Internet en milieu de travail: la protection des entreprises par l'adoption de politiques et directives appropriées relatives à l'utilisation des nouvelles technologies

Karl Delwaide*

---

* Avocat du cabinet Martineau Walker. LL.B et M.C.L. (1982), University of San Diego. L'auteur, avocat chez Martineau Walker, remercie très sincèrement Me Jean-François de Rico pour sa collaboration à la préparation et à la rédaction de ce texte.

Introduction

L'accès à 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 employés[1]. 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. 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 pas transformé du tout au tout les principes juridiques déjà établis. À titre d'exemple, pour expliquer sa position récente, soit qu'il ne réglementerait pas (pour l'instant) les services des nouveaux médias sur Internet, le

1. Http://www.mlb.com/le0699.htm.

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 médias.[2]

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.

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'au 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.

---

2. Conseil de la radiodiffusion et des télécommunications canadiennes, communiqué du 17 mai 1999.

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. La protection des intérêts légitimes des employeurs

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 ses installations 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 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 La 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*[3]:

> 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 procedures.[4]

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.

1.2 La diffamation

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

---

3. Au chapitre 6 intitulé «Employers, Employees, E-mail and The Internet», aux pages 6 et 7, The Computer Law Association Inc., 1996.
4. K.L. CASSER, précité, note 3, à la page 7.

engager sa responsabilité[5]. 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.

Quel type de faute un employé est-il susceptible de commettre dans l'utilisation de l'autoroute de l'information ou du courriel? Référons d'abord à la diffamation puisque celle-ci est un cas d'application de la responsabilité extra contractuelle en droit civil[6].

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 communications[7]. L'entreprise, propriétaire d'installations informatiques et qui fournit un accès à 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 son auteur, mais aussi de son employeur. M^me^ 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:

> [...] 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 newspapers.[8]

---

5. 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.
6. J.-L. BAUDOUIN et P. DESLAURIERS, *La responsabilité civile*, 5^e^ éd., Cowansville, Les Éditions Yvon Blais inc., 1998, à la page 301.
7. 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.
8. *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 «médisant 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 (M^e^ Charles Turmel, arbitre).

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 domaine[9].

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:

> Cependant, intenter 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 décider d'intenter son recours non pas contre l'auteur de l'acte, mais contre un ou plusieurs acteurs télématiques.[10]

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 le biais de l'article 1463 C.c.Q. (la responsabilité des commettants), soit par le biais de l'article 1457 C.c.Q. (la responsabilité extra contractuelle directe; par exemple, pour avoir omis d'adopter les politiques ou directives appropriées pour encadrer suffisamment la diffusion d'information sur Internet par les employés).

Dans *Stratton Oakmont Inc.* c. *Prodigy Services Co.*[11], 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 eut 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 fut retenue. Par contre, un autre gestionnaire de réseau, qui

---

9. Supreme Court of Western Australia, 31 mars 1994.
10. F. THÉMENS, *Internet et la responsabilité civile*, coll. Minerve, Cowansville, Éditions Yvon Blais, 1998, à la page 25.
11. 1995 WL 323710 (N.Y. Sup. Ct., 24 mai 1995).

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 diffamatoires[12].

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 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

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

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.
>
> (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 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 person.[13]

---

13. Stephen D. IMPARL, *Internet Law The Complete Guide*, STP Specialty Technical Publishers, Inc., North Vancouver, 1998, 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

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 Company[14].

Au Québec et même au Canada, en l'absence d'une législation de même nature que celle établie à l'article 230 du *Communications Decency Act of 1996*, plusieurs questions demeurent sans réponse.

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. 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 de la catégorie de rôles joués 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[15]? À titre d'exemple, nous soulignerons que l'auteur Stephen D. Imparl[16] a émis le commentaire suivant sur l'affaire *Blumenthal* c.

---

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.

14. *Ben Ezra, Weinstein, and Company, Inc.* c. *America Online, Inc.*, No. CIV 97-485 LH/LFG, April 23, 1998, in America Online, Online Defamation; *Sidney Blumenthal and Jacqueline Jordan Blumenthal* c. *Matt Drudge and America Online, Inc.*, Civil Action No. 97-1968 (PLF), April 22, 1998, in America Online, Online Defamation; *Jane Dow* c. *America Online, Inc.,* Case No. 97-2587, October 14, 1998, in America Online, Online Defamation; *Zeran* c. *America Online*, in America Online, Online Defamation; *Alexander G. Lunney* c. *Prodigy Services Company*, 97-07342, 98-00842, in America Online, Online Defamation; *Thomas Kempf* c. *Time, Inc. et al*., Case No. BC 184799*,* June 11, 1998, in America Online, Online Defamation; *Gerald Nicosia c. Diane De Rooy*, No. C98-3029 MMC, July 7, 1999, in America Online, Online Defamation; *Alan J. Truelove* c. *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.
15. P. TRUDEL, *Technologies de l'information et des communications*, Strategis 1997, au chapitre 3, «Les acteurs et la responsabilité».
16. Précité, note 13, à la page 8-24a.

Drudge and America Online Inc.[17]:

> 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 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.

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.

À ce sujet, un auteur[18] faisait remarquer que la situation des entreprises découlant des quelques décisions existant 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 *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

17. Voir note 14.
18. David POTTS, *Liability for Libel on the Internet*, à la page 6.

> events underlying the present complaint. Thus, the decision in *Stratton Oakmont* was made in an entirely different factual context.[19]

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» 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 valable[20]. 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?

Cependant, en ce qui concerne les relations employeur-employé, 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 un fondement juridique valable quant à son droit 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» c'est-à-dire 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, puis d'invoquer par la suite l'ignorance que de tels propos auraient été tenus. Nous suggérons d'emblée aux entreprises de choisir la voie de la prévention en adoptant les politiques et directives appropriées et en en informant leurs employés.

1.3 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

---

19. *Lunney* c. *Prodigy Services Company*, précité, note 14, à la page 6.
20. Par analogie, voir *1267623 Ontario Inc*. c. *Nexx Online Inc.*, Cour supérieure de l'Ontario, 14 juin 1999.

celui 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 de la *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*[21], la Cour suprême de la 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 coemployée 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, dans une affaire ontarienne[22], 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)*[23] 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

21. Vancouver Registry, no C944198, 27 juin 1996, http://www.courts.gov.bc.ca.
22. *In the matter of a claim by Prasad A. Bhamre*, décision rendue par E.J. Houston, arbitre, Ottawa, 2 octobre 1998.
23. [1987] 2 R.C.S. 84.

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'emploi[24].

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 de 2,2 millions de dollars suite à la distribution sur courrier électronique d'un texte intitulé «why beer is better than women»[25].

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

1.4 La perte de contrôle sur 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,

---

24. *CDPDJ (Lippé)* c. *P.G. Québec*, J.E. 98-2370 (T.D.P.), à la page 21.
25. Http://*www*.gahtan.com/alan/articles/monitor.htm.

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'informations[26].

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 d'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 2.2 ci-après[27].

---

26. *R.* c. *Stewart*, [1988] 1 R.C.S. 963, p. 975, et *Lac Minerals* c. *International Corona Resources*, [1989] 2 R.C.S. 574, p. 638-639.
27. 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», dans *Congrès annuel du Barreau du 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).

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 menée 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 litige[28].

Au Québec, différentes lois[29] 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 s'apprête à mettre en vigueur une loi de même nature applicable au secteur privé, le Projet de loi C-6, afin d'assurer l'intégrité dans la conduite du commerce électronique. 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 informations confidentielles sans autorisation de l'employeur. Dans cette affaire[30], 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 comporte-

---

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

29. *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.

30. *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, D.T.E. 95T-1337.

ment 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*[31], l'arbitre a réduit une sanction contre un employé qui avait utilisé le courriel pour émettre des commentaires péjoratifs 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 rules.[32]

L'employeur doit 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 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.

---

31. Canadian Railway Office of Arbitration, Case no. 2731, Calgary, 14 mai 1996.
32. *Id.*, p. 6.

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'étendre.[33]

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*[34] 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.

Nous n'entendons pas couvrir l'ensemble des questions relatives aux droits d'auteur. Nous nous en remettons aux experts en cette

---

33. 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.
34. L.R.C., c. C-42.

matière[35]. Pour les 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 toute circonstance 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.

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 lesquels 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 l'introduction du courriel en milieu de travail, ceux-ci soient aussi 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.

---

35. 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.

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. 183 et s.)

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 en toute circonstance 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*, 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 Beauregard, 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.[36]

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 communication d'affaires, en cours d'emploi, nous apparaît difficilement répondre aux principes mêmes d'une communication de nature privée[37].

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 (2.3) 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».

---

36. *Roy* c. *Saulnier*, [1992] R.J.Q. 2419, p. 2422 et 2425.
37. P. TRUDEL, F. AKRAN, K. BENYEKHLEF et S. HEIN, *Droit du cyberespace*, Les Éditions Thémis inc., 1997, aux pages 11-49, 11-54 et 11-56.

2.2 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 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 raisonnabilité. Il est à noter que certaines décisions laissent croire que le test de raisonnabilité 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 raisonnables.[38]

2.3 La protection de la vie privée d'une personne, même en milieu de travail

A. La définition générale du droit à la vie privée

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 Code civil 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.

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 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 y a gros à parier que le droit de l'employeur de procéder à la surveillance du courrier électronique de ses employés variera selon les circonstances.

---

38. 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 27, 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*, Colloque sur le droit du travail, Martineau Walker, 1997. 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*, Allocution présentée le 13 mars1996 lors d'un colloque organisé par la Ligue des droits et libertés, à la page 7.

Il faut reconnaître cependant que le droit à la vie privée n'est plus limité au droit de ne pas être surveillé ou dérangé dans sa demeure; ce droit comporte d'autres aspects dont ceux qualifiés par le professeur Patrick Glenn[39] 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.[40]

La jurisprudence récente de la Cour d'appel du Québec a reconnu le droit d'une personne de poursuivre en dommages l'auteur d'une atteinte à ces droits. Dans l'affaire *The Gazette* c. *Valiquette*[41], 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.

Quant au droit à l'anonymat, on retrouve un très bon exemple de sa portée dans l'affaire *Duclos* c. *Aubry et Éditions Vice-Versa Inc.*[42]

---

39. H.R. GLENN, «Le droit au respect de la vie privée», (1979) 39 *R. du B.* 879.
40. 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, p. 197 et s.
41. J.E. 97-133 (C.A.).
42. [1998] 1 R.C.S. 591.

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 M^me^ 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 eût pu être le cas d'une photo prise lors d'un événement public très médiatisé.

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?

Dans le cadre de dossiers soulevant l'application et l'interprétation de l'article 8 de la *Charte canadienne des droits et libertés*, la Cour suprême du Canada a dégagé certains paramètres relatifs à l'interprétation et à l'application de cette notion de «vie privée». Bien que la Charte canadienne ne soit applicable qu'à condition qu'il y ait une «action gouvernementale» impliquée, nous croyons que l'approche utilisée par la Cour suprême du Canada peut être utile dans la détermination des principes pertinents à notre analyse de la notion de vie privée en milieu de travail.

C'est ainsi que nous dégageons de cette jurisprudence deux concepts. D'une part, la Cour suprême du Canada s'est refusée de confiner au seul domicile de l'individu l'étendue de ce qui constituerait une «sphère de protection de la vie privée». Au surplus, la Cour suprême s'est appliquée à déterminer, *selon les circonstances*, s'il existait en faveur d'une personne une «attente raisonnable de protection de la vie privée» («legitimate expectation of privacy»). Si nous transposons ces principes au cadre des relations employeur-employé, nous déterminerons d'abord si le «lieu de travail» peut inclure une «sphère de protection de la vie privée» et, si oui, dans quelles circonstances.

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 Westin, précité, à la p. 363, 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'individu.[43]

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 cas, de documents provenant d'une entreprise. Le juge La Forest 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

43. [1988] 2 R.C.S. 417, p. 428.

> 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*[44], 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 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 plut tôt, la situation d'un employeur qui veut avoir accès à des dossiers de l'entreprise contenus sur les ordina-

44. [1990] 3 R.C.S. 36, p. 48.

teurs 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*[45], 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 La Forest affirme que:

> 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

45. [1990] 1 R.C.S. 425, p. 521-522.

> 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.[46]

En droit québécois, 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 travail.[47]

Dans l'arrêt *Société des alcools du Québec* et *Syndicat des employés de magasins et bureaux de la SAQ*, Me Jean-Pierre Lussier, arbitre, 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 surveillante 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 illégale.[48]

---

46. J. YOON et M.-H. CONSTANTIN, *Les outils technologiques et leur impact sur le droit du travail*, précité, note 38, p. 9 à 12.
47. P.-Y. BOURDEAU, *La surveillance par caméra vidéo des lieux de travail*, précité, note 38.
48. [1983] T.A. 335.

Dans un arrêt récent[49], 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 privée une signification essentiellement territoriale. La Cour d'appel ajoutait 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 menée par des moyens raisonnables, comme l'exige l'article 9.1 de la Charte québécoise[50].

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.

---

49. *Syndicat des travailleurs(euses) de Bridgestone Firestone de Joliette (C.S.N.)* c. *Trudeau*, J.E. 99-1786 (C.A.), p. 30.
50. *Id.*, p. 34 et 35.

> 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:
>
> > 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 salarié.[51]

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

---

51. *Id.*, p. 36 et 37.

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 *E.C.P.A.* 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 privée[52]. 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*[53]. Dans une contestation de congédiement formulée sur la base d'une atteinte à la vie privée (des dirigeants de la compagnie avaient vu une copie d'une correspondance électronique au contenu offensant et avaient congédié l'employé), une cour de district de l'État de Pennsylvanie a donné raison à l'employeur malgré le fait qu'afin de favoriser l'utilisation du

52. Une *question* intéressante pourra se soulever sur l'existence du «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?

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

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*[54], 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.*[55], 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

54. No. SCW112749, Cal. Sup. Ct., Los Angeles Cty., 1989.
55. 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. Ill. 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).

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.

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, selon lesquels 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 peuvent 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 tech-

nologiques à des fins personnelles pourvu, 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 qu'il a mis à leur disposition.

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.

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 privée.

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

Nous l'avons déjà souligné: l'arrivée des nouvelles technologies de l'information n'a pas transformé radicalement les principes juridiques déjà connus. Il s'agit plutôt d'adapter ces principes à la nouvelle réalité posée par les technologies de l'information. 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 entreprise[56].

ll 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 nous rappelant les trois principes généraux suivants:

> – Never access an employee's e-mail without their consent, or
>
> – Abolish passwords 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 privacy.[57]

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.

---

56. *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.
57. M.R. BROWN, *Are Employee E-mail Messages really Private?,* 16 octobre 1996, à la page 2.

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;
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;
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.

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.[58]

6. 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;

7. 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. L'employeur pourra alors souligner 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;

8. Elles devront rappeler aux employés les règles générales d'utilisation des outils technologiques dont, notamment, leur devoir 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;

9. 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

58. K.L. CASSER, *The Internet and Business: A Lawyer's Guide to the Emerging Legal Issues,* à «Employers, Employees, E-mail and The Internet», précité, note 3, à la page 5.

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;

10. 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;

11. 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);

12. 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 et des risques entraînés 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, voire d'insister sur l'utilisation d'une forme d'encryption appropriée aux circonstances, ce qui inclut de tenir compte des besoins du client concerné;

13. L'employeur devrait mettre en place un système où l'accès aux outils informatiques est protégé par un mot de passe. Chaque usager doit demeurer responsable d'assurer la confidentialité de ce mot de passe, la communication de celui-ci étant réservée 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;

14. Les politiques et directives devront indiquer que l'employeur aura le droit, *mais non le devoir*, 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, l'employeur devrait songer à opérer cette surveillance de façon intermittente et l'opérer envers tous les employés de façon uniforme ou 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 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;

15. 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 et une méthode sécuritaire de destruction devraient être établis. Cela est d'autant plus vrai si des renseignements personnels sont impliqués. L'entreprise s'assurera alors de respecter les dispositions des lois (provinciales et bientôt fédérale) 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;

16. 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 sont d'avis qu'un simple avis de «laisser un message non confidentiel» serait suffisant[59]. 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 contrôle et surveillance effectués de même que les sanctions qu'ils peuvent encourir s'ils ne respectent pas les politiques et directives de l'entreprise en la matière[60].

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 de 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».

---

59. J. YOON et M.-H. CONSTANTIN, *Les outils technologiques et leur impact sur le droit du travail*, précité, note 38, à la page 29.
60. 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 3, 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, p. 23 à 26; The Law Society of New South Wales, *Law Society Online,* et *Guideline to Assist Legal Practices 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 38, p. 28 à 30.