logiciels qui permettent de les utiliser, la loi sur le droit d'auteur a assumé la tâche importante de protéger les droits économiques de ceux qui créent les logiciels. L'importance de la propriété intellectuelle et de la protection que confère le droit d'auteur à ses créateurs continuera de s'étendre⁴⁴.»

L'employeur quant à lui doit avant tout s'assurer que les logiciels utilisés dans son entreprise n'ont pas été illégalement téléchargés sur Internet et qu'il possède toutes les licences d'utilisation nécessaires. La *Loi sur le droit d'auteur*⁴⁵ définit quatre types d'œuvres protégées : les œuvres littéraires, dramatiques, musicales et artistiques. La loi prévoit que chaque type d'œuvre susceptible d'être protégée par un droit d'auteur est inclus dans une ou plusieurs de ces catégories. Par exemple, les logiciels ont été classés comme des œuvres littéraires pour les fins d'application de la loi.

L'employeur a aussi le droit de voir à ce que son système de courrier électronique ne soit pas utilisé pour faire circuler des «œuvres» lui appartenant et qui sont protégées par un droit d'auteur. Par exemple, un employé envoie un message auquel du texte, un logiciel, des images, de la vidéo ou de la musique appartenant à l'entreprise peuvent être joints; le message et ses annexes sont livrés à un ou plusieurs correspondants. Dès qu'un tel message est envoyé à un nombre de personnes indéterminé ou à une liste de distribution non personnelle, la communication est considérée «au public» en vertu de l'article 3 (1) de la *Loi sur le droit d'auteur* qui énonce l'énumération des droits conférés au titulaire du droit et auquel renvoie l'article 27(1) qui porte sur la violation du droit d'auteur.

Dans le contexte d'affaires telles que celle de l'affaire *Napster*⁴⁶, aux États-Unis, on peut voir que la position des tribunaux se durcit par rapport aux violations des droits d'auteur qui résultent de l'utilisation des nouvelles technologies. L'Internet ne constitue dorénavant plus un «voile» suffisant pour justifier une violation des droits d'auteur d'un tiers, la Cour ayant jugé qu'en l'espèce, le fait que les fichiers musicaux (mp3) ne faisaient que transiter par un serveur, sans y demeurer définitivement, ne signifiait pas qu'il n'y avait pas d'infraction de la part de la personne qui opère le serveur, en l'occurrence Napster. Cette affaire s'est soldée, en septembre 2001, par un règlement pour un dédommagement substantiel payable par Napster aux

⁴⁴ M. Racicot, M.S. Hayes, A.R. Szibbo, P. Trudel, *Étude de la responsabilité relative au contenu circulant sur Internet*, Industrie Canada, 1997, <http://strategis.ic.gc.ca>.

⁴⁵ L.R.C., c. C-42.

⁴⁶ *A&M Records Inc. et al. v. Napster Inc.*, No C 99-05183 MHP (N.D. Cal. 2000)

compagnies de disques et artistes qui avaient intenté la poursuite. Cela donne une idée de l'ampleur de telles violations et de l'importance d'éviter que des employés s'engagent dans des activités pouvant compromettre l'employeur que ce soit en utilisant des serveurs réservés au travail pour des fins illégales, ou soit en rendant publiques des informations secrètes ou des œuvres protégées par des droits d'auteur.

Nous n'entendons pas couvrir l'ensemble des questions relatives aux droits d'auteur. Nous nous en remettons aux experts en cette matière⁴⁷. Aux fins de notre étude, nous constatons cependant que les tribunaux sanctionnent sévèrement une utilisation fautive des nouveaux moyens technologiques en milieu de travail lorsque cette utilisation fautive constitue une atteinte aux droits des tiers ou lorsque l'employeur a adopté une politique d'utilisation et porté celle-ci à la connaissance de ses employés.

* * *

Les éléments auxquels nous avons référé au présent chapitre constituent des exemples établissant le droit d'une entreprise de contrôler et de surveiller l'utilisation d'Internet et du courriel par ses employés. Selon les circonstances, tous et chacun de ces exemples constituent des intérêts sérieux et légitimes permettant à l'employeur de procéder à un tel contrôle et à une telle surveillance.

Mais une fois cela établi, cela ne signifie pas qu'en toutes circonstances et de toutes les façons, l'employeur est justifié de procéder à ce contrôle et à cette surveillance. D'une part, ces intérêts sérieux et légitimes doivent être contrebalancés avec ceux, tout aussi sérieux et légitimes, des employés. Et même lorsque les intérêts de l'employeur l'emporteront sur ceux des employés, la manière dont ces droits seront exercés demeure sujette à limitation.

⁴⁷ Pour une étude sur le sujet, voir M.-H. Côté, «La responsabilité des intermédiaires à l'égard des violations de droit d'auteur commises par des tiers sur l'Internet», (1998) 10 *Cahiers de propriété intellectuelle* 359, 370 et 392.

2. Les intérêts sérieux et légitimes des employés

La jurisprudence arbitrale reconnaît depuis longtemps qu'un employeur, dans l'exercice de son droit de gestion, peut imposer certains contrôles à ses employés et qu'il peut, à cet égard, procéder à une certaine surveillance de ceux-ci. La surveillance électronique est l'un des moyens par lequel l'employeur peut assurer ce contrôle et cette surveillance. Par exemple, il n'est pas rare que dans le domaine du transport, on utilise un système de tachygraphe. Dans d'autres industries, l'employeur utilisera un système d'horloge-poinçon pour contrôler le temps de travail de ses salariés.

Il n'est donc pas étonnant que suite à l'apparition d'Internet et à l'introduction du courriel en milieu de travail, ceux-ci aient été soumis au droit de contrôle et de surveillance de l'employeur. Bien que l'employeur ait un droit reconnu à ce contrôle et à cette surveillance (sujet à certaines limitations), il devra néanmoins l'exercer avec prudence, de manière raisonnable et en respectant le droit à la vie privée et à la dignité des employés.

C'est pourquoi, à ce stade, nous nous permettrons d'examiner certains des principes législatifs, doctrinaux et jurisprudentiels qui supportent la protection des intérêts sérieux et légitimes des employés à l'égard de l'utilisation des moyens de communication mis à leur disposition en milieu de travail.

(2.1) Les dispositions du Code criminel relatives à l'interception de communications privées (art. 183ss)

Le législateur fédéral a criminalisé l'acte d'interception de communications privées. Ainsi, le Parlement fédéral traduisait sa préoccupation d'assurer une certaine forme de protection aux communications privées. Il s'agit alors de déterminer si un courriel d'un employé est une «communication privée» au sens de la définition de l'article 183 du *Code criminel* :

«183. «communication privée» Communication orale ou télécommunication dont l'auteur se trouve au Canada, ou destinée par celui-ci à une personne qui s'y trouve, et 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. La présente définition vise également la communication radiotéléphonique traitée électroniquement ou autrement en vue d'empêcher sa réception en clair par une personne autre que celle à laquelle son auteur la destine.»

Dans l'affaire *Roy c. Saulnier*⁴⁸, la Cour d'appel a eu l'occasion de se pencher sur le cas d'un employeur qui soupçonnait son employé de vouloir organiser une entreprise concurrente et qui avait enregistré ses conversations téléphoniques avec certains clients. L'employé s'était objecté à la recevabilité en preuve de ces enregistrements en invoquant la *Charte des droits et libertés de la personne* et le respect de la vie privée. Sous la plume du juge Beaugard, la Cour d'appel affirmait ce qui suit :

«Voulant se ménager un moyen de preuve, l'appelant, tout à fait de bonne foi et ignorant des dispositions du *Code criminel* sur le sujet, décide d'enregistrer ce que l'intimé dit aux clients durant les heures de travail, à partir des lignes téléphoniques de l'appelant. Le but de l'appelant n'est pas d'écouter les conversations privées de l'intimée mais bien de voir ce que l'intimée dit à la clientèle de l'appelant.»

Quant au juge Moisan, il considère que ces conversations ne portent pas sur des matières relevant de la vie privée étant donné qu'elles ont eu lieu dans le cadre des affaires commerciales de l'entreprise :

«Quant au contenu des conversations qu'on veut mettre en preuve, elles ne portent pas sur des matières relevant de la vie privée de l'intimée, de ses relations familiales ou sociales, mais uniquement d'affaires commerciales de l'appelant.

Je ne puis me convaincre que, dans ce cadre de travail et dans ces matières, la vie privée de l'intimée soit en cause. Je ne puis non plus me convaincre que l'intimée puisse prétendre qu'elle pouvait raisonnablement s'attendre à ce que ses conversations d'affaires, en cours de travail, ne soient pas interceptées par l'employeur qui la paie pour recevoir ou faire des appels»⁴⁹.

La question soulevée sera donc de déterminer si la communication est faite «dans des circonstances» telles que son auteur (puisse) raisonnablement s'attendre à ce qu'elle ne soit pas interceptée par un tiers». Il s'agit d'une formulation législative de l'«attente raisonnable de protection de la vie privée». Nous suggérons qu'à l'égard des communications émanant de ses employés dans le cadre (ou aux fins) de leur travail, l'employeur ne devrait pas être considéré comme un «tiers». Après tout, les employés agissent pour et en son nom; c'est d'ailleurs de ce fait qu'ils peuvent engager la responsabilité civile de leur commettant. Et il y a plus! Une

⁴⁸ [1992] R.J.Q. 2419

⁴⁹ Idem, aux pages 2422 et 2425.

communication d'affaires, en cours d'emploi, nous apparaît difficilement répondre aux principes mêmes d'une communication de nature privée⁵⁰.

Si l'on s'interroge sur les communications effectuées à partir du lieu de travail, mais pour des fins personnelles (par exemple, au cours des pauses), nous référons le lecteur au paragraphe (2.2) ci-après. En résumé, nous insisterons sur l'importance pour l'entreprise de ne pas créer une impression chez ses employés que leurs communications personnelles sont et demeurent strictement privées.

Enfin, si on examine la question sous l'angle du «client» de l'entreprise qui communique avec celle-ci par courriel, nous soulignerons à nouveau l'importance de «prévenir» toute situation problématique en avisant les tiers (par exemple, en affichant une note au site Web de l'entreprise) que les outils informatiques de l'entreprise sont assujettis à de la surveillance et à des contrôles routiniers et réguliers à des fins de sécurité, de vérifications d'affaires ou de formation, selon le cas. Il s'agit en fait de d'annoncer clairement que les usagers du site Web de l'entreprise ne peuvent s'attendre raisonnablement à une protection de la «vie privée».

En terminant, soulignons que le Code criminel a été amendé, en 1997⁵¹, pour ajouter à l'article 342.1, qui traite de l'«utilisation non autorisée d'ordinateur», une disposition qui prohibe la possession et le trafic d'un mot de passe permettant de commettre les infractions prévues à cet article⁵², soit obtenir frauduleusement des services d'ordinateur, intercepter frauduleusement toute fonction d'un ordinateur, ou altérer les données contenues dans un ordinateur, cette dernière infraction étant prévue à l'article 430 du Code criminel. Quant à l'article 430, il prohibe le fait de détruire ou de modifier des données, de les dépouiller de leur sens, de les rendre inutiles ou inopérantes, d'empêcher ou de gêner l'emploi légitime qu'une personne peut en faire ou d'empêcher leur accès à une personne qui en y a droit⁵³.

⁵⁰ P. Trudel, F. Akran, K. Benyekhlef et S. Hein, *Droit du Cyberspace*, Les Éditions Thémis inc., 1997, aux pages 11-49, 11-54 et 11-56.

⁵¹ L.C. 1997, c.18 (Projet de loi C-17).

⁵² 342.1 d) *a en sa possession ou utilise un mot de passe d'ordinateur qui permettrait la perpétration des infractions prévues aux alinéas a), b) ou c), ou en fait le trafic ou permet à une autre personne de l'utiliser.* Mot de passe a été défini ainsi: «*mot de passe*» *Donnée permettant d'utiliser un ordinateur ou d'obtenir des services d'ordinateur.* Voir, pour l'application de ces dispositions, la décision *R. c. Lavoie*, J.E. 2000-773 (C.Q.), dans laquelle l'accusé avait créé et publié sur Internet des sites contenant des mots de passe permettant l'accès non autorisé à des systèmes informatiques, soit les sites du gouvernement, d'organismes militaires et d'organismes spécialisés dans les communications.

⁵³ Méfait concernant des données

430 (1.1) *Commet un méfait quiconque volontairement, selon le cas :*

a) détruit ou modifie des données;

b) dépouille des données de leur sens, les rend inutiles ou inopérantes;

c) empêche, interrompt ou gêne l'emploi légitime des données;

d) empêche, interrompt ou gêne une personne dans l'emploi légitime des données ou refuse l'accès aux données à une personne qui y a droit.

Il est important de garder en mémoire ces dispositions parce qu'un employé s'expose, en y contrevenant, à une condamnation en vertu du Code criminel⁵⁴ Un employeur pourrait donc, s'il a un motif raisonnable de croire qu'une telle infraction va être commise ou a été commise, surveiller l'usage qu'un de ses employés fait d'Internet ou de son courrier électronique.

(2.2) La protection de la vie privée d'une personne, même en milieu de travail

A. La définition du droit à la vie privée (contexte général)

Il est généralement accepté que le concept de «vie privée» recoupe au moins deux réalités : le droit à la vie privée comme tel et le droit de contrôler les renseignements qui touchent sa personne. Mais une constatation s'impose déjà quant au premier de ces deux aspects : malgré toute l'activité législative sur le sujet, ni la *Charte québécoise* ni le C.c.Q. ne comportent une définition formelle de ce qu'est la vie privée. En raison de la subjectivité qui est inhérente à ce concept, le législateur a plutôt choisi d'énumérer à l'article 36 C.c.Q. un certain nombre d'actions pouvant constituer une atteinte à la vie privée. Cet article se lit ainsi :

«36. Peuvent être notamment considérés comme des atteintes à la vie privée d'une personne les actes suivants :

1° Pénétrer chez elle ou y prendre quoi que ce soit;

2° Intercepter ou utiliser volontairement une communication privée;

3° Capter ou utiliser son image ou sa voix lorsqu'elle se trouve dans des lieux privés;

4° Surveiller sa vie privée par quelque moyen que ce soit;

5° Utiliser son nom, son image, sa ressemblance ou sa voix à toute autre fin que l'information légitime du public;

6° Utiliser sa correspondance, ses manuscrits ou ses autres documents personnels.»

L'emploi, dans cet article, de l'expression «Peuvent [...] être considérés» amène à conclure que la seule présence d'un des gestes décrits aux paragraphes 1 à 6 de l'article 36 C.c.Q. ne permet pas de conclure automatiquement à l'atteinte du droit à la vie privée. À titre d'exemple, on

⁵⁴

Voir à titre d'exemple la décision *R. c. Paré*, J.E. 97-1179 (C.Q.), dans laquelle un inspecteur de police avait été trouvé coupable d'avoir obtenu frauduleusement des services d'ordinateur, en faisant des recherches personnelles auprès du Centre de renseignements policiers du Québec, afin de transmettre les renseignements obtenus à des tiers qui n'y auraient pas eu accès normalement, y compris son beau-frère. La Cour du Québec a jugé qu'une telle utilisation était non seulement non autorisée, mais frauduleuse, parce que l'inspecteur savait pertinemment qu'une telle utilisation du fichier était interdite.

pourrait penser à une situation où l'employé consent, que ce soit de façon explicite ou implicite, à une telle atteinte.

Ajoutons aussi que les situations décrites aux paragraphes 1 à 6 de l'article 36 C.c.Q. ne sont pas exhaustives. En effet, l'emploi du terme «notamment» révèle une intention de ne pas limiter les situations pouvant porter atteinte au droit à la vie privée. Les tribunaux se voient attribuer une large discrétion afin d'évaluer si un geste porte atteinte à ce droit. Chaque cas constituera donc un cas d'espèce et il est à parier que le droit de l'employeur de procéder à la surveillance du courrier électronique de ses employés variera selon les circonstances.

À ces paramètres dressés par l'article 36 C.c.Q., viennent s'ajouter d'autres composantes du droit à la vie privée.

Il faut reconnaître que le droit à la vie privée n'est plus limité au droit de ne pas être surveillé ou dérangé dans sa demeure (l'intimité du foyer); ce droit comporte d'autres aspects dont ceux qualifiés par le professeur Patrick Glenn⁵⁵ de droit à la solitude et de droit à l'anonymat.

Les auteurs Deleury et Goubau ont également tenté d'expliquer la nature et l'étendue du droit à la vie privée :

Cette tranquillité, qui est une valeur psychologique protégée, revêt de multiples aspects concrètement dissemblables : demeurer inconnu; n'être pas épié, suivi, sollicité, questionné, dépeint; ne pas entendre prononcer son nom en public; ne pas voir divulgués sa biographie ou sa généalogie, l'état de sa fortune, de ses dettes; ne pas être comptables des actes de son existence quotidienne, etc.⁵⁶

Énoncé autrement, le droit à la vie privée a été décrit de la façon suivante par M. le juge Le Bel, alors qu'il était à la Cour d'appel du Québec, dans la décision. *Le Syndicat des travailleurs(euses) de Bridgestone Firestone de Joliette (C.S.N.) c. Trudeau*⁵⁷ :

«Le concept de vie privée reste flou et difficile à circonscrire. Les développements jurisprudentiels sur le sujet ne sont sans doute pas terminés. À l'occasion de l'examen d'une affaire relative à la captation et à l'utilisation d'une image, la Cour suprême du Canada a reconnu que les intérêts de vie privée n'étaient pas sujets à une limitation géographique stricte, en ce sens qu'ils s'arrêteraient aux murs du foyer. Ces intérêts de

⁵⁵ H.R. Glenn, «Le droit au respect de la vie privée», (1979) 39 R. du B., 879.

⁵⁶ E. Deleury, D. Goubau, *Le droit des personnes physiques*, Cowansville, Les Éditions Yvon Blais, 1994, à la page 137. Voir aussi P.A. Molinari et P. Trudel, «Le droit au respect de l'honneur, de la réputation et de la vie privée : aspects généraux et applications», dans *Formation permanente du Barreau du Québec, Application des Chartes des droits et libertés en matière civile*, Cowansville, Les Éditions Yvon Blais, 1988, aux pages 197 et s.

⁵⁷ [1999] R.J.Q. 2229 (C.A.),

protection de la vie privée peuvent se maintenir avec des intensités diverses, même dans les lieux où un individu peut être vu du public (voir *Éditions Vice-Versa c. Aubry*, [1998] 1 R.C.S., [1996] R.J.Q. 2137 (C.A.); voir aussi *Ville de Longueuil c. Godbout*, [1997] 3 R.C.S. 844). Ce droit comporte des composantes telles que le droit à l’anonymat et à l’intimité, au secret et à la confidentialité, dont la fonction ultime est la préservation du droit de chaque personne à son autonomie.⁵⁸ »

On retrouve un très bon exemple de la portée du droit à l’anonymat dans l’affaire *Duclos c. Aubry et Éditions Vice-Versa Inc.*⁵⁹ où la Cour suprême du Canada a reconnu une faute dans la publication sans autorisation d’une photo de l’intimée Aubry, demanderesse en première instance. La photographie montre Mme Aubry, qui n’est aucunement engagée dans la vie publique, assise à l’extérieur d’un édifice. Elle fut photographiée par un photographe amateur sans son consentement et la photo fut publiée dans un magazine artistique à faible tirage. Dans ce cas, la Cour a décidé que l’intérêt public à l’information ne pouvait justifier cette atteinte à des composantes du droit au respect de la vie privée (à savoir le droit à l’image, voire à l’anonymat), comme cela eut pu être le cas d’une photo prise lors d’un événement public très médiatisé.

Dans l’affaire *The Gazette c. Valiquette*⁶⁰, le journal appelant avait publié, sans le consentement du principal intéressé, deux articles racontant l’expérience d’un professeur sidatique de l’école secondaire Sophie-Barat à qui on a refusé l’accès à l’école le jour de la rentrée. Les articles ne nommaient pas le professeur spécifiquement, mais permettaient à ses proches, collègues et étudiants de le reconnaître, d’identifier sa maladie et de spéculer sur son orientation sexuelle. La preuve a démontré que l’intimé désirait avant tout garder le secret autour de sa condition et que le fait de se retrouver ainsi au centre d’un débat public avait eu sur lui un effet psychologique important. Dans ces circonstances, la Cour d’appel a décidé de ne pas retenir l’argument des appelants voulant qu’ils aient de bonne foi et dans l’intérêt public simplement dénoncé une politique discriminatoire dont M. Valiquette aurait été victime. Le journal, malgré la véracité des faits rapportés, aurait dû obtenir le consentement de celui-ci.

En définitive, d’une façon générale, le concept de «vie privée» reconnaît la protection de l’intimité au domicile, mais il est beaucoup plus vaste. Il recoupe aussi le droit à l’intimité ailleurs qu’au foyer de même que le droit d’être laissé en paix et de demeurer dans l’anonymat. Voyons ce qu’il en est maintenant en milieu de travail.

B. Le concept de vie privée en milieu de travail

Par le passé, les juristes se sont souvent posé la question, à savoir si le milieu du travail pouvait être considéré comme un lieu visé par la protection de la vie privée. Peut-on parler de «sphère de protection de la vie privée» au travail?

⁵⁸ Idem, à la page 2241.

⁵⁹ [1998] 1 R.C.S. 591.

⁶⁰ J.E. 97-133 (C.A.).

En cette matière, l'approche «traditionnelle» des tribunaux est bien illustrée par la décision *La Société des alcools du Québec et Syndicat des employés de magasins et bureaux de la SAQ* rendue par Me Jean-Pierre Lussier, arbitre, lequel s'exprimait ainsi :

«De façon générale, la surveillance électronique d'un salarié au travail ne contrevient pas, à mon avis, à cet article de la Charte (art. 5). Le salarié, dans l'exécution de ses fonctions, a des agissements qui n'appartiennent pas à sa vie privée, sauf exception. Bien sûr, il existe des cas où à l'occasion du travail on restera quand même dans le domaine de la vie privée. Je pense à des conversations privées entre salariés pendant des périodes de pause ou encore à des circonstances qui, de par leur nature même, sont du domaine strictement privé (aller à la salle de toilette, par exemple). Mais, de façon générale, un salarié au travail loue ses services à un employeur qui a le droit de prendre les mesures qui s'imposent pour vérifier la nature et la qualité du travail fourni. À cette fin, rien ne lui interdit de surveiller le salarié pour s'assurer de la qualité de son travail et on ne peut certes pas prétendre que pendant le temps où le salarié effectue sa prestation de travail, on est toujours dans le strict domaine de la vie privée.

Bref, une surveillance constante et assidue, même par le truchement d'appareils électroniques, ne contrevient pas à l'article 5 de la *Charte des droits et libertés de la personne*. Elle ne peut donc, à ce titre, être considérée comme illégale⁶¹.»

Comme l'a suggéré Me Yves Bourdeau, conseiller juridique de la Commission des droits de la personne et des droits de la jeunesse, il ne faut pas oublier que :

[...] Les notions de «lieu privé» et de «vie privée» sont relatives et dépendent de l'attente raisonnable de protection de la vie privée qu'on peut entretenir à l'égard d'un lieu particulier ou d'une situation donnée. Or, la jurisprudence a déterminé que les attentes des particuliers ne peuvent être très élevées quant au respect de leur vie privée sur les lieux de travail⁶²

⁶¹ [1983] T.A. 335.

⁶² P.-Y. Bourdeau, *La surveillance par caméra vidéo des lieux de travail*, Allocution présentée le 13 mars 1996 lors d'un colloque organisé par la Ligue des droits et libertés, à la page 7.

C'est ainsi qu'en 1997, dans leur ouvrage *Droit du cyberspace*, les auteurs P. Trudel, F. Abran, K. Benykhlef et S. Hein⁶³, soulignaient ce qui suit aux pages 11-49 et 11-54 :

«En principe, les agissements d'un employé, dans l'exécution de ses fonctions, ne relèvent pas de sa vie privée.

(...)

D'ailleurs, D'Aoust, Leclerc et Trudeau considèrent qu'il est même préférable d'examiner la question à l'étude sous l'angle de la condition de travail «raisonnable» plutôt que sous le concept de «droit à la vie privée» puisqu'en milieu de travail, sauf exception très particulière (par exemple, l'usage des toilettes, l'administration des premiers soins en cas de malaise ou d'accident, etc.), la vie privée du salarié est plutôt restreinte.»

Cependant, suite à des décisions récentes, mais qui s'accumulent, cette position traditionnelle doit être nuancée.

De fait, les tribunaux québécois se sont inspirés en cela de la jurisprudence développée par la Cour suprême du Canada en matière criminelle.

D'abord, dans l'affaire *R. c. Dyment*, la Cour suprême s'est refusée de confiner au seul domicile de l'individu l'étendue de la «sphère de protection de la vie privée» :

«Comme nous l'avons déjà souligné, les revendications d'ordre territorial étaient à l'origine légalement et conceptuellement liées à la propriété, ce qui signifiait que les revendications d'un droit à la propriété en ce sens étaient, sur le plan juridique, largement confinées au domicile. Mais, comme *Weston*, précité, à la p. 303, le fait observer, [traduction] «protéger la vie privée au domicile seulement [...] revient à protéger ce qui n'est devenu, dans la société contemporaine, qu'une petite partie du besoin environnemental quotidien de la vie privée de l'individu⁶⁴.»

Dans une décision récente, *Srivastava c. Hindu Mission Canada*, la Cour d'appel du Québec s'exprime ainsi, quant à la valeur des décisions de droit criminel dans une analyse de l'expectative de vie privée dans un contexte civil :

«Dans son dispositif, le juge [de première instance] affirme que les appelants ne citent que des causes criminelles, sauf une en matière civile. Avec égards, je crois que ceci ne constitue pas une faiblesse dans

⁶³ Précité, note 50

⁶⁴ [1988] 2 R..CS. 417, à la page 428.

l'argumentation des appelants. En effet, la jurisprudence concernant l'article 8 de la Charte canadienne protège la vie privée des citoyens contre l'ingérence d'autrui, la seule différence étant que la Charte canadienne ne s'applique qu'aux actions gouvernementales. Étant donné que les deux Chartes protègent essentiellement le même droit à la vie privée, il n'est pas surprenant de constater que les décisions concernant l'article 5 de la Charte québécoise font souvent appel aux principes énoncés en vertu de l'article 8 de la Charte canadienne. En effet, dans les causes civiles impliquant le droit à la vie privée, les juges commencent souvent leur analyse en se demandant si la personne visée possède une expectative raisonnable de vie privée. L'utilisation de cette notion empruntée du droit pénal restreint l'application de l'article 5 de la Charte québécoise, et amène avec elle le critère de l'ensemble des circonstances qui détermine si une personne a une expectative raisonnable de vie privée quant à un lieu, objet ou information

[...] Il faut souligner que la Charte canadienne ne s'applique pas en l'espèce (la requête ne vise pas une action gouvernementale) mais qu'on peut s'en inspirer pour interpréter la Charte québécoise.»⁶⁵

Ce n'est donc pas une raison valable d'écarter du domaine de la protection de la vie privée une communication ou une information personnelle pour le seul motif qu'elle est survenue ou a été obtenue en milieu de travail, en cours d'emploi. Il faut pousser plus loin l'analyse pour déterminer les circonstances particulières où cette communication ou information personnelle a été véhiculée.

Mes Jean Yoon et Marie-Hélène Constantin écrivent ce qui suit à cet égard :

«Comme nous l'avons vu plus haut, les tribunaux ont, en général, interprété la notion de vie privée en établissant une distinction entre ce qui constitue la sphère publique de la vie d'un individu et ce qui constitue sa sphère privée. Afin de déterminer ce qui constitue cette sphère privée, les tribunaux se sont fiés au critère de l'expectative raisonnable de vie privée.

Il est intéressant de noter que la Cour suprême du Canada, dans *Thomson Newspaper*, a reconnu qu'une distinction devait être apportée lorsqu'un tribunal est confronté à l'examen d'une question relative à la fouille et à la vie privée dans un milieu de travail. Dans cette décision, la Cour avait à se pencher sur le pouvoir d'un tribunal administratif de contraindre une personne à témoigner et à produire des documents. Il s'agissait, dans ce

⁶⁵ REJB 2001-23958, décision rendue le 30 avril 2001, (C.A.), aux paragraphes 68 et 69 (Requête pour autorisation de pourvoi à la Cour suprême 28686)

cas, de documents provenant d'une entreprise. Le juge LaForest a analysé cette question comme suit :

‘Bien que ces dossiers ne soient pas dépourvus d'intérêt de nature privée, il est raisonnable de dire qu'ils soulèvent des préoccupations beaucoup moins importantes que les documents personnels. L'argument suprême à l'appui d'une garantie constitutionnelle du droit au respect de la vie privée repose sur notre conviction, conforme à tant de nos traditions juridiques et politiques, qu'il appartient à l'individu de déterminer la façon dont il mènera sa vie privée. Il appartient à l'individu de décider quels sont les groupes ou personnes qu'il fréquentera, les livres qu'il lira, etc. Ces dossiers et documents ne contiennent habituellement pas de renseignements relatifs au mode de vie d'une personne, à ses relations intimes ou à ses convictions politiques ou religieuses. Bref, ils ne traitent pas de ces aspects de l'identité personnelle que le droit à la vie privée vise à protéger de l'influence envahissante de l'État.’

La Cour suprême établit donc clairement une distinction entre des documents appartenant à une entreprise et des documents strictement privés. Par analogie, il semble clair que le droit à la vie privée ne vise pas à empêcher l'accès par un employeur aux fichiers électroniques contenus dans les ordinateurs de ses employés lorsque ces fichiers sont des documents de l'entreprise fruit du travail des salariés.

De plus, dans *R. c. Wong*⁶⁶, la Cour suprême a clairement affirmé que les limites imposées à l'État dans son droit de surveillance sont beaucoup plus strictes que les limites qui s'imposeraient entre particuliers. La Cour s'exprime ainsi :

‘L'arrêt *R. c. Duarte* était fondé sur la notion selon laquelle il existe une distinction cruciale entre le fait de s'exposer au risque que l'on surprenne notre conversation et celui de s'exposer au risque, beaucoup plus dangereux que nos propos soient enregistrés électroniquement en permanence à la seule discrétion de l'État. Si l'on transpose cette notion pour l'appliquer à la technologie en cause en l'espèce, il s'ensuit nécessairement qu'il existe une différence importante entre le risque que nos activités soient observées par d'autres personnes et le risque que des agents de l'État, sans autorisation préalable, enregistrent de façon

⁶⁶ [1990] 3 R.C.S. 36, page 48.

permanente ces activités sur bande magnétoscopique, une distinction qui, dans certaines circonstances, peut avoir des conséquences en matière constitutionnelle. Refuser de reconnaître cette distinction, c'est refuser de voir que la menace à la vie privée inhérente à la vie en société, dans laquelle nous sommes soumis à l'observation ordinaire d'autrui, n'est rien en comparaison avec la menace que représente pour la vie privée le fait de permettre à l'État de procéder à un enregistrement électronique permanent de nos propos ou de nos activités. Voilà un facteur important à considérer lorsqu'il s'agit de déterminer s'il y a violation d'une attente raisonnable en matière de respect de la vie privée dans des circonstances données.'

Les décisions relatives à l'article 8 de la *Charte canadienne* ne s'appliquent donc pas de façon absolue afin d'établir ce qui constitue la vie privée en milieu de travail.

Comme nous l'avons affirmé plus tôt, la situation d'un employeur qui veut avoir accès à des dossiers de l'entreprise contenus sur les ordinateurs de l'entreprise qui ne sont utilisés que pour les fins du travail ne pose pas de difficulté réelle. L'employeur pourrait avoir accès à ces dossiers. Il reste cependant plusieurs zones grises où le droit de surveillance et de contrôle de l'employeur est moins bien défini.

Dans *Thomson Newspaper*⁶⁷, la Cour suprême rattache la protection garantie par la Constitution au type d'information qui pourrait être divulguée. L'information que la Cour semble vouloir protéger est celle qui se rattache aux caractéristiques personnelles de l'individu. De même, lorsque nous avons examiné l'article 35 du *Code civil du Québec*, nous avons pu constater que le législateur tentait, là encore, de protéger une zone touchant l'individu dans ses particularités les plus intimes. En effet, l'énumération, non limitative, de types d'actes qui peuvent violer la vie privée, s'attachent à la violation du domicile, à la violation de conversations ou correspondance privées ou à la violation du droit à l'image. Il s'agit donc de situations qui sont purement privées ou qui mettent en jeu le droit de l'individu de s'exprimer ou de communiquer ses idées personnelles aux individus de son choix sans peur de représailles.

La Cour suprême affirme, de plus, dans *Thomson Newspaper*, que le milieu de travail peut d'une certaine façon, constituer une aire privée de la vie d'un employé. En effet, le juge LaForest affirme que :

⁶⁷ [1990] 1 R.C.S. 425, aux pages 521-522.

‘Il va de soi que les personnes qui font partie d’une entreprise attachent plus d’importance à l’intégrité physique de leur domicile qu’aux dossiers et documents de l’entreprise. Mais cela ne signifie pas qu’ils n’attachent pas non plus d’intérêt à la protection des locaux de l’entreprise. Bien que l’on puisse raisonnablement dire que les dossiers d’entreprise ne contiennent habituellement pas de renseignements relatifs aux affaires, aux opinions et aux fréquentations personnelles d’un particulier, on ne peut affirmer la même chose avec autant de conviction de tout ce qui peut être trouvé ou observé dans les dossiers ou les locaux de l’entreprise. Les gens qui travaillent dans des bureaux (le genre de milieu de travail où l’on perquisitionnerait habituellement en vertu de la *Loi relative aux coalitions*) perçoivent ceux-ci comme un endroit personnel, un peu comme ils perçoivent leur domicile, et agissent en conséquence. Cela traduit en partie le besoin compréhensible d’humaniser un environnement fréquenté une bonne partie de la journée. Cela peut refléter en partie le simple fait que la vie humaine ne peut être compartimentée en sections professionnelles et personnelles étanches correspondant au bureau et au domicile. D’ailleurs, un bureau peut s’avérer plus privé que le domicile en ce qui concerne les relations familiales. Peu importe la raison, il est effectivement probable que l’on trouvera dans un bureau des lettres personnelles, des répertoires d’adresses et de numéros de téléphone privés et bien d’autres indices de la vie personnelle de son occupant’.⁶⁸»

À nouveau dans l’affaire *Srivastava*, M. le juge Robert, au nom de la Cour, énumère ainsi les différents facteurs qui doivent être pris en compte dans la détermination des attentes raisonnables de vie privée, dans ce cas, en milieu de travail (nous ajouterions «sur les lieux du travail») :

«La présence au moment de la perquisition;

La possession ou contrôle du bien ou du lieu faisant l’objet de la fouille ou perquisition;

La propriété du bien ou du lieu;

L’habilité à régir l’accès au lieu, y compris le droit d’en exclure autrui;

L’existence d’une attente subjective en matière de vie privée;

⁶⁸

J. Yoon et M.-H. Constantin, *Les outils technologiques et leur impact sur le droit du travail*, Colloque sur le droit du travail, Martineau Walker, 1997, aux pages 9 à 12.

Dans cette affaire, l'employé qui poursuivait son employeur pour violation de sa vie privée était un prêtre hindou, employé dans un temple de la région de Montréal. Sa ligne téléphonique au temple avait été mise sous écoute après que les membres du Conseil d'administration du temple se soient réunis et aient décidé de cette mesure parce qu'ils avaient des inquiétudes relativement à des appels interurbains non autorisés, ainsi qu'à des vols de sommes d'argent au temple. Les membres du conseil procédèrent ensuite, dans une réunion ultérieure, à l'écoute des cassettes, et découvrirent que le prêtre entretenait des contacts soutenus avec une dame membre de la communauté hindoue, qui fréquentait le temple. Ils conclurent de cette écoute que les deux interlocuteurs avaient une relation amoureuse et, après une intervention d'un des membres du temple, le prêtre remit sa démission. La Cour d'appel, dans sa décision, considère que l'écoute téléphonique en question est une atteinte à la vie privée du prêtre, et accorde des dommages à ce dernier, ainsi qu'à son interlocutrice, qui a elle aussi été victime des rumeurs de liaison amoureuse avec un prêtre marié.

La Cour, sous la plume du juge Robert, s'exprime ainsi :

«La décision du juge s'appuie sur le droit de propriété du téléphone ainsi que sur l'utilisation historique de celui-ci, toutefois elle ne traite pas de la conversation elle-même. Or, la question fondamentale en l'espèce est celle de savoir si la conversation est protégée et non le téléphone. En effet, je crois que l'emphase doit être mise sur l'attente subjective de la personne face à la conversation, son caractère raisonnable, ainsi que la nature de celle-ci. À défaut de quoi, il serait très difficile pour quelqu'un de prouver une expectative de vie privée quant à tout élément intangible ne pouvant être grevé d'un droit de propriété.

Il est possible dans ce cas d'assimiler la conversation téléphonique en cause à un échange d'informations entre deux personnes. Dans un tel cas, la nature de l'information ainsi que celle des interlocuteurs deviennent des facteurs importants afin de déterminer si la conversation est protégée par l'article 5 de la Charte québécoise. En l'espèce, il est évident que subjectivement, dans le temple, Sharma [le prêtre] s'attendait à pouvoir communiquer de manière privée avec Mme Srivastava au téléphone. De plus, les conversations enregistrées étaient de nature privée. Les appelants étaient des bons amis qui partageaient leurs peines et succès par le biais du téléphone. En conséquence, il serait illogique d'affirmer que les appelants n'avaient pas une expectative raisonnable de vie privée quant aux conversations. La nature et le ton des conversations démontrent clairement le contraire.

[...]

⁶⁹ *Srivastava c. Hindu Mission Canada*, précitée, note 65, paragraphe 68.

Les conversations téléphoniques interceptées par l'intimé étaient nécessairement privées et privilégiées. Les conversations entre un prêtre et ses fidèles sont protégées par l'article 9 de la Charte québécoise. Ainsi, le fidèle qui recherche conseil et directive spirituels auprès d'un prêtre jouit d'une assurance quasi constitutionnelle de non-divulgateion.

De même, l'assignation du prêtre au temple pendant des journées entières, impliquait l'utilisation par ce dernier de l'appareil téléphonique pour des besoins exclusivement privés. Bref, il existait peu ou pas de relation logique entre les écoutes téléphoniques et les motifs inscrits à la résolution pour les effectuer.»⁷⁰

En conclusion, nous constatons que la Cour d'appel du Québec semble avoir retenu ce que nous regrouperons en trois critères importants pour déterminer s'il existe ou non une attente raisonnable à une sphère de protection de la vie privée à l'égard d'un lieu particulier. Nous résumerons ces trois critères de la façon suivante :

- Qui contrôle la propriété ou l'accès au lieu concerné ?
- Qui contrôle l'utilisation du bien ou des outils informatiques qui feraient l'objet du contrôle et de la surveillance ?
- Existe-t-il une attente raisonnable de protection de la vie privée ?

C'est ce qui explique la différence qui doit être faite entre les cas de contrôle et de surveillance des activités d'un employé hors établissement (comme dans l'affaires *Bridgestone/Firestone*⁷¹) et les cas de contrôle et de surveillance sur les lieux du travail. Dans ces derniers cas, les deux premiers critères trouvent facilement réponse. D'où l'importance du dernier critère. C'est ce qu'énonce la Cour d'appel dans l'affaire *Srivastava*⁷². Il sera donc fortement conseillé à un employeur d'encadrer l'utilisation des ressources informatiques mises à la disposition de ces employés et ce, au moyen d'une politique et de directives claires. À notre avis, l'adoption de politiques ou directives en matière d'utilisation des outils informatiques de l'entreprise constitue la façon d'éviter de créer une attente raisonnable d'une sphère de vie privée dans le cadre de l'exercice des fonctions d'un employé au sein de l'entreprise.

Nous n'avons pas retracé de décision qui établirait qu'une interdiction totale faite aux employés d'une entreprise d'utiliser Internet et le courriel à des fins privées pourrait être considérée comme nulle parce que contraire au droit à la vie privée ou comme constituant une condition de

⁷⁰ Id., paragraphes 71 à 74.

⁷¹ Précitée, note 57.

⁷² Précitée, note 65

travail déraisonnable en contravention à l'article 46 de la *Charte québécoise des droits et libertés de la personne* ou à l'article 2087 C.c.Q.⁷³.

On peut renoncer à son droit à la vie privée⁷⁴. En conséquence, les politiques claires de l'entreprise et l'affichage à l'écran limitant l'usage d'Internet et du courriel aux seules fins de l'exercice des fonctions de l'employé pourront constituer un avis suffisant entraînant la renonciation de l'employé à sa sphère de protection de la vie privée, dans le cadre de son travail, s'il utilise néanmoins les outils informatiques à des fins personnelles.

C'est ce que nous déduisons de la distinction tirée par la Cour d'appel dans l'affaire *Srivastava* lorsqu'elle souligne que dans l'arrêt *Saulnier* de cette même Cour, le juge Moisan mettait l'accent sur le fait que le contenu des conversations interprétées qu'on voulait mettre en preuve, ne portait pas sur des matières relevant de la vie privée de l'employé, de ses relations familiales ou sociales, mais uniquement d'affaires commerciales. Donc, que la vie privée des interlocuteurs n'était pas en cause⁷⁵. Alors que, dans *Srivastava*, M. le juge Robert prend l'occasion de souligner que l'assignation du prêtre au temple pendant des journées entières, impliquait l'utilisation par ce dernier de l'appareil téléphonique pour des besoins exclusivement privés. D'où la nécessité pour l'employeur dans ce dernier cas (où le droit de l'employé d'utiliser le téléphone pour des fins personnelles était connu et reconnu) d'établir et de démontrer une relation logique entre les écarts téléphoniques et les motifs pour y procéder⁷⁶.

De plus, en pratique, il y a des milieux de travail où même le droit de logger ou de recevoir des appels téléphoniques est restreint aux seuls cas d'urgence.

Selon nous, s'il n'y a pas d'attente raisonnable d'une sphère de protection de la vie privée, l'employeur ne sera pas empêché pour ce motif d'exercer une surveillance de l'utilisation des outils informatiques par ses employés... sous réserve que la manière choisie pour exercer cette surveillance soit qualifiée de raisonnable. Vu la nature moins «envahissante» de la surveillance électronique (par opposition à une surveillance vidéo), il y a lieu de croire que les tribunaux accepteraient de reconnaître la validité d'une certaine forme de surveillance électronique permanente (par exemple, par enregistrement et conservation des données sur le disque dur de l'entreprise).

L'arrêt *Bridgestone/Firestone*⁷⁷ énonce les principes d'une surveillance hors établissement. La Cour d'appel du Québec, sous la plume de M. le juge Louis LeBel, a d'une part souligné que le *problème* de la surveillance d'un salarié (dans ce cas, absent du travail pour des raisons de santé à la suite d'un accident du travail) ne saurait se régler abruptement en donnant au concept de vie

⁷³ *Glopak inc. et Métallurgistes unis d'Amérique, section locale 7625*, 2000, R.J. DT-1841 (T.A.), à la page 1855.

⁷⁴ À titre d'exemple, *Lac D'Amiante du Québec Ltée, 2858-0702 Québec Inc.*, 2001 CSC 51, 13 septembre 2001, par. 42 (m. le juge Le Bel).

⁷⁵ *Srivastava c. Hindu Mission Canada*, précitée, note 65, par. 66

⁷⁶ *Idem*, par. 74.

⁷⁷ Précitée, note 65

privée une signification essentiellement territoriale. La Cour d'appel continuait qu'on ne saurait non plus en disposer en induisant de l'existence d'un contrat ou d'une relation de travail une renonciation aux protections de la vie privée de la part du travailleur. Dans cet arrêt, la Cour d'appel a souligné que bien que l'on doive reconnaître que la surveillance, au sens du paragraphe 36(4) C.c.Q. comporte à première vue une atteinte à la vie privée, cela ne signifiait surtout pas que toute surveillance par l'employeur hors des lieux du travail ait été illicite. La Cour d'appel soulignait qu'en substance bien qu'elle comporte une atteinte apparente au droit à la vie privée, la surveillance à l'extérieur de l'établissement pouvait être admise si elle était justifiée par des motifs rationnels et conduite par des moyens raisonnables, comme l'exige l'article 9.1 de la Charte québécoise⁷⁸.

C'est ainsi que la Cour d'appel concédait qu'un employeur avait un intérêt sérieux à s'assurer de la loyauté et de l'exécution correcte par le salarié de ses obligations, lorsque celui-ci recourt au régime de protection contre les lésions professionnelles. Mais avant d'employer une méthode de surveillance (en l'espèce la filature et l'enregistrement sur vidéo d'épisodes de la vie courante du salarié, hors des lieux du travail), il fallait que l'employeur démontre avoir des motifs sérieux lui permettant de mettre en doute l'honnêteté du comportement de l'employé. Au niveau du choix des moyens, il faut que la mesure de surveillance, notamment la filature, apparaisse comme nécessaire pour la vérification du comportement du salarié et que, par ailleurs, elle soit menée de la façon la moins intrusive possible. Lorsque ces conditions sont réunies, l'employeur a le droit de recourir à des procédures de surveillance qui doivent être aussi limitées que possible :

«Il ne saurait s'agir d'une décision purement arbitraire et appliquée au hasard. L'employeur doit déjà posséder des motifs raisonnables avant de décider de soumettre son salarié à une surveillance. Il ne saurait les créer a posteriori, après avoir effectué la surveillance en litige.

Au départ, on peut concéder qu'un employeur a un intérêt sérieux à s'assurer de la loyauté et de l'exécution correcte par le salarié de ses obligations, lorsque celui-ci recourt au régime de protection contre les lésions professionnelles. Avant d'employer cette méthode, il faut cependant qu'il ait des motifs sérieux qui lui permettent de mettre en doute l'honnêteté du comportement de l'employé.

Au niveau du choix des moyens, il faut que la mesure de surveillance, notamment la filature, apparaisse comme nécessaire pour la vérification du comportement du salarié et que, par ailleurs, elle soit menée de la façon la moins intrusive possible. Lorsque ces conditions sont réunies, l'employeur a le droit de recourir à des procédures de surveillance, qui doivent être aussi limitées que possible :

⁷⁸

Idem, aux pages 34 et 35.

‘In suspicious circumstances surrounding the medical condition of the grievor, the employer has every right to conduct a full investigation but only as a last step should it choose the intrusive alternative of invading the employee’s privacy by conducting surveillance. (Re Alberta Wheat Pool and Grain Workers’ Union, Local 333, 48 (L.A.C.) (4th) 341, p. 345, arbitre B. Williams)’

L’exécution de la surveillance doit ainsi éviter des mesures qui porteraient atteinte à la dignité d’un salarié⁷⁹.»

C’est ce sujet que nous abordons maintenant.

(2.3) Le droit à des conditions de travail justes et raisonnables

L’article 46 de la *Charte québécoise des droits et libertés de la personne* stipule ce qui suit :

«46. Toute personne qui travaille a droit, conformément à la loi, à des conditions de travail justes et raisonnables et qui respectent sa santé, sa sécurité et son intégrité physique.»

Le *Code civil du Québec*, à son article 2087, complète les exigences en la matière de la façon suivante :

«2087. L’employeur, outre qu’il est tenu de permettre l’exécution de la prestation de travail convenue et de payer la rémunération fixée, doit prendre les mesures appropriées à la nature du travail, en vue de protéger la santé, la sécurité et la dignité du salarié.»

Ces droits reconnus aux employés ont été invoqués soit dans le contexte où un employeur désirait procéder à une fouille de ses employés ou de leurs effets ou soit dans le but de tenter de circonscrire le droit d’un employeur de procéder à la surveillance de ses employés à l’intérieur ou à l’extérieur de son établissement.

C’est pourquoi, nous avons déjà tenté de tracer les paramètres relatifs au droit de fouille et à la surveillance des employés par l’employeur de la façon suivante :

«Bien que (sous réserve de contraintes légales ou contractuelles) l’employeur soit généralement libre d’administrer son entreprise et de gérer son personnel comme bon lui semble, les tribunaux d’arbitrage ont rejeté l’argument voulant que les droits de gérance permettent à eux seuls

⁷⁹ Idem, aux pages 36 et 37.

de procéder à une fouille. La jurisprudence reconnaît toutefois que l'employeur peut acquérir ce droit et ce, de deux façons :

- soit contractuellement; par exemple, par l'existence d'une clause spécifique dans le contrat d'emploi de l'employé, dans la convention collective, dans le formulaire d'embauche ou encore, dans le manuel de règlement remis à l'employé lors de son embauche;
- soit par le biais d'une pratique passée; dans ce dernier cas, la procédure de fouille devra avoir été appliquée de façon suffisamment constante et uniforme avant de conclure qu'elle fut connue et acceptée par les employés.

En d'autres termes, les employés doivent donc savoir que la vérification de leurs effets personnels fait partie de leurs conditions d'emploi.

En l'absence de clause particulière dans le contrat d'emploi ou d'une pratique passée, la jurisprudence a retenu certaines considérations qui pourraient constituer des justifications suffisantes pour qu'un employeur puisse procéder à la fouille des biens de ses employés. Parmi ces circonstances, on note l'épidémie de vols de biens appartenant à l'employeur, la nature de l'entreprise, les soupçons de vol contre un employé.

(...)

Même si l'employeur a obtenu implicitement ou expressément le droit de fouiller les effets de ses employés, ces fouilles devront toujours respecter le critère de la raisonnable. Il est à noter que certaines décisions laissent croire que le test de raisonnable sera appliqué plus rigoureusement dans le cas d'une fouille de la personne que dans celui d'une fouille de biens personnels.

(...)

Le droit à la surveillance électronique, tel qu'interprété jusqu'à maintenant par les tribunaux, n'est toutefois pas absolu et l'employeur se doit de respecter certains paramètres. Des autorités ont tenté de dégager cinq de ces paramètres :

1. L'employeur peut, en vertu de la notion de subordination juridique et sa fonction de gestion, contrôler le travail des salariés;
2. *Prima facie*, l'employeur ne pourrait recourir à l'utilisation de caméras pour surveiller le comportement et la productivité des salariés au travail;

3. Une surveillance continue pourrait constituer une condition de travail déraisonnable et contrevenir à l'article 46 de la *Charte des droits et libertés de la personne* (Québec);
4. Une telle surveillance est permise dans des circonstances particulières, par exemple lorsque l'employeur peut démontrer qu'un problème sérieux de sécurité existe et que ce type de surveillance pourra à court terme ou moyen terme l'aider à le surmonter;
5. L'employeur qui a des motifs sérieux de procéder à une surveillance électronique des lieux de travail doit porter le moins possible atteinte au droit du salarié à des conditions de travail justes et raisonnables⁸⁰.»

Par analogie avec les principes déjà connus en matière de surveillance et de fouille des employés développés par la jurisprudence arbitrale, plus particulièrement en matière de surveillance électronique par caméra vidéo, nous rappellerons ce qui suit :

- l'employeur peut, en vertu de la notion de subordination juridique et sa fonction de gestion, contrôler le travail des employés et, en conséquence, surveiller le courrier électronique d'affaires de ceux-ci;
- la surveillance du courrier électronique (de nature personnelle) d'un employé et l'accès à celui-ci seraient permis dans des circonstances particulières, par exemple lorsque l'employeur a des motifs raisonnables de croire que l'employé utilise le courrier électronique de façon contraire à la loi, à la convention collective, au contrat de travail, aux règlements ou pratiques internes de l'entreprise, etc.;
- mais, dans tous les cas, même lorsque l'employeur possède de tels motifs sérieux pour procéder à la surveillance du courrier électronique d'un employé et à y accéder, les moyens choisis pour ce faire doivent porter le moins possible atteinte aux droits fondamentaux de l'employé, dont le droit à la protection de la vie privée⁸¹.

⁸⁰ K. Delwaide, «La protection de la vie privée et les nouvelles technologies : L'accès au courrier électronique des employés par un employeur», *Congrès annuel du Barreau (1997)*, précité, note 34, plus particulièrement aux pages 641-642, 643 et 647-648. Voir aussi J. Yoon et M.-H. Constantin, *Les outils technologiques et leur impact sur le droit du travail*, précité, note 68. Pour les paramètres relatifs au droit de surveillance, voir *Association des techniciennes et techniciens en diététique du Québec et Centre hospitalier Côte-des-Neiges*, D.T.E. 93T-1329 (T.A.). Quant au cinquième paramètre, voir P.-Y. Bourdeau, *La surveillance par caméra vidéo des lieux de travail*, précité, note 62.

⁸¹ K. Delwaide, « La protection de la vie privée et les nouvelles technologies : L'accès au courrier électronique des employés par un employeur », précité, note 34, pages 658-659.

Nous ajouterons qu'il faut aussi tenir compte du fait que la nature de la surveillance des outils informatiques diffère de celle effectuée par caméra ou enregistrement audio ou vidéo. On peut certes concevoir qu'une surveillance vidéo permanente porte atteinte à la dignité d'un employé. Mais la conservation sur disque dur des frappes informatiques des employés ne nous apparaît pas rencontrer le même caractère d'atteinte à l'intégrité ou à la dignité d'un employé de façon à priver un employeur d'y avoir recours. Cela est nettement différent de la captation et de l'enregistrement vidéo des moindres faits et gestes des employés. Ainsi, il ne nous apparaît pas déraisonnable qu'il soit reconnu à l'employeur le droit de procéder aux vérifications générales d'usage sur l'utilisation de son système informatique, en lien avec la raison d'être d'un tel système (aide à l'exécution des tâches) et des paramètres d'utilisation qu'il aura fixés et énoncés à ses employés. Nous apparaît légitime le processus de vérification de la fiabilité du système informatique et de son rendement de même que la détermination des causes des problèmes de fonctionnement, s'il y en a.

D'un autre côté, les développements technologiques en la matière devront être examinés pour déterminer le droit d'un employeur de procéder, sans motif préalable, à une surveillance constante et directe de l'utilisation des outils informatiques d'un employé en particulier. Il se développe maintenant des «logiciels-filtres» qui bloquent l'accès à certains sites d'Internet ou à certaines utilisations informatiques. À ce moment, les tribunaux devraient considérer la raisonnable de l'implantation de tels logiciels-filtres afin d'éviter qu'un employeur procède de façon systématique à une surveillance directe d'un ou plusieurs employés identifiés et ce, sans raison valable.

Au surplus, si des motifs raisonnables étaient fournis à un employeur (comme des indications d'abus de système, vol de temps, temps supplémentaire exagéré et non justifié, plainte d'un client ou d'un employé, etc.) ou si une vérification d'usage du système informatique faisait ressortir un problème relié à un usage inapproprié des outils informatiques, la surveillance systématique et continue de l'employé visé par ces plaintes ou à la solution du problème pourrait devenir légalement justifiée... en autant qu'elle soit effectuée en lien avec les plaintes formulées ou au problème noté et pour une période de temps raisonnable à la vérification du bien-fondé de ces plaintes ou à la solution du problème.

* * *

De ce qui précède, nous devons conclure qu'en principe, l'employeur devrait se voir accorder une plus grande latitude à l'égard du contrôle et de la surveillance qu'il désire pratiquer sur ses employés en milieu de travail et ce, plus particulièrement à l'égard des outils de travail qu'il leur fournit et dont il est le propriétaire. Cependant, il serait incorrect de prétendre que les employés se verraient nier d'une façon générale une sphère de protection de vie privée en milieu de travail du simple fait que le lieu de travail ne pourrait en lui-même être tributaire d'une attente raisonnable de protection de la vie privée. Les décisions des tribunaux contiennent suffisamment d'indices, voire de commentaires directs, à l'effet que la sphère de protection de vie privée d'une personne n'est pas rattachée exclusivement aux lieux où elle désire invoquer cette protection.

Si nous tentons de paraphraser les critères de reconnaissance d'une sphère de protection de la vie privée en milieu de travail, nous suggérerions qu'un double test, objectif et subjectif, serve à qualifier cette sphère de protection de la vie privée. D'une part, certains gestes sont intrinsèquement en eux-mêmes (objectivement) de la nature d'une activité personnelle et privée.

Il y a donc objectivement attente raisonnable de protection de la vie privée à l'égard de ces gestes. Telles sont, par exemple, l'utilisation normale et courante des salles de toilette, la dispensation de premiers soins, les conversations personnelles normales et courantes d'employés dans les aires de travail, etc.

D'autre part, certains gestes et certains lieux peuvent voir naître chez les employés une attente raisonnable de protection de la vie privée et ce, subjectivement, par l'attitude de l'employeur, expressément ou implicitement. C'est ainsi que la convention collective, le contrat de travail, une politique ou des directives de même qu'une pratique passée dans l'entreprise peut faire en sorte que les employés se voient reconnaître un «droit» d'utiliser à des fins personnelles et privées les outils de travail mis à leur disposition par l'employeur. Dans ce cas, l'employeur peut avoir fait naître chez ses employés une attente raisonnable de protection de vie privée lorsqu'il permet à ses employés de conserver dans des classeurs, dans des fichiers informatiques, des données à caractère personnel, voire lorsque l'employeur permet à ses employés d'utiliser les outils technologiques à des fins personnelles en autant, évidemment, que cela n'entre pas en conflit avec leurs obligations d'assurer une prestation de travail adéquate qualitativement et quantitativement.

Dès lors, l'employeur aura avantage à clarifier la situation par l'adoption de politiques et directives claires quant aux droits qu'il entend attribuer à ses employés d'utiliser (ou non) à des fins personnelles et privées les outils de travail mis à leur disposition par l'employeur.

Et encore, même cela fait, l'employeur devra porter une attention particulière à la manière dont seront effectués les contrôles et la surveillance de l'utilisation des outils électroniques qu'il met à la disposition de ses employés.

(2.4) L'expérience américaine

L'étude de principes récemment développés en droit américain s'avère très intéressante aux fins de notre recherche. Le congrès américain a adopté en 1986 le *Electronic Communications Privacy Act (E.C.P.A.)*. La législation a pour but d'interdire l'interception de communications électroniques par des individus non-autorisés. Cette loi comporte plusieurs exemptions spécifiques à son application. Bien qu'aucune de ces exemptions ne vise explicitement les employeurs, certaines d'entre elles peuvent être appliquées dans un contexte de relation de travail.

Des exemptions à la loi trouvent application lorsque l'une des parties y consent, lorsque le fournisseur du service de communication peut surveiller les transmissions et lorsque la surveillance est accomplie dans le cours normal des affaires. L'exemption relative au consentement trouve application dans le cadre d'une relation de travail lorsque l'employé a consenti que ce soit en signant une politique d'utilisation qui prévoit une telle surveillance, ou dans le cas de l'envoi d'un courriel contenant la politique à tous les employés. Quant à l'exemption visant le fournisseur de service, elle trouve application lorsque les installations informatiques et les logiciels d'utilisation sont la propriété de l'employeur. La dernière exemption concernant l'interception dans le cadre des affaires vise seulement les communications à caractère professionnel et ne trouverait pas application dans le cadre de l'interception d'une communication personnelle.

À ce jour, les tribunaux américains n'ont pas encore décidé s'ils devaient appliquer les dispositions de la *Electronic Communications Privacy Act* à la surveillance par un employeur du courrier électronique de ses employés. Ils semblent plutôt réticents à limiter ce droit et interprètent largement les exceptions prévues par la *ECPA*. Rappelons que la *Business Extension Rule* fut notamment invoquée pour permettre aux employeurs d'accéder aux boîtes vocales de leurs employés, si cette surveillance se fait dans le cours normal de ses affaires et si elle est justifiable dans le cadre des activités de l'entreprise. Les tribunaux américains ont toutefois appliqué des critères similaires dans l'étude des cas de surveillance électronique sur l'autoroute de l'information. En même temps, il ressort de l'étude de ces décisions qu'ils interprètent très largement cette exception d'affaires, aussi bien que l'exception de consentement. Cette législation s'appuie sur le même principe que celui développé par les tribunaux canadiens, soit celui de l'attente raisonnable de protection de la vie privée⁸². Nous allons examiner quelques décisions rendues relativement à l'application de cette loi.

Dans chaque cas répertorié, le tribunal en est arrivé à la conclusion qu'un employé ne peut raisonnablement s'attendre à ce que ses communications électroniques soient protégées par son droit à la vie privée. D'abord l'affaire *Smyth c. The Pillsbury Company*⁸³. Dans une contestation de congédiement formulée sur la base d'une atteinte à la vie privée (des dirigeants de la compagnie avait vu une copie d'une correspondance électronique au contenu offensant et avait congédié l'employé), une cour de district de l'état de Pennsylvanie a donné raison à

⁸² Une question intéressante pourra se soulever sur l'existence d'un «consentement» d'un employé à ce que l'employeur accède au courriel contenant des renseignements personnels en regard de l'article 14 de la *Loi sur la protection des renseignements personnels dans le secteur privé*. L'article 14 ne permet pas de dégager des consentements «implicites». En l'absence d'un consentement écrit et donné par l'employé et autorisant l'employeur à consulter les renseignements personnels contenus dans un fichier informatique, l'utilisation des outils informatiques en milieu de travail par l'employé et l'inclusion par celui-ci de renseignements personnels le concernant, sachant que l'employeur a le droit de contrôler et surveiller cette utilisation, peut-il constituer un consentement répondant aux critères de l'article 14? Qu'en est-il des renseignements personnels provenant de tiers acheminés à un employé de l'entreprise?

⁸³ *Smyth c. The Pillsbury Co.*, 914 F. Supp. 97 (E.D. PA. 1996).

l'employeur malgré le fait qu'afin de favoriser l'utilisation du courrier électronique, l'employeur avait de façon répétée, assuré les employés que les correspondances électroniques avaient un caractère confidentiel. Dans sa décision, la cour conclut que l'intérêt de l'employeur à prévenir des correspondances inappropriées et son droit de s'assurer du professionnalisme dans l'utilisation de son système de courrier électronique prévalaient sur le droit à la vie privée de l'employé, qui dans le contexte d'un contrat caractérisé par un lien de subordination, ne pouvait prétendre qu'à une faible expectative de vie privée. La Cour considère que l'employé avait renoncé à son droit à la vie privée en envoyant, par courrier électronique, à son superviseur, des commentaires désobligeants sur certains gérants et sur les activités sociales de la compagnie. La Cour s'exprime ainsi:

«(...) Even if we found that an employee had a reasonable expectation of privacy as to the contents of his E:mail communications over the company E:mail system, we do not find that a reasonable person would consider the company's interception of these communications to be a substantial and highly offensive invasion of his privacy. By intercepting such communications the company is not, as in the case of urine analysis or personal property searches, requiring the employee to disclose any personal information about himself or invading the employee's person or personal effects.

Moreover, the company's interest in preventing inappropriate and unprofessional comments or even illegal activity over its E:mail system outweighs any privacy interest the employee may have in those comments.»

Dans *Shoars c. Epson*⁸⁴, on a refusé d'appliquer une loi californienne interdisant la surveillance électronique au sens classique du terme. Dans cette affaire, l'employé invoquait cette loi pour justifier son refus de procéder, à la demande de l'employeur, à la surveillance du courrier électronique des autres employés. Sa demande en dommages pour congédiement illégal fut rejetée de même que l'action des employés qui étaient visés par la surveillance. De même, dans *Bourke c. Nissan Motors Corp.*⁸⁵, la compagnie avait congédié un employé après avoir intercepté certains de ses messages personnels, à teneur sexuelle dans la plupart des cas. Le tribunal refusa de reconnaître un droit à la vie privée à ce salarié, d'abord parce qu'il avait signé une entente reconnaissant que le système devait être utilisé pour des raisons d'affaires et ensuite, parce qu'il savait que l'employeur interceptait de temps à autre certains des messages électroniques reçus ou envoyés par ses employés.

⁸⁴ No. SCW112749 Cal. Sup. Ct., Los Angeles Cty., 1989.

⁸⁵ No. YC003979 Cal. Ct. App. 2d Div., July 26, 1993. Voir également *Andersen Consulting, LLP c. UOP and Bickel & Brewer*, 991 F. Supp. 1041 (N.D. III. 1998), *McVeigh c. Cohen*, 983 F.Supp. 215 (D.D.C. 1998) et *Bohach c. City of Reno*, 932 F. Supp.1232 (D. Nev. 1996).

De même, dans la décision *Bill McLaren Jr. v. Microsoft Corporation*⁸⁶, l'accès par un employeur aux courriels d'un employé qui avaient été enregistrés dans un fichier « personnel » de son ordinateur, et pour lequel seul l'employé connaissait le mot de passe d'accès, a été jugé correct et considéré comme ne violant pas le droit à la vie privée de l'employé. L'employé arguait, au soutien de la violation de sa vie privée, que le fait de posséder un mot de passe personnel était l'équivalent de posséder un casier avec un cadenas dont lui seul connaîtrait le code, une décision américaine antérieure⁸⁷ ayant jugé que la fouille d'un tel casier par un employeur violait la vie privée de l'employé. La Cour est en désaccord avec cette proposition, et s'exprime ainsi :

First, the locker in Trotti was provided to the employee for the specific purpose of storing personal belongings, not work items. In contrast, McLaren's workstation was provided to him by Microsoft so that he could perform the functions of his job. [...] Thus, contrary to his argument on appeal, the e-mail messages contained on the company computer were not McLaren's personal property, but were merely an inherent part of the office environment.

Further, the nature of a locker and an e-mail storage system are different. The locker in Trotti was a discrete, physical place where the employee, separate and apart from the other employees, could store her tangible, personal belongings. The storage system for e-mails is not so discrete. As asserted by McLaren in his petition, e-mail was delivered to the server-based "inbox" and was stored there to read. McLaren could leave his e-mail on the server or he could move the message to a different location. According to McLaren, his practice was to store his e-mail messages in "personal folders". Even so, any e-mail messages stored in McLaren's personal folders were first transmitted over the network and were at some point accessible by a third-party. Given these circumstances, we cannot conclude that McLaren, even by creating a personal password manifested - and Microsoft recognized - a reasonable expectation of privacy in the contents of the e-mail messages such that Microsoft was precluded from reviewing the messages.

On peut donc voir que le fait que des courriels aient circulé sur le réseau interne, même s'ils furent par la suite enregistrés dans un fichier personnel, annihile pour ainsi dire l'expectative de vie privée de l'employé par rapport à ces courriels, puisque, lorsqu'ils se trouvaient sur le réseau, l'employeur y avait accès.

⁸⁶ Case No. 05-97-00824, 1999 Tex. App. Lexis 4103 (Tex. Crt Of App., May 28, 1999).

⁸⁷ *Trotti*, 677 S.W. 2d., 637.

Dans *United States of America v. Mark L. Simons*⁸⁸, un employé du FBI se servait de l'ordinateur de son employeur au bureau pour télécharger des fichiers d'Internet, certains de ces fichiers comprenant de la pornographie infantile. Une politique d'entreprise existait relativement à l'utilisation du courrier électronique, et stipulait que l'employeur pouvait en tout temps avoir accès aux messages de l'employé, ainsi que conserver des rapports de l'usage que ce dernier faisait de l'Internet. L'employeur, après avoir été averti par un contractant de l'entreprise que cet employé visionnait des sites pornographiques, effectua une fouille de son disque dur, et exécuta une copie de plusieurs des fichiers qui s'y trouvaient, certains contenant de la pornographie infantile. L'employé fit appel aux Cours de justice américaines pour qu'elles sanctionnent cette violation de son droit à la vie privée. La 4th Circuit Court, en appel, estima que les droits de l'employé en vertu du quatrième amendement (droit à la vie privée) n'avaient pas été violés, parce que l'employé ne pouvait pas avoir d'expectative raisonnable de vie privée par rapport aux fichiers contenus dans son disque dur. La Cour s'exprime ainsi :

Government employees may have a legitimate expectation of privacy in their offices or in part of their offices such as their desks or file cabinets. [...] However, offices practices, procedures or regulations may reduce legitimate privacy expectations.

[...]

Simons did not have a legitimate expectation of privacy with regard to the record or fruits of his Internet use in light of the FBIS Internet policy. The policy clearly stated that FBIS would “audit, inspect and/or monitor” employees’ use of the Internet, including all file transfers, all websites visited, and all e-mail messages “as deemed appropriate”. »

Plus récemment, dans *Konop v. Hawaiian Airlines*⁸⁹, une Cour américaine déclarait que la visite non autorisée du site Web personnel d'un employé par son employeur était une violation du *Wiretap Act* et du *Stored Communications Act*. La Cour ajouta qu'une telle intrusion pouvait également contrevenir aux dispositions de la *Railway Labor Act*, qui prohibent la surveillance indue de l'activité syndicale par l'employeur. En l'espèce, Robert Konop était un pilote de la Hawaiian Airlines, et il avait créé le site en réaction à certaines concessions que son syndicat envisageait dans ses négociations avec l'employeur, et qu'il jugeait inacceptables. Le site n'était pas ouvert au public, et les mots de passe pour y accéder étaient distribués à des employés choisis, qui devaient auparavant entrer l'information les concernant et acquiescer aux conditions d'utilisation du site, qui impliquaient de ne pas divulguer l'information à de tierces parties. L'employeur demanda à un pilote d'y avoir accès pour lui, en ouvrant un compte, ce que le pilote fit, en utilisant le nom d'un autre pilote. L'employeur, après avoir visionné le contenu du

⁸⁸ Case No. 99-4238, (4th Cir., February 28, 2000).

⁸⁹ No. 99-55106 9th Cir. January 8, 2001), withdrawn (9th Cir., August 28, 2001)

site, menaçait de poursuivre Konop en diffamation, parce que le site contenait des critiques sur les employés et officiers de la compagnie, et des messages enjoignant aux pilotes de considérer une représentation syndicale alternative. La Cour considéra que le site comporte des « communications électroniques », lesquelles sont protégées aux États-Unis par le *Wiretap Act*, tel qu'il fut amendé en 1986 par le *Electronic Communications Privacy Act*, et s'exprima ainsi :

It is perfectly clear that the framers of the Wiretap Act's current definition of "electronic communications" understood that term to include communications in transit and storage alike... It makes no more sense that a private message expressed in a digitized voice recording stored in a voice mailbox should be protected from interception, but the same words expressed in an e-mail stored in an electronic post office pending delivery should not. We conclude that it would be equally senseless to hold that Konop's messages to his fellow pilots would have been protected from interception had he recorder them and delivered them through a secure voice bulletin board accessible by telephone, but not when he set them down in electronic text and delivered through a secure web server accessible by a personal computer. We hold that the Wiretap Act protects electronic communications from interception when stored to the same extent as when in transit. (nos soulignés)

Et plus loin:

In *NLBR v. Unbelievable Inc.*⁹⁰, we upheld that the Board's finding that the employer "engaged in unfair labor practices by eavesdropping on private conversation between employees and [a] Union representative," which occurred in the employee break room. We see no principled distinction between the employer's eavesdropping in Unbelievable and Hawaiian's access of Konop's secure website.

La Cour, en plus de condamner l'ingérence de l'employeur dans des activités syndicales, considère donc que le *Wiretap Act* protège indépendamment les communications pendant leur transmission et une fois qu'elles sont enregistrées sur support informatique, et non pas que cette loi s'applique uniquement aux communications pendant leur transmission. Cette position ne fut cependant pas adoptée dans l'affaire *Eagle Investment Systems Corporation v. Einar Tamm*, et al.⁹¹, où la cour jugea que la *Wiretap Act* ne protégeait que les

⁹⁰ 71 F. 3d 1434 (9th Cir. 1995)

⁹¹ 2001 U.S. Dist., Lexis 7349 (D. Mass., May 22, 2001)

communications interceptées pendant leur retransmission, et non pas les communications enregistrées sur support informatique, se basant notamment sur l'existence de la *Stored Communications Act*, qui prévoit la protection des communications une fois enregistrées (« *prohibits an unauthorized person to access stored electronic communications* ») (l'avantage de l'utilisation de la *Wiretap Act* étant qu'elle permet d'exclure une preuve obtenue en violation de ses dispositions).

(2.5) L'expérience française

Quelques mots, en parallèle, sur l'expérience française récente. La Cour de cassation a rendu une décision le 2 octobre 2001⁹², dans laquelle elle a jugé qu'un employeur ne peut, sans violer l'intimité de la vie privée et le secret des correspondances du salarié, « *prendre connaissance des messages personnels émis par le salarié et reçus par lui grâce à un outil informatique mis à sa disposition pour son travail et ceci même au cas où l'employeur aurait interdit une utilisation non professionnelle de l'ordinateur* »⁹³.

Le droit français semble donc privilégier le droit à la vie privée par opposition au droit américain qui semble davantage privilégier le droit de propriété de l'employeur, en lui donnant un droit de regard sur l'usage qu'un employé fait de ses outils de communications technologiques. C'est d'ailleurs l'analyse retenue par Mme Juliette Lenfant, dans son mémoire de maîtrise intitulé *Le droit à la vie privée s'étend-il à l'utilisation du courriel par un employé dans le cadre de ses fonctions ?*, dans lequel elle trace un portrait des positions française, américaine et québécoise en matière de pouvoirs des employeurs de lire les courriels de leurs employés. Elle place les États-Unis à l'extrême du spectre où « il ne semble y avoir aucune expectative de vie privée en matière d'utilisation du courrier électronique », alors que la jurisprudence française affirme au contraire la supériorité des droits fondamentaux. L'auteure place le Québec au milieu, dans une position où l'interception des courriels, si elle est plus aisée qu'en France, doit tout de même satisfaire à des conditions de travail justes et raisonnables⁹⁴.

⁹² *Nikon France c. Monsieur O.*, Arrêt no 4164 FS-P+B+R+I, en date du 2 octobre 2001 de la Chambre sociale de la Cour de cassation

⁹³ Cité dans le commentaire de l'arrêt disponible sur le site:
<http://www.foruminternet.org/actualites/lire.phtml?id=172>

⁹⁴ Mai 2000, Publié par Juriscom.net, numéro du 31 octobre 2000, <http://Juriscom.net>.

3. L'encadrement interne de l'utilisation d'Internet et du courriel par les employés : l'adoption de politiques et de directives claires par l'employeur

En l'absence d'une ligne jurisprudentielle clairement établie à ce stade, nous tenterons de dégager certaines recommandations pratiques dans la mise en place d'une politique ou de directives relatives à l'utilisation d'Internet et du courriel par les employés d'une entreprise⁹⁵.

Il est fondamental de garder en tête cet équilibre entre les intérêts sérieux et légitimes des employeurs (tels que nous les avons résumés au chapitre 1) et les intérêts sérieux et légitimes des employés (tels que plus amplement décrits au chapitre 2). Nous avons déjà fait ressortir dans notre analyse que nous suggérerions aux employeurs de ne pas attendre d'être poussés par les événements pour adopter une politique et des directives quant à l'utilisation d'Internet et du courriel par leurs employés. Il nous apparaît préférable de prendre les devants à ce sujet en se rappelant les trois principes généraux suivants :

- « - Never access an employee's e-mail without their consent, or
- Abolish passwords (personnels et inconnus de la direction) and make clear to employees that they should have no expectation of privacy in their e-mail, or
 - Provide employees with a clear statement of policy describing the circumstances in which their personal e-mail will be accessed, thereby dispelling any false sense of complete privacy⁹⁶. »

Nous partageons ce point de vue qui nous semble conforme aux préoccupations légitimes des employeurs tout en avisant clairement les employés des paramètres délimitant leur «sphère de protection de la vie privée» en milieu de travail.

Voyons maintenant comment, en pratique, ces trois principes généraux viendront s'articuler.

Les politiques ou directives en la matière devraient tenir compte des éléments suivants :

1. Elles devront tenir compte des contrats de travail ou des conventions collectives applicables;
2. Elles devront être raisonnables, non discriminatoires, uniformes et claires. Toute ambiguïté risque d'être interprétée contre l'employeur;

⁹⁵ N'oublions pas cet autre aspect pratique de la réalité des nouvelles technologies qui imposera aux entreprises d'adopter une ligne de conduite relative au contrôle et à la surveillance de leurs communications avec leurs clients ou auprès de tout visiteur de leur site Web. Un exemple de cet aspect de la question nous est donné par B.P. Dillingham et M.G. Salomon dans «Legal and Practical Pitfalls, A Premium on Online Privacy Policies» in *The Internet Newsletter*, Août 1999, aux pages 3 et 4.

⁹⁶ M.R. Brown, *Are Employee E-mail Messages really Private?*, 16 octobre 1996, à la page 2.

3. Elles devront spécifier que le non-respect de ces politiques et directives entraînera des sanctions, tout en incluant et précisant les sanctions qui pourraient être prises en cas de violation des politiques et directives;
4. Elles pourront préciser qu'elles s'appliquent à tous les moyens de communication mis à la disposition des employés par l'employeur et qui associent l'utilisateur à l'entreprise. Cette précaution s'avère indispensable avec l'avènement de la *Loi concernant le cadre juridique des technologies de l'information*, dont l'article 34 est traité au paragraphe (1.4) du présent texte;
5. Elles préciseront que l'accès aux outils de communication et leur utilisation par les employés sont considérés comme équivalant à «acceptation» par l'employé de se conformer aux politiques et directives les concernant;
6. Les employés devraient être avisés formellement de l'existence des politiques et directives en matière de contrôle et de surveillance des outils informatiques et du contenu de ces politiques et directives. Des rappels occasionnels devraient être faits. Idéalement, un avis devrait être affiché dès le moment où un employé vient se «connecter» («log in») au système informatique de l'entreprise, ce message requérant, si possible, un geste positif d'acceptation par l'employé indiquant qu'il a bien lu l'avis et qu'il en accepte la teneur. L'auteur Karen L. Casser prend la position suivante à ce sujet :

«4. Post a notice when employees log onto the computer network and require an affirmative acknowledgment by having the employee indicate that she has read the screen before moving on. The notice should state clearly that the system and e-mail are not private and will be audited and the parameters of employee use. It should also state on-line etiquette for using the network and company resources. For example:

“All systems and electronic communications are to be used for business purposes only and in accordance with company policies and procedures. All systems are subject to periodic company audit for business and security purposes. Please keep these guidelines in mind when using company networks and the Internet.”⁹⁷»

7. L'employeur doit indiquer que les usagers renoncent à invoquer tout droit à la vie privée à l'égard de toute information visionnée, créée, emmagasinée, envoyée ou reçue à l'aide des outils informatiques fournis par l'entreprise, que ces informations aient été à des fins professionnelles ou personnelles;

⁹⁷ K.L. Casser, *The Internet and Business: A Lawyer's Guide to the Emerging Legal Issues*, in *Employers, Employees, E-mail and The Internet*, précité, note 6, à la page 5.

8. Les politiques et directives devront informer les employés si l'utilisation des outils de communication est (ou non) limitée à leur travail. Nous suggérons que l'employeur informe ses employés que l'utilisation d'Internet et du courriel est limitée aux seules fins de l'exécution des fonctions de l'employé dans le cadre des activités de l'entreprise. Si l'employeur entend accepter dans une certaine mesure que son personnel utilise les outils informatiques à des fins personnelles, nous suggérons que l'employeur souligne qu'il tolère, à titre de privilège, l'utilisation occasionnelle à des fins personnelles d'Internet et du courriel dans la mesure où cette utilisation ne cause aucun préjudice à l'employeur et qu'elle demeure dans les limites de ce qui est raisonnable. L'employeur devrait utiliser un langage qui amène à comprendre qu'il est de la responsabilité de l'employé d'éviter tout abus du privilège qui lui est accordé. L'employeur devrait rappeler aux employés que les outils technologiques qui leur sont fournis au travail appartiennent à la compagnie;
9. Elles devront rappeler aux employés les règles générales d'utilisation des outils technologiques dont, notamment, leur devoir de confidentialité, de prudence, de diligence, de professionnalisme et de respect des droits d'autrui. À titre d'exemple, des politiques de ce genre interdisent généralement la consultation de matériel pornographique, violent ou autrement offensant. À ce sujet, tenant compte des coûts et de la faisabilité technique, l'entreprise devrait considérer implanter les «logiciels-filtres» appropriés;
10. Elles devraient faire la liste des prohibitions formelles comme l'interdiction de distribuer du matériel offensant, l'interdiction d'obtenir l'accès à certains dossiers et l'interdiction de distribuer de l'information personnelle sur les autres employés. C'est à ce chapitre que l'on retrouvera généralement les interdictions visant à compléter les politiques anti-discrimination et anti-harcèlement de l'employeur de même que les dispositions visant à interdire de copier des logiciels, des fichiers ou toute autre information électronique sans la permission du détenteur des droits d'auteur, ce qui devrait couvrir non seulement les droits dont l'employeur est bénéficiaire, mais aussi la situation où un employé serait tenté de télécharger des logiciels ou autres «œuvres» dont des tiers seraient détenteurs des droits d'auteur;
11. Pour compléter ces interdictions, l'employeur devrait néanmoins prévoir qu'advenant le cas où des fichiers informatiques ou autres logiciels étaient téléchargés, ceux-ci doivent être vérifiés en tout temps pour détecter la présence de virus ou d'autres programmes destructifs avant d'être reproduits sur le système informatique de l'entreprise. Il y aurait lieu d'insister pour que les courriels provenant d'expéditeurs inconnus soient effacés sans être ouverts, sauf sur consultation préalable avec les personnes responsables du service informatique de l'entreprise;

12. Elles devront rappeler que les employés ne doivent utiliser ou révéler aucune information confidentielle au détriment de la compagnie. Il est nettement avantageux que l'employeur précise à ses employés quelles informations doivent être considérées comme confidentielles ainsi que les limites d'utilisation ou de communication de ces informations (par exemple, les autorisations préalables lorsqu'il est nécessaire de communiquer une information confidentielle dans le cadre de l'exécution des fonctions d'un employé aux fins des activités de l'entreprise);
13. Lorsque le secret professionnel est en jeu (par exemple dans le cas des cabinets comptables, cabinets d'avocats, etc.), il est fondamental que les politiques et directives insistent sur la responsabilité imposée à chaque usager de protéger le secret professionnel. À titre d'exemple, l'employeur pourrait exiger des employés que tout client soit avisé des dangers des risques impliqués par l'utilisation du courriel dans la communication de renseignements couverts par le secret professionnel. Les cabinets concernés devraient songer sérieusement à faire précéder leurs communications électroniques d'un message standard de confidentialité. Avec l'entrée en vigueur de la *Loi concernant le cadre juridique des technologies de l'information*, l'utilisation d'une forme d'encryption appropriée aux circonstances risque de devenir la norme applicable en matière de secret professionnel de même que pour tous les autres cas de confidentialité reconnus par la loi (ex. : renseignements personnels).
14. L'employeur devrait mettre en place un système où l'accès aux outils informatiques est protégé par un mot de passe (autre que purement personnel à l'employé). Chaque usager doit demeurer responsable d'assurer la confidentialité de ce mot de passe, la communication de celui-ci étant réservé aux supérieurs administratifs pour fins de contrôle, d'entretien ou de mise à jour et d'urgence. L'employeur peut même prévoir que chaque employé doit modifier périodiquement son mot de passe;
15. Les politiques et directives devront indiquer que l'employeur aura le droit de contrôler et de surveiller tout aspect de l'utilisation des outils informatiques selon les besoins de l'entreprise. Évidemment, en attente de décisions des tribunaux sur le droit d'un employeur de procéder à une surveillance constante de l'utilisation des outils technologiques en milieu de travail, l'employeur devrait considérer opérer cette surveillance de façon intermittente et de l'opérer envers tous les employés de façon uniforme ou de n'entreprendre celle-ci que lorsqu'il a des motifs raisonnables de croire à une utilisation fautive de l'employé visé. L'employeur devrait cependant spécifier expressément qu'il se réserve le droit d'augmenter la surveillance de l'utilisation des outils technologiques selon ce que requis par les circonstances et les besoins. D'ailleurs, l'employeur éviterait sans doute plusieurs contestations s'il mentionnait expressément que l'existence de motifs raisonnables le justifierait de procéder à augmenter la surveillance à l'égard de personnes en particulier, voire de maintenir une surveillance constante sur celles-ci;

16. L'employeur devrait indiquer les personnes (ou catégories de personnes) qui sont en charge du contrôle et de la surveillance des outils informatiques. Les politiques et directives préciseraient alors que ces personnes sont tenues à des obligations de confidentialité à l'égard des renseignements obtenus dans le cadre de l'exécution de leurs fonctions de contrôle et de surveillance des outils informatiques. De même, elles devraient indiquer les dispositions prises pour maintenir la confidentialité des documents ou renseignements obtenus dans le cadre du contrôle et de la surveillance de l'utilisation des outils informatiques. Par exemple, des enregistrements, de la preuve écrite ou des dossiers obtenus à partir de l'ordinateur d'un employé visé par une surveillance devraient être conservés dans un endroit sécuritaire avec accès limité à un nombre restreint de personnes. De plus, un calendrier précis pour la destruction des informations colligées devrait être établi. Cela est d'autant plus vrai si des renseignements personnels sont impliqués. L'entreprise s'assurera alors de respecter les dispositions des lois visant la protection des renseignements personnels qu'elle recueille, conserve, utilise ou communique dans le cadre du contrôle et de la surveillance des outils informatiques.
17. Enfin, au sujet de la conservation et la destruction des données, la méthode utilisée, en plus d'être sécuritaire, devra être arrimée avec les exigences de la *Loi concernant le cadre juridique des technologies de l'information*, plus particulièrement, pour rencontrer celles relatives au maintien de l'intégrité de la copie d'un document technologique, au transfert de l'information d'un support à un autre et aux conditions de destruction (notamment en documentant le transfert) (art. 15, 17, 18, 19 et 20);
18. Il est de loin préférable que les tiers qui communiquent avec les employés de l'entreprise soient eux aussi avisés que plus d'une personne peut avoir accès aux messages laissés dans les boîtes vocales ou dans le courriel, surtout si des renseignements personnels peuvent y être conservés et qu'ils pourraient être contrôlés et surveillés par l'employeur. Mes Jean Yoon et Marie-Hélène Constantin suggèrent qu'un simple avis de «laisser un message non confidentiel» serait suffisant⁹⁸. Nous ajouterions d'indiquer que l'entreprise procède au contrôle et à la surveillance des communications effectuées sur son réseau et ce, selon le cas, à des fins de sécurité, de vérifications d'affaires ou de formation.

Les éléments énumérés ci-haut ne peuvent être exhaustifs. Il importera sans doute de suivre les développements jurisprudentiels en la matière afin de les compléter et de les mettre à jour. Mais d'une façon générale, il importe de retenir que les employés de l'entreprise devraient recevoir les avis appropriés de façon à ce qu'ils comprennent clairement ce qui sera contrôlé et surveillé par l'entreprise, les circonstances qui amèneront ce contrôle et cette surveillance ainsi que ce qu'il adviendra de l'information découlant des contrôles et surveillances effectués de même que les

⁹⁸ J. Yoon et M.-H. Constantin, *Les outils technologiques et leur impact sur le droit de travail*, précité, note 68, à la page 29.

sanctions qu'ils peuvent encourir s'ils ne respectent pas les politiques et directives de l'entreprise en la matière⁹⁹.

En définitive, il importe qu'un employeur ne crée pas lui-même chez ses employés une attente raisonnable de protection de la vie privée dans le milieu de travail. L'adoption d'une politique et des directives claires dans l'utilisation d'Internet et du courriel aura d'abord et avant tout pour effet de minimiser, autant que faire se peut, cette «sphère de protection de la vie privée».

⁹⁹ Pour un portrait plus global des éléments fondamentaux à toute politique et directive en matière de contrôle et de surveillance des outils électroniques d'une entreprise, le lecteur pourra consulter Karen L. Casser, *The Internet and Business: A Lawyer's Guide to the Emerging Legal Issues*, déjà cité, note 6, au chapitre 6 intitulé «Employers, Employees, E-mail and The Internet»; M.S. Dichter et M.S. Burkhardt, *Electronic Interaction in the Workplace: Monitoring, Retrieving and Storing Employee Communications in the Internet Age*, Morgan Lewis & Vockius, L.L.P. 1996, aux pages 23 à 26; The Law Society of New South Wales, *Law Society Online et Guideline to Assist Legal Practitiices to Construct a Policy on the Use and Governance of Electronic Mail and Worldwide Web Access*, Law Society Online et J. Yoon et M.-H. Constantin, *Les outils technologiques et leur impact sur le droit du travail*, précité, note 68, aux pages 28 à 30.