Université de Montréal

Vie privée et bon usage des NTIC au travail : risques et responsabilités

Par
Hortense Y. Eone

Faculté de droit

Mémoire présenté à la Faculté des études supérieures
en vue de l'obtention du grade de Maître en droit (L.L.M.)
en Droit des affaires

Septembre 2010

Université de Montréal
Faculté des études supérieures et postdoctorales

Ce mémoire intitulé :

Vie privée et bon usage des NTIC au travail : risques et responsabilités

Présenté par :
Hortense Y. Eone

a été évalué par un jury composé des personnes suivantes :

Renée-Claude Drouin
président-rapporteur

Vincent Gautrais
directeur de recherche

Karim Benyekhlef
membre du jury

Jean-François Gaudreault-Desbiens
représentant du doyen de la FES

Résumé

Un nombre croissant de salariés ont aujourd'hui accès à l'Internet et à la messagerie électronique sur leur lieu de travail. Ils sont parfois tentés d'utiliser ces outils à des fins autres que professionnelles, ce qui constitue une source potentielle de conflits.

En effet, sous prétexte d'assurer la protection de leurs biens et équipements, de vérifier que les salariés exécutent leurs obligations et de prévenir les risques de responsabilité, les entreprises contrôlent de plus en plus souvent – et parfois subrepticement – l'utilisation qui est faite des ressources ainsi fournies. Les employés, de leur côté, revendiquent leur droit à ce que leurs activités personnelles en ligne demeurent privées, même lorsqu'elles sont réalisées durant leur temps de travail et avec le matériel de l'employeur. Peuvent-ils raisonnablement voir leurs droits protégés, bien que le droit à la vie privée soit traditionnellement atténué en milieu de travail et que les entreprises aient accès à des technologies offrant des possibilités d'espionnage toujours plus intrusives?

Comment trouver un équilibre viable entre le pouvoir de direction et de contrôle de l'employeur et les droits des salariés? Il s'agit d'une problématique à laquelle les tribunaux sont de plus en plus souvent confrontés et qui les amène régulièrement à réinterpréter les balises établies en matière de surveillance patronale, au regard des spécificités des technologies de l'information.

Ce contexte conflictuel a également entraîné une évolution des pratiques patronales, dans la mesure où un nombre grandissant d'employeurs se dotent d'outils techniques et juridiques leur permettant de se protéger contre les risques, tout en s'aménageant un droit d'intrusion très large dans la vie privée des salariés.

Mots-clés : Surveillance, internet, courrier électronique, expectative de vie privée, obligation, salarié, loyauté, droits, employeur, politique d'entreprise

Abstract

A growing number of employees now have access to the Internet and email in the workplace. They are sometimes tempted to use these tools for other purposes than business, creating thus a potential source of conflict.

Indeed, under the pretext of protecting the company's property and equipment, verifying that the employees execute their contractual obligations, and preventing risks of liability, employers more frequently – and sometimes surreptitiously – monitor the use of the resources so provided.

Employees, on the other side, are claiming their right to have their personal online activities remain private, even when these are conducted during their working hours and with the equipment provided by the employer. However, can they reasonably expect to have their rights protected, when the right to privacy in the workplace has traditionally been mitigated and when employers have access to spying technologies that are more and more invasive?

How then to find a workable balance between employer's management rights and employees' rights? It is an issue that courts increasingly face and that regularly induces them to reinterpret the rules set for the employer's surveillance with regard to the specificities of information technologies.

That situation of conflict has also brought changes to the practices in the workplace, insofar as employers are increasingly likely to adopt legal and technical tools enabling them to protect themselves against risks, while keeping a large right of intrusion into employees' privacy.

Keywords: Monitoring, internet, email, expectancy of privacy, obligation, employee, loyalty, rights, employer, company policy

Table des matières

Liste des annexes

Liste des tableaux et abréviations

A.2d	Atlantic Reporter (2e série)
ABCA	Court of Appeal of Alberta
ABQB	Court of Queen's Bench of Alberta
A.G.A.A.	Alberta Grievance Arbitration Awards
Alta. G.A.	Alberta Grievance Arbitration
art.	Article
Avcb-vsgb	Association de la Ville et des Communes de la Région de Bruxelles-Capitale
B.C.C.A.A.A.	British Columbia Collective Agreement Arbitration Award
BC S.C.	British Columbia Supreme Court
Bull. civ.	Bulletin des arrêts des chambres civiles de la Cour de cassation
C.A.	Cour d'appel
C.A.F.	Cour d'appel fédérale
C.c.Q.	Code civil du Québec
C.cr.	Code criminel
C.F.	Cour fédérale
C.L.A.	Canada Labour Arbitration
C.Q.	Cour du Québec
C.R.T.	Commission des relations de travail
C.S.	Cour supérieure
C.S.I.	Computer Security Institute
C.V.P.C.	Commissaire à la protection de la vie privée du Canada
Cal.	Californie (décisions de la Cour suprême)
CAL. CIV. CODE	California Civil Code
CanLII	Canadian Legal Information Institute / Institut canadien d'information juridique

CEFRIO	Centre francophone de recherche en informatisation des organisations
Civ. 1re	Première Chambre civile de la Cour de cassation
Civ. 2e	Deuxième Chambre civile de la Cour de cassation
CNIL	Commission Nationale de l'Informatique et des Libertés
coll.	Collection
Coll. Agr. Arb.	Collective Agreement Arbitration
collab.	Collaboration
conf.	Confirmé
Cons. d'Ét.	Conseil d'État
CRTFP	Commission des relations de travail dans la fonction publique
D.	Recueil Dalloz
D.A.T.C.	Décisions d'arbitrage en relations de travail relevant de la juridiction fédérale (QL/LN)
D.E.A.	Diplôme d'études approfondies
D.E.S.S.	Diplôme d'études supérieures spécialisées
D.T.E.	Droit du travail Express
DARES	Direction de l'animation de la recherche, des études et des statistiques
Def. Counsel. J.	Defence Councel Journal
Dr. Ouvrier	Droit ouvrier
DSI	Directeur des systèmes d'information
E.D. Pa.	Eastern district of Pennsylvania
éd. Entr.	Éditions Entreprise et Affaires
EYB	Éditions Yvon Blais
F.B.I.	Federal Bureau of Investigation
F. Supp.	Federal Supplement (USA)
G.A.	Grievance Arbitration

Gaz. Pal.	Gazette du Palais
Harvard J. of L. & Tech.	Harvard Journal of Law & Technology
Hastings Comm/Ent L.J	Hastings Communications and Entertainment Law Journal
j.	Juge
J.C.P.	Juris-classeur périodique (semaine juridique)
J.C.P.éd. Entr.	Juris-classeur périodique, édition entreprise
J. du Bar.	Journal du Barreau
J.E.	Jurisprudence Express
J.O.	Journal Officiel
L.A.	Labour Arbitration
L.A.C.	Labour Arbitration Cases
L.C.	Lois du Canada
L.Q.	Lois du Québec
L. Ed.	United States Supreme Court Reports, Lawyers Edition
L.R.C.	Lois réformées du Canada
L.R.Q.	Lois réformées du Québec
LAX	Labour Arbitration Xpress NetLetter (QL/LN)
LN	LexisNexis
N.J.	Décisions de la Cour suprême de l'État du New Jersey
NBCA	New-Brunswick Court of appeal
NSHRC	Nova Scotia Human Rights Commission
NTIC	Nouvelles technologies de l'information et de la communication
NWTSC	Cour suprême des Territoires du Nord-Ouest
O.L.A.A.	Ontario Labour Arbitration Award
obs.	Observations
Ont. L.A.	Ontario Labour Arbitration
P.2d	Pacific Reporter (2^{e} série)

Pub. L.	Public Law (USA)
QC A.G.	Tribunal d'arbitrage (Conférence des arbitres du Québec) (CanLII)
QC C.D.C.H.A.D.	Comité de discipline de la Chambre de l'assurance de dommages (Québec) (CanLII)
QC C.D.O.I.I.	Comité de discipline de l'Ordre des infirmières et infirmiers du Québec (CanLII)
QC C.Q.	Cour du Québec (CanLII)
QCCQ	Cour du Québec (CanLII)
QCCRT	Commission des relations du travail (CanLII)
QCCS	Cour supérieure (CanLII)
QC T.D.P.	Tribunal des droits de la personne (Québec) (CanLII)
QC T.T.	Tribunal du Travail (CanLII)
QL	Base de données Quicklaw
Queen's L.J.	Queen's Law Journal
R.C.S.	Recueil de la Cour suprême
R. du B.	Revue du Barreau
REJB	Répertoire électronique de jurisprudence du Barreau
R.J.Q.	Recueil de jurisprudence du Québec
R.J.D.T.	Revue de jurisprudence en droit du travail
RSI	Responsable de la sécurité informationnelle
RSSI	Responsable de la sécurité des systèmes d'informations
S.D.N.Y.	Southern District of New York
Soc.	Chambre sociale de la Cour de cassation
somm.	Sommaire
somm.com.	Sommaire commercial
Stat.	United States Statutes at Large
T.A.	Tribunal d'arbitrage
TI	Technologies de l'information

Trib. gr. inst.	Tribunal de grande instance
U. Mich. J.L. Reform	University of Michigan Journal of Law Reform
U.S.C.	United States Code
vol.	Volume

À mes parents.

Remerciements

Je tiens à remercier Monsieur le professeur Gautrais, de m’avoir donné l’opportunité d’effectuer ce travail de recherche, ainsi que pour sa grande disponibilité et ses précieux conseils et commentaires.

Je souhaite également remercier tous ceux et celles qui m'ont permis de mener à bien ce long travail.

Mes remerciements vont aussi, bien entendu, à ma famille et à mes amis, pour leurs encouragements et leur soutien sans failles.

Introduction

> « À l'heure de la révolution numérique et des réseaux l'homme au travail est "tracé" dans les ordinateurs de l'entreprise comme le pilote d'avion ou le conducteur de TGV le sont par les enregistrements de la boîte noire. Est-ce que les intérêts de l'employeur ne vont pas l'inciter à une exploitation abusive de ces traces alors que les boîtes noires ne sont interrogées que dans des circonstances exceptionnelles et selon des procédures parfaitement définies […] telle est la question [….]. »[1]
>
> J.-P. de Longevialle, Commissaire, CNIL[2]

Les entreprises qui recourent aux nouvelles technologies de l'information et de la communication[3] se trouvent rapidement confrontées au problème du contrôle de l'usage qu'en font les employés. Leur principale préoccupation est, certes, de tirer le meilleur profit des NTIC pour améliorer la productivité de leurs salariés et augmenter leurs profits, cependant, elles souhaitent également conserver la maîtrise de ces ressources. Elles vont donc généralement chercher à se doter d'outils (juridiques et techniques) pour contrôler les activités virtuelles des salariés, tout en réduisant au minimum les droits et libertés de ces derniers, si ce n'est en les supprimant complètement. Cette surveillance suscite un débat croissant. En premier lieu, parce qu'elle concerne un nombre croissant d'individus : près de 60 % des salariés utilisent au moins occasionnellement un outil informatique au travail[4], tandis que 42 % des internautes admettent naviguer au bureau[5]. Ensuite, ces outils offrent,

---

[1] Jean-Pierre DE LONGEVIALLE (COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS), *Intervention à la 26ème conférence internationale sur la vie privée et la protection des données personnelles. Session sur le thème de « La protection de la vie privée de l'employé et les intérêts de l'employeur »*, Wroclaw, 2004, en ligne : <http://26konferencja.giodo.gov.pl/data/resources/LongevialleJP_paper.pdf> (site consulté le 26 juillet 2010).

[2] Commission Nationale de l'Informatique et des Libertés (ci-après citée « CNIL »).

[3] Ci-après cité : « NTIC ».

[4] DIRECTION DE L'ANIMATION DE LA RECHERCHE, DES ÉTUDES ET DES STATISTIQUES (DARES), *Conditions de travail : une pause dans l'intensification du travail. Premières Synthèses*, Paris, Publications Dares, 2007, n° 01.2, en ligne : <http://www.travail-solidarite.gouv.fr/IMG/pdf/2007.01-01.2.pdf> (site consulté le 25 juillet 2010).

[5] STATISTIQUE CANADA, *Enquête canadienne sur l'utilisation d'Internet*, 2010, en ligne : <http://www.statcan.gc.ca/daily-quotidien/100510/dq100510a-fra.htm> (site consulté le 28 juillet 2010); Voir également EUROPEAN INDUSTRIAL RELATIONS OBSERVATORY (EIRO), *New technology and respect for privacy at the workplace*, Février 2007, en ligne:

« par un effet secondaire »[6], de nouvelles possibilités de surveillance potentiellement sources d'atteintes aux droits des travailleurs. Toute utilisation d'un ordinateur laisse, en effet, des « traces » que l'employeur peut aisément suivre[7], ce qui suscite des questionnements quant à la légitimité de tels contrôles.

En fait, la possibilité de contrôler l'activité des employés a été reconnue à l'employeur[8] : en vertu de son pouvoir de direction, ce dernier est en droit de s'attendre à ce que le salarié, placé sous sa subordination, exécute loyalement les obligations découlant du contrat de travail[9]. De plus, le contrôle patronal s'impose parfois, compte tenu des dispositions relatives à la protection des informations personnelles qui obligent l'entreprise à mettre en œuvre les mesures appropriées pour assurer la sécurité des renseignements personnels qu'elle détient sur autrui[10]. Et si l'employeur a le droit de surveiller l'activité des salariés, il peut donc la « cybersurveiller », puisque « "[c]ybersurveiller" l'activité d'un salarié, c'est contrôler l'utilisation que les salariés font de leur outil informatique, et conserver le cas échéant, des informations, identifiantes ou pas »[11]. À cet égard, Murielle Cahen propose une définition qui semble plus complète de la cybersurveillance :

> « La cybersurveillance peut être définie comme tout moyen de contrôle technique, sur une personne ou un processus, lié aux nouvelles technologies et plus particulièrement aux réseaux numériques de communication. Plus précisément, la cybersurveillance

---

<http://www.eurofound.europa.eu/eiro/2007/02/articles/ee0702079i.htm> (site consulté 25 juillet 2010), qui précise que 45 % des internautes consultent l'Internet au travail.

[6] COMMISSION NATIONALE INFORMATIQUE ET LIBERTÉS, *21ème rapport d'activité 2000*, 2001, p. 122, en ligne : <http://lesrapports.ladocumentationfrancaise.fr/BRP/014000460/0000.pdf> (site consulté le 26 juillet 2010).

[7] Dominique SERIO et Cédric MANARA, « Traçabilité et responsabilité dans les relations de travail », Caprioli-avocats.com, Première publication : *Les premières journées internationales du droit du commerce électronique, Actes du colloque de Nice des 23, 24 et 25 octobre 2000, coll. Actualités de droit de l'entreprise, dirigée par J. RAYNARD*, Litec, 2002, p. 149 s., Date de la mise à jour : janvier 2001, en ligne : <http://www.caprioli-avocats.com/tracabilite/74-tracabilite-responsabilite-relations-travail> (consulté le 19 août 2010).

[8] *Roy* c. *Saulnier*, [1992] R.J.Q. 2419 (C.A.) (à propos de l'interception de conversations téléphoniques); *Syndicat des travailleuses et travailleurs de Bridgestone/Firestone de Joliette (C.S.N.)* c. *Trudeau*, REJB 1999-14156 (C.A.) (relativement à la surveillance vidéo).

[9] C.c.Q., art. 2085 et 2088.

[10] *Loi sur la Protection des renseignements personnels dans le secteur privé*, L.R.Q. 1993, c. P-39.1, art. 10.

[11] Nicolas IVALDI, et Pascaline VINCENT, « Cybersurveillance des salariés et chartes informatiques », Caprioli-avocats.com, Septembre 2005, en ligne : <http://www.caprioli-avocats.com/donnees-perso/87-cybersurveillance> (site consulté le 19 août 2010).

> regroupe les voies et moyens aboutissant à l'accès des données ou signaux transmis par voie électronique ainsi que le contrôle des moyens techniques permettant ces transmissions. La cybersurveillance se fait techniquement, au moyen de logiciels de surveillance permettant d'enregistrer tous les évènements ou messages survenus pendant un temps donné et à un endroit déterminé. Les écoutes téléphoniques font partie intégrante de la cybersurveillance, tout comme le traçage d'internautes sur le web ou encore sur un réseau Intranet. La surveillance et l'interception de courriers électroniques sont considérées comme de la cybersurveillance. »[12]

Puisque l'on reconnaît à l'employeur le droit de surveiller ses salariés, la question aujourd'hui n'est donc plus de savoir s'il peut contrôler l'utilisation des ressources informatiques mis à la disposition du personnel, mais dans quelle mesure une telle surveillance peut s'exercer[13]. Si les NTIC lui offrent la possibilité technique d'espionner ses salariés, est-ce pour autant qu'il est autorisé à lire leur correspondance électronique ou à vérifier l'historique de leurs navigations? Le simple fait qu'il soit propriétaire des équipements informatiques lui donne-t-il un droit absolu de s'immiscer dans la vie privée des salariés pour contrôler toutes leurs activités virtuelles? De même, peut-il, par des moyens juridiques (par exemple des clauses contractuelles), interdire au salarié de correspondre avec qui bon lui semble, ou l'empêcher, par des procédés techniques (bridage), d'accéder aux sites qui l'intéressent? Bref, y a-t-il des limites au contrôle et à la surveillance que les employeurs peuvent exercer sur les activités en ligne des salariés[14]? La question est donc de savoir s'il existe un droit à la vie privée au travail et, dans l'affirmative, de voir comment ce droit s'articule avec les droits de l'employeur.

L'introduction des outils de communication électroniques (ordinateur, logiciels, accès Internet et courrier électronique) dans l'entreprise a provoqué de profondes mutations dans l'organisation du travail et les rapports collectifs et individuels. Tout d'abord, parce que ces

---

[12] Murielle CAHEN, « La validité des chartes Internet », Legalbiznext.com, 10 novembre 2005, en ligne : <http://www.legalbiznext.com/droit/La-validite-des-chartes-Internet> (site consulté le 19 août 2010).

[13] Hildegard SCHMIDT, « E-mail, internet et le lieu de travail : une relation difficile? », Avcb-vsgb.be, Mai 2006, p. 1, en ligne : <http://www.avcb-vsgb.be/documents/documents/personnel/email-internet-travail.pdf> (site consulté le 19 août 2010).

[14] *Id.*

technologies permettent à des collègues ou des contacts d'affaires éloignés géographiquement de communiquer et d'échanger des informations et documents en faisant fi des contraintes temporelles ou spatiales. Par ailleurs, l'organisation en réseau des activités de l'entreprise et la rapidité des échanges permet aux salariés d'une même organisation de travailler en temps réel, même s'ils sont disséminés dans différentes filiales à travers le monde. Cela permet indéniablement d'améliorer la qualité du travail et d'augmenter la productivité des travailleurs. Cependant, ces nouvelles méthodes de travail favorisent l'interpénétration entre vie personnelle et vie professionnelle, univers pourtant bien étanches autrefois : le salarié, grâce à son ordinateur portable, peut désormais travailler en tous lieux et heures. Ce qui lui procure une certaine autonomie, puisqu'il a de plus en plus souvent l'opportunité de choisir à quel moment il veut travailler et d'où il souhaite le faire. Bien entendu, la conséquence est un relâchement du lien de subordination qui peut créer une certaine confusion chez les différents acteurs. D'un côté, les salariés peuvent, parfois en toute bonne foi, surestimer leur autonomie, déduisant, par exemple, que le fait de pouvoir emporter chez soi l'ordinateur portable fourni par l'entreprise vaut autorisation de s'en servir à des fins personnelles. De l'autre côté, l'employeur, précisément pour éviter ce type de situation, peut être tenté d'installer des « mouchards » pour surveiller l'utilisation des ressources informatiques ainsi mis à la disposition des salariés. Finalement, on assiste à une transformation inexorable du cadre de travail qui appelle un regard renouvelé sur la notion de vie privée.

De plus, une adaptation des règles applicables est nécessaire, puisqu'il n'y a pas de « régime légal dérogatoire »[15] propre à ce domaine. Ce qui peut parfois choquer, compte tenu de la sophistication toujours plus poussée des techniques de surveillance. Nombreux en effet sont ceux qui pensent qu'il faudrait des règles spéciales, mieux adaptées pour protéger les droits des salariés[16]. Or, dans le domaine des NTIC, comme dans beaucoup

---

[15] N. IVALDI et P. VINCENT, préc., note 11.

[16] Alexandre MAITROT DE LA MOTTE, « Le droit au respect de la vie privée », dans Pierre TABATONI, *La protection de la vie privée dans la société d'information*, t. 3, coll. « Cahiers Académie des Sciences morales et politiques », Paris, Les Presses Universitaires de France, 2002, p. 255, à la page 323.

d'autres, le législateur n'est pas toujours prompt à apporter les clarifications nécessaires aux différents questionnements. Et quand il le fait, il est souvent trop tard, compte tenu de l'évolution rapide des techniques dans ce domaine. D'ailleurs, la doctrine est divisée sur la nécessité d'une intervention législative : alors que certains pensent que les règles de droit commun sont parfaitement applicables à l'Internet et qu'il n'est pas nécessaire d'en adopter de nouvelles, d'autres ont une approche « cessessioniste »[17] et considèrent que ce régime n'apporte pas les réponses appropriées aux problématiques propres au réseau et qu'il faut par conséquent adopter des règles spéciales et distinctes[18]. La détermination du régime applicable est d'autant plus compliquée qu'il arrive souvent qu'il y ait une confusion des rôles entre les différents acteurs de l'Internet. En principe, chacun des intervenants du réseau (opérateurs de télécommunications, fournisseurs d'hébergement, de contenus ou d'accès à l'Internet) remplit une fonction bien distincte et est soumis à un régime juridique propre à son secteur d'activité[19]. Cependant, il peut arriver que l'un d'eux remplisse plusieurs fonctions (par exemple, un fournisseur d'accès sera aussi souvent un hébergeur), et même « qu'un tiers devienne à ses dépens un acteur du réseau »[20], comme c'est le cas des entreprises qui offrent un accès à l'Internet à leurs salariés. La question est alors de savoir si elles sont susceptibles de se voir appliquer les mesures propres aux prestataires de l'Internet.

En fin de compte, c'est au juge qu'il revient, lorsqu'il est saisi, d'apporter des précisions sur les différentes notions relatives à la surveillance des employés et de tenter de maintenir un équilibre viable entre les intérêts fondamentalement opposés des différents protagonistes, à savoir les revendications des salariés d'une protection de leurs droits fondamentaux (Partie 2) et les motifs invoqués par les employeurs pour justifier leur contrôle de l'utilisation de leurs ressources informatiques (Partie 1).

---

[17] Xavier LEMARTELEUR, *L'employeur : un fournisseur d'accès à l'internet comme les autres? Implications juridiques de la fourniture d'accès à l'internet par l'entreprise*, mémoire de DESS, Paris, Faculté de droit, Université Paris II Panthéon-Assas, 2003, p. 6.

[18] *Id.*

[19] *Id.*, p. 8.

[20] *Id.*, p. 6.

Partie 1 : Les justifications de la surveillance de l'employeur sur l'utilisation des NTIC

Les NTIC, parce qu'elles sont « tour à tour outil de travail, moyen de communication, lieu de stockage de la richesse d'une entreprise [et] vecteur d'activité »[21], constituent une nouvelle source de tension entre employeurs et employés.

Du point de vue des salariés, ces outils sont ludiques, d'usage facile et offrent un accès instantané et quasi illimité à une multitude d'informations utiles, aussi bien pour le travail que pour la vie privée. Sur le plan strictement professionnel, les employés utilisent de plus en plus l'Internet pour consulter des sites spécialisés ou participer à des forums de discussion (afin, par exemple, de défendre ou promouvoir la politique de l'entreprise); ils se servent également du courrier électronique pour communiquer avec leurs collègues de travail ou leurs contacts d'affaires externes. Sur le plan personnel, ils peuvent, par exemple, utiliser le réseau pour organiser leurs vacances et autres loisirs, faire leurs courses en ligne, se livrer à des jeux virtuels ou tout simplement rechercher un autre emploi. Or, ces activités en ligne privées sont souvent gourmandes en bande passante et représentent des charges, en termes de coût et d'espace, dont les salariés ont rarement conscience[22]. Il est vrai que, pour ce qui concerne plus particulièrement le courrier électronique, cet argument n'est pas vraiment valable. Il n'en demeure pas moins que, hormis pour les entreprises disposant d'importants capitaux ou œuvrant dans le domaine de l'Internet, l'aspect financier peut être d'une grande importance, puisque l'utilisation du réseau à des fins personnelles peut parfois représenter la moitié du débit[23]. Par ailleurs, la visite de certains sites et le téléchargement de divers contenus (logiciels, vidéos, photographies, etc.) peuvent contribuer à ralentir

---

[21] Fabrice FÉVRIER, *Pouvoir de contrôle de l'employeur et droits des salariés à l'heure d'Internet. Les enjeux de la cybersurveillance dans l'entreprise*, mémoire de D.E.A., Nanterre, Faculté de droit, Université de Nanterre – Paris X, 2003, p. 15.

[22] LE JOURNAL DU MANAGEMENT, « Réguler l'accès Internet des salariés. Contrôle technique contrôle éthique », Mars 2004, en ligne : Lejournaldunet.com : <http://www.journaldunet.com/management/dossiers/040331acces/lead.shtml> (site consulté le 30 juillet 2010).

[23] *Id.*

l'activité du réseau et à réduire les capacités de stockage du système d'information de l'entreprise. C'est, par exemple, la saturation du disque dur d'un ordinateur qui a permis à un organisme régional français de découvrir les activités illicites de son directeur de cabinet[24]. L'imprudent utilisait le seul poste de travail connecté à l'Internet – celui de la secrétaire – pour acheter, télécharger et stocker des milliers d'images à caractère pédophile. Il se servait de sa carte bancaire pour payer ses achats, ce qui a permis de l'identifier. Il a non seulement été licencié par son employeur, mais a, de plus, été condamné à une peine d'emprisonnement de 6 mois, dont 3 fermes, pour recel d'images pornographiques de mineurs.

Les principales sources d'encombrement du réseau de l'entreprise sont : le téléchargement de vidéos, films ou musique et la consultation d'émissions de radio ou de télévision en ligne. Internet tend, en effet, à devenir un support de « consommation » de plus en plus attractif permettant de suivre les événements en direct ou de consulter les contenus en flux continu (« *streaming* »). Un tel engouement laisse présager, avec la généralisation du Web 2.0, l'émergence de nouvelles pratiques tout aussi gourmandes en bande passante.

Du point de vue patronal, l'ordinateur et le réseau sont mis à la disposition des salariés dans un souci d'améliorer la rentabilité et les performances de l'entreprise : l'employeur tolèrera donc difficilement un usage privé inapproprié qui pourrait nuire à la bonne marche de ses affaires.

La première crainte de l'employeur est, bien entendu, la baisse de la productivité du travail, en raison du temps passé à échanger des messages personnels et/ou naviguer sur Internet. Mais les activités privées des salariés peuvent aussi engendrer de nombreux risques (contamination par des virus, logiciels espions, vers, etc.; atteintes aux droits de propriété intellectuelle : avec, par exemple, la contrefaçon de logiciels; divulgation d'informations confidentielles concernant l'entreprise, ses employés, ainsi que ses usagers et clients; commission d'infractions par les salariés : consultation de sites illicites; diffusion de propos

[24] Trib. gr. inst. Mans, 16 févr. 1998, J.C.P. 1999.II.10011.

diffamatoires, racistes ou contraires aux bonnes mœurs; etc.) susceptibles d'engager la responsabilité de l'employeur[25]. L'employeur peut alors être tenté de se préconstituer des preuves en installant des outils de contrôle spécifiques, afin de s'en servir dans le cadre d'une procédure disciplinaire. Et de fait, la surveillance des réseaux numériques est devenue partie intégrante des politiques de gestion des ressources humaines de la majorité des entreprises. On estime qu'environ 38 % des entreprises québécoises disposent aujourd'hui d'une politique encadrant l'utilisation d'Internet[26], tandis que les activités en ligne des salariés seraient surveillées par 66 % des employeurs[27]. Pour ces derniers, ces contrôles sont nécessaires pour protéger leurs intérêts[28] et sont justifiés à la fois par leur droit de propriété sur les biens professionnels et par le lien de subordination découlant du contrat de travail[29].

En réalité, il ne s'agit pas là de préoccupations nouvelles, puisque les employeurs se sont de tout temps souciés des questions liées au rendement et à la sécurité des biens professionnels et du lieu de travail. Et, à cette fin, ils ont toujours exercé une surveillance plus ou moins étroite sur les activités de leurs employés. Cette préoccupation s'est amplifiée avec l'avènement de la société de l'information et la vulgarisation des moyens de communication électroniques. Le contremaître a alors fait place au « mouchard électronique » chargé du contrôle des présences physiques (avec les badges d'accès), puis

---

[25] Isabelle RENARD, « Les DSI et les RSSI sont ils responsables pénalement? », Lejournaldunet.com, 02 février 2005, en ligne : <http://www.journaldunet.com/solutions/0502/050202_juridique.shtml> (site consulté le 19 août 2010).

[26] CEFRIO et SOM RECHERCHES ET SONDAGES, *NetPME 2009. Utilisation des TI par les entreprises québécoises : plus de 1800 PME sondées. Faits saillants*, 2009, p. 4, en ligne : <https://www.cefrio.qc.ca/index.php?eID=tx_nawsecuredl&u=4818&file=fileadmin/doc_bloc_achat/netpmefaitssaillants2009secur.pdf&t=1280346654&hash=65ef29f39fc1033a7bc8174925ff7363> (site consulté le 27 juillet 2010).

[27] AMERICAN MANAGEMENT ASSOCIATION, THE EPOLICY INSTITUTE, *2007 Electronic Monitoring & Surveillance Survey. Over Half of All Employers Combined Fire Workers for E-Mail & Internet Abuse*, 2008, résumé en ligne : <http://press.amanet.org/press-releases/177/2007-electronic-monitoring-surveillance-survey/> (site consulté le 27 juillet 2010).

[28] Isabelle DE BENALCÁZAR, *Droit du travail*, coll. Universités, Série manuel, Paris, Gualino, 2004, p. 95.

[29] F. FÉVRIER, préc., note 21, p. 15.

au « contremaître virtuel », capable de contrôler la productivité des « cybertravailleurs »[30]. L'employeur a désormais la possibilité technique d'effectuer, à tout moment, un contrôle de l'activité de son personnel : le travailleur laisse, en effet, des traces à chaque mouvement électronique et il est très aisé de l'espionner. La tentation est très forte pour l'employeur et nombreux sont ceux qui ont sauté le pas et installé des dispositifs de contrôle spécifiques. L'objectif avoué étant d'être armé face aux diverses menaces qui peuvent mettre en péril les intérêts de l'entreprise. Le premier des ces intérêts est d'ordre financier : les entreprises investissent souvent des sommes colossales dans la constitution et l'entretien de leurs parcs informatiques et elles veulent s'assurer que les infrastructures informatiques, et surtout les informations, d'une valeur inappréciable, qu'elles abritent, bénéficient d'une protection optimale. Par ailleurs, de nombreux employeurs considèrent la surveillance comme une mesure essentielle pour assurer la productivité et prévenir ou mettre fin à toute forme d'atteinte aux droits de l'entreprise ou à ceux d'autrui (fuites de renseignements confidentiels, harcèlement entre salariés ou envers les clients ou usagers, etc.). Ils se trouvent ainsi justifiés à recourir à des techniques toujours plus sophistiquées pour contrôler le travail de leur salariés. La question étant de savoir si les menaces sécuritaires (Chapitre 1), la prévention des abus (Chapitre 2) et les risques de responsabilité (Chapitre 3), habituellement invoqués par les employeurs, sont des motifs légitimes de surveillance reconnus comme tels par le droit.

Chapitre 1. L'impératif de sécurité

La sécurité du système informatique constitue un enjeu majeur à la fois pour les organisations et leurs salariés. Elles doivent en effet faire face à une cybercriminalité qui mobilise toujours davantage leurs finances et dont les employés malveillants et les tiers chargés de la gestion des données externalisées constituent des facteurs de risque en

---

[30] COMMISSION NATIONALE INFORMATIQUE ET LIBERTÉS, « La cybersurveillance des salariés en entreprise », *20ème rapport d'activité 1999*, 2000, p. 182, en ligne : <http://lesrapports.ladocumentationfrancaise.fr/BRP/004001043/0000.pdf> (site consulté le 26 juillet 2010).

croissance[31]. Ainsi, selon une enquête du *Computer Security Institute* (CSI) et du *Federal Bureau of Investigation* (FBI) sur les risques de sécurité, les pertes liées aux incidents de sécurité s'élevaient à plus de 130 millions de dollars en 2005[32]. Or, au-delà des conséquences catastrophiques en termes d'image que l'entreprise peut subir, une négligence de sécurité peut engager la responsabilité de cette dernière, puisque la loi lui impose de prendre les mesures appropriées pour assurer la sécurité et la confidentialité des données personnelles qu'elle détient sur autrui[33]. La mise en place d'une protection efficace du système d'information devient donc une nécessité pour tout employeur avisé (Section 1). Toutefois, la question de la sécurité informationnelle a également des répercussions sur la situation des travailleurs dans la mesure où les dispositifs de sécurité incluent généralement des procédures de contrôle et de surveillance souvent en contradiction avec leurs droits fondamentaux et notamment le droit au respect de leur vie privée. Aussi importe-t-il de se demander si la sécurité informatique constitue un fondement juridique à la surveillance de l'employeur (Section 2).

Section 1. La nécessaire protection du système d'information

Avec les NTIC, les entreprises se retrouvent face à la problématique suivante : comment concilier l'ouverture – facilitée grâce à l'Internet – de l'organisation sur l'extérieur avec la sécurité de son système d'information? Ces technologies exposent en effet, l'entreprise, et particulièrement ses services informatiques, à diverses menaces susceptibles de causer des dommages fort coûteux et parfois irréversibles (1.1.). Il est donc indispensable qu'elle prenne les mesures nécessaires pour assurer le bon fonctionnement de son système

---

[31] KPMG, *Les vols d'information liés à la malveillance interne ont augmenté de plus de 50 % au premier semestre 2009. Selon le Baromètre KPMG du vol et de la perte d'informations*, Paris, 2009, en ligne : <http://www.kpmg.fr/fr/Press/documents/cp-it-dataloss-dec09.pdf> (site consulté le 22 août 2010).

[32] COMPUTER SECURITY INSTITUTE, FEDERAL BUREAU OF INVESTIGATION, *2005 CSI/FBI Computer Crime and Security Survey*, 2005, p. 14, en ligne : <http://www.cpppe.umd.edu/Bookstore/Documents/2005CSISurvey.pdf> (site consulté le 22 août 2010). L'enquête CSI/FBI 2005 sur les risques de sécurité a été réalisée auprès de 700 entreprises américaines et comptabilise les montants fournis par les 639 sociétés qui étaient en mesure de fournir une estimation des pertes liées aux incidents de sécurité.

[33] *Loi sur la protection des renseignements personnels dans le secteur privé*, préc., note 10, art. 10.

informatique, tout en garantissant la sécurité et la confidentialité des informations à caractère personnel qu'elle détient sur autrui (1.2.).

1.1. Les risques d'atteinte à la sécurité informatique

La sécurité du système d'information représente un enjeu crucial pour les entreprises : toute organisation moderne dispose, en effet, d'un certain nombre de données qu'elle souhaite protéger contre toute utilisation non autorisée, tels les éléments de propriété intellectuelle et industrielle (secrets commerciaux, dessins, secrets de fabrication, résultat de recherche et développement…), les renseignements relatifs aux clients ou contacts d'affaires, les informations stratégiques de nature commerciale ou financière, etc. Parallèlement, l'entreprise doit être capable d'aller chercher à l'extérieur les informations qui lui sont utiles pour son activité et de les traiter afin de générer de nouvelles informations qu'elle remettra éventuellement en circulation, à travers l'Internet et l'Intranet[34]. De nos jours, « l'information est devenue valeur, parfois la seule détenue par une entreprise »[35] et la compétitivité d'une organisation dépendra souvent de sa capacité à préserver ses informations de façon sécuritaire. Or, si les réseaux numériques facilitent les communications et la recherche d'informations, ils sont également une source majeure de vulnérabilité face aux risques de contaminations, d'intrusions ou de destructions de données[36].

Une utilisation inadéquate des ressources informatiques peut, par exemple, entraîner la propagation de virus ou encore une augmentation du trafic susceptibles de nuire grandement à l'efficacité et à la sécurité du réseau informatique de l'entreprise. À cet égard, les nouveaux moyens de communication offerts par le web 2.0 (forums de discussion,

---

[34] Vincent ROQUES, *La sécurité des données d'entreprises en réseau*, mémoire de DEA, Montpellier, Institut de Recherche et d'Étude pour le Traitement de l'Information Juridique, Université Montpellier I, 2002, p. 15.

[35] Isabelle RENARD, « Responsabilité de l'entreprise et de ses dirigeants du fait de la perte de données informatiques », Lejournaldunet.com, 23 janvier 2003, en ligne : <http://www.journaldunet.com/solutions/0301/030123_chro_juridique.shtml> (site consulté le 19 août 2010).

[36] V. ROQUES, préc., note 34, p. 5.

blogues, sites de partages ou de réseautage, etc.) constituent autant de nouvelles portes d'entrée et de sortie qui échappent au contrôle de l'entreprise, multipliant ainsi les sources de vulnérabilité. De même, le courrier électronique, utilisé aussi bien pour les échanges professionnels que privés, est aussi le vecteur de virus idéal. En effet, les courriels expédiés d'un ordinateur infecté, surtout lorsqu'ils contiennent des pièces attachées, peuvent à leur tour contaminer l'ordinateur du destinataire. Le danger est décuplé lorsque ces messages sont transférés à d'autres utilisateurs du réseau. Or, pour les grandes entreprises, la plus grosse part de leurs affaires se négocie par le courrier électronique, qui est le moyen privilégié pour communiquer en interne ou avec les partenaires d'affaires et les consommateurs[37]. Les entreprises sont également plus souvent la cible de pourriels (ou « *spam* »), parfois porteurs de virus de toutes sortes ou de logiciels-espions : 40 % des courriers électroniques qu'elles reçoivent entrent en effet dans cette catégorie[38]. Cependant, il n'est pas toujours aisé pour l'utilisateur moyen de faire le tri entre un courriel utile et une simple publicité sans en avoir préalablement lu le contenu. Et, en l'absence de filtre efficace, l'entreprise peut être confrontée à une infection de son système d'information ou à la saturation du serveur électronique, sans oublier la perte de temps occasionnée par la lecture des courriels publicitaires en constante augmentation.

La cybercriminalité prolifère et évolue en même temps que les technologies : le principal souci des employeurs était autrefois d'éliminer le vol de temps et la navigation sur des sites illicites, ils doivent désormais se préoccuper également des risques juridiques et

---

[37] CEFRIO et SOM RECHERCHES ET SONDAGES, *NetQuébec 2008. Portrait de l'utilisation des TI et d'Internet au Québec*, 2008, p. 2, en ligne : <https://www.cefrio.qc.ca/index.php?eID=tx_nawsecuredl&u=4818&file=fileadmin/doc_bloc_achat/DEPnetquebecwebSECUR.pdf&t=1280345975&hash=c6efb88e785aabb676a1ccb9a91acd79> (site consulté le 27 juillet 2010) : selon cette étude, les salariés québécois utilisent le courriel à raison de 67,9 % pour les échanges avec leurs collègues et 91 % pour les communications avec les clients et fournisseurs de l'entreprise).

[38] *Id.*; Selon l'encyclopédie Wikipedia, « Le spam, pourriel ou polluriel est une communication électronique non sollicitée, en premier lieu via le courrier électronique. Il s'agit en général d'envois en grande quantité effectués à des fins publicitaires. ». Cette définition peut être consultée à : WIKIPEDIA, « Spam », 2010, en ligne: <http://fr.wikipedia.org/wiki/Pourriel> (site consulté 30 juillet 2010).

sécuritaires[39] liés à certaines pratiques (téléchargement illégal, logiciels espions, fuite d'information confidentielles, etc.).

Sur le plan sécuritaire, les principales craintes des entreprises concernent l'utilisation, la communication, la consultation et la modification non autorisées des informations qu'elles détiennent[40]. De tels agissements sont, notamment, réprimés par les articles 380 et suivants du *Code Criminel* (visant la fraude), ainsi que les articles 342.1 (relatif à l'utilisation non autorisée d'un ordinateur)[41] et 430(1.1) (qui punit l'infraction de méfait de données informatiques) du même Code.

La cybercriminalité peut être le fait aussi bien des membres du personnel que de personnes externes à l'entreprise. De fait, les menaces sécuritaires proviennent désormais essentiellement de l'intérieur de l'entreprise. En effet, le nombre d'employés tentés de voler des informations vitales appartenant à leur employeur est en hausse constante, tout comme le nombre de victimes des ces actes malveillants qui est passé de 0,1 million en 2008 à environ 1,6 million en 2009[42]. Parfois, ces malveillances sont le fait d'anciens employés frustrés par les conditions de leur départ et qui vont profiter de leur bonne connaissance de l'organisation pour exploiter les failles de son système d'information. C'est ainsi qu'un ex-salarié de la société pharmaceutique *Smith and Nephew France* avait orchestré toute une campagne de harcèlement et de dénigrement contre son ancien employeur[43]. Il avait envoyé, de manière régulière, des messages électroniques dénigrant l'entreprise non seulement aux salariés des différentes sociétés du groupe, en France et à l'étranger, mais également à ses partenaires commerciaux et financiers, ses concurrents et à des sociétés de presse. Il avait ainsi transmis plus de 700 000 messages électroniques non sollicités. Afin

---

[39] Voir *infra*, Partie 1, Chapitre 1, Section 1, p. 10.

[40] Valérie SÉDALLIAN, « Légiférer sur la sécurité informatique : la quadrature du cercle? », Juriscom.net, 08 décembre 2003, p. 3 et 5, en ligne : <http://www.juriscom.net/documents/secu20031208.pdf> (site consulté le 19 août 2010).

[41] L'article 342.1 du *Code criminel* permet, notamment, d'appréhender l'interception des données d'autrui et plus particulièrement celle du courrier électronique.

[42] KPMG, préc., note 31.

[43] Trib. gr. inst. Mans, 7 nov. 2003 : Juritel n° JTL OGH711TGI–Internet, en ligne : <http://www.juritel.com/Ldj_html-941.html> (site consulté le 30 juillet 2010).

de ne pas être identifié, il opérait à partir de sites extérieurs comportant une rubrique « envoyez cet article à un ami ». Dans le champ « expéditeur », il indiquait une adresse fantaisiste, qui correspondait généralement à celle de dirigeants de son ancienne entreprise, et dans le champ « message » il remplaçait le texte d'origine du site par des allégations mensongères, voire diffamatoires, sur les produits du groupe. Cette manipulation lui permettait de déjouer les paramètres de filtrage du système de protection de son ex-employeur. Le salarié avait finalement pu être retracé grâce aux adresses IP laissées sur les serveurs des sites qu'il avait utilisés. Ces dernières appartenaient au fournisseur d'accès Wanadoo qui avait fourni l'identité de l'abonné. Le Tribunal de grande instance du Mans a jugé que la falsification de l'adresse électronique de l'expéditeur constituait un « accès frauduleux à un système d'information » et que la saturation des boîtes de réception de messageries électroniques s'inscrivait dans le délit d'entrave à un tel système[44]. Ce qui a valu au salarié une condamnation à dix mois de prison avec sursis et à deux ans de mise à l'épreuve, en plus d'un licenciement pour faute grave effectué par son nouvel employeur.

Il faut toutefois souligner que si la plupart des actes dommageables pour l'entreprise résultent d'actes de malveillance, certains proviennent d'erreurs ou de causes accidentelles : il suffira parfois de l'utilisation d'une disquette personnelle contaminée ou de l'ouverture d'un courrier privé infecté (aussitôt retransmis aux amis et collègues avec qui l'on souhaite partager l'excellente blague que l'on vient de recevoir) pour corrompre tout le système d'information de l'entreprise. Il n'y a généralement aucune malice dans ces gestes; toutefois, avec la rapidité des communications et la mise en réseau des activités de l'entreprise, ils peuvent avoir des conséquences désastreuses pour l'organisation, avec un risque de contamination généralisée du réseau et une plus grande difficulté à circonscrire et éliminer le problème.

Les risques auxquels les entreprises sont confrontées peuvent être d'origine naturelle, humaine ou technique et peuvent porter atteinte à l'intégrité des systèmes d'information

---

[44] *Id.*

(intrusion non autorisée ou contamination par virus, ver, logiciel espion, etc.), à la disponibilité des systèmes et des données (sabotage ralentissant la bande passante d'Internet par exemple) et à la confidentialité des informations (par exemple l'intrusion non autorisée (« hacking ») ou l'espionnage)[45]. Concrètement, le système n'est plus en mesure de fonctionner selon les spécifications normales, si bien que les informations qu'il contient ou génère ne sont plus fiables[46]. Or, l'une des obligations qui incombent à l'entreprise est de garantir la sécurité et la confidentialité des données personnelles qu'elle détient sur ses clients, ses usagers et son personnel. En effet, les articles 10, 11 et 12 de la *Loi sur la Protection des renseignements personnels dans le secteur privé*[47] imposent, entre autres, à l'entreprise de mettre en place des mesures de sécurité visant à assurer la confidentialité des renseignements (article 10), de s'assurer que les renseignements sont à jour et exacts (article 11) et de s'assurer de plus qu'ils ne seront pas utilisés une fois l'objectif pour lequel ils ont été recueillis accompli (article 12). Le système de protection mis en place devra donc, par des mesures appropriées, garantir que le système d'information demeure, en tout temps, digne de confiance et que les informations qu'il contient et génère ne sont ni erronées ni frauduleuses[48].

1.2. L'obligation de sécurité informatique

Pour évaluer la responsabilité de l'employeur en matière de sécurité informatique, il est nécessaire de définir l'obligation de sécurité informationnelle (1.2.1.), ainsi que sa portée (1.2.2.).

---

[45] V. SÉDALLIAN, préc., note 40, p. 3.

[46] LUC GOLVERS, « L'informatique et la protection de la vie privée », Droit-technologie.org, 11 janvier 2001, p. 15, en ligne : <http://www.droit-technologie.org/upload/dossier/doc/33-1.pdf> (site consulté le 19 août 2010).

[47] Préc., note 10.

[48] L. GOLVERS, préc., note 46, p. 15.

1.2.1. Définition de l'obligation de sécurité informatique

Au Québec, l'obligation de sécurité informatique découle, notamment, de l'article 10 de la *Loi sur la protection des renseignements personnels dans le secteur privé*[49] et de l'article 25 de la *Loi concernant le cadre juridique des technologies de l'information*[50].

C'est le Responsable de la Sécurité des Systèmes d'Informations (RSSI) qui est chargé de veiller à la sécurité du réseau, en s'assurant que « l'information est valide, [que] les infrastructures garantissent l'intégrité des données et [qu']il est possible de détecter les actions malveillantes »[51]. Sa mission consiste également à garantir la confidentialité des données traitées par le système. La sécurité informationnelle s'apprécie, en effet, en fonction du « triptyque DIC bien connu des spécialistes de la sécurité informatique: Disponibilité, Intégrité et la Confidentialité des fonctions et informations »[52]. À ces critères, il faut ajouter « l'authenticité et l'irrévocabilité de l'information »[53].

Le rôle du RSSI consiste également à adapter les mesures de sécurité en fonction de l'origine du risque et de la nature des informations à protéger : il est en effet certain que le degré de sécurisation à apporter à un fichier uniquement composé des noms et adresses de clients ne peut pas être le même que lorsqu'il s'agit d'informations sensibles, éventuellement couvertes par le secret professionnel, telles les données médicales ou bancaires »[54]. Il faudra donc que l'entreprise opère des choix en termes de gestion des risques, afin de trouver un compromis satisfaisant entre les besoins de circulation de

---

[49] Préc., note 10.

[50] L.R.Q. 2001, c. C-1.1.

[51] Martin DUBOIS, « Nouvelles technologies de l'information et des communications et sécurité informationnelle », dans *Développements récents en droit de l'accès à l'information (2002)*, Service de la formation permanente du Barreau du Québec, 2002, *Droit civil en ligne* (DCL), EYB2002DEV565, p. 9.

[52] V. SÉDALLIAN, préc., note 40, p. 3.

[53] Ana I. VICENTE, *La convergence de la sécurité informationnelle et la protection des données à caractère personnel. Vers une nouvelle approche juridique*, mémoire de maîtrise, Montréal, Faculté des études supérieures, Université de Montréal, 2003, p. 11.

[54] V. SÉDALLIAN, préc., note 40, p. 3.

l'information, des délais d'exécution raisonnables et le niveau de sécurité exigé au regard des caractéristiques des données[55].

Les mesures de sécurité adoptées par l'entreprise consistent souvent en une protection physique des lieux (contrôle d'accès aux locaux, protection contre les incendies, etc.). Toutefois, s'agissant de données numériques, la sécurité aura surtout un aspect « logique » (dispositifs pare-feu, installation d'antivirus, mots de passe, verrouillage de classeurs, chiffrement/cryptologie, etc.), organisationnel (accès aux données en fonction des habilitations, sauvegardes, maintenance, mise à jour des logiciels pour installer les correctifs) et juridique (contrat d'assurance, par exemple)[56].

L'impératif de sécurité informationnelle implique également que les mesures de sécurité appliquées sur le lieu physique de l'entreprise soient étendues à toutes les personnes ou entités qui sont autorisées à accéder à distance aux données de l'entreprise : les télétravailleurs et les travailleurs mobiles doivent en effet bénéficier d'outils informatiques dotés d'une protection adéquate[57]. Il en va de même pour les personnes dûment mandatées par un contrat, par exemple dans le cadre de l'impartition des données, et qui doivent, elles aussi, utiliser des méthodes appropriées garantissant la sécurité des informations fournies[58]. Enfin, l'entreprise doit s'assurer que tous les supports qui abritent ou véhiculent ses informations stratégiques (mémoires d'ordinateur, disques durs, clés USB, réseaux numériques, etc.) sont sécurisés[59].

La sécurité du système d'information suppose également des actions de sensibilisations et de formation du personnel[60], car, comme indiqué précédemment, une grande majorité des

---

[55] *Id.*

[56] Blandine POIDEVIN, « Quelle responsabilité en matière de sécurité informatique? », Jurisexpert.net, 8 avril 2002, en ligne : <http://www.jurisexpert.net/quelle_responsabilit_en_mati_re_de_s_cur/> (consulté le 19 août 2010).

[57] M. DUBOIS, préc., note 51, p. 6-7.

[58] *Id.*, p. 7.

[59] Ian J. TURNBULL, « Information systems », dans Ian J. TURNBULL, Shari SIMPSON CAMPBELL, Donald F. HARRIS et Brian KIMBALL, *Privacy in the workplace: the employment perspective*, Canadian Privacy Institute, CCH Canadian, Toronto, 2004, p. 208.

[60] V. SÉDALLIAN, préc., note 40, p. 2.

atteintes à la sécurité des données dont les entreprises sont victimes sont le fait d'employés négligents ou imprudents. Les salariés bénéficiant d'un ordinateur portable doivent ainsi exercer une surveillance de tous instants sur leur outil de travail. C'est ce qu'a rappelé la Commissaire à la protection de la vie privée du Canada, dans une affaire où une banque s'était vu reprocher sa carence à protéger les renseignements personnels d'un particulier à la suite du vol d'un ordinateur portatif contenant ses données[61]. L'appareil, qui contenait les renseignements personnels de 960 clients de la banque, avait disparu alors qu'il était en la possession d'une planificatrice financière qui l'avait laissé sans surveillance dans son véhicule. L'automobile avait été parquée dans le garage souterrain de l'employée, qui avait pris le soin d'en verrouiller toutes les portières. La responsabilité de la banque a été admise pour manquement au principe 4.7 de la *Loi sur la Protection des renseignements personnels et les documents électroniques*[62], selon lequel les renseignements personnels doivent être protégés grâce à des mesures de sécurité correspondant à leur degré de sensibilité. Après avoir constaté que la banque avait mis en place des politiques et procédures qui semblaient conformes à ce principe (ainsi, pour ce qui concerne les ordinateurs portatifs, ces règles impliquaient l'utilisation de mots de passe et la mise en sécurité des ordinateurs), la commissaire adjointe a néanmoins relevé qu'en l'espèce, l'employée n'avait pas suivi les recommandations de son employeur concernant la sécurité matérielle et avait laissé l'ordinateur sans surveillance sur le siège de son véhicule.

Enfin, pour garantir une protection optimale, les mesures de sécurité doivent être examinées et mises à jour régulièrement, afin de tenir compte à la fois de l'évolution des menaces et des changements organisationnels de l'entreprise[63].

Toutefois, les auteurs ne s'accordent pas sur le degré d'intensité de l'obligation de sécurité informationnelle à laquelle l'entreprise est tenue.

---

[61] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Résumé de conclusions d'enquête en vertu de la LPRPDÉ n° 289. Le vol d'un ordinateur portatif met en cause la responsabilité d'une banque*, 3 février 2005, 2005 IIJCan 15488 (C.V.P.C.), en ligne : <http://www.canlii.org/>.

[62] L.C. 2000, c. 5.

[63] M. DUBOIS, préc., note 51, p. 9.

1.2.2. Portée de l'obligation de sécurité informatique

1.2.2.1. Une gestion prudente et diligente du système d'information

L'obligation de sécurité informationnelle est généralement considérée comme une obligation de « moyens »[64]. En effet, pour de nombreux auteurs, cette obligation ne saurait en être une de résultat, notamment parce que l'idée d'une « politique de sécurité sans failles est à la fois économiquement et matériellement impossible »[65] : quel que soit le degré d'efficacité des mesures de protection mises en œuvre, il n'existe pas de « risque zéro » dans ce domaine[66]. Cependant, pour certains auteurs, certaines dispositions législatives québécoises donneraient à penser qu'il s'agit d'une obligation de « résultat » : en effet, l'article 25 de la *Loi concernant le cadre juridique des technologies de l'information*, qui exige des « mesures de sécurité propres à […] assurer la confidentialité »[67], tout en énumérant de façon non limitative les moyens ou précautions à adopter, semble imposer une obligation de résultat[68]. De plus, l'utilisation du terme « doit » à l'article 10 de la *Loi sur la protection des renseignements personnels dans le secteur privé*[69] laisserait également présumer que l'intention du législateur était d'en faire une obligation de résultat[70]. À cet égard, il faut cependant souligner que cet article a été modifié en 2006[71] et exige désormais l'usage de « mesures de sécurité […] raisonnables »[72]. Par conséquent, l'obligation de sécurité en matière renseignements personnels devrait s'apprécier en tenant compte,

---

[64] V. SÉDALLIAN, préc., note 40, p. 3.

[65] Nicolas W. VERMEYS, *Qualification et quantification de l'obligation de sécurité informationnelle dans la détermination de la faute civile*, thèse de doctorat, Montréal, Faculté des études supérieures, Université de Montréal, 2009, p. 85-87.

[66] M. DUBOIS, préc., note 51, p. 9.

[67] Préc., note 50.

[68] N. W. VERMEYS, *Qualification et quantification de l'obligation de sécurité informationnelle dans la détermination de la faute civile*, préc., note 65, p. 94-95.

[69] Préc., note 10.

[70] Sylvain LEFEBVRE, *Nouvelles technologies et protection de la vie privée en milieu de travail en France et au Québec*, coll. Droit social, Aix-en-Provence, Presses universitaires d'Aix-Marseille, 1998, p. 185.

[71] *Loi modifiant la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels et d'autres dispositions législatives*, L.Q. 2006, c. 22, art. 113.

[72] *Loi sur la protection des renseignements personnels dans le secteur privé*, préc., note 10.

notamment, de la sensibilité des renseignements personnels traités, de leur quantité, de la finalité de leur utilisation, ainsi que du support employé. Finalement, avec l'existence de ce « critère de raisonnabilité »[73], l'article 10 de la *Loi sur la protection des renseignements personnels dans le secteur privé*[74] semble imposer une obligation de moyens[75].

Toutefois, si l'on n'exige pas une sécurité absolue, le recours à des standards de sécurité plus élevés est néanmoins nécessaire à l'égard de certaines données considérées comme sensibles, telles les données bancaires ou médicales[76]. C'est d'ailleurs la solution préconisée en France et par certains organismes américains[77]. Aussi certains auteurs proposent-ils que le régime applicable à l'obligation de sécurité informationnelle soit celui de l'« obligation de moyens renforcée »[78]. Il s'agit d'un régime de présomption de faute qui opère un renversement du fardeau de la preuve et met à la charge du responsable de la sécurité des systèmes d'informations le soin d'établir « qu'il a adopté toutes les mesures de sécurité qu'adopterait un RSI raisonnablement prudent et diligent »[79] pour protéger le système d'information de l'entreprise. Les organisations doivent, en somme, non seulement protéger leur système d'information contre les attaques externes, mais également contrôler les flux entrant et sortant, ainsi que l'utilisation des postes de travail en interne. Le contrôle notamment de l'accès à l'Internet est crucial, et cela d'autant plus qu'une absence d'encadrement de l'utilisation qu'en font les salariés peut constituer une faute contractuelle de l'entreprise qui les emploie. C'est ce qu'a jugé la Cour d'appel de Paris[80] à l'encontre

---

[73] Karl DELWAIDE et Antoine AYLWIN, « Leçons tirées de dix ans d'expérience : la Loi sur la protection des renseignements personnels dans le secteur privé du Québec », p. 33, Commissariat à la protection de la vie privée du Canada, en ligne : <http://www.priv.gc.ca/information/pub/dec_050816_f.pdf> (site consulté le 19 août 2010).

[74] Préc., note 10.

[75] N. W. VERMEYS, *Qualification et quantification de l'obligation de sécurité informationnelle dans la détermination de la faute civile*, préc., note 65, p. 93.

[76] *Id.*, p. 108.

[77] *Id*., p. 108-109.

[78] *Id*., p. 108.

[79] *Id.*, p. 107 et 111.

[80] Paris, 4 mai 2007, en ligne : <http://www.legalis.net/spip.php?page=jurisprudence-decision&id_article=2096> (site consulté le 30 juillet 2010).

d'une société qui avait résilié son contrat de location d'un système antivirus après avoir constaté que le fournisseur était incapable d'éradiquer les nombreux virus dont son système informatique était infecté et d'apporter une solution efficace aux difficultés qu'elle avait à faire fonctionner correctement le matériel mis en place. Le prestataire avait alors fait valoir que l'entreprise avait, par sa faute, rendu inefficace la protection qu'il s'était engagé à lui fournir en laissant son personnel se connecter à des sites illicites et sans lien avec l'activité de l'employeur, notamment pour télécharger des jeux ou des contenus pornographiques, dont la plupart étaient infectés de virus. Par conséquent, l'entreprise ne pouvait prétendre que la défaillance de la protection antivirus constituait un juste motif de résiliation des contrats. La Cour a donné raison au prestataire, considérant

> « qu'il ne peut rentrer dans les obligations contractuelles [du prestataire] d'assurer une protection de la société […] contre des virus contenus dans des sites informatiques étrangers à son activité, voire illégaux tels que les sites qui permettent de télécharger gratuitement des programmes habituellement payants ».[81]

Cependant, si la Cour évoque une exclusion de garantie en cas de mauvaise utilisation du matériel, elle n'apporte pas de précision sur le fondement de sa décision et laisse en suspens de nombreuses questions, dont celle de l'étendue des obligations du prestataire de services antivirus ou celles de ses clients[82]. Toutefois, cette décision admet que la sécurité juridique des contrats liés à la sécurité informatique peut être remise en cause par une faille de sécurité résultant de la carence et de la négligence d'une entreprise à surveiller les activités de ses salariés[83]. Ce faisant, la Cour souligne la nécessité pour les entreprises de réguler l'accès des salariés à l'Internet.

---

[81] *Id.*

[82] LEGALIS.NET, « Virus le client responsable d'être allé sur des sites étrangers à son activité », 04 décembre 2007, en ligne : <http://www.legalis.net/article.php3?id_article=2098> (site consulté le 30 juillet 2010).

[83] Eric A. CAPRIOLI, « Les contrats informatiques face à la jurisprudence récente. Gare au surf incontrôlé des salariés », Caprioli-avocats.com, Première publication : Avril 2008, en ligne : <http://www.caprioli-avocats.com http://www.caprioli-avocats.com/securite-informatique/146-surf-incontrole-des-salaries> (consulté le 19 août 2010).

En définitive, l'obligation de sécurité présente un caractère préventif et renvoie à une « notion très générique : celle des "*règles de l'art*" »[84]. Ce sont ces dernières qui permettront de gérer de façon appropriée la part de « risque résiduel de faille » inhérente à tout système de sécurité[85].

En pratique, le succès de la politique de sécurité d'une entreprise est tributaire de l'évaluation, par ses dirigeants, du « ratio risques-coût »[86] qui permettra, en fonction des moyens alloués, de déterminer le seuil au-delà duquel le risque est inacceptable[87]. Pourtant, le système d'information d'une entreprise ne s'évalue pas uniquement en termes de coûts, mais également en termes de « valeur », celle-ci étant représentée par les données confidentielles et/ou à forte valeur stratégique qu'il abrite[88]. Toutefois, il semblerait que le choix soit souvent vite fait, puisque de nombreuses organisations ne disposent pas d'une gestion des données personnelles organisée et de qualité. En effet, une enquête du *Computer Security Institute* révèle que plus de 35 % des organisations consacrent moins de 2 % de leur budget en technologies de l'information à la sécurité de leur système informatique[89]. Il y a plusieurs raisons à ce laxisme. Tout d'abord, la culture de sécurité est un fait relativement nouveau au sein des organisations : de nombreux dirigeants avouent ne pas toujours bien appréhender les enjeux liés à la sécurité des informations, tandis que d'autres admettent tout simplement leur manque d'intérêt ou même leur ignorance en la

---

[84] V. SÉDALLIAN, préc., note 40, p. 3.

[85] M. DUBOIS, préc., note 51, p. 6.

[86] V. SÉDALLIAN, préc., note 40, p. 4.

[87] M. DUBOIS, préc., note 51, p. 9.

[88] I. RENARD, « Responsabilité de l'entreprise et de ses dirigeants du fait de la perte de données informatiques », préc., note 35.

[89] COMPUTER SECURITY INSTITUTE, FEDERAL BUREAU OF INVESTIGATION, préc., note 32; Voir également PRICEWATERHOUSECOOPERS, *IT security survey*, Décembre 2009, résumé en ligne : <http://www.pwc.fr/securite-informatique-les-attaques-ciblant-les-donnees-de-lentreprise-ont-presque-double-en-2009-dans-le-monde.html> (site consulté le 22 août 2010) : la dernière enquête annuelle de *PricewaterhouseCoopers*, réalisée auprès de 7200 entreprises dans 130 pays, apporte une nuance à ce constat, puisqu'elle relève une augmentation significative des budgets consacrés par les organisations à la sécurité de leurs systèmes d'information, et ce, malgré la crise économique et financière.

matière[90]. Le problème, c'est que ces excuses ne les exonèrent pas de leurs responsabilités : l'obligation de sécurité est une obligation légale à laquelle ils sont tenus, en vertu de l'adage « nul n'est censé ignorer la loi ». À cet égard, l'article 93 de la *Loi sur la Protection des renseignements personnels dans le secteur privé* prévoit que :

> « Si une personne morale commet une infraction prévue par la présente loi, l'administrateur, le dirigeant ou le représentant de cette personne morale qui a prescrit ou autorisé l'accomplissement de l'acte ou de l'omission qui constitue l'infraction ou qui y a consenti est partie à l'infraction et passible de la peine qui y est prévue. »[91]

De plus, la sécurité est inhérente aux NTIC et devrait constituer une priorité pour les entreprises dont les serveurs sont exposés à des risques bien réels. En effet, une faille de sécurité peut entraîner non seulement un impact négatif sur l'image de marque de l'entreprise, mais également une contamination de son système d'information, ainsi que la perte de confiance de ses différents contacts d'affaires. Un ralentissement des flux et l'accessibilité des données confidentielles peuvent également s'ensuivre. Mais pour l'entreprise, cela implique également des frais, souvent très élevés, de réparation et de remise à niveau du système. Parfois, l'entreprise n'a pas vraiment d'autre choix : la mise en place de mesures de sécurité représente un coût (en termes financier, humain, de temps) que certaines organisations – notamment les petites structures ou les jeunes entreprises – ne peuvent pas assumer. Et surtout, elles n'ont pas les outils juridiques appropriés, contrairement aux grandes entreprises qui disposent généralement de toute une « armada » de juristes et d'avocats pour les informer et les conseiller. D'autres entreprises font, en revanche, le choix délibéré de ne pas trop investir dans la sécurité de leur système d'information. Il faut dire que les poursuites pour les manquements à l'obligation de sécurité demeurent exceptionnelles[92], malgré les nombreuses dénonciations médiatiques. Si

---

[90] I. RENARD, « Responsabilité de l'entreprise et de ses dirigeants du fait de la perte de données informatiques », préc., note 35.

[91] *Loi sur la Protection des renseignements personnels dans le secteur privé*, préc., note 10, art. 93.

[92] V. SÉDALLIAN, préc., note 40, p. 4.

bien que les dirigeants peuvent, cyniquement, en conclure qu'en n'adoptant pas les mesures de sécurité informatique adéquates ils ne faisaient pas courir un si grand risque de poursuites pénales à leur entreprise[93].

Néanmoins, les organisations peuvent parfois éprouver des difficultés à établir qu'elles ont pris toutes les mesures de sécurité appropriées[94], aussi la probabilité d'obtenir réparation est assez élevée pour les personnes lésées par la perte, la détérioration ou le piratage de leurs données. Bien entendu, en cas de poursuite, l'appréciation de la responsabilité de l'entreprise se fera, notamment, « en fonction des mesures préventives qui ont été prises [et] de l'état de l'art de la sécurité informatique »[95]. Cependant, les tribunaux seront probablement moins cléments en cas d'absence de diligence minimale ou lorsqu'il s'agit de risques connus. Ainsi, en cas d'infection virale, l'entreprise ayant subi la « première vague de contamination » d'un nouveau virus inconnu des antivirus les plus courants ne verra sans doute pas sa responsabilité engagée; en revanche, si l'infection est propagée par une entreprise dont le système informatique est contaminé par un virus datant de plusieurs mois, sa responsabilité sera sans aucun doute retenue[96].

Par ailleurs, la plupart des pays sanctionnent lourdement les manquements à l'obligation de sécurité. Ainsi, au Québec, les manquements à l'obligation de sécurité de la *Loi sur la Protection des renseignements personnels dans le secteur privé*[97] exposent l'entreprise à des dommages-intérêts, conformément au régime de droit civil (article 1458 C.c.Q.). Dans l'affaire *Stacey* c. *Sauvé Plymouth Chrysler (1991) Inc.*[98], la responsabilité d'un concessionnaire automobile a été reconnue en raison de sa carence à prendre les mesures adéquates pour protéger les renseignements personnels d'un client. Dans cette affaire, un

---

[93] *Id.*

[94] N. W. VERMEYS, *Qualification et quantification de l'obligation de sécurité informationnelle dans la détermination de la faute civile*, préc., note 65, p. 105.

[95] Blandine POIDEVIN, « Quelle responsabilité en matière de sécurité informatique? », préc., note 56.

[96] *Id.*

[97] Préc., note 10.

[98] J.E. 2002-1147 (C.Q.).

employé du concessionnaire avait utilisé les renseignements personnels du demandeur, malgré le refus de ce dernier, pour éviter à un autre client de payer certaines taxes. Or, il s'est avéré, plus tard, que le bénéficiaire de ces manœuvres était un mauvais payeur dont les défauts de paiement ont été inscrits au dossier de crédit du demandeur. Ce dernier a donc poursuivi le concessionnaire pour les dommages subis à la suite de cette divulgation illégale de ses renseignements personnels. Cette décision n'est pas vraiment reliée à la sécurité informatique, mais elle est néanmoins intéressante dans la mesure où la responsabilité de l'entreprise a été retenue non pas en raison de sa participation à la fraude ou de sa qualité d'employeur, mais plutôt sur le fondement de l'article 10 de la *Loi sur la Protection des renseignements personnels dans le secteur privé*[99] mettant à sa charge l'obligation de sécurité et de confidentialité des données détenues[100].

La *Loi sur la Protection des renseignements personnels dans le secteur privé*[101] prévoit par ailleurs des sanctions pénales de 1 000 à 10 000 dollars (10 000 à 20 000 dollars en cas de récidive) pour « [q]uiconque recueille, détient, communique à un tiers ou utilise un renseignement personnel sur autrui » en contravention, notamment, avec ses dispositions relatives à la sécurité et à la confidentialité des données[102]. En pratique, les condamnations financières semblent être plutôt raisonnables. Une entreprise a ainsi été condamnée à verser 700 dollars à un particulier à la suite de la divulgation, sans son autorisation, de ses renseignements personnels[103]. De même, un agent d'assurances a écopé d'amendes totalisant 3 000 dollars pour avoir hébergé, directement sur le site Internet de l'agence, les liens informatiques, code d'utilisateur et mot de passe de son frère, pour rendre service à ce dernier qui éprouvait des difficultés à mémoriser ses codes d'accès[104]. Or, la mise en place ce procédé n'avait pas été suivie d'une protection adéquate des renseignements personnels

---

[99] Préc., note 10.

[100] K. DELWAIDE et A. AYLWIN, préc., note 73, p. 35.

[101] Préc., note 10.

[102] *Id.*, art. 91.

[103] *Séguin* c. *Général Motors Acceptance Corporation du Canada ltée*, 2007 QCCQ 14509 (CanLII).

[104] *Chambre de l'assurance de dommages* c. *Kotliaroff*, 2008 CanLII 19078 (QC C.D.C.H.A.D.)

des 12 000 clients de l'agence, qui étaient hébergés sur le site et étaient alors devenus accessibles, à tout visiteur, aux clients et aux employés. Malgré le nombre élevé de victimes et la durée de l'affichage des données (deux semaines), cette espèce, en raison des circonstances particulières qui entourent les faits, est davantage marquée par l'aspect disciplinaire que par la volonté de réparer le préjudice qui a pu en découler.

Les condamnations pécuniaires peuvent être plus élevées lorsque la responsabilité d'une entité est engagée à la suite d'une perte de données personnelles massive. C'est ce que l'on peut déduire de l'affaire *Union des consommateurs* c. *Canada (Procureur général)*[105], dans laquelle l'Union des consommateurs a pu négocier, en juin 2008, un règlement hors cours accordant des dommages à 120 000 individus dont les renseignements personnels avaient été subtilisés, à la suite d'un vol d'ordinateurs survenu, quelques années auparavant, dans des locaux de l'Agence des douanes et du revenu du Canada. Un recours collectif avait été intenté contre le gouvernement fédéral, au nom de toutes les personnes dont les renseignements personnels avaient été ainsi exposés. Les victimes réclamaient le paiement, pour chacune d'entre elles, des frais occasionnés par ce vol, ainsi que 1 000 dollars à titre de dommages, pour compenser les pertes de temps, le stress, les troubles et les inconvénients subis, et 500 dollars à titre de dommages punitifs, en raison de la négligence dont l'Agence avait fait preuve. Finalement, elles ont obtenu une compensation de soit 150 dollars, soit 200 dollars, selon les critères établis[106]. Si ces chiffres peuvent sembler dérisoires lorsqu'ils sont pris individuellement, ils atteignent, néanmoins, des montants conséquents lorsqu'ils sont additionnés, puisque, dans l'hypothèse la plus optimiste, on obtiendrait un total de 24 000 000 dollars. Ce qui nous rapproche des montants relevés aux États-Unis où les dommages-intérêts ne sont souvent pas plafonnés et où les juridictions n'hésitent pas à frapper sur le plan financier. *ChoicePoint*, une entreprise hébergeant des

---

[105] 2006 QCCS 448 (CanLII) (transaction ratifiée par la Cour fédérale, C.F. Ottawa, n° T-1869-07, 23 juin 2008, j. Martineau, en ligne : <http://recours-collectifs.ca/Wdocs/562008517102ULL.pdf> (site consulté le 25 juillet 2010). Le texte intégral de la transaction est disponible en ligne : <http://www.cra-arc.gc.ca/gncy/clssctn/txt-fra.pdf> (site consulté le 25 juillet 2010)).

[106] *Id.*

données bancaires, en a fait l'amère expérience à la suite du piratage d'un de ses serveurs[107]. Sa négligence relativement à la sécurité des données personnelles de ses clients lui a valu une amende record de 10 millions de dollars, ainsi que 5 millions de dollars de dommages-intérêts, infligés par la *Federal Trade Commission*[108].

En France également, les amendes sont, dans une moindre mesure, assez élevées, puisque celui qui ne prend pas toutes les précautions utiles pour préserver la sécurité des données personnelles et notamment pour empêcher que celles-ci ne soient communiquées à des tiers non autorisés encourt une peine de 5 ans d'emprisonnement et une amende de 300 000 euros[109]. De plus, l'entreprise engage sa responsabilité civile vis-à-vis des personnes dont les données personnelles n'ont pas été protégées de manière adéquate. Elle pourra, notamment, être condamnée à une réparation intégrale des dommages en vertu des principes prévus aux articles 1382 et suivants du Code civil français.

Finalement, on peut espérer que l'affaire *ChoicePoint* sonnera le glas des politiques attentistes des entreprises en matière de sécurité et incitera les patrons à réévaluer leurs stratégies dans ce domaine. Car, bien que les incidents relatifs au vol et à la perte d'informations soient globalement en diminution, le nombre de personnes qui en sont affectées à travers le monde a augmenté de plus de 50 % entre 2008 et 2009 et s'élevait à plus de 200 millions en 2009[110]. La mise en place d'une politique de prévention contre les pertes de données – et des technologies permettant de protéger ces informations – est d'autant plus nécessaire que l'entreprise est souvent la seule à supporter les conséquences d'une faille de sécurité résultant de ses propres carences et négligences. Ainsi, en cas d'intrusion non autorisée dans le système d'information d'une organisation, celle-ci n'obtiendra pas forcément la condamnation de son auteur si elle n'a pas mis en place des

---

[107] CÉDRIC CRÉPIN, « Pertes de données : à quand une politique d'entreprise responsabilisante », Droit-tic.com, 6 mars 2006, en ligne : <http://www.droit-ntic.com/news/afficher.php?id=347> (site consulté le 19 août 2010).

[108] *Id*.

[109] Code pénal, art. 226-17.

[110] KPMG, préc., note 31; Voir également PRICEWATERHOUSECOOPERS, préc., note 89.

mesures de sécurité appropriées. C'est ce qu'a appris, à ses dépens, une société française lorsque les juges lui ont expliqué que le fait de ne pas avoir respecté son obligation de sécurité la privait de tout recours contre un internaute qui avait pénétré son système d'information pour y détourner des fichiers contenant des données personnelles de clients[111]. Dans cette affaire, l'administrateur du site *Kitetoa.com*, spécialisé dans la dénonciation des brèches de sécurité des systèmes d'informations des organisations, avait, à plusieurs reprises, pénétré le site Internet de la plaignante. Ces intrusions, effectuées uniquement grâce aux fonctionnalités du navigateur grand public Netscape, lui avaient permis d'accéder aux fichiers de données nominatives de l'entreprise. L'internaute avait, dès sa première incursion, avisé l'administrateur du site de la faille de sécurité constatée, mais sa mise en garde était restée sans réponse. Il avait réitéré son avertissement un an plus tard, après une nouvelle intrusion réussie. Finalement, la presse s'était fait l'écho des dénonciations de *Kitetoa.com*, avec à l'appui une diffusion des photos d'écrans contenant des données personnelles, cependant illisibles, détenues par cette société. Cette dernière avait alors poursuivi l'administrateur de « Kitetoa.com » pour accès ou maintien frauduleux dans son système de traitement automatisé des données. La Cour d'appel a statué qu'il :

> « ne peut être reproché à un internaute d'accéder aux données, ou de se maintenir dans les parties des sites qui peuvent être atteintes par la simple utilisation d'un logiciel grand public de navigation, ces parties de site, qui ne font, par définition, l'objet d'aucune protection de la part de l'exploitant du site ou de son prestataire de services, devant être réputées non confidentielles à défaut de toute indication contraire et de tout obstacle à l'accès »[112].

Et que bien qu'il s'agisse de données nominatives, elle a conclu que :

> « l'internaute y accédant dans de telles conditions ne peut inférer de leur nature qu'elles ne sont pas publiées avec l'accord des intéressés »[113].

---

[111] Paris, 30 oct. 2002, *Gaz.Pal.*2003.205.

[112] *Id.*

[113] *Id.*

Par conséquent, les agissements du journaliste ne pouvaient pas être considérés comme un accès ou un maintien frauduleux dans un système automatisé de traitement de données. Il a donc été relaxé. Quant à la plaignante, qui s'était portée partie civile, elle a été déboutée, non seulement en raison de ses carences et négligences, mais également du fait que l'éventuel préjudice n'aurait pu être subi que par d'autres.

L'affaire *ChoicePoint* pourrait également constituer un signal fort pour les victimes – qu'il s'agisse d'entreprises ou de particuliers – indiquant que leur droit à la sécurité de leurs données n'est pas seulement théorique et peut être effectivement garanti par les organismes compétents. Il faut, de plus, signaler un important mouvement en faveur de la médiatisation des atteintes à la sécurité des données, notamment aux États-Unis où un nombre croissant d'États se dotent de lois contraignant les organisations à révéler les pertes de données personnelles dont elles sont victimes. C'est l'État de Californie qui a initié cette tendance en adoptant le *California Database Breach Act*[114], qui oblige les organismes qui détiennent des renseignements personnels à informer les personnes dont la confidentialité des données personnelles a été compromise chaque fois que la sécurité de leur système informatique est atteinte.

1.2.2.2. Quelques techniques de limitation de l'obligation de sécurité

Malgré le laxisme et les insuffisances évoqués ci-dessus, un nombre croissant d'entreprises ont bien compris les enjeux liés à la sécurité des données et mis en place des mesures de protection parfois très coûteuses. Certaines organisations ont recours à la technique de l'impartition ou de l'infogérance qui leur permet, par contrat, « d'externaliser » vers des prestataires de services informatiques tout ou partie de leurs travaux informatiques. Le principal avantage pour l'entreprise est de bénéficier, à moindre coût, d'un savoir-faire souvent éprouvé. De plus, elle peut ainsi se libérer de tous les problèmes associés à la gestion interne d'un service informatique pour mieux se concentrer sur son cœur de métier.

---

[114] CAL. CIV. CODE § 1798.82 (West 2003).

Cependant, l'entreprise ne se décharge que d'une partie de ses responsabilités. L'article 26 de la *Loi concernant le cadre juridique des technologies de l'information* précise, en effet, le partage des responsabilités entre l'entreprise et le prestataire de services comme suit :

> « Quiconque confie un document technologique à un prestataire de services pour qu'il en assure la garde est, au préalable, tenu d'informer le prestataire quant à la protection que requiert le document en ce qui a trait à la confidentialité de l'information et quant aux personnes qui sont habilitées à en prendre connaissance.
>
> Le prestataire de services est tenu, durant la période où il a la garde du document, de voir à ce que les moyens technologiques convenus soient mis en place pour en assurer la sécurité, en préserver l'intégrité et, le cas échéant, en protéger la confidentialité et en interdire l'accès à toute personne qui n'est pas habilitée à en prendre connaissance. Il doit de même assurer le respect de toute autre obligation prévue par la loi relativement à la conservation du document. »[115]

Pour bénéficier d'une limitation de responsabilité, l'entreprise devra donc choisir un prestataire offrant de sérieuses garanties sur les procédures de traitement des données mises en place, notamment en termes de sauvegarde et d'archivage des données. Elle devra également lui donner, de préférence dans le cadre d'un contrat définissant les obligations de chacun, des instructions claires quant à la protection à apporter aux documents confiés. Cependant, les risques humains ou naturels demeurent et l'obligation du prestataire est souvent une obligation de moyens, si bien qu'en l'absence de stipulation expresse, la responsabilité de ce dernier sera difficile à retenir[116]. Aussi l'entreprise serait-elle avisée de souscrire une assurance de responsabilité professionnelle qui, en cas d'impossibilité d'imputer les dommages au prestataire, la couvrira et permettra néanmoins d'indemniser les victimes[117].

---

[115] Préc., note 50, art. 26.

[116] Blandine POIDEVIN, « Quelle responsabilité lors de la diffusion de virus? », Jurisexpert.net, 20 décembre 2001, en ligne : <http://www.jurisexpert.net/quelle_responsabilit_lors_de_la_diffusio/> (site consulté le 19 août 2010).

[117] *Id.*

Par ailleurs, les entreprises peuvent recourir à des clauses exonératoires pour tenter de limiter ou d'exclure leur responsabilité. La technique habituellement utilisée consiste à inclure un avis automatique aux messages électroniques émis depuis leur réseau et qui indique, généralement, que les messages sont filtrés, afin d'en expurger les éventuels virus, ce qui peut entraîner la suppression des pièces jointes au contenu suspect. Afin de minimiser les effets pervers de ces interceptions, les utilisateurs sont parfois invités à s'assurer auprès de leurs interlocuteurs que les messages ont bien été reçus dans leur intégralité. On peut cependant se demander quelle est la valeur de ces avis[118]. De plus, ils soulèvent la question du respect de la vie privée des employés et de leurs correspondants externes, puisqu'ils mentionnent parfois que l'entreprise « se réserve le droit de contrôler le contenu de toute communication électronique ».

Section 2. La sécurité informatique : un motif de surveillance suffisant?

La *Loi sur la protection des renseignements personnels dans le secteur privé* impose à l'entreprise de mettre en œuvre « les mesures de sécurité propres à assurer » une protection adéquate des renseignements personnels en leur possession[119]. Mais la loi ne donne aucune précision sur les moyens spécifiques à adopter. Il revient donc à l'employeur de déterminer quelles sont les mesures de protection qu'il souhaite mettre en place et celles-ci peuvent inclure la cybersurveillance, lorsque l'organisation dispose d'un système informatique connecté à l'Internet. Pour justifier une telle surveillance, les entreprises avancent généralement leur qualité de propriétaire des ressources informatiques[120]. En effet, en tant que propriétaires des lieux et des outils de travail, elles sont tenues à une obligation de sécurité[121] qui s'étend aux outils informatiques. Par conséquent, le droit de surveiller les

---

[118] Voir *infra*, Partie 1, Chapitre 3, Section 2, 2.1, p. 106.

[119] Préc., note 10, art. 10.

[120] F. FÉVRIER, préc., note 21, p. 21-24.

[121] C.c.Q., art. 2087.

lieux de travail qui est reconnu à l'employeur s'étendrait aux ordinateurs, aux réseaux et même aux informations qui y circulent.

L'argument sécuritaire semble largement admis par la jurisprudence québécoise qui a ainsi reconnu que l'employeur pouvait recourir à la surveillance électronique des salariés pour protéger les lieux de travail, les équipements et même les secrets industriels[122]. Les tribunaux ont ainsi admis la mise en place d'une telle surveillance sur les lieux de travail pour prévenir ou réprimer le vol[123] ou les actes de vandalisme[124] au sein de l'entreprise. Ils ont également validé un dispositif de caméras vidéo installées, à titre préventif et alors même que l'employeur n'avait pas été victime de vols, dans une basilique où se trouvent des biens de grande valeur et où il y a une affluence constante de visiteurs[125]. La jurisprudence a également jugé que l'installation de caméras permettant le contrôle de l'accès aux lieux de travail ne constituait pas une condition de travail déraisonnable lorsque la mise en place d'un tel dispositif ne visait qu'à éviter l'espionnage industriel et à protéger les secrets industriels, ainsi que l'équipement de l'entreprise, tout en assurant la sécurité de ces lieux[126]. On peut également citer une décision de la Nouvelle-Colombie dans laquelle l'arbitre reconnaît un droit de surveillance à un employeur qui contrôlait l'usage des ordinateurs grâce à la sauvegarde régulière de leur contenu dans le système informatique de l'entreprise[127]. L'arbitre indique que, en vertu de son droit de propriété sur les ordinateurs mis à la disposition des employés, l'employeur a le droit d'exercer une telle surveillance

---

[122] Yves SAINT-ANDRÉ, « Le respect du droit à la vie privée au travail : mythe ou réalité?, dans *Développements récents en droit du travail (2004)* », Service de la formation permanente du Barreau du Québec, 2004, *Droit civil en ligne* (DCL), EYB2004DEV408, p. 7.

[123] *Société des alcools du Québec* c. *Syndicat des travailleuses et travailleurs de la Société des alcools du Québec (SCFP), section locale 3535T*, D.T.E. 2005T-229 (T.A.).

[124] *Glopak Inc.* c. *Métallurgistes unis d'Amérique, section locale 7625*, D.T.E. 2000T-998 (T.A.); *Manufacture de Lambton Ltée* c. *Syndicat des employés de Manufacture Lambton (CSD)*, D.T.E. 2003T-997 (T.A.).

[125] *Syndicat des travailleuses et des travailleurs de la Fabrique Notre-Dame (CSN)* c. *Fabrique de la paroisse Notre-Dame*, D.T.E. 2006T-56 (T.A.); *Syndicat national de l'automobile, de l'aérospatiale, du transport et des autres travailleuses et travailleurs du Canada* c. *BMW Canbec*, D.T.E. 2007T-697 (T.A.).

[126] *Poulies Maska Inc.* c. *Syndicat des employés de Poulies Maska Inc.,* D.T.E. 2001T-620 (T.A.).

[127] *International Association of Bridge, Local Union No. 97, and Structural and Ornamental Ironworkers (the "Employer")* and *Office and Technical Employees' Union, Local 15 (the "Union")*, [1997] B.C.C.A.A.A. No. 630 (Coll. Agr. Arb.) (QL/LN).

dans le cadre de l'exploitation de son système informatique. L'arbitre précise également que les employés d'une entreprise n'ont aucune expectative de vie privée relativement au contenu de leur ordinateur professionnel.

La situation est beaucoup plus complexe dans d'autres pays comme la France, par exemple, où la surveillance pour des motifs de sécurité semble se heurter à la conception particulière de la sécurité telle qu'elle découle des principes législatifs et jurisprudentiels[128]. Comme le soulignent certains auteurs, il ressort de l'analyse des dispositions du Code du travail et de la jurisprudence que la sécurité n'y est pas définie sous son acception habituelle, à savoir la « protection des biens de l'entreprise », mais est plutôt envisagée comme une protection faite au profit des salariés[129]. Ainsi, l'article L.122-34 de ce code, qui impose à l'employeur d'assurer, par voie de règlement intérieur, « l'hygiène et la sécurité sur les lieux de travail » a essentiellement pour objectif de protéger « le salarié et son intégrité »[130]. Quant à la jurisprudence, malgré un abondant contentieux relatif à la surveillance patronale, aucune décision « ne semble reconnaître ou faire référence à l'exigence de "sécurité" dans le sens de la sécurité des biens de l'entreprise »[131]. Il y a bien un arrêt de la Cour de cassation qui retient l'argument sécuritaire[132], toutefois, compte tenu du contexte bien particulier entourant cette décision, il semblerait qu'il s'agisse d'un cas d'espèce ne pouvant donner lieu à généralisation[133]. Dans cette affaire, un syndicaliste avait refusé de se prêter à la fouille des agents de sécurité imposée par la direction d'une chaîne de télévision. On était alors à une pleine période d'attentats et l'entreprise avait fait l'objet de plusieurs alertes à la bombe. La Cour de cassation a jugé que cette fouille était justifiée par ces circonstances exceptionnelles et les exigences de sécurité.

---

[128] F. FÉVRIER, préc., note 21, p. 19-23.

[129] *Id.*

[130] *Id.*

[131] *Id.*, p. 22.

[132] Soc. 3 av. 2001, *Dr. ouvrier*, 2002.204.

[133] F. FÉVRIER, préc., note 21, p. 19-23.

Cependant, une évolution semble se profiler dans le sens de la reconnaissance, par les tribunaux français, de l'argument sécuritaire comme motif légitime de la surveillance des salariés. Ainsi, un jugement du Tribunal de grande instance de Paris du 19 avril 2005[134] a jugé inadaptée et disproportionnée la mise en place d'une pointeuse biométrique utilisant la technologie des empreintes digitales pour contrôler le temps de présence des salariés dans l'entreprise. Les juges ont cependant énoncé que l'utilisation de l'empreinte digitale

> « qui met en cause le corps humain et porte atteinte aux libertés individuelles peut cependant se justifier lorsqu'elle a une finalité sécuritaire ou protectrice de l'activité exercée dans les locaux identifiés ».[135]

Ce qui n'était pas le cas en l'espèce. Toutefois, le fait que les juges aient pris le soin de faire cette précision semble valider la finalité sécuritaire du contrôle patronal.

Pour ce qui concerne plus particulièrement la sécurité des systèmes informatiques, un arrêt de la Cour d'appel de Paris du 17 décembre 2001 a estimé que

> « [l]a préoccupation de la sécurité du réseau justifiait que les administrateurs de systèmes et de réseaux fassent usage de leurs positions et des possibilités techniques dont ils disposaient pour mener les investigations et prendre les mesures que cette sécurité imposait »[136].

De son côté, la CNIL a autorisé la mise en place de dispositifs biométriques à des fins de sécurité, non seulement pour préserver l'intégrité physique des personnes[137], mais également afin de protéger les biens et les installations[138] ainsi que les informations[139]. Elle

---

[134] Trib. gr. inst. Paris, 19 av. 2005, en ligne : <http://www.legalis.net/jurisprudence-decision.php3?id_article=1433> (site consulté le 30 juillet 2010).

[135] *Id.*

[136] Paris, 17 déc. 2001, J.C.P. 2002.éd. Entr.1336, note J. Deveze et M. Vivant.

[137] COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, *Communication de la CNIL relative à la mise en œuvre de dispositifs de reconnaissance par empreinte digitale avec stockage dans une base de données*, 2007, p. 7, en ligne : <http://www.cnil.fr/fileadmin/documents/approfondir/dossier/CNI-biometrie/Communication-biometrie.pdf> (site consulté le 26 juillet 2010).

[138] *Id.,* p. 8.

[139] *Id.*

a ainsi autorisé la mise en place de dispositifs de contrôle de l'accès : aux locaux sensibles d'une banque[140]; à un service d'informations financières[141]; aux salles informatiques d'un organisme abritant des systèmes sensibles et vitaux pour son fonctionnement[142] ou à un centre chargé du traitement automatisé des infractions routières au niveau national[143]. Ces autorisations de la CNIL sont accordées selon des critères stricts et doivent, notamment, être fondées sur un fort impératif de sécurité représentant un « enjeu majeur dépassant l'intérêt strict de l'organisme »[144].

Les tribunaux québécois ont peu eu l'occasion de trancher sur l'utilisation de la biométrie au travail. Une décision prise avant l'entrée en vigueur de la *Loi concernant le cadre juridique des technologies de l'information*[145] avait conclu à la légalité d'un système de reconnaissance biométrique de la main mis en place pour contrôler les entrées et sorties des salariés[146]. Toutefois, l'adoption de cette loi semble remettre en cause cette position dans la mesure où le recours aux procédés biométriques y est encadré très strictement. En effet, l'article 44 de cette loi énonce que l'utilisation de ces technologies doit faire l'objet d'un consentement exprès de la personne concernée et que les données ainsi recueillies doivent

---

[140] COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, *Délibération 2005-023. Délibération portant autorisation de la mise en œuvre par la Banque de France d'un traitement automatisé de données à caractère personnel ayant pour finalité de contrôler l'accès aux locaux sensibles*, 17 février 2005, en ligne : <http://www.legifrance.gouv.fr> (site consulté le 26 juillet 2010).

[141] COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, *Délibération 2005-206. Délibération portant autorisation de mise en œuvre d'un traitement automatisé de données à caractère personnel reposant sur la reconnaissance de l'empreinte digitale et ayant pour finalité de contrôler l'accès logique à un service d'informations financières de la société Bloomberg L.P.*, 22 septembre 2005, en ligne : <http://www.legifrance.gouv.fr> (site consulté le 26 juillet 2010).

[142] COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, *Délibération 2005-281. Délibération portant autorisation de la mise en œuvre par la Cité des Sciences et de l'Industrie d'un traitement automatisé de données à caractère personnel reposant sur l'utilisation d'un dispositif biométrique de reconnaissance de l'empreinte digitale et ayant pour finalité le contrôle de l'accès aux locaux*, 22 novembre 2005, en ligne : <http://www.legifrance.gouv.fr> (site consulté le 26 juillet 2010).

[143] COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, *Délibération 2006-132. Délibération portant autorisation de la mise en œuvre par la société Atos Worldline d'un traitement automatisé de données à caractère personnel reposant sur la reconnaissance des empreintes digitales et ayant pour finalité le contrôle de l'accès aux locaux*, 09 mai 2006, en ligne : <http://www.legifrance.gouv.fr> (site consulté le 26 juillet 2010).

[144] COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, *Communication de la CNIL relative à la mise en œuvre de dispositifs de reconnaissance par empreinte digitale avec stockage dans une base de données*, préc., note 137, p. 7.

[145] Préc., note 50.

[146] *Syndicat des travailleurs de Mométal (C.S.N.)* c. *Mométal Inc.*, [2001] R.J.D.T. 1967 (T.A.).

être détruites dès que l'objectif qui fonde leur usage est réalisé. En outre, l'article 45 de la même loi impose à toute entreprise désirant recourir à un tel système l'obligation d'informer au préalable la Commission d'accès à l'information. Cette Commission dispose, à cet égard, de pouvoirs étendus, dont celui d'interdire ou suspendre l'utilisation de toute banque de données créée dans ce cadre ou d'en ordonner la destruction en cas d'atteinte au respect de la vie privée[147]. Par conséquent, l'entreprise qui souhaite utiliser des procédés biométriques devrait faire preuve d'une extrême prudence. Et cela d'autant plus que la portée réelle de ces articles 44 et 45 précités reste incertaine, comme le relève la Commission de l'éthique de la science et de la technologie :

> « Ces deux dispositions sont inscrites au chapitre de la loi qui détermine les règles pour établir un lien entre une personne et un document technologique. Les règles pour la collecte des données biométriques peuvent-elles s'appliquer pour d'autres fins, par exemple pour assurer le contrôle des accès à des locaux ou autres sites physiques ou virtuels? »[148]

Pour conclure sur la finalité sécuritaire du contrôle patronal en France, elle tend à s'imposer progressivement comme un motif légitime de surveillance des salariés. Néanmoins, il faudra sans doute attendre que la Cour de cassation se prononce plus clairement sur la question pour que la sécurité informationnelle devienne un fondement autonome. En attendant, il doit être rapproché d'autres notions jurisprudentielles connues, telles que « l'intérêt de l'entreprise » ou encore le « bon fonctionnement de l'entreprise »[149]. En effet, le fondement sécuritaire « semble à lui seul incapable de justifier un contrôle des salariés, c'est-à-dire un contrôle des personnes »[150]. La doctrine de la CNIL n'exige-t-elle pas un impératif de sécurité supérieur dont les enjeux surclasseraient « l'intérêt strict de

---

[147] *Loi concernant le cadre juridique des technologies de l'information*, préc., note 50, art. 45 al. 2.

[148] COMMISSION DE L'ÉTHIQUE DE LA SCIENCE ET DE LA TECHNOLOGIE, *L'utilisation des données biométriques à des fins de sécurité : questionnement sur les enjeux éthiques. Document de réflexion*, Québec, Conseil de la science et de la technologie, 2005, p. 37, en ligne : <http://www.cst.gouv.qc.ca/IMG/pdf/Biometrie-reflexion.pdf> (site consulté le 25 juillet 2010).

[149] F. FÉVRIER, préc., note 21, p. 22-23.

[150] *Id.*, p. 15.

l'organisme »[151]? En réalité, à l'heure actuelle, pour la majorité des auteurs, « l'intérêt légitime de l'employeur pour surveiller l'usage de l'Internet par ses employés repose sur l'existence des abus »[152] liés à l'usage des outils informatiques. En d'autres termes, la légitimité de la surveillance de l'employeur reposerait sur des fins disciplinaires. C'est ce fondement plus « classique », et beaucoup mieux accepté, que nous allons examiner à présent.

Chapitre 2. La répression des abus

Internet est devenu un moyen de communication quasiment incontournable au sein des entreprises. Cependant, si l'employeur a l'obligation de fournir le matériel professionnel à ses employés, rien ne l'oblige à leur fournir un accès à l'Internet, ni même un ordinateur, si ces outils ne sont pas indispensables à l'accomplissement de leurs tâches. De fait, de nombreuses entreprises considèrent qu'il s'agit là d'un privilège réservé à certains salariés (ceux qui en ont l'utilité dans le cadre de leur travail) ou n'autorisent qu'une connexion restreinte à certains sites professionnels. En prenant ainsi clairement position, l'employeur peut réduire, sinon éliminer, les problèmes liés à navigation improductive. Les outils de communication numériques exercent, en effet, un attrait indéniable pour les employés : ils offrent un service bien plus simple et rapide que le courrier ordinaire. De plus, ils peuvent être utilisés de façon très discrète, contrairement au téléphone ou au fax, par exemple. La gratuité joue également un rôle qui ne semble toutefois pas déterminant : la plupart des foyers disposent d'un ordinateur et il possible aujourd'hui d'avoir Internet à la maison pour une somme modique. Cependant, les possibilités d'utilisation ne sont pas les mêmes qu'au bureau : les entreprises disposent, en effet, d'une bande passante plus large qui permet des connexions Internet plus rapides, si bien que les utilisateurs obtiennent les informations

---

[151] COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, *Communication de la CNIL relative à la mise en œuvre de dispositifs de reconnaissance par empreinte digitale avec stockage dans une base de données*, préc., note 137, p. 7.

[152] Yves AKDENIZ et John BELL, « La vie privée et l'Internet : perspectives du Royaume Uni », dans Pierre TABATONI, *La protection de la vie privée dans la société d'information*, t. 3, coll. « Cahiers Académie des Sciences morales et politiques », Paris, Les Presses Universitaires de France, 2002, p. 152, à la page 158.

désirées beaucoup plus rapidement que chez eux. Par ailleurs, la navigation au bureau offre la liberté – ou plutôt l'opportunité – d'aller sur ses sites préférés, sans que cela n'empiète sur les activités familiales ou les loisirs. On peut ainsi, organiser ses vacances, faire ses courses en ligne ou même se livrer à des activités moins avouables comme la consultation de sites pornographiques. Il n'est, en effet, pas toujours loisible de s'isoler à la maison pour surfer tranquillement sur des sites « adultes » ou – pire – télécharger et stocker de tels contenus sur l'ordinateur familial! Alors, on le fait sur le lieu de travail. Selon des statistiques récentes citées par la société *GFI*, 70 % des visites sur les sites pornographiques ont ainsi lieu pendant les heures de bureau[153].

Pour toutes les raisons qui viennent d'être évoquées, la navigation à des fins privées sur le lieu de travail constitue une activité relativement courante. Ces visites sont majoritairement dédiées au courrier électronique, aux sites de loisirs et de réseautage social. Ainsi, selon une étude de l'*American Management Association* et *The ePolicy Institute*, 61 % des activités en ligne seraient consacrées aux jeux, 50 % aux réseaux sociaux (*Facebook*, *MySpace*, *Twitter*, etc.) et 40 % au divertissement[154]. La dépendance aux jeux électroniques peut devenir si prenante qu'elle conduit parfois les employés à commettre des actes d'insubordination caractérisés. Ainsi, dans l'affaire *Alliance de la fonction publique du Canada* et *Musée des beaux-arts du Canada*[155], un salarié a été suspendu pour une période de deux mois pour s'être, notamment, livré à des jeux électroniques pendant son temps de travail et pour les avoir réinstallés sur son ordinateur chaque fois que l'employeur les en supprimait. Il faut préciser que l'employé utilisait en outre son ordinateur pour « clavarder » et visionner des sites pornographiques. La part des activités inappropriées reliées au sexe est colossale : 96 % des contenus bloqués par le système de filtrage des entreprises seraient à caractère sexuel, romantique ou pornographique[156]. Pour certains

---

[153] GFI, *White Paper. The Importance of an Acceptable Use Policy*, 2010, p. 2, en ligne: <http://www.gfi.com/whitepapers/acceptable_use_policy.pdf> (site consulté le 28 juillet 2010).

[154] AMERICAN MANAGEMENT ASSOCIATION, THE EPOLICY INSTITUTE, préc., note 27.

[155] D.T.E. 2003T-89 (T.A.).

[156] AMERICAN MANAGEMENT ASSOCIATION, THE EPOLICY INSTITUTE, préc., note 27.

salariés, la visite de sites pornographiques fait même partie de la routine quotidienne : un employeur a ainsi congédié un salarié en raison, entre autres, d'une utilisation inadéquate de l'équipement informatique consistant, notamment, à télécharger, tous les jours, sur le disque dur de son poste de travail un nombre considérable de photographies à caractère sexuel ou pornographique[157].

Or, pour les employeurs, l'utilisation de leurs ressources par les salariés doit se faire dans le respect de leurs obligations contractuelles. Du contrat de travail découlent, en effet, deux principes essentiels : l'obligation de loyauté et de fidélité et l'obligation de discrétion. Ces principes encadrent la bonne exécution de la prestation de travail que le salarié s'est engagé à fournir et leur non-respect peut donner lieu à des sanctions disciplinaires. Ces obligations sont prévues par l'article 2085 C.c.Q., qui définit le lien de subordination, et l'article 2088 C.c.Q., relatif à la loyauté et à la discrétion. Ces obligations s'appliquent lorsque le salarié utilise les ressources informatiques mises à sa disposition. Par conséquent, il est tenu d'utiliser ces outils avec prudence et diligence (Section 1) et doit, dans le cadre de son obligation de loyauté et de discrétion, agir dans l'intérêt de l'entreprise (Section 2).

Section 1. L'obligation d'exécuter le travail avec prudence et diligence

L'obligation principale du salarié est de fournir le travail (1.2.) en contrepartie de la rémunération versée par l'employeur. Et il doit accomplir ses tâches conformément aux instructions de l'employeur (1.1.), en veillant notamment à préserver la sécurité des biens et équipements professionnels (1.3.) et les droits des tiers.

1.1. Le devoir d'obéissance

Le contrat de travail est caractérisé par le lien de subordination entre l'employeur et le salarié, tel qu'il ressort de l'article 2085 C.c.Q. rédigé comme suit :

---

[157] *Perreault* c. *Syndicat des employés de soutien de l'Université de Sherbrooke*, 2004 CanLII 14513 (QC T.T.).

> « 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. »

Il en découle que l'employeur a un pouvoir de direction qui l'autorise à donner des instructions auxquelles le salarié doit se conformer dans le cadre de l'exécution de son contrat de travail[158]. Le devoir d'obéissance du salarié implique une obligation de faire et de ne pas faire. Pour ce qui concerne les ressources informatiques, les instructions patronales sont souvent consignées dans une politique et peuvent, notamment, imposer aux employés de n'utiliser les outils informatiques mis à leur disposition qu'aux fins du travail, et ce, tant pendant les heures régulières de travail qu'en dehors de celles-ci.

En premier lieu, l'obligation du salarié consistera tout simplement à se servir des ressources mises à sa disposition aux fins et conditions prévues. Le conseil de la ville de Malartic a ainsi destitué un haut cadre, notamment, parce qu'il n'utilisait jamais son ordinateur, pourtant mis à sa disposition afin de faciliter les communications avec ses collèges dont les bureaux étaient situés dans d'autres bâtiments, aux fins de son travail[159]. Il ne répondait pas aux messages qu'on lui adressait, prétextant, entre autres, ne pas savoir comment accéder au courrier électronique provenant des autres services de la ville. Ce qui était pour le moins étrange, puisqu'il possédait un ordinateur personnel chez lui et qu'il passait, en outre, un temps considérable à naviguer à des fins personnelles sur Internet au bureau.

Le devoir d'obéissance implique également que l'employé doit s'interdire toute utilisation non autorisée du système informatique. C'est ce qui ressort de l'affaire *Frezza* et *Réseau CP Rail*[160], dans laquelle un employé avait été congédié pour avoir utilisé, sans autorisation, le système informatique de l'employeur en accédant illégalement à la

---

[158] Robert P. GAGNON, « Le contrat de travail », dans *Droit du travail*, Collection de droit 2006-2007, vol. 8, École du Barreau du Québec, 2006, *Droit civil en ligne* (DCL), EYB2006CDD196, p. 9.

[159] *Potvin* c. *Ville de Malartic*, REJB 2003-46527 (C.S.); *Syndicat canadien des communications, de l'énergie et du papier, section locale 522* c. *CAE Électronique Ltée*, REJB 2000-16857 (T.A.).

[160] [1997] D.A.T.C. no 389 (C.L.A.) (QL/LN).

messagerie électronique de ses supérieurs. Pourtant, un message d'avertissement apparaissait à l'écran chaque fois qu'un utilisateur entrait dans le système, avisant ce dernier qu'un usage non autorisé du système l'exposait à des actions légales, incluant des poursuites en vertu du *Code criminel*. L'arbitre a considéré que la diffusion de ce message impliquait que chaque employé savait qu'un usage non autorisé du système était interdit. Et cela d'autant plus que les employés avaient déjà été formellement informés des conséquences d'une utilisation non autorisée. Dans *Sirois* c. *Sodema*[161], jugée plus récemment, la Commission des relations du travail rend une décision identique. Il s'agissait également d'une utilisation non autorisée du système informatique et l'employeur avait informé chaque salarié que l'accès au système informatique était limité et leur avait fait signer un engagement indiquant qu'ils encouraient le congédiement en cas de non-respect de cette clause. La Commission précise notamment que :

> « les règles étaient claires et sérieuses pour l'employeur, au point d'y prévoir une sanction en cas de défaut soit le congédiement immédiat »[162].

Elle avait donc maintenu le congédiement, rejetant par la même occasion l'argument du salarié selon lequel ses agissements n'avaient causé aucun dommage ou préjudice à l'employeur, puisqu'il n'avait fait que consulter des fichiers interdits, sans les altérer ou sans s'en servir à des fins personnelles.

Bien entendu, le devoir d'obéissance implique que le salarié ne peut, même pour « la bonne cause », s'introduire, sans autorisation de sa hiérarchie, dans des parties du système informatique auxquelles il ne pourrait accéder avec son propre mot de passe, et ce, juste pour prouver les insuffisances du système de sécurité de l'entreprise qui l'emploie[163].

Cependant, de nombreux employeurs ne donnent aucune directive relativement à l'usage des outils de communication électronique et s'en remettent au bon jugement de leurs

---

[161] 2005 QCCRT 91 (CanLII).

[162] *Id.*

[163] V. SÉDALLIAN, préc., note 40, p. 11; Soc. 1er oct. 2002, *Gaz. Pal.* 2003.33, note Tessalonikos.

employés. Le problème c'est que les employés n'ont pas toujours le bon sens escompté ou la force de résister à la tentation d'une petite visite sur Internet pour se détendre. Or, la notion de temps s'estompe vite une fois que l'on est sur Internet et le « petit surf d'un quart d'heure » initialement prévu peut rapidement durer une heure ou deux. Surtout lorsque le salarié, depuis son poste de travail, se croit à l'abri de toute surveillance ou s'imagine que ses actes, parce qu'ils sont accomplis à partir d'un ordinateur de l'entreprise, lui assurent l'anonymat et le mettent à l'abri des poursuites des tiers (par exemple pour téléchargement illégal de pièces musicales).

Aussi les entreprises ont-elles intérêt à adopter des directives de conduite claires et érigées en règlement. Elles pourront ainsi plus facilement les communiquer à leurs employés et éventuellement s'en servir pour prouver qu'un employé a contrevenu aux instructions patronales et mérite donc la sanction disciplinaire infligée. Il découle, en effet, de l'affaire *Commission des normes du travail* c. *Bourse de Montréal* que l'absence d'une politique sur l'utilisation d'Internet et du matériel électronique de l'entreprise peut conduire à la modification, voire à l'annulation d'une sanction disciplinaire[164].

Dans cette affaire, un analyste informatique employé par la Bourse de Montréal avait été congédié sans préavis pour avoir utilisé les outils informatiques à des fins non autorisées. L'employeur lui reprochait tout d'abord d'avoir conservé un fichier infecté d'un virus afin de l'examiner davantage, et ce, malgré l'ordre donné à tous les employés de le supprimer. Cependant, l'employé s'est immédiatement exécuté lorsqu'on lui avait à nouveau fait la demande et aucun dommage consécutif à ce délai de quelques jours n'avait été constaté. Le deuxième grief concernait l'utilisation de son ordinateur, ainsi que d'autres postes de travail, pour effectuer des travaux au profit d'une entreprise de décodage de signaux provenant de l'espace. Toutefois, l'employé avait indiqué qu'il n'utilisait les ordinateurs que lorsqu'il n'y avait pas d'autres tâches à accomplir et il n'y avait eu aucun dommage spécifique attribué à son activité. En dernier lieu, l'employeur reprochait au salarié d'avoir

---

[164] REJB 2002-31243 (C.Q.).

effectué une opération sur un site de piraterie informatique. Ce site fournissait des outils pour repérer le mot de passe permettant à un utilisateur d'accéder à un ordinateur. L'employé avait admis avoir visité ce site et utilisé l'un des outils proposés pour vérifier si son propre mot de passe pouvait être découvert. L'expérience avait été concluante. Cependant, l'employé ne l'avait pas renouvelée sur d'autres ordinateurs, car pour être fonctionnel, cet outil devait être utilisé à partir du poste de travail de l'utilisateur dont le mot de passe était recherché. Aucune des vérifications faites n'avait permis de révéler que l'employé avait utilisé cet outil pour tenter de fouiller dans les comptes des administrateurs ou de découvrir les mots de passe de ses collègues ou même de dirigeants de la Bourse. Après une analyse des politiques de l'entreprise, la Cour du Québec a jugé que les règles fixées par l'employeur concernant l'utilisation des ordinateurs étaient imprécises et ambiguës. En effet, la seule directive se rapportant à l'utilisation du matériel informatique reçue par l'employé visait uniquement le courrier électronique et ne traitait pas de l'usage des autres outils informatiques. Puisque la politique manquait de clarté et n'était pas assez large pour couvrir les fautes du salarié, la Cour a conclu que l'employeur n'avait pas établi que l'employé avait commis une faute grave. L'employeur a donc été condamné à verser au demandeur la somme correspondant au préavis de cessation de travail réclamée par ce dernier.

D'autres décisions sont venues confirmer cette jurisprudence. On peut notamment mentionner l'affaire *Alliance de la fonction publique du Canada* et *Musée des beaux-arts du Canada*[165] dans laquelle l'arbitre a conclu qu'un employeur est fondé à prendre des mesures disciplinaires lorsqu'un employé utilise son ordinateur professionnel en violation d'une politique claire de l'entreprise ou qu'une telle utilisation entraîne une diminution considérable de la productivité. Et cela était d'autant plus justifié en l'espèce que l'employé avait persisté dans sa conduite inconvenante, malgré les diverses mesures disciplinaires prises à son encontre.

---

[165] Préc., note 155.

1.2. Le rendement

Il découle du contrat de travail que le salarié est tenu d'exécuter la prestation de travail pour laquelle il est rémunéré[166] avec diligence[167]. L'obligation de diligence est une notion suffisamment large qui peut

> « référer tant à la quantité qu'à la qualité de travail que le salarié devrait normalement fournir et à laquelle l'employeur est légitimement en droit de s'attendre, compte tenu de la nature du travail ou des termes du contrat »[168].

Cela implique, entre autres, que le salarié doit consacrer son temps de travail à l'activité de l'entreprise qui l'emploie. Or, le temps qu'il consacre au « surf » à des fins personnelles ou à l'échange de courriels privés durant les heures de travail est du temps qu'il « vole » à son employeur, puisque ce dernier lui versera une rémunération pour du temps passé à autre chose que l'accomplissement de son travail. Pour les employeurs, de tels agissements constituent autant de motifs de sanctions. À cet égard, on note une recrudescence du nombre de congédiements reliés à un usage inapproprié des NTIC. Ainsi, selon une enquête réalisée en 2007 par l'*American Management Association* et *The ePolicy Institute*, 30 % des employeurs avaient congédié des salariés pour non-respect des politiques d'utilisation de l'Internet, et 28 % l'avaient fait à la suite d'un usage inapproprié de la messagerie électronique[169]. L'analyse de la répartition des motifs de congédiement montre, notamment, le souci des employeurs de bannir les contenus inappropriés circulant dans leur système informatique et de faire respecter leur règlement intérieur : 84 % des salariés congédiés consécutivement à un usage abusif de l'Internet l'avaient été en raison de leur implication dans la diffusion de contenus inappropriés ou offensants, 48 % pour non-respect des politiques de l'entreprise et 34 % à la suite d'un usage personnel excessif[170]. Les

---

[166] C.c.Q., art. 2085.

[167] *Id.*, art. 2088.

[168] Robert P. GAGNON, « Le contrat de travail », préc., note 158, p. 9.

[169] AMERICAN MANAGEMENT ASSOCIATION, THE EPOLICY INSTITUTE, préc., note 27.

[170] *Id.*

statistiques sont, dans une moindre mesure néanmoins, les mêmes pour ce qui concerne l'usage du courrier électronique[171].

Ces manquements font parfois l'objet de dénonciations très médiatisées. La ville de Québec a ainsi défrayé la chronique, notamment en novembre 2007, lorsqu'elle a épinglé 29 salariés, dont 14 policiers, pour usage inapproprié de l'Internet et de la messagerie électronique pendant leurs heures de travail. On leur reprochait notamment d'avoir utilisé l'Internet de façon excessive et d'avoir consulté ou échangé des contenus à caractère pornographique. Aucun congédiement n'a cependant été prononcé, les mesures disciplinaires allant de la simple lettre de réprimande versée au dossier à une suspension sans solde d'un an[172]. La ville de Beloeil a également attiré l'attention médiatique lorsqu'elle a congédié un technicien aux travaux de voirie qui consacrait jusqu'à trois heures par jour de son temps de travail à la navigation sur Internet à des fins personnelles[173]. Il avait ainsi visité 10 105 sites sur une période de deux ans. La preuve a démontré que 99 % de cette activité n'avait aucun lien le travail de l'employé, puisqu'elle était consacrée à la visite de sites de « clavardage », de rencontres, d'informations et d'achats en ligne.

Avec le développement des NTIC, les cas de « vol de temps » ont décuplé, car ces outils offrent une utilisation discrète. En effet, à moins de regarder par-dessus l'épaule des salariés assis devant un ordinateur ou de disposer d'un dispositif de traçage, rien ne permet souvent de distinguer celui qui se livre à des activités récréatives de celui qui vaque à ses tâches régulières. Pour les employeurs, le temps que l'employé consacre à des activités personnelles au bureau est du temps qui leur est dû. Et en l'occupant à autre chose qu'à son travail, l'employé ne fournit pas sa prestation de travail ou ne la fournit pas pleinement. Par

---

[171] *Id.*

[172] LCN CANOE, « Internet au travail. Une autre enquête à la Ville de Québec », 20 avril 2010, Lcn.canoe.ca, en ligne : <http://lcn.canoe.ca/lcn/infos/regional/archives/2010/04/20100402-170342.html> (site consulté le 18 août 2010).

[173] *Syndicat des employés municipaux de Beloeil (SCFP)* et *Beloeil (Ville de)*, D.T.E. 2007T-874 (T.A.).

conséquent, il ne remplit pas ses obligations et la baisse de rendement découlant de ses activités non professionnelles constitue un juste motif de sanction contre lui.

Le problème avec le concept de « vol de temps », c'est que la preuve de la faute de l'employé et du préjudice de l'employeur est parfois difficile à rapporter. De plus, les sanctions finalement retenues contre les fautifs ne sont pas toujours à la hauteur des attentes des employeurs. Ainsi que l'a si bien relevé l'arbitre dans l'affaire *Fiset* c. *Service d'administration P.C.R. Ltée* : « On a parlé de vol de temps. Mais où commence le vol, s'il y a vol? »[174]. En effet, le fait que l'employé consacre de longues heures à la navigation sur Internet ou à l'échange de courriels n'implique pas automatiquement une baisse de sa productivité, ni même une faute de sa part. En premier lieu, il est tout à fait possible que cette activité soit réalisée au profit de l'entreprise. Les entreprises reconnaissent elles-mêmes que le courrier électronique est devenu un moyen incontournable pour traiter les affaires, tant au sein de l'organisation qu'avec les contacts d'affaires[175]. De plus, il arrive bien souvent que l'usage à des fins privées des outils électroniques soit effectué pendant le temps de pause du salarié ou pour de brèves périodes de temps, par exemple pour rechercher une information (sur un horaire, un itinéraire, etc.) ou donner des nouvelles, si bien que l'impact sur le temps de travail demeure négligeable.

Dans *Fiset* c. *Service d'administration P.C.R. Ltée*[176], l'employeur avait congédié un salarié après avoir découvert que ce dernier entretenait une liaison qui donnait lieu à une correspondance abondante et régulière échangée par Internet, à partir de son poste de travail. Des vérifications de son profil d'utilisateur démontraient qu'il utilisait l'Internet à des fins personnelles sur une base quotidienne, à raison d'environ 30 messages par jour. Pour contester son congédiement, l'employé avait fait valoir qu'il ignorait que le règlement d'entreprise interdisait l'utilisation de l'Internet à des fins personnelles puisque d'autres

---

[174] D.T.E. 2003T-41 (C.R.T.), par. 31, conf. par *Services d'administration P.C.R. Ltée* c. *Daigle*, D.T.E. 2003T-177 (C.S.).

[175] CEFRIO et SOM RECHERCHES ET SONDAGES, *NetQuébec 2008. Portrait de l'utilisation des TI et d'Internet au Québec*, préc., note 37, p. 2.

[176] *Fiset* c. *Service d'administration P.C.R. Ltée*, préc., note 174.

salariés, y compris le directeur, en faisaient régulièrement usage au bureau. L'arbitre a accueilli son argumentation essentiellement pour trois motifs.

En premier lieu, l'employeur n'avait pas pu établir la faute du salarié, l'entreprise n'ayant jamais émis aucune directive générale sur l'utilisation de l'Internet à des fins personnelles. De plus, aucun avis spécifique n'avait été fait au salarié en ce sens. Par conséquent, on pouvait difficilement lui reprocher d'enfreindre un règlement qui n'existait pas ou n'était connu de personne au sein de l'entreprise. En effet, pour que le comportement d'un employé soit considéré comme de l'insubordination, il faut que ce dernier ait contrevenu à un ordre légitime transmis de façon claire et non ambiguë[177]. De plus, même si l'utilisation d'Internet à des fins personnelles a été établie (l'historique des navigations du salarié était clair à ce sujet, et ce, dernier avait fini par reconnaître les faits), on pouvait difficilement le réprimander pour une activité pratiquée par d'autres salariés, y compris le directeur qui, à l'occasion, partageait ses trouvailles avec les employés ou les invitait à venir voir sur son poste certains des messages qu'il avait reçus. L'employeur avait d'ailleurs admis que l'utilisation à des fins personnelles était acceptée ou tolérée dans une certaine mesure. Cependant, aucune directive ne venait préciser ce qui était tolérable pour l'entreprise et ce qui ne l'était pas. Par conséquent, en l'absence d'indication permettant aux employés de connaître les limites à ne pas dépasser, l'employeur ne pouvait pas décider de sanctionner un employé sans risquer de tomber dans le domaine du pur arbitraire.

En deuxième lieu, l'employeur n'a pas davantage réussi à prouver son préjudice, comme le résument les propos de l'arbitre :

> « [40] En principe, un salarié n'est pas recruté pour faire du temps mais pour fournir une prestation de travail dont la durée est l'un des éléments de mesure.

---

[177] Nathalie-Anne BÉLIVEAU, Karina BOUTIN et Nicolas ST-PIERRE, « Les "motifs sérieux" et la "cause juste et suffisante" de congédiement », dans *Un abécédaire des cessations d'emploi et des indemnités de départ (2005)*, Service de la formation permanente du Barreau du Québec, 2005, *Droit civil en ligne* (DCL), EYB2005DEV866, p. 10.

> [41] Dans un contexte comme celui des conditions de travail du plaignant chez l'intimé, l'essentiel c'est que la prestation de travail à laquelle le salarié s'est engagé et pour laquelle il reçoit sa rémunération, soit fournie adéquatement et que l'employeur ne subisse pas de préjudice du comportement du salarié.
>
> [42] Dans le cas sous étude, il n'a en rien été démontré que le plaignant a fait défaut de fournir sa prestation de travail ou que l'employeur ait subi un préjudice du fait de ses communications. »[178]

Force est de constater que, si l'obligation du salarié tend parfois, selon les circonstances et les postes, à se rapprocher d'une obligation de résultat, elle demeure en général une obligation « de moyens dont l'intensité varie selon la nature du travail à fournir »[179]. Ainsi, il suffit qu'un employé jouisse d'une certaine autonomie et d'une souplesse dans l'organisation de son emploi du temps ou que sa rémunération ne soit pas fonction du nombre d'heures de travail pour que le « temps », pris comme unité de mesure de la prestation de travail due par le salarié, perde toute pertinence. En l'espèce, le salarié travaillait régulièrement de 50 à 55 heures alors que sa durée hebdomadaire était d'environ 45 heures. Ses heures n'étaient pas réellement contrôlées et son salaire n'était pas calculé directement en fonction de ses heures de travail. Par ailleurs, en raison de ses responsabilités, il arrivait parfois qu'on l'appelle chez lui, en dehors de ses heures habituelles de travail, et il était quelques fois contraint de revenir au travail pour régler la situation. Si bien que l'on pouvait difficilement établir la « soustraction de temps ». En définitive, l'évaluation de la qualité et la quantité de la prestation de travail devraient être fonction, notamment, de la nature du travail, du degré d'autonomie et de spécialisation de l'employé. Et le contrôle et la surveillance qui en découlent devraient être modulés ou effectués selon des procédures différentes suivant qu'il s'agit, par exemple, d'un cadre

---

[178] *Fiset* c. *Service d'administration P.C.R. Ltée*, préc., note 174, par. 40, 41 et 42.

[179] R. P. GAGNON, « Le contrat de travail », préc., note 158, p. 9.

bénéficiant d'une large liberté d'action ou d'un employé exerçant un métier peu spécialisé[180].

Quant à la sanction enfin, elle a été jugée disproportionnée parce que l'employeur n'avait pas respecté le principe de progressivité des sanctions en vertu duquel il aurait dû commencer par donner au salarié les avis nécessaires concernant son utilisation de l'Internet. Les réprimandes faites antérieurement au salarié ne pouvaient, en effet, pas être prises en compte, puisque celles-ci concernaient une situation différente, en l'occurrence son usage abusif des appels interurbains. Par conséquent, l'arbitre a conclu qu'un avertissement était la « mesure ultime à laquelle son agir a[vait] pu l'exposer »[181]. Le congédiement a donc été annulé pour absence de cause juste et suffisante.

L'affaire *Fiset*[182] est intéressante à plus d'un titre. Outre qu'elle apporte des précisions sur la notion de « vol de temps », elle met en lumière les difficultés liées à la question de la preuve – celle de la faute du salarié et celle du préjudice de l'employeur – en cas d'utilisation inappropriée des outils de communication électroniques. Elle confirme également la nécessité d'une gradation des sanctions disciplinaires. Et surtout, elle réaffirme l'utilité d'un règlement indiquant clairement les attentes des employeurs en matière d'utilisation des outils électroniques. Le doute profite, en effet, à l'employé. D'où l'intérêt pour l'employeur d'avoir un outil pour balayer – ou en tout cas minimiser – ce risque. Ainsi, dans l'affaire *Syndicat canadien des communications, de l'énergie et du papier, section locale 522* c. *CAE Électronique Ltée*[183], l'employeur a pu invoquer avec succès un « usage de l'internet incompatible avec les règles de l'entreprise » pour congédier un employé qui avait passé 329 heures, sur une période de cinq mois, à naviguer sur Internet, alors même qu'il déclarait un peu plus de 466 heures supplémentaires sur la même période! Ce qui a permis à l'arbitre de conclure qu'il y avait forcément un lien entre la

---

[180] Sophie ROMPRÉ, *La surveillance de l'utilisation d'Internet au travail*, Montréal, Éditions Yvon Blais, 2009, p. 53-54.

[181] *Fiset* c. *Service d'administration P.C.R. Ltée*, préc., note 174.

[182] *Id.*

[183] Préc., note 159.

somme de travail que le salarié ne pouvait accomplir, en raison de ses navigations sur l'Internet, et qui était, soit reportée, soit accomplie en heures supplémentaires.

De plus, l'examen de la liste des sites visités révélait que la majorité d'entre eux avaient des contenus pornographiques. Or, l'employeur avait une politique très stricte interdisant la détention ou la diffusion de tout matériel à caractère sexuel ou pornographique. Le salarié avait tenté de minimiser l'importance de son utilisation de l'Internet, prétendant que quelqu'un d'autre avait sans doute utilisé son mot de passe pour y accéder et que, de toute façon, très souvent son ordinateur était connecté à l'Internet sans pour autant qu'il regarde le contenu affiché à l'écran. Cependant, les heures de connexion correspondaient au temps de présence du salarié au sein de l'entreprise. Par ailleurs, sur le plan technique, le relais Internet était automatiquement interrompu s'il s'écoulait plus de quinze minutes sans qu'aucune activité ne soit relevée sur le site visité, si bien que le temps d'activités des rapports produits était exprimé en temps réel.

Dans cette affaire, le vol de temps était aggravé par le fait que le salarié était un cadre autonome et qu'il avait agi en violation des politiques et des règles en vigueur au sein de l'entreprise[184]. Par ailleurs, l'usage de l'Internet était réservé à certains salariés qui s'étaient engagés à respecter certaines règles, notamment, une utilisation restreinte à des fins de travail et durant les heures de travail[185].

1.3. La sécurité des biens et équipements professionnels

La prudence requise par l'article 2088 C.c.Q., oblige le salarié à exécuter son travail de façon sécuritaire pour lui-même, pour ses collègues de travail et même pour les tiers[186]. La forme et l'intensité de cette obligation dépendent essentiellement de la nature du travail et des circonstances dans lesquelles il est exécuté[187]. Pour ce qui concerne l'utilisation des

---

[184] Voir *infra*, Partie 2, Chapitre 2, Section 1, 1.1.3, p. 167.

[185] *Id.*

[186] R. P. GAGNON, « Le contrat de travail », préc., note 158, p. 13.

[187] *Id.*

outils informatiques, l'employé doit prendre soin de ses outils de travail, afin de les protéger des dangers pouvant tant les atteindre physiquement qu'affecter leur contenu. Quant à la sécurité des collègues de travail et des tiers, il s'agira moins de leur sécurité physique que des atteintes morales dont ils peuvent faire l'objet (intimidation, harcèlement, diffamation, atteinte à la vie privée, etc.) et qui feront l'objet de développements ultérieurs, dans les paragraphes consacrés au devoir de loyauté et aux risques de responsabilité de l'employeur.

Pour ce qui est de la sécurité des biens professionnels proprement dite, elle repose essentiellement sur l'obligation de prudence et de diligence et implique un respect des règles élémentaires de sécurité. Il n'est pas nécessaire qu'un employé qui ne travaille pas sur Internet reste connecté, juste parce qu'il pense en avoir l'usage à un moment ou un autre : un tel comportement pourrait faciliter l'intrusion de personnes externes et leur permettre de détourner des fichiers confidentiels ou introduire des virus et autres programmes nocifs pouvant causer de sérieux dégâts dans le système informatique.

Une autre mesure de précaution peut consister à ne pas se servir de sa boîte électronique à des fins de stockage des documents. De nombreux utilisateurs conservent, en effet, leurs courriers électroniques tels quels et ne pensent pas à sauvegarder les documents professionnels attachés dans des fichiers spécialement créés à cet effet sur leur ordinateur ou sur le serveur commun. Outre le fait que les informations ainsi stockées ne sont pas disponibles pour les collègues qui pourraient en avoir l'utilité dans le cadre de leur travail, celles-ci ne sont pas à l'abri d'une suppression accidentelle et sont encore plus vulnérables aux dangers extérieurs. Pour éviter ces risques, certaines entreprises disposent de logiciels permettant la suppression automatique des messages et pièces jointes après un délai prédéfini[188]. Les salariés sont donc invités, généralement dans le cadre de la politique

---

[188] GFI Software, *White paper. Archiving technologies*, p. 6, en ligne : <http://www.gfsfrance.com/whitepapers/stubbingwp.pdf> (site consulté le 28 juillet 2010).

d'utilisation de la messagerie électronique, à sauvegarder leurs documents dans les emplacements appropriés de leur poste de travail avant l'expiration de ce délai.

Une conduite prudente et diligente implique également que l'employé prenne toutes les précautions nécessaires pour assurer la sécurité physique du matériel, comme, par exemple ne pas laisser un ordinateur portable contenant des données personnelles de clients sans surveillance sur le siège d'un véhicule[189] : l'impératif de sécurité ne se limite, en effet, pas qu'au temps de travail. De même, l'employé doit s'abstenir de procéder à des opérations qui, comme l'avait fait valoir l'employeur dans *Commission des normes du travail* c. *Bourse de Montréal*[190], sont susceptibles de causer un dommage ou de nuire au bon fonctionnement des outils et du réseau. À cet égard, dans l'affaire *Syndicat canadien des communications, de l'énergie et du papier, Section locale 145* c. *Québec-livres (Division de : Communications Québécor Inc.)*[191], un employé a été suspendu pour cinq jours pour avoir, à plusieurs reprises, débranché de façon intempestive son ordinateur portatif, provoquant, chaque fois, un « gel » total du système informatique, ce qui avait obligé l'employeur à débourser d'importantes sommes pour réparer ces pannes. On peut également citer l'affaire *Télébec ltée* c. *Association canadienne des employés de téléphone*[192], dans laquelle un employé a été congédié après avoir supprimé du réseau informatique de l'entreprise tous les fichiers et systèmes d'exploitation qui s'y trouvaient, détruisant ainsi des données accumulées au cours des dix jours précédents, ainsi que les procédures d'exécution de son travail. L'employé venait juste d'être informé de la suppression de son poste. L'arbitre a estimé que la sanction disciplinaire retenue par l'employeur était justifiée, car l'employé s'était rendu coupable d'un acte d'inconduite gravissime qui avait pour effet de rompre le lien de confiance essentiel au maintien du lien d'emploi. De tels gestes peuvent, en effet, être constitutifs de sabotage ou d'entrave à

---

[189] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Résumé de conclusions d'enquête en vertu de la LPRPDÉ n° 289. Le vol d'un ordinateur portatif met en cause la responsabilité d'une banque*, préc., note 61.

[190] Préc., note 164.

[191] 2006 CanLII 27316 (QC A.G.).

[192] [2000] R.J.D.T. 1869 (T.A.).

l'activité de l'entreprise[193]. De fait, la destruction d'informations ou de fichiers informatiques renvoie à l'obligation de loyauté, tel que l'a rappelé l'arbitre dans l'affaire *Syndicat des spécialistes et professionnels d'Hydro-Québec, (SCFP-FTQ, section locale 4250)* c. *Hydro-Québec*[194], où il a été statué que la destruction, par un salarié, de fichiers sur son poste de travail, au motif qu'il était frustré d'avoir subi une entrevue de deux heures avec ses supérieurs hiérarchiques, alors qu'il pensait que cela ne prendrait qu'un quart d'heure, était un geste grave constitutif d'un manque de loyauté.

De tels actes de sabotage peuvent même conduire à des poursuites criminelles. Les articles 430 (1.1) (qui permet d'appréhender les méfaits visant les données) et 342.1 (1) (qui vise l'utilisation non autorisée d'un ordinateur) du *Code criminel* prévoient des peines pouvant aller jusqu'à 10 ans d'emprisonnement. Aux États-Unis, une ex-employée des garde-côtes a été condamnée à cinq mois de prison et 35 000 dollars de dommages-intérêts pour avoir détruit des informations de la base de données du personnel et altéré le fonctionnement du système informatique[195]. Elle s'était livrée à ce forfait parce qu'elle était furieuse de constater que son employeur ne tenait pas compte de ses avertissements quant au comportement illégal d'un fournisseur informatique. La remise à jour des données détruites avait mobilisé plus de cent personnes et 1 800 heures travail!

Section 2. L'obligation de loyauté et de discrétion

Il découle des articles 2088 C.c.Q. (relatif aux devoirs et obligations du salarié) et 1375 C.c.Q. (relatif à la bonne foi dans les relations contractuelles) que le salarié doit se comporter de façon honnête et loyale envers l'employeur[196].

---

[193] *Syndicat canadien des communications, de l'énergie et du papier, Section locale 145* c. *Québec-livres (Division de : Communications Québécor Inc.)*, préc., note 191; *Syndicat des spécialistes et professionnels d'Hydro-Québec, (SCFP-FTQ, section locale 4250)* c. *Hydro-Québec*, 2007 CanLII 20291 (QC A.G.).

[194] Préc., note 193.

[195] LEGALIS.NET, « Fraude informatique : 5 mois de prison », 09 juillet 1998, en ligne : <http://www.legalis.net/spip.php?page=archives&id_rubrique=60> (site consulté le 30 juillet 2010).

[196] R. P. GAGNON, « Le contrat de travail », préc., note 158, p. 10.

L'article 2088 C.c.Q. dispose que :

> « 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 à la cessation du contrat, et survivent en tout temps lorsque l'information réfère à la réputation et à la vie privée d'autrui. »[197]

Cet article codifie en fait des obligations et devoirs reconnus depuis longtemps par les tribunaux[198]. Le premier alinéa de cette disposition impose à tout salarié, peu importe son poste ou son niveau hiérarchique, d'agir avec loyauté envers l'employeur[199]. Ce devoir de loyauté emporte aussi un devoir de confidentialité pour le salarié qui ne doit pas utiliser ou divulguer à des tiers les informations confidentielles obtenues dans le cadre de son emploi[200].

L'employé est tenu à ces obligations pendant la durée du contrat de travail et pendant un délai raisonnable après la cessation de ce dernier[201]. C'est en se fondant sur ces dispositions que la jurisprudence a pu considérer qu'un employé qui avait créé un site Internet pour son employeur en y incluant, à l'insu de ce dernier, un lien direct vers son propre site Internet – créé en reproduisant textuellement celui de l'employeur – avait manqué de loyauté[202]. Ce manque de loyauté s'était poursuivi bien après la cessation du contrat de travail, puisque ce lien n'avait pas été supprimé et que le salarié avait continué à recevoir des informations appartenant à l'employeur. En agissant de la sorte, le salarié se faisait de la publicité par le truchement du site de son ex-employeur, puisque toute personne qui visitait le site de ce

---

[197] C.c.Q., art. 2088

[198] R. P. GAGNON, « Le contrat de travail », préc., note 158, p. 10.

[199] MARIE-FRANCE BICH, « La viduité post-emploi : loyauté, discrétion et clauses restrictives », dans *Développements récents en droit de la propriété intellectuelle (2003*), Service de la formation permanente du Barreau du Québec, 2003, *Droit civil en ligne* (DCL), EYB2003DEV358, p. 6.

[200] N.-A. BÉLIVEAU, K. BOUTIN et N. ST-PIERRE, préc., note 177, p. 18-19.

[201] C.c.Q., art. 2088 al. 2.

[202] *D'Astous* c. *Sesno*, REJB 2000-22668 (C.Q.).

dernier pouvait directement accéder à son site personnel et à son adresse de courrier électronique. De plus, l'homonymie des deux sites accentuait les risques de confusion pour la clientèle de l'ex-employeur.

Quant au second alinéa de l'article 2088 C.c.Q., il met à la charge de l'ex-salarié une obligation perpétuelle de discrétion concernant les renseignements personnels relatifs aussi bien à l'ex-employeur qu'aux collègues de travail, aux clients et aux tiers[203].

L'obligation de loyauté, dans son acception la plus large, peut être définie comme l'obligation pour le salarié d'assumer les « meilleurs intérêts »[204] de l'entreprise. En d'autres termes, il s'agit pour le salarié d'une « obligation de probité, de droiture, d'honnêteté, de bonne foi et de fidélité »[205]. Cela implique, comme le résume Marie-France Bich :

> « pas de mensonge, pas de vol, de fraude, d'appropriation ou de détournement des biens de l'employeur, d'usage d'un bien de l'employeur à des fins personnelles etc. »[206].

Le premier alinéa de l'article 2088 C.c.Q. fait référence aux obligations de loyauté et de discrétion comme des obligations formellement distinctes, cependant, la jurisprudence les a associées, considérant le devoir de discrétion du salarié comme étant l'une des facettes de son obligation de loyauté[207]. Et, en pratique, selon les espèces, l'obligation de discrétion ne manquera pas d'éclairer la portée concrète de l'obligation de loyauté[208]. Toutefois, pour les besoins de l'étude, nous examinerons séparément l'obligation de confidentialité (2.1.1.) et l'obligation d'exclusivité et de fidélité du salarié (2.1.2.).

---

[203] M.-F. BICH, préc., note 199, p. 31-32.

[204] *Belisle* c. *Rawdon (Municipalité)*, 2005 QCCRT 453 (IIJCan).

[205] N.-A. BÉLIVEAU, K. BOUTIN et N. ST-PIERRE, préc., note 177, p. 17.

[206] M.-F. BICH, préc., note 199, p. 6-7.

[207] R. P. GAGNON, « Le contrat de travail », préc., note 158, p. 10.

[208] *Id.*

2.1. L'obligation de confidentialité

En vertu du contrat de travail, le salarié est tenu de ne pas divulguer à des tiers ou d'utiliser l'information à caractère confidentiel obtenue dans le cadre de son emploi[209]. L'obligation de confidentialité a des effets très étendus qui peuvent conduire l'employeur à intervenir hors des lieux de l'entreprise et parfois même alors que le salarié ne fait plus partie des effectifs de l'entreprise. Il arrive, en effet, que l'employeur demande la saisie de documents, y compris la fouille d'ordinateurs et autres supports informatiques, lorsqu'elle soupçonne, par exemple, qu'un employé ou un ex-employé détient des informations confidentielles lui appartenant[210]. En effet, à la lumière de la jurisprudence, les tribunaux sanctionnent notamment l'utilisation de renseignements confidentiels ou privilégiés propres à l'ancien employeur ou la possession des fichiers, disquettes, dossiers ou tout élément de propriété intellectuelle lui appartenant[211]. De tels agissements sont parfois découverts bien des mois après le départ du salarié indélicat, notamment à la faveur d'une remise à niveau de routine du système informatique ou de vérifications effectuées directement sur le poste de travail de l'ex-employé. Ainsi, dans l'affaire *People* v. *Eubanks*[212], c'est à l'occasion d'une opération de nettoyage, effectuée sur le poste d'un ex-salarié, que l'employeur a découvert que ce dernier avait, à plusieurs reprises, transféré des secrets de fabrication à son nouvel employeur par courriel.

L'entreprise doit donc pouvoir mettre en œuvre toutes les mesures nécessaires pour protéger sa propriété intellectuelle, ainsi que les données confidentielles relatives à ses employés, clients et contacts d'affaires contre les employés malhonnêtes ou imprudents. Or, les organisations avouent une préoccupation croissante face aux atteintes à ces données

---

[209] *Id.*

[210] *124670 Canada Ltée (Clinique de médecine industrielle et préventive du Québec)* c. *Remmouche*, EYB 2004-69859 (C.S.); *Refplus Inc.* c. *Kehar*, EYB 2006-104760 (C.S.); *Sherelco Inc.* c. *Laflamme*, EYB 1992-75301 (C.S.); *Shermag Inc.* c. *Zelnicker*, REJB 2004-69078 (C.S.).

[211] ANDRÉ BARIL, « Chronique – L'obligation de loyauté, de diligence et de discrétion d'un salarié après la cessation de son emploi », dans *Repères*, Septembre 1999, *Droit civil en ligne* (DCL), EYB1999REP109, p. 5-6.

[212] 927 P.2d 310 (Cal. 1996).

stratégiques : plus de 22 % des incidents de sécurité concernent en effet des fuites d'informations[213]. Les informations visées concernent, notamment, les listes de clients, les rapports financiers ou les secrets de fabrication. Les salariés peuvent subtiliser ces informations sensibles pour leur propre compte, par exemple, pour créer une entreprise concurrente, réaliser des profits en spéculant en bourse ou tout simplement négocier un meilleur emploi ailleurs. Les salariés peuvent aussi céder aux sirènes de l'espionnage économique. Généralement ce sont les entreprises concurrentes qui sollicitent le salarié, mais cela peut aussi se faire à sa propre initiative. L'espionnage économique répond à des motivations diverses : appât du gain, envie de pimenter une vie jugée trop terne, pression économique, dettes, chantage, etc. La tentation peut être d'autant plus forte que l'apprenti-espion dispose de supports de plus en plus miniaturisés et toujours plus performants accessibles sur le marché (disquettes, CD, DVD, clés USB … que le salarié indélicat aura parfois « empruntés » à l'employeur) et qui lui faciliteront la tâche pour copier ou transférer les informations convoitées. Il n'est même plus nécessaire de recourir à de tels outils : il suffit d'une adresse électronique et de quelques clics pour transmettre à un concurrent des informations vitales de l'entreprise[214]. Pour éviter ce risque, les entreprises ont tendance à resserrer leur contrôle sur la correspondance électronique de leurs salariés. Cependant, comme le souligne Dan Griguer, il s'agit là d'un argument biaisé, car la problématique de la sauvegarde des intérêts de l'entreprise va bien au-delà du courrier électronique : la question s'était déjà posée pour le téléphone, certes, dans des proportions moindres puisqu'il impossible transférer un dossier par cette voie[215]. Le problème ne s'est pas réellement posé pour le fax, en raison du système du rapport d'émission qui permet de contrer une éventuelle fuite des informations[216]. L'auteur en conclut que ce serait moins

---

[213] AMERICAN MANAGEMENT ASSOCIATION, THE EPOLICY INSTITUTE, préc., note 27.

[214] *People* v. *Eubanks*, préc., note 212.

[215] DAN GRIGUER, « Le débat sur l'utilisation, à titre privé, du courrier électronique au sein de l'entreprise serait-il dépassé? », Legalbiznext.com, 28 juillet 2004, en ligne : <http://www.legalbiznext.com/droit/Le-debat-sur-l-utilisation-a-titre> (site consulté le 19 août 2010).

[216] *Id.*

l'aspect sécuritaire et confidentiel que le souhait de contrôler le travail du salarié et les éventuelles pertes de temps dues à la navigation sur Internet et à l'échange de courriels qui motive l'employeur à surveiller l'utilisation des ressources électroniques[217].

Les fuites de données peuvent aussi résulter de l'imprudence ou de la naïveté des salariés. Il arrive parfois que ceux-ci soient victimes des manœuvres de concurrents prétendant être des clients ou des prospects à la recherche de renseignements et qui arrivent habilement à leur soutirer des informations confidentielles[218]. La fuite de données confidentielles peut également provenir de la transmission d'un courrier électronique à un destinataire non autorisé. Cela peut être le cas à la suite d'une erreur de manipulation (par exemple, on ne sélectionne pas le bon nom dans la liste des contacts ou le document approprié pour la pièce jointe). Une telle erreur peut aussi simplement résulter d'informations erronées concernant l'interlocuteur visé (celles-ci n'ayant, par exemple, pas été mises à jour à la suite d'un changement d'adresse, de poste ou d'employeur). Les salariés ont donc intérêt à faire preuve de la plus grande prudence, au risque de se retrouver dans des situations fort embarrassantes, aussi bien pour eux-mêmes que pour l'entreprise.

Les salariés peuvent aussi involontairement divulguer des informations confidentielles concernant leur entreprise, simplement grâce aux métadonnées liées aux documents électroniques qu'ils transfèrent par courriel à leurs interlocuteurs de tous ordres. En effet, chaque manipulation effectuée sur un document électronique laisse des traces, les métadonnées (également appelées les « données sur les données »), qui permettent de savoir qui est l'auteur du document, quand et comment ce dernier a été créé, par qui il a été manipulé et quels traitements il a subis[219]. Les interlocuteurs peuvent, par exemple, permettre de découvrir où le fichier qu'ils ont reçu est classé, puisque le chemin leur est

---

[217] *Id.*

[218] V. ROQUES, préc., note 34, p 21.

[219] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Les risques associés aux métadonnées. Fiche d'information*, en ligne : <http://www.priv.gc.ca/fs-fi/02_05_d_30_f.cfm> (site consulté le 25 juillet 2010); Dan PINNINGTON, « Beware the Dangers of Metadata », Lawpro.ca, Juin 2004, en ligne : <http://www.lawpro.ca/LawPRO/metadata.pdf> (site consulté le 19 août 2010).

indiqué par le document lui-même (par exemple : C/Utilisateurs/Ventes/Cosmétiques/Clients/Facturation)[220]. Ce qui peut s'avérer fort utile en cas d'espionnage effectué par intrusion dans le système informatique de l'entreprise : le pirate n'aura qu'à suivre l'arborescence ainsi fournie pour accéder rapidement aux informations qui l'intéressent. Certaines métadonnées peuvent être très utiles dans des situations particulières : ainsi, en matière de négociations contractuelles, les interlocuteurs utilisent souvent les fonctions « suivi de modifications » et « commentaires » qui permettent à chacun de voir les modifications et commentaires proposés par les autres, de telles informations pouvant avoir une importance capitale en cas de litige ultérieur. Cependant, ces renseignements peuvent aussi s'avérer néfastes ou en tout cas fort embarrassants, lorsque les interlocuteurs – et les destinataires subséquents du document – ont accès à des informations et commentaires que l'on avait pris soin d'effacer, parfois à dessein, pour qu'ils ne les découvrent pas[221].

Finalement, l'utilisation des outils de communication électroniques peut sérieusement remettre en cause la sécurité et la confidentialité des informations vitales de l'entreprise, le salarié étant souvent placé dans des situations où il peut, de façon volontaire ou non, diffuser de telles informations, et ce, en contravention avec son obligation de loyauté et des dispositions relatives à la protection des renseignements personnels. Le salarié peut également faire l'objet de sanctions pénales, notamment lorsque les informations détournées sont utilisées à des fins criminelles[222].

2.2. L'obligation d'exclusivité et de fidélité

La loyauté implique tout d'abord l'exclusivité par rapport à l'entreprise : le salarié s'engage personnellement vis-à-vis de son employeur et ne peut se livrer à une activité

---

[220] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Les risques associés aux métadonnées. Fiche d'information*, préc., note 219.

[221] *Id.*; D. PINNINGTON, préc., note 219.

[222] *R.* c. *Martineau*, REJB 2003-48758 (C.Q.).

professionnelle pour son propre compte ou celui d'un tiers pendant son temps de travail. Il s'agit là d'une obligation propre au contrat de travail, ce qui confère aux clauses d'exclusivité un caractère informatif, puisque leur objet est généralement de rappeler une obligation inhérente au contrat de travail lui-même[223]. L'exclusivité concerne également le matériel fourni par l'employeur et que le salarié doit utiliser de façon appropriée et à des fins professionnelles. En clair, le salarié ne doit pas utiliser ses outils de travail pour son propre compte ou celui d'un tiers. Or, ce principe n'est pas toujours respecté, que ce soit au bureau où l'employé pourra, par exemple, utiliser son ordinateur pour mettre à jour son curriculum vitae ou à la maison, où l'ordinateur portable pourra servir à réaliser de menus travaux informatiques personnels. Le problème de l'exclusivité se pose avec encore plus d'acuité dans l'hypothèse du télétravail, notamment lorsque le télétravailleur est à temps partiel. En effet, lorsque le travailleur œuvre depuis son domicile, il lui est souvent difficile de résister à la tentation d'utiliser le matériel fourni par l'employeur à des fins privées ou même pour le compte d'un autre employeur. Aussi est-il conseillé, dans une telle hypothèse, d'insérer dans le contrat de travail une clause qui rappellera au salarié que le matériel appartient à l'employeur et doit donc être réservé (tout comme l'utilisation de « sa force de travail » d'ailleurs) aux activités accomplies pour le compte de ce dernier[224]. Cependant, si le salarié est employé à temps partiel, l'employeur ne pourra pas lui reprocher d'offrir ses services à un autre sans courir le risque de se voir accuser de le priver de moyens de subsistance. Aussi l'employeur serait avisé d'insérer une clause de non-concurrence afin de se protéger contre les éventuels agissements déloyaux de son employé impliquant, notamment, l'utilisation du matériel ou des données lui appartenant[225].

L'obligation d'exclusivité n'implique nullement qu'on exige du salarié qu'il adhère sans réserve aux « valeurs de l'entreprise », car ce serait porter atteinte à sa liberté

---

[223] Antoine MAZEAUD, *Droit du travail*, 5e éd., Paris, Montchrestien, 2006, p. 320.

[224] I. DE BENALCÁZAR, préc., note 28, p. 69.

[225] *Id.*

individuelle[226]. En réalité, ce que l'on attend de lui c'est surtout qu'il évite de se placer dans une situation où il pourrait avoir à choisir entre ses propres intérêts ou ceux d'un tiers et ceux de l'employeur[227].

On se trouvera en situation de conflit d'intérêts lorsque le salarié effectue, par exemple, des travaux pour le compte d'un tiers, depuis son lieu habituel de travail et avec les outils fournis par son employeur. Peu importe que ces activités soient ou non rémunérées. Ainsi, dans *Syndicat des spécialistes et professionnels d'Hydro-Québec, (SCFP-FTQ, section locale 4250)* c. *Hydro-Québec*[228], l'employeur avait congédié un employé pour avoir utilisé, à de nombreuses reprises, et en violation du Code de conduite de l'entreprise, le matériel informatique et le courrier électronique de l'entreprise pour effectuer des travaux pour le compte de l'association à but non lucratif dirigée par sa mère. Le salarié effectuait en effet du soutien technique, pendant ses heures de travail, au profit de cet organisme. De plus, il avait installé, sans autorisation, un logiciel qui lui permettait, notamment, d'accéder directement, depuis son poste de travail, au site Internet de cette association et d'y effectuer des travaux. L'un des arguments invoqués par l'employé était le fait que ces activités, bien qu'exercées à titre personnel, n'étaient pas rémunérées. Toutefois, l'arbitre conclut que cet élément était sans importance et qu'il y avait perte de confiance, l'employé ayant agi en violation du Code de conduite de l'entreprise.

Il y aura également conflit d'intérêts lorsque l'employé utilise l'équipement de l'employeur au bénéfice de sa propre entreprise. Ainsi, dans l'affaire *Syndicat des spécialistes et professionnels d'Hydro-Québec* c. *Hydro-Québec*[229], l'arbitre maintient le congédiement d'un analyste support informatique qui avait utilisé son adresse électronique professionnelle, ainsi que son numéro de pagette, à des fins de publicité pour sa propre entreprise d'agent immobilier. En plus d'utiliser les outils de communication de

---

[226] A. MAZEAUD, préc., note 223, p. 320.

[227] N.-A. BÉLIVEAU, K. BOUTIN et N. ST-PIERRE, préc., note 177, p. 17.

[228] Préc., note 193.

[229] *Syndicat des spécialistes et professionnels d'Hydro-Québec* c. *Hydro-Québec*, 2003 CanLII 20475 (QC A.G.).

l'employeur pour solliciter la clientèle, le salarié avait, à plusieurs reprises, consulté et diffusé des contenus à caractère sexuel et pornographique, le tout en violation du Code de conduite de l'entreprise.

L'affaire *Collège Ahuntsic* et *Syndicat du personnel de soutien du Collège Ahuntsic*[230] constitue aussi un autre bel exemple de conflit d'intérêts. Elle concerne un technicien en informatique qui utilisait son temps de travail au profit de sa propre entreprise et d'un organisme dont il gérait les activités à titre de bénévole. L'employeur lui a infligé une suspension de trois mois, en raison non seulement de ce vol de temps, mais également parce qu'il déclarait des heures supplémentaires les jours où il vaquait à ses occupations privées. De plus, le salarié utilisait le téléphone et l'ordinateur de l'employeur dans le cadre de ses activités personnelles et les cartes de visite de son entreprise personnelle comportaient l'adresse de courriel de l'employeur. Toutefois, l'arbitre a jugé que la durée de la suspension était disproportionnée. En effet, le vol de temps en l'espèce n'était pas considérable et la réputation de l'employeur n'avait pas été entachée par ces activités. De plus, avant la sanction contestée, l'employeur n'avait effectué aucune mise au point avec l'employé quant à ses activités personnelles au travail. L'arbitre a donc conclu qu'une suspension de trois semaines était plus raisonnable au vu des circonstances.

2.3. La préservation de la réputation et de l'image de l'entreprise

Le devoir de loyauté implique également que le salarié s'interdit tout comportement de nature à porter atteinte à la réputation de l'entreprise sans motifs valables[231]. Ainsi, dans *Cogeco Câble Canada* c. *Syndicat canadien de la fonction publique, section locale 3624*[232], un employé a reçu une suspension de 33 jours pour avoir utilisé une adresse IP flottante appartenant à son employeur pour pénétrer le système d'un compétiteur, puis communiqué

---

[230] D.T.E. 2007T-889 (T.A.).

[231] R. P. GAGNON, « Le contrat de travail », préc., note 158, p. 10.

[232] *Cogeco Câble Canada Inc.* et *Syndicat canadien de la fonction publique, section locale 3624*, D.T.E. 2001T- 1039 (T.A.).

aux médias l'existence d'une faille de sécurité dans le système d'information de ce dernier. Pour l'employeur, cette mesure était, notamment, justifiée par le fait que ces agissements auraient pu avoir des conséquences néfastes pour l'entreprise, puisqu'ils visaient un concurrent. Toutefois, l'absence de politique d'utilisation d'Internet a été considérée comme un facteur atténuant et la sanction initiale a été remplacée par une suspension de 10 jours.

Les employés doivent également s'abstenir de dénigrer ou de critiquer leur employeur, que ce soit au sein de l'entreprise ou à l'extérieur de celle-ci. Cela est particulièrement valable pour les propos tenus dans des blogues personnels qui, même exploités en privé et en dehors des lieux de travail, peuvent parfois conduire au congédiement. Ainsi, dans *Alberta* v. *Alberta Union of Provincial Employees*[233], l'employeur a congédié une employée après avoir découvert, par hasard, le blogue que cette dernière exploitait et dans lequel elle insultait ses collègues et dénigrait son employeur, ainsi que des clients de l'entreprise. Bien que les noms des personnes visées aient été modifiés, celles-ci étaient aisément identifiables au vu des détails fournis sur le site. Le congédiement fut confirmé par l'arbitre qui jugea qu'en mettant ces commentaires désobligeants sur son site, l'employée avait commis des gestes dont la gravité avait irrémédiablement miné la confiance de l'employeur. De plus, l'employée n'avait exprimé aucun remords et avait plutôt justifié ses actes par l'exercice de son droit à la liberté d'expression. Par ailleurs, elle n'avait pris aucune mesure pour bloquer l'accès aux contenus litigieux. Cette décision a, toutefois, été annulée non sur le fond, mais pour non-respect de la procédure disciplinaire prévue dans la convention collective[234]. Il est fort regrettable que l'employeur ait été négligent sur ce point, car la Cour du banc de la reine confirme par ailleurs que le congédiement reposait bien sur une cause juste et suffisante.

---

[233] *Alberta* v. *Alberta Union of Provincial Employees* (R. Grievance), [2008] A.G.A.A. No. 20 (G.A.) (QL/LN), [2008] 174 L.A.C. (4th) 371 (Alta. G.A.).

[234] *Alberta Union of Provincial Employees v. Alberta*, 2009 ABQB 208 (CanLII).

Dans une autre affaire aux faits quelque peu similaires, un employé a été congédié pour avoir, notamment, tenu des propos racistes et antisémites sur son blogue personnel et fait référence à son employeur qui était clairement identifié[235]. Bien que les commentaires aient été postés en dehors des heures et lieux de travail, l'employeur faisait valoir que son intervention était justifiée, en raison du caractère raciste et haineux des messages. Il ajoutait que ceux-ci étaient destinés à être lus par les autres employés et cela ne pouvait qu'exacerber les tensions au sein de l'entreprise, déjà aux prises avec des problèmes de vandalisme et une difficile cohabitation multiculturelle. L'arbitre conclut qu'il y avait bien un lien entre les écrits du blogue et le travail. De plus, il jugea que les nombreuses références à l'employeur constituaient une faute. Toutefois, au vu des circonstances, il conclut que la sanction était trop sévère. En effet, les propos litigieux ne visaient pas directement l'employeur, ni les clients ou les produits de l'entreprise, ou même un salarié en particulier. De plus, l'employé avait un dossier vierge et avait exprimé des remords dans une lettre adressée à l'employeur dans laquelle il s'excusait et admettait ses torts. Par conséquent, l'arbitre ordonna sa réintégration.

Outre le droit de sanctionner les employés pour leurs activités inappropriées, l'employeur peut également engager une action en responsabilité civile contre eux, puisque, dans une telle hypothèse, l'obligation de loyauté de l'employé « chevauche son obligation de respecter la réputation de son employeur et de ses représentants »[236]. Se posera alors la question de la preuve, dont le fardeau repose sur l'employeur. Ainsi, dans l'affaire *Syndicat des spécialistes et professionnels d'Hydro-Québec, (SCFP-FTQ, section locale 4250)* c. *Hydro-Québec*[237], l'arbitre conclut que les activités du plaignant n'avaient pu nuire à l'image de l'entreprise, dans la mesure où il n'y avait eu aucune diffusion publique de ces

---

[235] *EV Logistics* v. *Retail Wholesale Union, Local 580* (Discharge Grievance), [2008] B.C.C.A.A.A. No. 22 (Coll. Agr. Arb.) (QL/LN).

[236] Gaétan LÉVESQUE et Stéphane FOREST, « L'atteinte à la réputation dans le cadre des rapports collectifs de travail », dans *Développements récents en droit du travail (2002),* Service de la formation permanente du Barreau du Québec, 2002, *Droit civil en ligne* (DCL), EYB2002DEV618, p. 26.

[237] Préc., note 193.

activités commerciales, hormis auprès de deux sociétés. De plus, aucun service comportant les coordonnées de l'employeur n'avait été offert au public. Finalement, l'arbitre a substitué une suspension de 9 mois au congédiement.

L'image de marque et la réputation de l'entreprise pourront, en revanche, être mises en péril si le nom de l'entreprise apparaît sur un courriel dont le contenu est inapproprié. C'est ce qui a notamment été jugé dans l'affaire *Bell Canada* c. *Association canadienne des employés de téléphone*[238] concernant un employé qui utilisait le courrier électronique mis à sa disposition par l'employeur pour transférer, à d'autres employés de la compagnie ou à des personnes à l'extérieur, des messages à caractère sexuel ou pornographique.

Le fait pour les employés de télécharger des logiciels ou des documents inappropriés, tels que le matériel pornographique, pourra également entacher la réputation de l'entreprise[239]. De tels téléchargements peuvent même constituer des actes criminels, lorsque, par exemple, les contenus mettent en scène des mineurs. Ainsi, la production, l'impression, la publication, l'importation, la distribution et la possession à cette fin de pornographie juvénile exposent son auteur à une peine d'emprisonnement pouvant aller jusqu'à 10 ans[240], tandis que la possession simple de pornographie juvénile est passible d'un emprisonnement maximal de 5 ans[241]. Et le fait, pour le contrevenant d'utiliser la propriété ou le nom d'un tiers (par exemple, il se sert de l'ordinateur de son employeur pour télécharger et stocker ces contenus illicites ou paie ses téléchargements avec la carte de crédit de l'entreprise ou encore diffuse de tels contenus grâce à son courrier électronique professionnel) pour accomplir son forfait constitue un facteur aggravant[242].

---

[238] D.T.E. 2000-254 (T.A.); Voir également *Syndicat des spécialistes et professionnels d'Hydro-Québec* c. *Hydro-Québec*, préc., note 229.

[239] *Syndicat canadien des communications, de l'énergie et du papier, section locale 522* c. *CAE Électronique Ltée*, préc., note 159; *Bell Canada* c. *Association Canadienne des Employés de Téléphone*, préc., note 238; *Blais* c. *Société des Loteries Vidéos du Québec Inc*., D.T.E. 2003T-178 (C.R.T.).

[240] *Code criminel*, art. 163.1(2) et 163.1(3).

[241] *Id.*, art. 163.1(4).

[242] Pour une illustration, voir *R.* c. *Chassé*, REJB 2002-33523 (C.Q.).

La nécessité de préserver l'image et la réputation de l'entreprise peut parfois entrer en conflit avec la liberté d'expression du salarié lorsque ce dernier porte des appréciations publiques sur son entreprise ou sur des tiers (qu'il s'agisse d'individus ou d'organismes). Cela pourra arriver, par exemple, lorsque les employés participent à des forums de discussions. Ces espaces offrent aux individus une formidable tribune pour échanger idées et opinions sur divers sujets. Les salariés peuvent être amenés à y livrer des opinions qui pourraient, si leur identification sur ce site est associée au nom de l'entreprise qui les emploie, porter atteinte à l'image de cette dernière en donnant à penser qu'ils s'expriment en son nom. Ainsi, dans *Arpin* c. *Grenier*[243], une entreprise a poursuivi l'un de ses hauts cadres en raison non seulement du caractère diffamatoire de ses propos diffusés sur un forum de discussion, mais également d'un usage non autorisé de son adresse électronique professionnelle. Le salarié avait, en effet, publié un texte contenant des propos qui pouvaient être considérés comme offensants pour certains groupes ou personnalités politiques. Le texte avait été signé du nom du salarié suivi de son adresse électronique professionnelle. Or, l'entreprise avait mis à la disposition de chaque employé une adresse de courriel distincte, mais elles étaient toutes regroupées au nom de la compagnie. La Cour du Québec a conclu qu'un tel usage constituait une atteinte à la fois au droit de propriété de l'entreprise sur les adresses électroniques et à sa vie privée.

De plus, cette utilisation s'était faite en violation de l'obligation de loyauté de l'employé. À cet égard, la Cour relève qu'en sa qualité de cadre haut placé (il était adjoint au président et responsable du marketing de l'entreprise), le salarié jouissait de la confiance de son employeur, bénéficiait de toutes les entrées, représentait la compagnie et disposait de toutes les informations nécessaires à la survie de l'entreprise. Il savait ou aurait dû savoir que l'utilisation de l'adresse Internet fournie par l'employeur pourrait causer des dommages à ce dernier, surtout si cet usage était douteux. En effet, le texte diffusé avait un caractère diffamant et était accessible à un public assez large. De plus, le fait que le nom de

---

[243] REJB 2004-65808 (C.Q.).

l'entreprise apparaisse à la signature pouvait amener à associer l'opinion de son auteur avec l'entreprise. Et de fait, le président de l'entreprise avait découvert le texte litigieux en effectuant des recherches pour savoir pourquoi, depuis quelque temps, il rencontrait des difficultés à obtenir du financement et recevait un accueil plus froid des investisseurs potentiels.

Pour ce qui concerne l'atteinte au droit de propriété, la Cour conclut que l'adresse Internet fournie par l'employeur à ses employés lui appartient et qu'elle n'était mise à leur disposition qu'à des fins professionnelles, à moins d'une autorisation expresse pour des fins différentes. Si bien que toute utilisation à des fins personnelles pouvait porter atteinte aux droits patrimoniaux de son titulaire, et donc à sa vie privée. Par conséquent, l'utilisation sans permission du nom de l'entreprise constituait une atteinte à la vie privée de celle-ci.

Quant à la question de la liberté d'expression du salarié, la Cour conclut qu'en l'espèce, l'obligation de loyauté et le respect de la vie privée de l'entreprise avaient préséance sur la liberté du salarié, dans la mesure où l'entreprise, qui était la personne dont les droits étaient ici bafoués, n'était pas une

> « personnalité publique qui s'expose à la critique […mais] simplement une entreprise recherchant du financement pour la continuation de ses affaires et qui est victime du geste malencontreux posé par un de ses employés. »[244]

Tout salarié avisé devrait donc éviter d'utiliser son adresse électronique professionnelle à des fins autres que l'exécution de ses tâches.

Cependant, même une activité purement privée, exercée en dehors des heures de travail, depuis un poste personnel, peut néanmoins être préjudiciable pour une entreprise lorsque sa dénomination sociale est, par exemple, mentionnée par un de ses salariés sur un forum de discussion ou un site de partage. Certes, le fait que des salariés revendiquent fièrement, sur *Facebook* ou *MySpace*, leur appartenance à une entreprise peut apporter à celle-ci une

---

[244] *Id.*

grande visibilité; toutefois, cela peut également être une source de publicité non désirée, car les sites sociaux sont de formidables collecteurs de données personnelles qu'ils revendent chèrement à des entreprises souhaitant les exploiter à des fins commerciales. Nombreux sont d'ailleurs les organismes qui visitent de tels sites, à la recherche de la moindre information de ce genre dont ils pourraient tirer profit. Par ailleurs, les salariés doivent être vigilants en tout temps et ils doivent notamment s'assurer que le contenu des textes qu'ils publient ne porte pas préjudice à leur employeur. Ainsi, dans l'affaire *Montour Limitée* c. *Syndicat des employé-e-s de la Cie Montour (CSN)*[245], un employé a été congédié pour violation de son obligation de loyauté après la découverte de sa participation à un forum de discussion où il précisait le nom de son employeur et se vantait de ne pas « travailler très fort », tout en étant bien payé. Il indiquait, notamment, que durant son quart de travail de huit heures, il n'en effectuait en réalité que quatre et passait les quatre autres heures à jouer aux cartes. Même si ces propos fâcheux avaient été diffusés plus de deux ans plus tôt, ils continuaient d'être accessibles au grand public : il suffisait pour cela de taper le nom de l'entreprise dans les moteurs de recherche les plus usuels. Les faits avaient d'ailleurs été signalés à l'employeur par un fournisseur qui, souhaitant avoir les coordonnées de l'entreprise, avait effectué une recherche sur Internet et était tombé sur les écrits litigieux. Or, l'entreprise qui était spécialisée dans la fabrication de produits alimentaires, avait mis en place des normes de qualité supérieure et bénéficiait d'une certification internationale. Pour conserver cette certification qui la démarquait de ses concurrentes, elle devait observer des règles très strictes en matière de lavage et d'assainissement de tout son équipement. L'employé, qui était préposé au lavage, connaissait très bien l'importance capitale du respect des règles d'hygiène puisqu'il avait suivi un cours portant sur ce sujet. L'arbitre a maintenu le congédiement en raison de la perte de confiance résultant de ces agissements.

---

[245] 2006 IIJCan 43801 (QC A.G.); Voir également *Alberta* v. *Alberta Union of Provincial Employees* (R. Grievance), préc., note 233, à propos d'une employée qui insultait son employeur et ses collègues sur son blogue personnel; Pour une autre illustration, voir *EV Logistics* v. *Retail Wholesale Union, Local 580* (Discharge Grievance), préc., note 235, où un employé écope d'une suspension temporaire pour avoir diffusé des propos racistes sur son blogue et fourni sur son site des informations permettant d'identifier clairement son employeur.

Ces deux dernières décisions révèlent à quel point obligation de loyauté et liberté d'expression du salarié peuvent parfois être délicates à concilier. Elles mettent, en effet, en lumière la difficulté pour les salariés d'exercer leur droit de critiquer lorsqu'il s'agit de leur employeur[246], surtout lorsqu'ils sont tenus à une obligation de loyauté « renforcée » en raison, par exemple, de leur fonction ou de l'activité de l'entreprise.

La réputation de l'entreprise peut également être entachée lorsque le salarié manque de convivialité vis-à-vis de ses collègues, des clients de l'employeur ou de tiers. Cela pourra être le cas lorsque l'employé utilise le courrier électronique professionnel pour intimider ou harceler des collègues de travail[247] ou des personnes à l'extérieur de l'entreprise. En effet, même si l'article 2088 C.c.Q. ne l'énonce pas directement, on estime que le salarié est tenu à une obligation de « courtoisie et de civilité »[248] envers les clients de l'entreprise et ses collègues de travail. On peut définir ces obligations comme suit :

> « [l']obligation de courtoisie du salarié vise à assurer la réputation et l'image de l'employeur à l'égard de sa clientèle, [alors que] l'obligation de civilité vise, quant à elle, à maintenir un milieu de travail sain et harmonieux »[249].

En somme, l'utilisation d'Internet et du courrier électronique à des fins personnelles durant les heures de travail constitue, dans presque tous les cas, un acte déloyal vis-à-vis de l'employeur, car ces actes sont assimilés à de la fraude ou à du vol et peuvent entraîner le congédiement, surtout lorsque l'entreprise s'est dotée d'une politique claire à ce sujet[250]. Cependant, même lorsque l'utilisation de ces outils est effectuée en dehors des heures de bureau, elle peut présenter un caractère déloyal si, par exemple, l'employé visite des sites aux contenus inappropriés. Les administrateurs des sites Internet ont les moyens de connaître les adresses IP de ceux qui se connectent ou tentent de se connecter à leurs sites.

---

[246] V. SÉDALLIAN, préc., note 40, p. 11.

[247] *Dufresne* c. *Pratt & Whitney Canada Inc.*, D.T.E. 94T-405 (C.T.).

[248] N.-A. BÉLIVEAU, K. BOUTIN et N. ST-PIERRE, préc., note 177, p. 16.

[249] *Id.*

[250] *Id.*, p. 10.

Les entreprises de jeux en ligne indiquent que « 40 % à 60 % de ceux qui accèdent à leurs services possèdent des adresses d'affaires (.com) »[251]. Les exploitants de sites Internet peuvent donc, à partir de leurs données de connexion, tirer toutes sortes de conclusions, notamment quant au manque de sérieux des employés de telle ou telle entreprise dont ils reçoivent régulièrement la visite, ou quant à l'absence de rigueur de ces entreprises qui laissent leurs salariés naviguer sur de tels sites. Finalement, il suffit d'une simple visite d'un salarié sur un site Internet, depuis son poste de travail, pour qu'une organisation soit éventuellement étiquetée et voit sa réputation ternie. Les entreprises se passeraient bien de ce genre de publicité négative, tout comme elles éviteraient volontiers celle résultant de la participation de salariés à des chaînes de messages du style « envoyez ce message à tous vos amis et connaissances » qui circulent régulièrement : l'employé qui se prête à ces pratiques, grâce à son adresse électronique professionnelle, expose en effet son employeur à voir son nom faire le tour de planète, pour des causes généralement futiles. L'entreprise sera parfois même victime de canulars, certains messages laissant, par exemple, croire qu'elle est l'instigatrice de telle action de solidarité ou qu'elle la soutient. Qui n'a pas reçu un message concernant un jeune enfant atteint d'une maladie rarissime et dont la vie dépendait d'une coûteuse opération que telle entreprise bien connue s'était engagée à financer, à condition que des particuliers forment une « chaîne de solidarité électronique » autour de la cause? Chaque courriel envoyé étant censé donner lieu au versement, par l'entreprise commanditaire, de quelques centimes de dollars (ou d'euros). Donc, plus il y aurait de participants à la chaîne, plus grandes seraient les chances de récolter la totalité de la somme d'argent nécessaire à l'opération. Généralement, l'engouement retombe au bout de quelques jours avec un communiqué de l'entreprise démentant la rumeur.

Signalons, pour conclure sur ce point, que la violation du devoir de loyauté et de discrétion autorise l'employeur à exercer son pouvoir disciplinaire et les mesures arrêtées dans ce cadre peuvent aller jusqu'au congédiement du salarié pour « cause juste et suffisante » au

---

[251] FRANÇOIS CÔTÉ, « Surveillance des technologies de l'information », Ogilvyrenault.com, Décembre 1999, en ligne : <http://www.ogilvyrenault.com/fr/centreDeResources_1665.htm> (site consulté le 18 août 2010).

sens de l'article 2094 C.c.Q.[252]. L'obligation de loyauté s'apprécie en fonction de plusieurs critères[253] qui tiennent, notamment, à l'activité de l'entreprise, ainsi qu'à la nature de l'emploi, au positionnement hiérarchique et au niveau de responsabilités de l'employé[254]. De plus, l'existence ou non d'une politique au sein de l'entreprise, ainsi que la tolérance ou non de l'employeur vis-à-vis de certains comportements joueront aussi un grand rôle. Bien entendu, la conduite de l'employé et son aptitude à avouer ses agissements pourront également avoir une certaine influence dans l'appréciation de ses obligations et surtout de la mesure disciplinaire éventuellement applicable.

Chapitre 3. Les risques de responsabilité

Les employeurs ont de tout temps contrôlé le comportement de leurs employés, non seulement pour s'assurer qu'ils accomplissaient bien leurs tâches, mais également pour vérifier que leur conduite restait conforme à l'ordre public et aux bonnes mœurs, ainsi qu'aux règles élémentaires de civilité. Les agissements des salariés peuvent, en effet, donner lieu à des actions en réparation visant non seulement leurs auteurs, mais également l'employeur qui leur aura fourni les moyens pour accomplir ces actes préjudiciables. Avec l'introduction des NTIC en entreprise, les employeurs ont vite réalisé qu'ils devaient redoubler de vigilance dans la mesure où ces ressources peuvent servir à commettre en catimini toutes sortes d'infractions ou d'incivilités dont ils peuvent être tenus responsables.

En naviguant sur l'Internet, les salariés peuvent, par exemple, télécharger des contenus assujettis à des droits de propriété intellectuelle ou s'introduire sans autorisation dans le système informatique de tiers, accédant éventuellement ainsi à des informations confidentielles qu'ils peuvent même modifier. Les salariés peuvent également se servir des

---

[252] M.-F. BICH, préc., note 199, p. 6.

[253] Voir *infra*, Partie 2, Chapitre 2, Section 1, 1.1.3, p. 167.

[254] M.-F. BICH, préc., note 199, p. 6; Voir également Sylvain LEFEBVRE, « Naviguer sur Internet au travail: et si on nageait en eaux troubles? », dans Service de la formation permanente du Barreau du Québec, *Développements récents en droit du travail 2008*, Cowansville, Éditions Yvon Blais, 2008, p. 51, à la page 108 et suiv.

ressources informatiques mises à leur disposition pour diffamer, harceler ou véhiculer des propos diffamatoires ou offensants. L'utilisation du courrier électronique doit bénéficier d'une attention particulière, notamment en raison du caractère instantané des messages. Les échanges se font en temps réel ou presque : chaque commentaire ou question appelle une réponse quasi immédiate, et dans la précipitation, il peut arriver que le salarié, par erreur, transmette à des destinataires non autorisés des informations confidentielles relatives à des clients ou des collègues. De plus, contrairement au courrier classique, les messages électroniques sont rédigés spontanément, au fur et à mesure que les idées viennent : les règles de politesse et de bienséance sont souvent oubliées et le ton n'est pas toujours mesuré, si bien que leurs destinataires – visés ou non – peuvent parfois se sentir agressés.

Bref, l'utilisation illicite ou fautive de ces outils de communication peut être source de préjudice pour autrui et donner lieu à des actions en réparation, soit directement contre le salarié fautif, soit contre son employeur. Or, si la responsabilité de l'auteur des actes dommageables ne pose aucune difficulté, la question se pose de savoir si et dans quelle mesure l'employeur doit assumer la responsabilité des agissements frauduleux de ses salariés. Il serait donc intéressant de voir quels sont les fondements de la responsabilité de l'employeur (Section 1), quelles sont généralement les activités en ligne du salarié qui peuvent engager cette responsabilité (Section 2) et si l'employeur peut limiter sa responsabilité ou s'en exonérer (Section 3).

Section 1. Les fondements de la responsabilité civile de l'employeur

Se poser la question de la responsabilité dans le contexte des réseaux numériques revient à s'interroger sur l'identité de celui « qui répond de l'information circulant dans les réseaux »[255] et « ayant causé des conflits ou des dommages »[256]. Or, dans les

---

[255] Pierre TRUDEL, France ABRAN, Karim BENYEKHLEF et Sophie HEIN, avec la collab. de Mylène BEAUPRÉ, Luc BOUCHER, Martin MICHAUD, François OUELLETTE, Serge PARISIEN, François THÉMENS et Véronique WATTIEZ-LAROSE, *Droit du cyberespace*, Montréal, Éditions Thémis, 1997, p. 5-1.

[256] *Id.*

environnements électroniques, les acteurs ne sont pas toujours identifiables ou peuvent se trouver hors d'atteinte[257]. La question se pose avec encore plus d'acuité en entreprise où, même lorsque l'adresse IP de l'ordinateur ayant servi à la commission d'un acte dommageable désigne une organisation, il n'est pas toujours aisé de déterminer qui, au sein de cette dernière, en est le véritable auteur.

Les risques de responsabilité de l'employeur du fait de ses salariés peuvent être de nature pénale ou civile, certains comportements pouvant donner ouverture aux deux régimes. Ainsi, la détention et la diffusion de matériel de pornographie juvénile constituent une infraction criminelle[258]; cependant, de tels agissements peuvent également causer un préjudice à la victime qui serait alors fondée à demander réparation.

La question de la responsabilité pénale ne sera pas développée dans la présente étude; il est toutefois utile de préciser que les personnes morales, tout comme les personnes physiques, peuvent engager leur responsabilité sur le plan pénal. Ce régime est prévu par l'article 2 du *Code criminel*. La Cour suprême du Canada a, de son côté, précisé, dans *R.* c. *Canadian Dredge and Dock Co.*[259], que les personnes morales et les personnes physiques sont sur le même pied d'égalité face à une infraction. Cependant, la mise en œuvre d'une telle responsabilité présente certaines difficultés en raison, d'une part, de la nécessité de l'existence d'un texte de loi incriminant un comportement (en vertu de l'adage « nullum crimen sine lege »)[260] et, d'autre part, de l'exigence de l'élément moral (« mens rea ») pour certaines infractions[261].

---

[257] *Id.*, p. 5-13.

[258] *Code criminel*, art. 163.1.

[259] [1985] 1 R.C.S. 662, 673.

[260] Jean-Louis BAUDOUIN et Patrice DESLAURIERS, « Introduction générale », dans *La responsabilité civile, Volume I – Principes généraux*, 7e édition, 2007, *Droit civil en ligne* (DCL), EYB2007RES1, n° 1.76.

[261] P. TRUDEL et al., préc., note 255, p. 5-23.

Pour ce qui concerne la responsabilité civile de l'employeur, elle pourrait être recherchée en raison de sa qualité soit de commettant du salarié fautif (1.1.) soit d'intermédiaire technique (1.2.).

1.1. La responsabilité civile du commettant

Si les risques juridiques liés à l'utilisation de l'Internet et des réseaux numériques par les salariés se caractérisent par leur nouveauté, ils restent cependant régis par le droit commun de la responsabilité civile[262] : la victime peut, outre la responsabilité personnelle du préposé, rechercher également celle l'employeur, en vertu des règles de la responsabilité pour autrui. Le rôle des tribunaux est alors d'interpréter et d'adapter les principes existants au contexte des NTIC. À cet égard, l'article 1457 C.c.Q. rend le salarié responsable du préjudice causé par sa faute personnelle à un tiers, tandis que l'article 1463 C.c.Q. oblige l'employeur à réparer le préjudice causé par la faute de ses préposés dans l'exécution de leurs fonctions. Il reste à savoir si et dans quelle mesure les juges vont admettre la responsabilité de l'entreprise du simple fait d'une utilisation inappropriée des outils électroniques professionnels par le salarié.

L'employeur peut tout d'abord être poursuivi en raison de sa faute personnelle, telle que définie à l'article 1457 C.c.Q. La victime peut en effet tenter de démontrer qu'une faute distincte et propre au commettant a contribué à la réalisation du préjudice[263]. Une telle faute pourra, notamment, résulter d'un certain laxisme dans la surveillance du préposé, de la tolérance face à des agissements dommageables répétés ou même d'une carence de l'employeur à fournir la formation appropriée[264]. En effet, dans le cadre des

---

[262] N. IVALDI et P. VINCENT, préc., note 11.

[263] Alicia SOLDEVILA, La responsabilité pour le fait ou la faute d'autrui et pour le fait des biens, dans *Responsabilité*, Collection de droit 2007-2008, vol. 4, École du Barreau du Québec, 2007, *Droit civil en ligne* (DCL), EYB2007CDD89, p. 17.

[264] *Id.*

communications électroniques, la faute « en sera généralement une d'omission et non d'action, alors que l'intermédiaire aura manqué à une obligation de diligence »[265].

Toutefois, selon certains auteurs, un employeur ne peut être poursuivi sur le fondement de l'article 1457 C.c.Q. uniquement en raison de ses carences ou omissions à exercer une surveillance adéquate de l'utilisation d'Internet. Ainsi, Sophie Rompré avance que le défaut de prévenir ou de faire cesser le harcèlement psychologique au travail ne peut être considéré comme une faute directe de l'employeur et ne peut donner lieu qu'à un recours de la victime contre ce dernier en vertu du régime de responsabilité du commettant[266]. L'auteure conclut que le même raisonnement devrait être appliqué à l'utilisation fautive d'Internet au travail, si bien que « [l]a négligence ou le défaut de l'employeur d'assurer un contrôle adéquat de l'utilisation d'Internet ne devrait […] être qu'un facteur pris en considération par les tribunaux dans l'évaluation de la faute de l'employeur »[267].

La responsabilité de l'employeur peut ensuite être recherchée en raison des faits commis par son salarié. Cette responsabilité est le corollaire du pouvoir disciplinaire de l'employeur[268]. L'exercice de ce pouvoir est généralement une faculté, mais peut dans certaines hypothèses, comme le harcèlement sexuel entre salariés, constituer « une obligation à charge du chef d'entreprise »[269].

La responsabilité du commettant est « objective »[270], puisque la jurisprudence a interprété les dispositions du *Code civil du Bas-Canada*[271], puis celles du nouveau Code civil[272]

---

[265] P. TRUDEL et al., préc., note 255, p. 5-17.

[266] S. ROMPRÉ, préc., note 180, p. 26.

[267] *Id.*

[268] Jean-Louis BAUDOUIN et Patrice DESLAURIERS, « La responsabilité des commettants », dans *La responsabilité civile, Volume I – Principes généraux*, 7e édition, 2007, *Droit civil en ligne* (DCL), EYB2007RES10, n° 1-757.

[269] A. MAZEAUD, préc., note 223, p. 89

[270] J.-L. BAUDOUIN et P. DESLAURIERS, « La responsabilité des commettants », préc., note 268, n° 1-749 et 1-754.

[271] *Code civil du Bas-Canada*, art. 1054.

[272] *Code civil du Québec*, art. 1463.

comme instaurant à l'égard de l'employeur une présomption irréfragable dont il ne peut se dégager simplement en prouvant l'absence de comportement fautif[273].

S'il est certain que sur le plan social, la responsabilité du commettant repose sur la volonté d'indemniser la victime, son fondement juridique est difficile à cerner, même s'il n'est pas vraiment remis en question[274]. Les arguments suivants ont, notamment, été avancés : la faute du commettant dans le choix de son préposé ou dans sa surveillance, le risque que le commettant doit assumer en contrepartie du profit qu'il tire de l'activité du préposé[275]. En définitive, ce fondement juridique repose, comme pour tous les cas de responsabilité du fait d'autrui, sur la notion de garde décrite comme suit :

> « La garde, au sens large du terme (c'est-à-dire le pouvoir de surveillance et de contrôle sur autrui), reste le fondement juridique de la responsabilité pour le fait d'autrui. […]. Ce droit de contrôle emporte un pouvoir de supervision ou de surveillance, et donc une responsabilité pour le préjudice causé au tiers lorsqu'il y a manquement. La dépendance du mineur à l'égard du titulaire de l'autorité parentale, du préposé à l'égard de son patron, permet, en effet, de présumer qu'un exercice diligent et adéquat de leur pouvoir de surveillance et de contrôle aurait pu permettre d'empêcher le fait qui a causé le dommage. En ce sens, la responsabilité n'est pas à proprement parler une responsabilité du fait d'autrui, mais une responsabilité de son propre fait. Bien que le commettant ou les parents n'aient pas eux-mêmes matériellement causé le dommage, leur responsabilité est retenue parce que leur défaut de surveillance ou de contrôle est présumé, soit de façon complète, soit sous réserve d'une preuve contraire, avoir été la cause du préjudice subi par la victime. »[276]

À ce jour, il y a peu de décisions québécoises relatives à la responsabilité de l'employeur du fait de l'utilisation inadéquate de ses outils informatiques. Cela s'explique peut-être en partie par le fait qu'il est devenu relativement rare de voir la responsabilité du commettant

---

[273] J.-L. BAUDOUIN et P. DESLAURIERS, « La responsabilité des commettants », préc., note 268, n° 1-754.

[274] A. SOLDEVILA, préc., note 263, p. 18.

[275] *Id.*, p. 17-18.

[276] J.-L. BAUDOUIN et P. DESLAURIERS, « La responsabilité des commettants », préc., note 268, n° 1-670.

évoquée devant les tribunaux[277]. Cependant, en raison de la banalisation de la cybercriminalité – même en milieu de travail – et de la difficulté, parfois, à remonter jusqu'aux auteurs des actes dommageables commis avec les moyens fournis par l'entreprise, il ne faut pas négliger la possibilité d'une recrudescence des actions en réparation mettant en cause l'employeur.

Les tribunaux semblent être réticents à admettre la responsabilité de l'employeur du seul fait d'un usage inapproprié des moyens de communication par les salariés. Ainsi, dans l'affaire *Lemay* c. *Dubois*[278], une salariée poursuivait une collègue pour harcèlement, diffamation et violation de son droit au respect de la vie privée. L'employeur avait été appelé en instance à titre de codéfendeur solidaire. La plaignante reprochait à sa collègue d'avoir publié, sur un site Internet public, des informations de nature privée. Ces informations avaient été divulguées dans un communiqué annonçant la date de diffusion d'un reportage sur l'entreprise que la défenderesse avait réalisé. Aussi la plaignante soutenait que ces actes avaient été accomplis par leur auteur dans le cadre de son travail, ce qui engageait la responsabilité de l'employeur. La Cour du Québec a, certes, reconnu que la préposée agissait bien dans l'intérêt et au profit de l'employeur lorsqu'elle avait rencontré la plaignante pour la réalisation du reportage; toutefois, elle a rejeté la demande au motif que :

> « cela est insuffisant pour conclure qu'elle agissait dans l'intérêt ou le bénéfice de son employeur lorsqu'elle a choisi de publier, sur un site Internet public, un avis de diffusion comprenant des informations violant le droit de cette dernière au respect de sa vie privée »[279].

Quant aux autres faits reprochés, soit l'envoi et la publication de messages hostiles ou préjudiciables à la vie privée de la plaignante, le Tribunal a considéré que :

---

[277] *Id.*, n° 1-743.

[278] 2005 CanLII 15315 (QC C.Q.)

[279] *Id.*

> « le seul fait que [la salariée] les ait envoyés à certaines occasions au moyen d'un ordinateur appartenant à [l'employeur était] insuffisant pour permettre au Tribunal de conclure qu'elle agissait dans l'exécution de ses fonctions »[280].

Une solution similaire a été adoptée dans la décision albertaine *Inform Cycle Ltd.* v. *Rebound Inc.*[281]. Dans cette affaire, la société *Inform Cycle* poursuivait un ex-employé et *Rebound Inc.* – son nouvel employeur – pour avoir utilisé son nom pour créer un site Internet qui avait ensuite été redirigé vers un site de pornographie homosexuelle. L'employé était persuadé que son employeur lui devait une somme d'argent (1500 dollars) et espérait la récupérer en lui revendant ce nom de domaine. Bien que le salarié ait utilisé son ordinateur portable personnel pour enregistrer « www.informcyle.com » comme nom de domaine, il avait effectué ces démarches en utilisant la connexion Internet de son nouvel employeur et avait confirmé l'enregistrement en utilisant à la fois un téléphone et un ordinateur appartenant à *Rebound*. Dans un premier temps, l'employé avait redirigé ce site Internet vers le site de *Rebound*, puis l'avait réacheminé vers un site homosexuel alors qu'il s'apprêtait à partir en vacances. L'argument principal d'*Inform* était que *Rebound* n'avait pas de politique relative à l'utilisation d'Internet et accordait une grande autonomie à son employé. *Inform* avançait également que *Rebound* avait bénéficié des agissements de son employé, puisque les deux sociétés sont concurrentes. Cet argument n'a pas été retenu par la Cour du banc de la reine qui a conclu que le préjudice d'*Inform* résultait uniquement des actes de son ex-employé, qui avait agi pour son propre compte et dans son seul intérêt, et ce, à l'insu de son nouvel employeur. En effet, rien dans la preuve n'étayait la thèse selon laquelle la création du site Internet et le réacheminement de ses visiteurs vers un site pornographique étaient reliés de quelque façon que ce soit aux tâches de l'employé chez *Rebound* ou que ces activités étaient effectuées au profit de l'employeur. La responsabilité de commettant de la société *Rebound* n'a donc pas été retenue.

---

[280] *Id.*

[281] 2007 ABQB 319 (CanLII).

Inform recherchait également la responsabilité personnelle de l'employeur et des gérants de *Rebound*, notamment, en raison de leur incapacité à désactiver immédiatement le lien litigieux : il avait, en effet, fallu cinq jours pour découvrir qui était l'auteur du site et joindre l'intéressé sur son lieu de vacances afin d'obtenir les codes permettant d'accéder à son compte pour effectuer cette désactivation. De plus, une fois le lien neutralisé, le site www.informcycle.com avait été redirigé, pendant quelques jours, vers le site Internet de *Rebound*. S'agissait-il d'un détournement effectué de façon délibérée ou était-ce juste la conséquence de la désactivation? Rien n'était certain. Quoi qu'il en soit, la Cour, tout en reconnaissant que le moyen n'était pas sans fondement, ne l'a pas retenu à ce stade.

En somme, d'après ces deux décisions, l'employeur ne peut être tenu responsable des dommages causés par un employé en cas d'utilisation fautive des NTIC lorsque celle-ci est faite pour le bénéfice exclusivement personnel de ce salarié[282].

Sur ce point, la jurisprudence française a opéré une évolution intéressante. Dans un premier temps, elle s'est montrée réticente à admettre la responsabilité de l'employeur du seul fait d'un usage inapproprié des moyens de communication par ses salariés[283]. Le Tribunal de grande instance de Lyon a ainsi écarté la responsabilité d'une entreprise après avoir relevé que le salarié auteur des agissements dommageables avait agi à l'insu de son employeur et que les actes commis étaient étrangers à l'exercice de ses fonctions[284]. Le salarié fautif avait intentionnellement saturé la bande passante de son ex-employeur pour se venger de son manque de reconnaissance. Sa responsabilité a été reconnue tant sur le plan pénal que civil, tandis que celle de l'employeur a été écartée.

Toutefois, les juges français ont finalement admis la responsabilité de l'employeur du fait de l'usage inapproprié des outils professionnels par ses préposés. Dans l'affaire *Lucent*

---

[282] S. ROMPRÉ, préc., note 180, p. 23.

[283] X. LEMARTELEUR, préc., note 17, p. 49.

[284] Trib. gr. inst. Lyon, 20 févr. 2001, *Gaz. Pal.*, 2001.2.somm.1686, note Alain Blanchot.

Technologies[285], un salarié de la société Lucent, avait créé à son domicile un site Internet satirique, dénommé « escroca.com », dénonçant les abus supposés de la société *Escota*, concessionnaire d'un réseau d'autoroutes en France, vis-à-vis des usagers. Il avait ensuite procédé anonymement à la mise en ligne de ce site depuis son poste de travail. La société *Escota* avait alors assigné l'auteur du site, l'employeur de ce dernier, ainsi que l'hébergeur. La Cour d'appel d'Aix-en-Provence, confirmant les juges de première instance[286], a condamné le salarié pour contrefaçon de marques et l'employeur du fait des fautes commises par son salarié. Quant à l'hébergeur, sa responsabilité n'a pas été retenue.

Pour retenir la responsabilité de l'entreprise, conformément à l'article 1384, alinéa 5 du Code civil, les juges ont relevé que l'employeur avait mis à la disposition de ses salariés, y compris l'auteur du site incriminé, un ordinateur connecté à Internet. Par ailleurs, le salarié fautif était technicien de tests dans cette entreprise œuvrant dans le domaine de la construction d'équipements et de systèmes de télécommunication et l'usage quotidien de ces outils de communication entrait dans le cadre de ses fonctions. De plus, les juges ont relevé que le directeur des ressources humaines de l'entreprise avait émis une note autorisant les salariés à utiliser les équipements informatiques et les accès au réseau mis à leur disposition pour consulter des sites pouvant ne présenter aucun lien direct avec leur activité au sein de la société et ceci dès lors que ces utilisations demeuraient raisonnables, s'effectuaient en dehors des heures de travail et respectaient les dispositions légales applicables. Les juges ont considéré que l'entreprise n'avait émis aucune interdiction spécifique quant à l'éventuelle réalisation de sites Internet ou la gestion des pages

---

[285] Aix-en-Provence, 13 mars 2006, en ligne : <http://www.legalis.net/jurisprudence-decision.php3?page=jurisprudence-decision&id_article=1611> (site consulté le 30 juillet 2010); Voir également Aix-en-Provence, 17 janv. 2005, en ligne : <http://www.foruminternet.org/telechargement/documents/ca-aix20050117.pdf> (site consulté le 30 juillet 2010) qui confirme le licenciement pour faute grave d'un salarié, pour avoir porté atteinte à l'image de son employeur en créant, à l'insu de ce dernier, un site Internet humoristique alors que le règlement intérieur de l'entreprise interdisait l'usage du matériel de l'employeur à des fins personnelles. Le préjudice ainsi subi par l'entreprise était d'autant plus grave que l'auteur du blogue ne s'identifiait pas sur le site.

[286] Trib. gr. inst. Marseille, 11 juin 2003, en ligne : <http://www.legalis.net/jurisprudence-decision.php3?page=breves-article&id_article=234> (site consulté le 30 juillet 2010).

personnelles. En conséquence, ils en ont déduit que la faute du salarié avait été commise dans le cadre de ses fonctions.

En clair, l'employeur doit déterminer de manière très précise et sans équivoque l'utilisation qui peut être faite des ressources informatiques qu'il met à la disposition de ses salariés.

Certains ont critiqué cette décision au motif qu'elle contribuait à aggraver la situation de l'employeur qui offre un accès Internet à ses employés, en lui imposant des obligations supplémentaires[287]. En effet, si l'entreprise peut, techniquement, être assimilée à un fournisseur d'accès Internet, en pratique, elle répond néanmoins à des impératifs différents en matière de responsabilité[288]. Une chose est certaine, c'est que l'interprétation de la qualité de fournisseur d'accès Internet de l'entreprise par la jurisprudence « rejaillit » forcément sur le régime de la responsabilité qui lui est applicable[289].

1.2. L'employeur, un simple prestataire de service Internet?

Lorsque les entreprises offrent un accès à l'Internet à leur personnel, elles agissent, techniquement, comme des fournisseurs de services. Cependant, elles ne bénéficiaient pas des mêmes exonérations de responsabilité que ces derniers. Toutefois, la théorie de « l'employeur-fournisseur » d'accès a été appliquée par la jurisprudence française dans l'affaire qui a opposé *SA BNP Paribas* à la société *World Press Online* (ci-après citée : « WPO »)[290]. Des courriers électroniques mensongers annonçant la fermeture de la société WPO avaient été envoyés depuis une adresse *Yahoo*. Or, ces messages avaient incité certains partenaires d'affaires de WPO à mettre fin à leurs relations commerciales. WPO

---

[287] Eric A. CAPRIOLI, « La qualité de fournisseur d'accès à l'internet : un nouveau risque juridique pour l'entreprise », Caprioli-avocats.com, Juin 2005, en ligne : <http://www.caprioli-avocats.com/donnees-perso/88-fournisseur-acces-internet> (site consulté le 19 août 2010).

[288] X. LEMARTELEUR, préc., note 17, p. 52.

[289] FORUM DES DROITS SUR L'INTERNET, *Relations du travail et internet. Panorama législatif et jurisprudentiel*, 2006, p. 9, en ligne : <http://www.foruminternet.org/telechargement/documents/dossier-travail-20060126.pdf> (site consulté le 26 juin 2010).

[290] Paris, 5 févr. 2005, en ligne : <http://www.foruminternet.org/telechargement/documents/ca-par20050204.pdf> (site consulté le 30 juillet 2010).

avait alors diligenté une enquête auprès du fournisseur de l'adresse électronique afin d'obtenir l'adresse IP de leur expéditeur. L'adresse obtenue correspondait à celle d'un poste d'ordinateur installé dans les locaux de la banque *BNP Paribas*. WPO somma donc la banque de lui communiquer les données de nature à permettre l'identification de l'auteur des messages. Devant l'inertie de *BNP Paribas*, WPO assigna la banque en référé pour obtenir ces informations. Les juges de première instance avaient ordonné à la banque de communiquer l'identité ainsi que toute information de nature à permettre l'identification de l'expéditeur du message. Cette ordonnance a été partiellement confirmée en appel, puisque la Cour d'appel de Paris énonce sans ambiguïté que :

> « la demande de la société ne se heurte à aucune contestation sérieuse alors qu'en sa qualité, non contestée, de prestataire technique […], la banque est tenue, […], d'une part, de détenir et de conserver les données de nature à permettre l'identification de toute personne ayant contribué à la création d'un contenu des services dont elle est prestataire et, d'autre part, à communiquer ces données sur réquisition judiciaire ».[291]

Cependant, la Cour d'appel atténue son ordonnance en précisant que la loi n'impose pas à la banque « de traiter les données qu'elle doit conserver et communiquer ni de procéder elle-même à l'identification de l'auteur du message litigieux ».

La question essentielle était alors de savoir quelle était la véritable portée de cette décision pour les entreprises qui fournissent un accès Internet à leurs salariés : venait-elle assouplir la position de l'employeur en le faisant bénéficier de la responsabilité allégée des prestataires de services Internet ou, au contraire, consolider ses obligations en maintenant sa responsabilité de commettant, mais avec un devoir de surveillance renforcé sur ses préposés?

Reconnaître à l'entreprise la qualification juridique de fournisseur d'accès à l'Internet aurait des conséquences non négligeables pour les employeurs, dans la mesure où ces

---

[291] *Id.*

derniers pourraient désormais être assujettis au régime de responsabilité limitée dont bénéficient les prestataires de services Internet, en contrepartie, cependant, de la conservation des traces des usagers de leur réseau pendant une période minimale d'un an[292]. L'étendue de leurs obligations à cet égard constitue une grande source d'inquiétude pour les entreprises, car cela implique qu'elles devront disposer de moyens nécessaires pour conserver de telles données, ce qui risque de poser quelques difficultés à certaines organisations[293]. Mais les employeurs craignent surtout de voir leur responsabilité civile, voire pénale, engagée en l'absence de journal des connexions[294], ce qui peut paraître excessif dans la mesure où leur activité de fournisseur d'accès à l'Internet est négligeable, ce service n'étant offert qu'à leurs collaborateurs en interne et à des fins non commerciales[295]. Aussi pour certains auteurs, imposer aux entreprises une obligation de conservation des données en raison de la fourniture d'un accès Internet à leurs salariés ne reflète pas la réalité juridique[296].

Il est à noter que, pour être exonéré de sa responsabilité, il ne suffit pas à l'employeur-fournisseur d'accès de détenir et conserver les données de connexion de ses salariés : il faut également que les données fournies permettent l'identification effective de l'auteur des faits dommageables. La société *Tiscali Média* s'est ainsi vue reprocher sa négligence quant aux données pour le moins fantaisistes qu'elle avait communiquées concernant un abonné qui s'était livré à des actes de contrefaçon grâce le réseau[297]. Les éditeurs de bandes dessinées victimes de ces agissements souhaitaient exercer une action en réparation contre leur auteur et avaient sommé *Tiscali* de leur fournir ses coordonnées. Les informations qui leur avaient

---

[292] E. A. CAPRIOLI, « La qualité de fournisseur d'accès à l'internet : un nouveau risque juridique pour l'entreprise », préc., note 287.

[293] FORUM DES DROITS SUR L'INTERNET, *Relations du travail et internet. Panorama législatif et jurisprudentiel*, préc., note 289, p. 10.

[294] *Id.*

[295] E. A. CAPRIOLI, « La qualité de fournisseur d'accès à l'internet : un nouveau risque juridique pour l'entreprise », préc., note 287.

[296] *Id.*

[297] Civ. 1re, 14 janv. 2010, *Bull. civ.* I, n° 8.

alors été communiquées étaient les suivantes : Nom : Bande; Prénom : Dessinée; Date de naissance : 25/03/1980; Adresse : Rue de la BD; Code postal : 1000; Ville : Bruxelles; Adresse email de confirmation : pitbullteam@hotmail.com. Ces informations n'étant pas de nature à permettre l'identification de l'auteur du site litigieux, les sociétés victimes se sont retournées contre *Tiscali*. Cette dernière soutenait que sa responsabilité ne pouvait pas être recherchée, car elle n'avait qu'un rôle technique de fournisseur d'hébergement et n'exerçait pas de fonction éditoriale sur les pages personnelles litigieuses dont elle ne concevait ni ne contrôlait le contenu. La Cour de cassation n'a pas été convaincue par ce raisonnement et a jugé que le fait, pour *Tiscali*, d'héberger les pages personnelles créées par ses abonnés, tout en offrant aux annonceurs la possibilité de mettre en place des espaces publicitaires payants, directement sur ces pages, excédait « les simples fonctions techniques de stockage »[298]. La Cour a estimé que, dès lors que *Tiscali* exploitait commercialement son site Internet, elle devait être considérée comme ayant la qualité d'éditeur, de sorte qu'elle ne pouvait invoquer le bénéfice du régime de responsabilité allégé. Par conséquent, les actes de contrefaçon, dont avaient été victimes les sociétés plaignantes, ont été imputés à *Tiscali*, qui a été condamnée à des dommages-intérêts en lieu et place du véritable auteur des contenus litigieux.

Cette reconnaissance de la responsabilité de *Tiscali*, a créé un vif émoi parmi les hébergeurs de pages personnelles qui se rémunèrent avec la publicité et qui, jusqu'alors, bénéficiaient d'une responsabilité allégée[299]. Toutefois, dans une décision rendue quelques mois plus tard, la Cour d'appel de Paris semble vouloir réduire la portée de cet arrêt et circonscrire ce régime de responsabilité aggravée aux seuls fournisseurs d'hébergement offrant aux annonceurs la possibilité de placer des espaces publicitaires directement sur les

---

[298] *Id*.

[299] Voir notamment Paris, 14 av. 2010 : Juritel n° JTL KTK421CA–Internet, en ligne : <http://www.juritel.com/Ldj_html-1478.html> (site consulté le 30 juillet 2010), confirmant la décision de première instance qui avait rejeté la qualité d'éditeur de la société *Dailymotion*, car cette dernière commercialisait des espaces publicitaires, mais n'était pas à l'origine des contenus diffusés, ceux-ci étant fournis par les utilisateurs eux-mêmes.

pages personnelles des internautes[300]. Dans cette affaire, la société *Dailymotion*, dont la responsabilité était recherchée, exploitait bien un site commercialisant des espaces publicitaires; toutefois, seules les pages d'accueil et les cadres standards d'affichage de son site étaient ouverts aux annonceurs, à l'exclusion des pages personnelles des utilisateurs. La Cour a jugé que cette activité n'excluait pas la qualité d'intermédiaire technique dès lors qu'il n'était pas établi que *Dailymotion* disposait d'une capacité d'action sur les contenus mis en ligne.

Appliquée à l'employeur, la solution de l'arrêt *Tiscali* aurait pour conséquence d'engager la responsabilité de ce dernier lorsqu'il est dans l'impossibilité de fournir les renseignements permettant d'identifier de façon certaine le salarié auteur d'un contenu litigieux[301]. Or, relativement aux agissements fautifs de ses salariés, l'employeur est souvent confronté à une difficulté de taille : l'administration de la preuve. Il peut en effet arriver que l'on ne puisse pas identifier de façon certaine l'auteur d'un acte commis à l'aide d'un ordinateur : ce sera notamment le cas lorsque plusieurs personnes ont techniquement la possibilité d'accéder au même poste de travail pendant le même quart de travail. Ainsi, dans *Belisle* c. *Rawdon (Municipalité)*[302], la preuve a démontré que plusieurs personnes pouvaient avoir accès à l'ordinateur du plaignant, l'hypothèse d'un utilisateur extérieur n'étant pas exclue. La confusion peut aussi résulter d'une usurpation d'identité : les actes de piratage visant les adresses électroniques, personnelles ou professionnelles, et s'accompagnant de l'usurpation de l'identité de l'ordinateur émetteur ont en effet tendance à se banaliser[303].

---

[300] *Id.*

[301] E. A. CAPRIOLI, « La qualité de fournisseur d'accès à l'internet : un nouveau risque juridique pour l'entreprise », préc., note 287.

[302] Préc., note 204.

[303] Henri PESCHAUD, « Cyberpreuve de l'identité de l'auteur d'un courriel antisémite », Legalbiznext.com, 05 juillet 2004, en ligne : <http://www.legalbiznext.com/droit/Cyberpreuve-de-l-identite-de-l> (site consulté le 19 août 2010); Voir également *Carrier* c. *Centre local de développement (CLD) des Etchemins*, 2005 QCCRT 183 (CanLII); Trib. gr. inst. Carcassonne, 16 juin 2006, en ligne : <http://www.legalis.net/breves-article.php3?id_article=1645> (site consulté le 30 juillet 2010).

L'état actuel de la jurisprudence française semble donc montrer une opposition entre les régimes de responsabilité des prestataires de l'Internet et celui du commettant et, en l'absence d'une position claire de la Cour de cassation, « le débat reste ouvert entre l'irresponsabilité et la responsabilité de principe »[304]. Il semblerait, néanmoins, que la responsabilité de l'employeur demeure[305], et cela, pour une raison essentielle : l'entreprise a une obligation générale de surveiller les informations qu'elle traite et demeure responsable des fautes commises par ses préposés pendant leur temps de travail, en vertu de l'article 1384 alinéa 5 du Code civil[306]. Par conséquent, celui qui subit un préjudice du fait des agissements illicites d'un salarié sera fondé, une fois ce dernier identifié, à agir en réparation non seulement contre le salarié indélicat, mais également contre son employeur[307]. De plus, les juges ont tendance à rechercher largement cette responsabilité : ils considèrent en effet que, dès lors que le salarié agit sur le lieu de son travail, pendant le temps et à l'occasion de celui-ci, il n'agit pas hors du cadre de ses fonctions et engage par conséquent la responsabilité de son commettant[308]. Ce mouvement est encore plus sensible lorsqu'il s'agit de l'utilisation fautive du matériel informatique et électronique par les salariés. La jurisprudence récente semble en effet considérer que, non seulement l'employeur a le pouvoir, mais qu'il a également le devoir de prendre les mesures nécessaires pour garantir la sécurité et une utilisation conforme aux lois de son système informatique[309]. Cela devrait inciter les employeurs à la plus grande prudence et les pousser à encadrer de façon très stricte l'utilisation des outils de communication électroniques par leurs salariés.

---

[304] FORUM DES DROITS SUR L'INTERNET, *Relations du travail et internet. Panorama législatif et jurisprudentiel*, préc., note 289, p. 10.

[305] *Id.*, p.47.

[306] E. A. CAPRIOLI, « La qualité de fournisseur d'accès à l'internet : un nouveau risque juridique pour l'entreprise », préc., note 287.

[307] *Id.*

[308] B. POIDEVIN, « Quelle responsabilité en matière de sécurité informatique? », préc., note 56.

[309] J.-P. DE LONGEVIALLE, préc., note 1; Isabelle RENARD, « Les droits et devoirs des entreprises », Lejournaldunet.com, Mars 2004, en ligne : <http://www.journaldunet.com/management/dossiers/040331acces/renard.shtml> (site consulté le 19 août 2010).

Au Québec, le débat autour de la qualité de fournisseur d'accès Internet de l'employeur n'a pas eu lieu. Cependant, avant que la loi ne prévoie des dispositions spécifiques sur la responsabilité des prestataires de services, certains s'étaient interrogés sur la possible extension du régime de la responsabilité pour le fait d'autrui aux intermédiaires des réseaux électroniques[310]. Une telle analyse semble, toutefois, se heurter à l'interprétation restrictive du régime de responsabilité faite par la doctrine québécoise. Il avait en effet été admis, sous l'empire du *Code civil du Bas-Canada*, que l'énumération des cas de responsabilité pour le fait d'autrui de l'article 1054 était limitative et que le régime particulier de cet article ne pouvait être étendu par analogie[311]. Cette analyse semble devoir être maintenue avec le nouveau Code civil[312]. De plus, le législateur est venu « exclu[re] l'obligation de surveillance active pour les intermédiaires »[313] dans le domaine particulier des technologies de l'information. Ainsi, l'article 22 de la *Loi concernant le cadre juridique des technologies de l'information*, qui régit l'hébergement – activité à laquelle l'intervention de l'employeur dans le réseau est généralement rapprochée – prévoit que :

> « Le prestataire de services qui agit à titre d'intermédiaire pour offrir des services de conservation de documents technologiques sur un réseau de communication n'est pas responsable des activités accomplies par l'utilisateur du service au moyen des documents remisés par ce dernier ou à la demande de celui-ci. »[314]

Par conséquent, le prestataire qui ne surveille pas les contenus diffusés sur son réseau ou qui ne cherche pas à détecter les situations susceptibles d'indiquer que des documents permettent la réalisation d'activités illicites ne commet pas de faute[315]. Cette absence de responsabilité repose sur le fait que le prestataire de service n'exerce aucun contrôle en

---

[310] P. TRUDEL et al., préc., note 255, p. 5-19.

[311] Jean-Louis BAUDOUIN, *La responsabilité civile délictuelle*, 3e éd., Cowansville, Éditions Yvon Blais, 1990, n° 399, p. 319-320.

[312] P. TRUDEL et al., préc., note 255, p. 5-19.

[313] Pierre TRUDEL, « La responsabilité des acteurs du commerce électronique » dans Vincent GAUTRAIS (dir.), *Droit du commerce électronique*, Montréal, Éditions Thémis, 2002, p. 607, n° 32, à la page 623.

[314] Préc., note 50, art. 22 al. 1.

[315] P. TRUDEL, « La responsabilité des acteurs du commerce électronique », préc., note 313, n° 33, p. 623.

amont sur l'information diffusée à travers son réseau[316]. Ce régime vise aussi bien l'hébergeur, l'archiveur, le transporteur ou tout autre intermédiaire qui fournit des services sur un réseau de communication ou qui conserve ou transporte des documents technologiques[317].

Bien que cette notion de contrôle ne soit pas clairement identifiée par les lois, elle est mentionnée dans plusieurs décisions de justice[318] et sert, notamment, à déterminer les responsabilités des divers acteurs vis-à-vis des documents circulant dans un réseau[319]. Le critère est alors celui de l'intensité du contrôle, puisque « [p]lus on a le contrôle sur un document, plus on en répond »[320]. Le contrôle « serait même un pré-requis à l'imputation de toute responsabilité »[321], comme le souligne Henry H. Perritt :

> « In all three categories of tort liability (defamation, copyright infringement and invasion of privacy), the requisite fault cannot be proven without showing either that the actor and potential tort feasor exercised **some actual control** over content or that it was feasible for it to control content and that it could foresee the possibility of harm **if it did not control content**. »[322]

---

[316] Pierre TRUDEL, « La responsabilité civile : qui répond de l'information? » dans Michel RACICOT, Mark S. HAYES, Alec R. SZIBBO et Pierre TRUDEL, *L'espace cybernétique n'est pas une terre sans loi. Étude des questions relatives à la responsabilité à l'égard du contenu circulant sur Internet*, Ottawa, Industrie Canada, 1997, p. 135, à la page 180.

[317] P. TRUDEL, « La responsabilité des acteurs du commerce électronique », préc., note 313, n° 33, p. 624.

[318] Vincent GAUTRAIS et Pierre TRUDEL, *Circulation des renseignements personnels et Web 2.0*, Montréal, Éditions Thémis, 2010, p. 59. Ces auteurs mentionnent notamment les décisions suivantes, pour illustrer les situations permettant de « déterminer si des documents détenus par une Administration devaient être qualifiés comme étant sous le contrôle d'une autorité soumise à la législation relative au droit d'accès » : *Commissaire à la protection de la vie privée* c. *Conseil canadien des relations de travail*, 2000 CanLII 15487 (C.A.F.), en ligne : <http://www.canlii.org/fr/ca/caf/doc/2000/2000canlii15487/2000canlii15487.html> (cité à la page 60) et *Dhont* c. *Minister of Education et al*, 2008 NWTSC 40, en ligne : <http://www.canlii.org/en/nt/ntsc/doc/2008/2008nwtsc40/2008nwtsc40.html> (cité à la page 61).

[319] *Id.*, p. 64.

[320] *Id.*, p. 71.

[321] *Id.*, p. 59-60.

[322] *Id.*, p. 65, citant Henry H. PERRITT JR., « Tort Liability, the First Amendment and Equal Access to Electronic Networks », (1992) 5 *Harvard J. of L. & Tech.* 65, 110-111 (les soulignements sont de Messieurs Gautrais et Trudel).

À cet égard, la *Loi concernant le cadre juridique des technologies de l'information*[323] permet de déterminer le moment à partir duquel un acteur du réseau devient responsable vis-à-vis d'un document. C'est notamment le moment de la prise de connaissance par l'intermédiaire des informations circulant dans son réseau qui constitue l'élément de bascule entraînant un renforcement de ses obligations[324]. Ainsi, l'article 22 de cette loi précise, en son deuxième alinéa, que le prestataire

> « peut engager sa responsabilité, notamment s'il a de fait connaissance que les documents conservés servent à la réalisation d'une activité à caractère illicite ou s'il a connaissance de circonstances qui la rendent apparente et qu'il n'agit pas promptement pour rendre l'accès aux documents impossible ou pour autrement empêcher la poursuite de cette activité »[325].

Cette prise de connaissance des faits illicites pourra avoir lieu à la suite du signalement d'un tiers, généralement à la suite d'un dommage lié à cette activité. Elle pourra aussi résulter de la surveillance par l'intermédiaire de son réseau.

Toutefois, le fait qu'un intermédiaire ait techniquement la possibilité de prendre connaissance des documents circulant dans son réseau n'entraîne pas automatiquement sa responsabilité vis-à-vis de ceux-ci : il suffit par exemple que l'utilisateur ait recours à des procédés permettant de déjouer le système de filtrage pour empêcher cette prise de connaissance. Or, la présomption de contrôle sur les informations diffusées doit être atténuée lorsqu'il s'agit de l'Internet où « chaque individu a la possibilité de devenir un fournisseur de contenu, et chaque intermédiaire de prendre part à cette diffusion »[326]. Aussi une majorité d'auteurs concluent qu'il est difficile d'imposer une responsabilité aux

---

[323] Préc., note 50.

[324] V. GAUTRAIS et P. TRUDEL, préc., note 318, p. 81.

[325] *Loi concernant le cadre juridique des technologies de l'information*, préc., note 50, art. 22 al. 2.

[326] P. TRUDEL et al., préc., note 255, p. 5-6.

fournisseurs de service alors que ceux-ci n'ont aucune possibilité de contrôle[327]. Les législateurs de plusieurs pays ont d'ailleurs adopté des dispositions allant dans ce sens[328].

Finalement, c'est le « contrôle accru » sur les documents qui pourra faire naître la responsabilité du prestataire à leur égard[329]. Ce sera le cas, par exemple, lorsque l'intermédiaire exerce une surveillance, « constante ou occasionnelle », du réseau qui lui permet d'avoir connaissance du caractère illicite des documents en circulation[330]. Il en ira de même si le prestataire est à l'origine de la transmission du document, s'il sélectionne les récipiendaires des messages circulant dans son réseau ou modifie le contenu de ces derniers[331]. Il exerce alors un contrôle « physique » sur ces documents qui vient augmenter sa responsabilité à leur égard[332].

Pour l'employeur, la connaissance des faits illicites pourra résulter de l'exercice d'une surveillance de ses réseaux numériques qui lui aura permis de déceler une activité suspecte ou de bloquer des contenus inappropriés. Cette capacité de contrôle lui confère un rôle actif, puisqu'il bénéficie, entre autres, de la possibilité :

- de sélectionner ou de modifier l'information du document, en supprimant par exemple les pièces jointes dont le contenu semble suspect. En agissant de la sorte, l'employeur exerce alors une fonction éditoriale puisqu'il devient celui qui prend la décision de faire circuler ou non le document[333];

---

[327] *Id.*

[328] Voir notamment *Communication Decency Act*, 47 U.S.C. (1996) (en particulier : § 230); *Digital Millennium Copyright Act*, 17 U.S.C. (1998); *Loi concernant le cadre juridique des technologies de l'information*, préc., note 50; *Loi n° 2004-575 pour la confiance dans l'économie numérique*, J.O. 22 juin 2004, p. 11168.

[329] V. GAUTRAIS et P. TRUDEL, préc., note 318, p. 83.

[330] P. TRUDEL, « La responsabilité des acteurs du commerce électronique », préc., note 313, n° 58, p. 632.

[331] V. GAUTRAIS et P. TRUDEL, préc., note 318, p. 83-84.

[332] *Id.*, p. 84.

[333] P. TRUDEL, « La responsabilité des acteurs du commerce électronique », préc., note 313, n° 85, p. 641.

- de ne pas délivrer le message à son destinataire. En opérant une telle sélection, l'employeur perd alors son rôle passif[334];
- de conserver le message pendant quelque temps, afin de l'expurger des virus ou de s'assurer qu'il ne contient pas de contenus illicites. En procédant à une telle interception, l'employeur perd également son rôle passif, puisqu'elle a la possibilité d'interrompre définitivement la circulation de ce message[335].

L'on pourrait alors être tenté de conclure que l'employeur qui ne possède aucun dispositif de contrôle et de surveillance des communications électroniques n'encourrait aucune responsabilité, sauf preuve de sa connaissance des faits litigieux et de son inaction après la découverte de tels faits. Une telle analyse viendrait, comme le note Nicolas W. Vermeys,

> « mettre en exergue le constat étrange selon lequel, en vertu de la Loi, il est préférable, pour un prestataire de services, de jouer à l'autruche plutôt que d'être vigilant et responsable s'il veut éviter toute responsabilité pour les contenus qu'il diffuse »[336].

Toutefois, lorsque ce prestataire est également l'employeur, il ne peut pas se permettre d'ignorer les activités qui se déroulent dans son réseau, car il conserve, comme indiqué précédemment, une obligation générale de surveillance et est soumis, en sa qualité de commettant, à un lourd fardeau[337].

De plus, les prestataires de services ne bénéficient pas d'une irresponsabilité totale, puisque leur responsabilité pourra être engagée, selon les principes du droit commun de la responsabilité, en cas de faute de leur part. Une telle faute pourra être retenue s'il est démontré que les agissements de l'intermédiaire ne correspondaient pas au comportement

---

[334] *Id*., n° 86, p. 641.

[335] *Id.*, n° 87, p. 642.

[336] Nicolas W. VERMEYS, « Chronique – Responsabilité civile et Web 2.0 », dans *Repères*, Juillet 2007, *Droit civil en ligne* (DCL), EYB2007REP607, p. 8.

[337] E. A. CAPRIOLI, « La qualité de fournisseur d'accès à l'internet : un nouveau risque juridique pour l'entreprise », préc., note 287; S. ROMPRÉ, préc., note 180, p. 27-28.

qu'aurait eu une personne prudente et raisonnable placée dans en pareilles circonstances[338]. Par ailleurs, la *Loi concernant le cadre juridique des technologies de l'information*[339] instaure un régime conditionnel d'exonération de responsabilité selon lequel le prestataire de services n'a pas l'obligation de surveiller les usagers de son service afin de prendre connaissance des éventuels agissements illicites, mais engage sa responsabilité dès lors qu'il le fait[340]. Les facteurs permettant de conclure à la responsabilité de l'intermédiaire sous ce régime sont, notamment, l'accomplissement des activités litigieuses par l'utilisateur du réseau[341], la connaissance de l'intermédiaire de l'existence des activités illicites[342] et le pouvoir d'action de ce dernier sur le document circulant dans son réseau[343].

Pour certains auteurs cependant, l'employeur ne peut bénéficier du régime d'exonération de responsabilité de la *Loi concernant le cadre juridique des technologies de l'information*[344], qui est fondamentalement incompatible avec le lien de subordination et pourrait avoir un indésirable effet dissuasif quant au contrôle de l'utilisation de l'Internet par les employés[345].

Finalement, l'employeur semble être pris dans un cercle vicieux : d'un côté, il est contraint, sous peine d'engager sa responsabilité pour négligence de sécurité, de contrôler les communications électroniques effectuées en son sein, notamment pour protéger son système d'information contre d'éventuels actes de piratage; cependant, d'un autre côté, s'il met en place un système de contrôle, il risque de voir sa responsabilité vis-à-vis des actes illicites de ses salariés aggravée. De plus, les employés et les tiers impliqués pourront éventuellement poursuivre l'employeur pour atteinte à leur vie privée découlant de cette

---

[338] P. TRUDEL, « La responsabilité des acteurs du commerce électronique », préc., note 313, n° 26, p. 620-621.

[339] Préc., note 50.

[340] P. TRUDEL, « La responsabilité des acteurs du commerce électronique », préc., note 313, n° 58, p. 632.

[341] V. GAUTRAIS et P. TRUDEL, préc., note 318, p. 74-75.

[342] *Id.*, p. 81-84.

[343] *Id.*, p. 79-81.

[344] Préc., note 50.

[345] S. ROMPRÉ, préc., note 180, p. 27-28.

surveillance. Il sera alors intéressant de voir si les tribunaux québécois, à l'instar de juridictions d'autres pays, seront tentés d'adopter une interprétation large de la responsabilité de l'employeur dans ce domaine.

À cet égard, les magistrats français semblent avoir opté pour une responsabilisation accrue de l'entreprise dans ce domaine et ont, à plusieurs reprises, conclu que l'entreprise est responsable de l'utilisation que ses préposés font de son système d'information et qu'elle doit par conséquent les surveiller[346].

Les juges américains semblent également avoir adopté une interprétation extensive de la responsabilité de l'employeur, notamment vis-à-vis des diverses formes de harcèlement. C'est ce qui ressort notamment de l'affaire *Blakey* v. *Continental Airlines Inc.*[347] dans laquelle une salariée poursuivait son employeur pour discrimination et harcèlement sexuel en raison des gestes et commentaires hostiles et sexistes incessants qu'elle subissait de la part de ses collègues masculins. Ces derniers prirent très mal la poursuite de leur collègue et se mirent à poster des messages et commentaires dénigrants sur le babillard électronique des pilotes de la compagnie. Ce site, bien que n'appartenant pas à *Continental*, était accessible à tous ses pilotes ainsi qu'à tout son personnel navigant. Les salariés pouvaient notamment y trouver toutes les informations utiles concernant les vols ou leurs horaires de travail. De plus, ils disposaient d'un forum spécial où ils pouvaient échanger informations et idées. L'employée fut déboutée dans un premier temps, mais l'affaire fut portée devant la Cour suprême du New Jersey qui devait, notamment, déterminer si le babillard électronique des pilotes constituait une extension du lieu de travail habituel, alors même que le serveur qui hébergeait ce site et en assurait la maintenance appartenait à *CompuServe*, un fournisseur Internet externe et indépendant. La Cour conclut que, compte tenu son mode de fonctionnement, ce babillard pouvait être considéré comme un service faisant partie du réseau appartenant à Continental et qui, en l'espèce, avait simplement été externalisé par

---

[346] Civ. 2e, 19 juin 2003, *Bull civ.* II, n° 202; Aix-en-Provence, 13 mars 2006, préc., note 285; I. RENARD, « Les droits et devoirs des entreprises », préc., note 309.

[347] 751 A.2d 538 (N.J. 2000).

cette entreprise. Le Tribunal précise qu'un employeur n'a pas l'obligation de surveiller les communications privées de ses employés, mais qu'il lui incombe, toutefois, de prendre des mesures concrètes pour mettre fin au harcèlement sur le lieu de travail s'il a connaissance ou aurait dû avoir connaissance de l'existence d'actes de cette nature. À défaut d'agir, il pourrait engager sa responsabilité. Lorsqu'il est question de harcèlement en milieu de travail, l'employeur est en effet considéré comme étant le seul à avoir le pouvoir de faire cesser les comportements inappropriés de ses employés. Et il pourra difficilement expliquer ses négligences ou carences lorsque le harcèlement est perpétré à travers son propre réseau, puisque ce dernier est considéré comme étant un prolongement du lieu de travail. En effet, parce qu'il dispose des moyens techniques lui permettant de contrôler l'usage que les employés font des outils de communication mis à leur disposition, les tribunaux ont tendance à considérer qu'il est en position d'être proactif et de prendre les mesures appropriées pour prévenir ou mettre fin au harcèlement[348].

Dans de telles conditions, il est du meilleur intérêt pour l'employeur de prendre les devants et d'agir en amont. Toutefois, certains auteurs déplorent que la jurisprudence n'aille pas suffisamment loin et ne précise pas l'étendue réelle de la responsabilité de l'employeur en cas de carence à contrôler les activités virtuelles des employés ou à prévenir le harcèlement sexuel[349]. On reproche également aux tribunaux leur réticence à faire le lien entre le droit de l'employeur de surveiller les activités de ses employés et ses obligations en regard de ces activités et à en tirer toutes les conséquences[350].

Quoi qu'il en soit, l'employeur a, en définitive, intérêt à suivre de près les activités se déroulant sur son réseau, afin d'être capable de déceler les actes de harcèlement et les autres comportements à risques et d'intervenir rapidement pour prévenir ou mettre fin aux

---

[348] Donald P. HARRIS, Daniel B. GARRIE, Matthew J. ARMSTRONG, « Sexual Harassment: Limiting the Affirmative Defense in the Digital Workplace », 39 *U. MICH. J.L. REFORM* 73, 87 (2005-2006).

[349] *Id.*

[350] *Id.*

éventuels dommages. Il a également avantage à définir les comportements interdits dans le cadre d'une politique d'entreprise.

Section 2. Les principaux chefs de responsabilité

Le contrôle patronal ne cesse de se resserrer, notamment parce que les employeurs souhaitent éviter les comportements susceptibles de créer ou maintenir un climat empoisonné qui pourrait démotiver les employés ou faire fuir les meilleurs éléments vers la concurrence. Les employeurs prennent de plus en plus conscience qu'il y va de leur intérêt d'offrir un lieu de travail sain et cette préoccupation se reflète dans leurs politiques de gestion des ressources humaines. Cependant, ils ne semblent pas toujours réaliser que la cybercriminalité n'épargne pas le monde du travail ni que les incivilités peuvent également être commises à travers leur réseau.

Les agissements frauduleux ou illicites des salariés accomplis grâce aux moyens de communication électroniques fournis par l'employeur peuvent se dérouler directement dans les locaux de l'entreprise ou hors de ses murs. Il pourra, par exemple, s'agir de l'intrusion ou de la tentative d'intrusion dans un système informatique, de l'usurpation de l'identité d'un tiers, de divers actes d'intimidation ou de harcèlement (diffamation, injures, etc.), de la consultation de sites interdits (notamment ceux qui diffusent la pornographie juvénile) ou de l'incitation à la commission d'infractions.

Il importe de souligner que si l'activité privée d'un employé sur Internet peut, en fin de compte, engager la responsabilité de l'employeur, elle est aussi source de risques pour le salarié lui-même. Ainsi, ce dernier peut être victime de fraudes lorsqu'il effectue des transactions bancaires en ligne. La consultation de sites bancaires est, en effet, une activité que l'on effectue de plus en plus souvent lorsque l'on est au bureau. Or, on assiste depuis quelques années à une recrudescence des attaques de « *phishing* » (ou « hameçonnage »). Il s'agit de fraudes réalisées grâce à la contrefaçon du site Internet d'une entreprise (souvent une institution financière) renommée. Généralement, les fraudeurs envoient aux internautes

des messages électroniques supposément en provenance de l'entreprise ciblée et les invitent à confirmer un certain nombre d'informations en cliquant sur un lien inclus dans le message. Ce lien renvoie vers un site contrefait reprenant la marque, le logo ou les couleurs de l'entreprise. Les fraudeurs n'ont plus alors qu'à récupérer les différentes informations personnelles et confidentielles saisies par les victimes (numéro de carte de crédit ou de compte bancaire, codes d'accès aux services en ligne, identifiants de connexion à l'Internet, etc.). Or, dans ces hypothèses qui mettent en lumière l'imprudence des internautes, la responsabilité de l'employeur pourra difficilement être questionnée. Toutefois, on peut se demander ce qui se passerait si le système informatique de l'employeur n'est pas suffisamment protégé[351]. Il suffira, par exemple, que ce système soit infecté par un logiciel espion capable de collecter les mots de passe, grâce à l'enregistrement des séquences de touches activées par le ou les utilisateur(s), pour que les salariés et l'employeur soient exposés à de très graves préjudices. Qui sera alors tenu responsable des éventuels dommages résultant des opérations bancaires effectuées dans ce cadre[352]? Cet exemple démontre qu'il n'est pas nécessaire que les agissements du salarié soient illégaux pour que la question de la responsabilité de l'employeur se pose[353].

Les comportements répréhensibles imputables à l'employeur les plus fréquents sont les atteintes aux droits des personnes (2.1.) et les atteintes à la confidentialité et aux droits de propriété intellectuelle (2.2.).

2.1. Les atteintes aux droits des personnes

Il s'agit essentiellement des atteintes à la dignité, à l'honneur et à la réputation d'autrui, qu'il s'agisse des collègues de travail ou de tiers externes à l'entreprise. Or, malgré des politiques de gestion des ressources humaines plutôt volontaristes, le constat est que collègues et amis s'échangent régulièrement des contenus à caractère sexuel, raciste ou

---

[351] H. SCHMIDT, « E-mail, internet et le lieu de travail : une relation difficile? », préc., note 13, p. 1.

[352] *Id.*

[353] *Id.*

sexiste grâce au réseau de leur employeur[354]. Ces contenus « politiquement incorrects » peuvent être à la base d'actions en réparation intentées par des destinataires les ayant perçus comme constitutifs de harcèlement ou de discrimination à leur égard. Généralement, les personnes impliquées dans la diffusion de ce type de matériel ne se préoccupent pas vraiment de ce qu'il adviendra de leur message une fois que le destinataire qu'ils ont choisi l'aura reçu. Ou alors, ils ont la bien naïve conviction que la distribution de ces contenus demeurera confinée à un groupe restreint. Cependant, l'expéditeur ne dispose d'aucun moyen pour s'assurer que ses messages ne seront pas ultérieurement transmis à des destinataires non visés initialement : bien souvent, de transfert en transfert, ces contenus douteux finissent par aboutir dans la messagerie électronique de personnes auxquelles ils n'étaient, à coup sûr, pas destinés. Souvent, ceux qui participent à la diffusion de tels contenus n'ont même pas conscience de la gravité de leurs actes[355] ou du fait qu'ils enfreignent la loi, puisque, comme l'indiquait candidement un employé impliqué dans le scandale qui secoua la compagnie *Dow Chemical* il y a quelques années, tout le monde autour d'eux le fait[356] et que, en définitive, ils ne font généralement que transmettre des contenus que d'autres ont créés et mis en circulation. Cette désinvolture – ou inconscience – est nourrie par le caractère informel de la correspondance électronique : contrairement aux courriers classiques, le ton y est souvent convivial, voire familier. De plus, les messages électroniques sont, en principe, éphémères et ont vocation à être détruits aussitôt après avoir été lus. Malheureusement, l'expéditeur perd le contrôle de ses écrits une fois qu'il clique sur le bouton « envoyer » et bien des personnes conservent les messages reçus (notamment les blagues), soit pour les partager plus tard avec d'autres, soit en vue d'une éventuelle poursuite pour discrimination, harcèlement ou pour tout autre motif, contre ceux qui ont participé de quelque manière que ce soit à de tels actes.

---

[354] William G. PORTER II, Michael C. GRIFFATON, « Between the Devil and the Deep Blue Sea: Monitoring the Electronic Workplace », 70 *DEF. COUNSEL. J.* 65 (2003).

[355] Voir notamment *Poliquin* v. *Devon Canada Corporation*, 2009 ABCA 216 (CanLII), par. 28, où le salarié, tout en admettant avoir commis une faute en transférant à des collègues et contacts d'affaires un courriel à caractère raciste, minimise l'impact de ses actes avec ces propos : « it "[p]robably shouldn't have gone out, but it's not that damaging" ».

[356] W. G. PORTER II, M. C. GRIFFATON, préc., note 354.

Or, en matière de discrimination et de harcèlement sexuel, la responsabilité de l'employeur est très lourde, et les négligences ou carences de l'employeur dans ce domaine sont sévèrement punies, surtout aux États-Unis, où elles peuvent donner lieu à de très lourdes condamnations, en vertu du *Civil Rights Act* de 1964[357] qui interdit les actes de discrimination fondés sur la race, la couleur, la religion, le sexe ou l'origine ethnique. Ainsi, en 1995, la société américaine *Chevron* avait défrayé la chronique en raison du montant pharamineux (2,2 millions de dollars) qu'elle avait dû verser à ses employées dans le cadre d'un procès pour harcèlement sexuel intenté contre elle à la suite de la diffusion, au sein de l'entreprise, de plusieurs messages électroniques sexistes, dont notamment un courriel intitulé « 25 reasons why beer is better than women »[358]. On peut également citer une affaire concernant une ancienne éditrice du *Microsoft's Systems Journal* qui avait poursuivi son ex-employeur pour discrimination sexuelle[359]. Elle avait fait valoir que son supérieur hiérarchique ne l'avait pas promue au poste d'éditeur technique convoité simplement parce qu'elle était une femme. Son collègue mâle qui avait obtenu ce poste, était en effet incapable d'accomplir les tâches techniques reliées à ses nouvelles fonctions et s'en déchargeait sur elle, alors même qu'elle avait échoué à obtenir le poste. À l'appui de ses allégations, la salariée avait produit des courriers électroniques que son supérieur avait fait circuler à l'ensemble des salariés du journal et qui laissaient présumer qu'il avait des préjugés négatifs vis-à-vis des femmes. Ces courriels comportaient des insinuations sexistes ou des contenus à caractère sexuel plus explicites et tout aussi dégradants pour les femmes. *Microsoft* avait tenté d'exclure ce courriel de la preuve, alléguant qu'il s'agissait juste d'une tentative malheureuse de faire de l'humour, mais les juges ont admis la pertinence du courriel.

---

[357] *Civil Rights Act*, Pub. L. No. 88-352, 78 Stat. 241 (1964).

[358] F. CÔTÉ, préc., note 251.

[359] *Strauss* v. *Microsoft Corp.*, 856 F. Supp. 821 (S.D.N.Y. 1994).

Le Québec dispose également d'une forte protection des travailleurs en matière de harcèlement et de discrimination. L'article 81.19 de la *Loi sur les normes de travail*[360] oblige, en effet, l'entreprise à fournir à ses employés un environnement de travail sain et exempt de toute forme de harcèlement. L'article 2087 C.c.Q., de son côté, impose à l'employeur de « prendre les mesures appropriées à la nature du travail, en vue de protéger la santé, la sécurité et la dignité du salarié ». Quant à la *Charte des droits et libertés de la personne*[361], elle interdit de harceler une personne pour plusieurs motifs, dont le sexe, énumérés à l'article 10.

Le harcèlement est défini par l'article 81.18 de la *Loi sur les normes de travail* comme suit :

> « Pour l'application de la présente loi, on entend par "harcèlement psychologique" une conduite vexatoire se manifestant soit par des comportements, des paroles, des actes ou des gestes répétés, qui sont hostiles ou non désirés, laquelle porte atteinte à la dignité ou à l'intégrité psychologique ou physique du salarié et qui entraîne, pour celui-ci, un milieu de travail néfaste.
>
> Une seule conduite grave peut aussi constituer du harcèlement psychologique si elle porte une telle atteinte et produit un effet nocif continu pour le salarié. »[362]

Il est généralement admis que « cette définition, à elle seule, englobe toutes les formes de harcèlement [...], qu'il s'agisse de harcèlement sexuel, racial, discriminatoire, ou qu'il soit question d'abus d'autorité »[363]. Bien avant l'entrée en vigueur, le 1er juin 2004, de cette loi, la Cour suprême du Canada avait, avec les arrêts *Robichaud* c. *Canada (Conseil du Trésor)*[364] et *Janzen* c. *Platy enterprises Ltd.*[365], élaboré le principe général de la

---

[360] L.R.Q. 1979, c. N-1.1.

[361] L.R.Q., c. C-12.

[362] *Loi sur les normes de travail*, préc., note 360, art. 81.18.

[363] Isabelle LAUZON et Linda BERNIER, *Manuel d'employés et politiques d'entreprise : tout ce que l'employeur doit savoir*, Nouv. éd., Cowansville, Éditions Yvon Blais, 2004, p. 71.

[364] [1987] 2 R.C.S. 84.

[365] [1989] 1 R.C.S. 1252.

responsabilité d'un employeur en cas de harcèlement sexuel pratiqué par l'un de ses employés. Il découle de ce principe que c'est à l'employeur que revient l'obligation de prévenir le harcèlement psychologique et de le faire cesser lorsqu'il est porté à sa connaissance, car « seul l'employeur peut remédier aux effets du harcèlement puisque lui seul est en mesure de fournir le redressement le plus important, celui d'un milieu de travail sain »[366]. La responsabilité de l'employeur va donc résulter de son absence d'intervention[367] : s'il n'agit pas en temps opportun et avec l'efficacité requise, sa responsabilité sera engagée dès lors que les gestes reprochés, quelles que soient leur nature et leur portée, ont été accomplis à l'occasion de l'emploi[368]. Ainsi, dans *Davison* v. *Nova Scotia Safety Association*[369], la responsabilité de l'employeur a été reconnue pour n'avoir pris aucune mesure pour faire cesser le harcèlement sexuel dont se plaignait une employée. Cette dernière mentionnait, notamment, un épisode où elle était entrée dans le bureau du directeur général, pour lui remettre un document, et avait aperçu une photo de femme nue sur l'écran de son ordinateur. Le directeur avait ensuite imprimé cette photo et, devant elle, en avait remis une copie à au moins un employé de sexe masculin. Le tout se déroulait pendant les heures de bureau. De plus, ce directeur faisait incessamment des blagues et allégations à connotation sexuelle en présence de la plaignante et d'autres employés. Le Tribunal a relevé que, non seulement l'employeur n'avait rien fait pour remédier à cette situation, mais que, de surcroît, les membres du comité de direction s'étaient livrés à des actes de représailles envers la plaignante et avaient fini par la congédier, prétextant qu'elle intentait à l'entreprise un faux procès en violation des droits humains et tentait indument d'utiliser cette plainte, à laquelle elle faisait sans cesse référence, comme levier pour sa carrière. L'employeur et les directeurs ont été condamnés à des dommages-intérêts d'un montant total de 13 000 dollars, auxquels il faut ajouter 7 000 dollars de dommages

---

[366] *Robichaud* c. *Canada (Conseil du Trésor)*, préc., note 364.

[367] *Québec (Commission des droits de la personne et des droits de la jeunesse)* c. *Québec (Procureur général)*, 1998 CanLII 30 (QC T.D.P.), par. 200.

[368] *Robichaud* c. *Canada (Conseil du Trésor)*, préc., note 364 ; *Janzen* c. *Platy enterprises Ltd.*, préc., note 365.

[369] 2005 NSHRC 4 (CanLII).

exemplaires infligés à l'employeur afin de prévenir tout nouvel acte de représailles des cadres envers les employés.

L'employeur sera donc exonéré de toute responsabilité s'il a pris ou prend les moyens appropriés pour que les actes prohibés ne se produisent pas ou cessent[370]. Il lui faudra donc démontrer concrètement qu'il a pris les mesures nécessaires pour prévenir le harcèlement ou mettre un terme aux comportements prohibés[371]. Il s'agirait d'une obligation de moyens et non de résultat, puisque, aux termes de la loi, l'obligation de l'employeur ne consiste pas à faire en sorte qu'il n'y ait pas de harcèlement dans son entreprise, mais plutôt à mettre en œuvre les moyens raisonnables pour y instaurer la tolérance zéro vis-à-vis de ce genre de comportements[372]. L'une de ces mesures consistera en l'adoption d'une politique claire qui, si elle est connue de tous et appliquée uniformément, démontrera aux tribunaux le sérieux de l'entreprise pour combattre le harcèlement sous toutes ses formes[373].

Cependant, l'employeur doit être d'une extrême prudence lorsqu'il entend réprimer des actes supposés de harcèlement. Ainsi, dans l'affaire *Dufresne* c. *Pratt & Whitney Canada*[374], un employé fut congédié à la suite de plaintes de harcèlement sexuel. Une première plainte le visant avait été déposée par une employée à qui il envoyait des invitations à sortir par courrier électronique. Cette première plainte avait, par la suite, été retirée. Cependant, une enquête effectuée par l'employeur avait permis de découvrir que l'employé utilisait le courrier électronique à des fins personnelles et qu'il entretenait même une correspondance érotique avec deux employées, avec lesquelles il avait une liaison amoureuse. Toutefois, comme aucun des messages envoyés à la plaignante n'était de nature sexuelle, l'employeur s'était contenté d'aviser le salarié visé que son comportement était à la limite du harcèlement sexuel. Son usage personnel du courrier électronique lui fut

---

[370] *Québec (Commission des droits de la personne et des droits de la jeunesse)* c. *Québec (Procureur général)*, préc., note 367.

[371] *Robichaud* c. *Canada (Conseil du Trésor)*, préc., note 364 ; *Janzen* c. *Platy enterprises Ltd.*, préc., note 365.

[372] I. LAUZON et L. BERNIER, préc., note 363, p. 72.

[373] *Poliquin* v. *Devon Canada Corporation*, préc., note 355; I. LAUZON et L. BERNIER, préc., note 363, p. 72.

[374] Préc., note 247.

également reproché. Cependant, il fut congédié lorsqu'une deuxième employée porta plainte. Bien que l'employeur ait produit des preuves tirées de la banque d'archives de la messagerie électronique de l'employé congédié, le commissaire du travail conclut qu'il n'y avait pas eu de harcèlement et rétablit donc l'employé dans ses fonctions.

Outre le harcèlement sexuel, les employeurs appréhendent également que leurs salariés se servent de leur réseau pour diffuser des propos haineux ou à caractère raciste. La Cour de cassation française a ainsi eu à trancher dans une affaire relative au licenciement d'un salarié à la suite de l'envoi, grâce à la messagerie électronique de l'employeur, d'un courriel contenant des injures et menaces antisémites à un tiers établi à l'étranger[375]. Le destinataire de ce courriel s'en était plaint à l'employeur qui avait alors licencié le salarié qui en était l'auteur. La Cour a confirmé le licenciement après avoir souligné qu'il était établi, notamment grâce à l'historique des envois électroniques de la société, que le salarié visé était bien l'auteur du courriel incriminé. La victime aurait également pu, en l'espèce, chercher à obtenir réparation du salarié ainsi que de son employeur pour le préjudice subi.

Il faut dire que les salariés ne se rendent pas toujours compte que leurs mauvaises plaisanteries ou leurs actes de représailles peuvent engager la responsabilité de l'employeur. Ainsi, dans *Lemay* c. *Dubois*[376], les actes de la défenderesse étaient motivés par sa volonté de montrer la plaignante « sous son vrai jour ». La responsabilité de l'employeur n'a toutefois pas été retenue, notamment en raison du motif purement personnel à l'origine des agissements reprochés

L'intimidation est très présente en milieu de travail et les salariés peuvent faire preuve de beaucoup d'ingéniosité lorsqu'ils souhaitent tourmenter un collègue ou toute autre personne. Le Tribunal de grande instance de Carcassonne[377] a ainsi été saisi d'une affaire de détournement d'identité concernant une salariée qui, pour se moquer d'une collègue qui

---

[375] Soc. 2 juin 2004, *Bull. civ.* V, n° 152.

[376] Préc., note 278.

[377] Trib. gr. inst. Carcassonne, 16 juin 2006, préc., note 303.

n'avait pas voulu participer à un mouvement de grève, avait décidé d'utiliser l'identité de cette dernière sur des sites de rencontres. Les juges ont qualifié ces agissements de « violences volontaires », car la défenderesse avait non seulement usurpé l'identité de sa collègue pour s'inscrire sur ces sites, mais elle l'y décrivait comme une fille facile et en quête de relations sexuelles. Elle avait, en plus, communiqué les coordonnées téléphoniques de sa victime, si bien que cette dernière avait été submergée d'appels d'hommes intéressés par son profil. La plaignante en avait été si perturbée qu'elle avait été mise en arrêt de travail pendant dix jours. Finalement, la défenderesse avait été surprise en flagrant délit alors qu'elle répétait la blague. Profitant de ses fonctions de responsable informatique, elle avait utilisé le poste de travail de son directeur, dont elle avait les codes d'accès. Le Tribunal a conclu que la défenderesse avait agi dans l'intention de nuire à la victime dont elle connaissait la fragilité psychologique. Les juges ont même relevé une circonstance aggravante de préméditation, constituée par le fait d'avoir utilisé non pas son propre ordinateur mais celui de son directeur, sans doute afin d'éviter que les faits ne lui soient imputés, ce qui impliquait nécessairement qu'elle avait agi de façon délibérée. Cette « plaisanterie » a coûté à son auteur près de 11 000 euros : 4 000 euros ayant été alloués à la victime à titre de dommages-intérêts et 4 519 euros à la caisse d'assurance maladie pour les prestations versées à la victime consécutivement à son arrêt de travail. La responsabilité de l'employeur n'avait toutefois pas été recherchée dans cette affaire.

Plus près de nous, et sur le même registre, la Commission des relations du travail a, dans l'affaire *Carrier* c. *Centre local de développement (CLD) des Etchemins*[378], confirmé le congédiement de deux employés qui avaient ourdi un sordide complot pour discréditer leur directeur général et obtenir sa destitution. On leur reprochait, notamment, d'avoir subtilisé, détenu et utilisé des documents confidentiels (fichiers, courriels, déclarations d'impôt, contrats de travail, dossier de divorce, correspondances privées…) appartenant, soit à leur employeur, soit en propre au dirigeant visé, afin de faire chanter ce dernier et de le

[378] Préc., note 303.

contraindre à démissionner. Certaines des informations utilisées contre le dirigeant avaient été obtenues grâce à un subterfuge : l'une des employés impliqués dans la machination s'était inscrite sous un faux nom sur le réseau de rencontres en ligne fréquenté par la victime et avait initié une relation virtuelle avec lui, afin de le ridiculiser et de lui soutirer des informations confidentielles. L'employeur, considérant que les agissements des deux employés constituaient une faute grave et de nature à rompre tout lien de confiance, les avait congédiés. Les salariés contestaient leur congédiement qu'ils jugeaient discriminatoire. Ils s'estimaient, en effet, victimes de représailles eu égard à leurs activités de représentants syndicaux. Après avoir reconnu que les dirigeants syndicaux bénéficient généralement d'une grande liberté, le Tribunal précise toutefois que leurs droits et libertés comportent néanmoins des limites et qu'en l'espèce, les plaignants avaient outrepassé leur mandat en se livrant à des manœuvres aussi graves et cyniques que celles qui leur étaient reprochées. Il en conclut que leur congédiement avait été prononcé pour une cause juste et suffisante qui n'était pas reliée à leurs activités.

2.2. Les atteintes à la confidentialité et aux droits de propriété intellectuelle

La majorité des employeurs redoutent que certains employés insouciants ou malhonnêtes diffusent des informations concernant l'entreprise ou ses clients, en contravention, notamment, avec les principes relatifs au secret professionnel ou à la confidentialité ou encore au domaine boursier. Ainsi, la *Loi sur les valeurs mobilières*[379] interdit la manipulation des informations boursières visant à influencer ou tenter d'influencer le cours ou la valeur d'un titre[380]. Elle interdit également la communication ou l'utilisation frauduleuse d'informations privilégiées[381], tout comme la divulgation d'informations fausses ou trompeuses[382]. L'employeur a donc un intérêt particulier à veiller à ce que l'information boursière ne soit pas utilisée de façon frauduleuse ou abusive par ses salariés,

[379] L.R.Q. 1982, c. V-1.1.

[380] *Id.*, art. 195.2.

[381] *Id.*, art. 187 et suiv.

[382] *Id.*, art. 196 et 197.

de tels agissements pouvant compromettre sa réputation sur les marchés boursiers, voire engager sa responsabilité. Un tel risque existera si, par exemple, les salariés d'une entreprise cotée en bourse divulguent sur des forums de discussions des informations financières la concernant. La Commission des Opérations de Bourse française (ci-après désignée « COB ») a été confrontée, il y a quelques années, à des agissements frauduleux opérés par des salariés qui, sans y être habilités, proposaient des produits financiers aux investisseurs, grâce à le réseau Internet de leur société. La COB avait alors émis un communiqué de presse dans lequel elle mettait en cause les sociétés dont les « insuffisances manifestes dans les procédures de contrôle relatives à l'accès au réseau depuis les locaux professionnels »[383] avaient permis la commission de tels actes. Elle avait invité les entreprises à la plus grande vigilance, face aux risques d'utilisation du réseau à des fins personnelles ou frauduleuses par des salariés indélicats et éventuellement par des personnes externes, soulignant que de tels agissements pouvaient engager la responsabilité de la société et/ou de ses dirigeants. Cette mise en garde visait tout particulièrement les sociétés de bourse en ligne et les entreprises financières qui ont l'obligation d'effectuer un contrôle des plus serrés de l'utilisation des ressources informatiques par leurs salariés. À cet égard, il serait intéressant de voir comment se fera l'imputation des responsabilités dans le cadre des plaintes déposées par la direction de la Société Générale et des associations de petits porteurs à la suite des malversations d'un courtier en bourse qui auraient, officiellement, causé une perte de 4,9 milliards d'euros en 2008[384]. Pour l'instant, seul le courtier a été formellement mis en examen. Pourtant, les analystes s'accordent pour dire qu'il n'aurait pas pu déjouer toutes les procédures de contrôle, surtout pendant plus d'un an, à l'insu de ses supérieurs hiérarchiques. Quoi qu'il en soit, la réputation de la banque en ressortira

---

[383] COMMISSION DES OPÉRATIONS DE BOURSE, *Communiqué à l'attention des sociétés disposant d'un site ou d'un accès internet sur les possibilités d'utilisation du réseau*, Paris, 2000, en ligne : <http://www.amf-france.org/documents/general/3390_1.pdf> (site consulté le 25 juillet 2010).

[384] LE MONDE.FR, « Selon son ancien chef, Jérôme Kerviel "mentait" mais était "crédible" », Lemonde.fr, 21 juin 2010, en ligne : <http://www.lemonde.fr/economie/article/2010/06/21/selon-son-ancien-chef-jerome-kerviel-mentait-mais-etait-credible_1376141_3234.html> (site consulté le 30 juillet 2010).

certainement sérieusement écornée en raison, soit du manque de fiabilité de son système de sécurité, soit du laxisme de ses cadres quant à la prise de risques excessive de son salarié.

En ce qui concerne plus particulièrement la confidentialité des informations, force est de constater que les agissements des salariés ne sont pas toujours conformes aux exigences en matière de protection des renseignements personnels et du droit à la vie privée. La commissaire à la vie privée du Canada a ainsi, notamment, eu à déplorer la conduite pour le moins légère d'un vice-président de société vis-à-vis des ces règles[385]. Ce dernier avait envoyé un message électronique à tous les salariés de l'entreprise afin d'obtenir le nom de l'employeur d'une tierce personne. Cet individu n'avait aucun lien avec l'entreprise, n'y avait jamais travaillé, à quelque titre que ce soit, et n'évoluait même pas dans le même secteur d'activité. Il s'avéra ultérieurement que la sœur du vice-président représentait en cour l'ancienne femme de ce monsieur dans le différend juridique qui les opposait. Bien que la quête du vice-président n'ait pas porté fruit, aucun employé n'ayant répondu à son message, la commissaire à la vie privée a désapprouvé ces agissements qui ne répondaient, de toute évidence, pas à des motivations professionnelles. Elle a aussi fustigé le manque de responsabilisation de la société et sa désinvolture dans la gestion des renseignements personnels et du droit à la vie privée d'autrui.

La question de la confidentialité revêt une telle importance, que la plupart des organismes prennent des mesures préventives pour minimiser les risques liés aux actes – accidentels ou volontaires – de leurs employés susceptibles d'occasionner des fuites. Outre la mise en place quasi systématique de dispositifs de filtrage, les entreprises ont de plus en plus recours à l'adjonction automatique d'un « avis de non-responsabilité » ou d'une « clause de confidentialité » à chaque courrier électronique émis depuis l'entreprise. Ces avertissements rappellent ceux qui figurent sur les formulaires de télécopie de la majorité des entreprises. Il existe des variantes à ces avis, avec des contenus plus ou moins détaillés;

---

[385] COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Résumé de conclusions d'enquête en vertu de la LPRPDÉ n° 346. Un courriel soulève des questions concernant les motifs, la crédibilité et la responsabilisation*, 15 juin 2006, 2006 CanLII 37531 (C.V.P.C.), en ligne : <http://www.canlii.org/>.

toutefois, même les moins élaborées d'entre eux incluent généralement des dispositions visant la confidentialité des données et la protection de la propriété intellectuelle. On peut se demander, avec Myriam Delawari et Christophe Landat, « [q]uelle valeur accorder […] à cette "clause" élusive de responsabilité » incluse non dans un contrat mais dans un courrier[386]. Si le *Code civil du Québec* prévoit la possibilité pour toute personne de recourir à des clauses exonératoires, notamment en invoquant la force majeure de l'article 1470 C.c.Q., cette faculté est strictement encadrée et les dispositions de l'article 1476 C.c.Q., excluent expressément la possibilité pour un individu d'exclure ou de limiter, par simple avis, son obligation de réparer le préjudice causé à des tiers. Cet article leur accorde tout au plus la valeur d'une « dénonciation d'un danger ». De plus, si l'on considère que l'entreprise a un devoir général de surveillance des informations qu'elle manipule[387], un tel avis ne sera certainement pas suffisant pour la dégager de sa responsabilité. Cependant, les juges pourront considérer que cet avis atteste de la bonne foi de l'employeur[388], surtout si ce dernier prend soin d'avertir les destinataires non « visés » des conséquences liées à l'utilisation non autorisée des informations qu'ils n'auraient pas dû recevoir et leur indique la procédure à suivre pour mettre fin, ou à tout le moins minimiser le préjudice découlant de cette violation de la confidentialité. De plus, la personne qui a connaissance d'un tel avis est tenue de prendre les mesures qui s'imposent pour éviter le dommage et si elle ignore la mise en garde qu'il contient, « elle pourra être considérée comme ayant été elle-même fautive », ce qui pourra affecter son droit d'obtenir réparation du préjudice subi[389]. Autrement dit, on pourra difficilement considérer que l'employeur a rempli ses obligations s'il se contente d'adjoindre un avertissement aux messages sortants de l'entreprise et ne fait

---

[386] Christophe LANDAT et Myriam DELAWARI, « Les enjeux du développement d'Internet au regard de la relation salariale et pré-salariale », Droit.ntic.com, 2001, p. 111, en ligne : <http://www.droit-ntic.com/pdf/cybersurv.pdf> (site consulté le 29 juillet 2010).

[387] E. A. CAPRIOLI, « La qualité de fournisseur d'accès à l'internet : un nouveau risque juridique pour l'entreprise », préc., note 287.

[388] C. LANDAT et M. DELAWARI, préc., note 386, p. 111.

[389] Pierre DESCHAMPS, « L'exonération et le partage de responsabilité », dans *Responsabilité*, Collection de droit 2007-2008, École du Barreau du Québec, vol. 4, 2007, *Droit civil en ligne* (DCL), EYB2007CDD90, p. 8-9.

rien de plus pour empêcher les activités illicites à travers son réseau ou pour inciter ses salariés à un usage responsable du système informatique. Il pourra, en revanche, plus facilement démontrer son sérieux s'il a également pris des mesures pour minimiser les risques, notamment en mettant en place un système de filtrage approprié et une politique d'utilisation des ressources informatiques dont il s'assure qu'elle est scrupuleusement respectée.

Un autre sujet de préoccupation pour les employeurs est le respect des droits de propriété intellectuelle d'autrui et, notamment, les droits d'auteur rattachés à certains documents informatiques ou les licences d'utilisation de certains logiciels. L'échange et le partage des vidéos ou de fichiers musicaux sont en hausse constante et les employés peuvent participer à ces transactions en violation de ces droits. Or, la reproduction ou le piratage d'œuvres ou de logiciels peuvent entraîner de lourdes pertes financières pour les titulaires de droits de propriété, sans compter le préjudice sur l'image de marque. Aussi ces derniers n'hésitent pas à poursuivre les personnes qui violent leurs droits ainsi que ceux qui leur apportent une aide quelconque dans la réalisation de leurs forfaits. La *Northwestern University* a ainsi été amenée à congédier une employée qui avait stocké plus de 2000 fichiers MP3 sur son ordinateur professionnel[390]. La salariée avait prétendu que ces fichiers provenaient de sa propre collection de CD et non d'un quelconque site Internet proposant des pièces musicales. Cependant, l'université avait été alertée sur des téléchargements illégaux d'œuvres musicales effectués depuis ses locaux par au moins l'une des entreprises victimes de ces activités. De même, une entreprise américaine a dû négocier un arrangement hors cour d'un montant d'un million de dollars avec l'industrie américaine du disque parce qu'elle avait mis à la disposition de ses employés un serveur destiné au téléchargement, à la conservation et au partage de fichiers MP3[391].

---

[390] W. G. PORTER II, M. C. GRIFFATON, préc., note 354.

[391] *Id.*

En France, il existe une incrimination autonome de fourniture de moyens pour lutter contre la fraude informatique au sens large. Ainsi, la *Loi pour la confiance dans l'économie numérique*[392] sanctionne, notamment, « le fait d'offrir, de détenir, de céder, de mettre à disposition un équipement informatique permettant la commission d'une infraction »[393]. De son côté, la *Loi relative au droit d'auteur et aux droits voisins dans la société de l'information*[394] a introduit dans le Code de la propriété intellectuelle[395] des dispositions concernant le téléchargement illicite et visant les différents intervenants (en amont, les fournisseurs d'accès Internet et, en aval, leurs abonnés). L'article 21 de cette loi réprime le fait d'« éditer, de mettre à la disposition du public ou de communiquer au public, sciemment et sous quelque forme que ce soit, un logiciel manifestement destiné à la mise à disposition du public non autorisée d'œuvres ou d'objets protégés »[396]. Tandis que les articles 25 et 28 mettent en place des mesures préventives afin d'inciter les fournisseurs d'accès à sensibiliser les internautes aux dangers du téléchargement[397], et les utilisateurs à veiller à ce que leur accès à l'Internet ne soit pas utilisé pour des échanges illégaux[398].

Section 3. Les possibilités de limitation ou d'exonération de responsabilité

L'employeur qui a dédommagé un tiers en raison du préjudice causé par son préposé peut se retourner contre ce dernier, en vertu du régime de la responsabilité du commettant : l'article 1463 C.c.Q. lui offre un recours récursoire sur le fondement de l'article 1457

---

[392] Préc., note 328.

[393] Code pénal, art. 323-3-1.

[394] *Loi n° 2006-961 relative au droit d'auteur et aux droits voisins dans la société de l'information*, J.O. 3 août 2006, p. 11529.

[395] *Loi n° 92-597 relative au code de la propriété intellectuelle*, J.O. 3 juil. 1992, p. 8801.

[396] *Id.*, art. L. 335-2-1.

[397] *Id.*, art. L. 336-2.

[398] *Id.*, art. L. 335-12.

C.c.Q. ou de ses relations contractuelles[399]. Certains employeurs pourraient donc être tentés, face à la montée en puissance des risques de poursuites liés à une utilisation inappropriée de leurs outils de communication électroniques, de chercher à « renforcer *a priori* la responsabilité » de leurs salariés[400]. Ils pourront ainsi imposer aux employés des « clauses de responsabilités financières » qui leur permettront de récupérer les sommes versées à des tiers en cas de dommages découlant de leurs agissements fautifs[401]. Il ne semble, toutefois, pas que les employeurs québécois aient été tentés par l'avenue offerte par les clauses de responsabilité financières ou que les tribunaux se soient prononcés sur la validité de telles clauses. En revanche, certains employeurs s'y sont aventurés en France, mais ils se sont heurtés à la jurisprudence de la Cour de cassation qui, dans un souci de protection du salarié, invalide systématiquement ce type de clauses en dehors des cas de faute lourde du salarié[402].

La responsabilité de l'employeur ne sera évidemment engagée que si toutes les conditions de mise en œuvre de l'article 1463 C.c.Q. sont réunies. Aux termes de cet article, il faut qu'il y ait un lien de préposition entre le préposé et le commettant, qu'il y ait une faute du préposé selon les critères de l'article 1457 C.c.Q. et que le préjudice ait été causé par le préposé dans le cadre de l'exécution de ses fonctions. En revanche, la faute du commettant n'est aucunement nécessaire, en raison du caractère irréfragable de présomption de l'article 1463 C.c.Q. Comme le notent Messieurs Jean-Louis Baudouin et Patrice Deslauriers :

> « En fait, il ne s'agit pas d'une simple règle de preuve, mais bien d'une règle de fond. Le Code ne laisse, en effet, aucun moyen d'exonération possible au commettant dès l'instant où toutes les conditions d'application du régime de responsabilité se trouvent réunies. La preuve qu'il a bien choisi son préposé, qu'il a exercé sur lui une surveillance adéquate, que le geste de celui-ci était totalement

---

[399] Jean-Louis BAUDOUIN et Patrice DESLAURIERS, « La responsabilité du fait des autres - Schéma général », dans *La responsabilité civile, Volume I – Principes généraux*, 7e édition, 2007, *Droit civil en ligne* (DCL), EYB2007RES7, n° 1-751.

[400] D. SERIO et C. MANARA, préc., note 7.

[401] *Id.*

[402] *Id.*

> imprévisible, qu'il a tout fait pour éviter ou prévenir le dommage est insuffisante. Le seul système de défense étant de parvenir à se situer en dehors du régime, il doit donc établir qu'il n'est pas véritablement le commettant de l'auteur du préjudice, que son préposé n'a pas commis de faute, que le préjudice est dû à une force majeure, à la faute de la victime ou à l'acte d'un tiers, ou enfin que la faute de son préposé a été commise en dehors du cadre de l'exécution de ses fonctions. »[403]

Bien entendu, la situation de l'employeur sera parfois considérée avec plus ou moins de sévérité compte tenu des circonstances particulières entourant la commission des faits dommageables.

S'agissant de l'utilisation des outils informatiques de l'entreprise, l'un des facteurs aggravants pour l'employeur pourrait consister à s'être abstenu d'agir ou d'avoir différé son intervention alors qu'il avait eu connaissance de la survenance des actes préjudiciables[404]. L'absence de politique visant à encadrer l'usage des outils électroniques – et tout particulièrement à certains comportements prohibés, tels le harcèlement – ou la non-application de celle-ci pourra également être considérée avec la plus grande sévérité[405]. De plus, le niveau de contrôle ou de supervision exercé par l'employeur sur les moyens de communication électroniques offerts sera déterminant dans l'appréciation de sa responsabilité[406]. En effet, comme le précisent certains auteurs :

> « [il] existe un lien étroit entre le contrôle exercé sur l'information présumément dommageable et la responsabilité qui en découle. Ainsi, plus grande est la discrétion de décider ce qui sera publié (ou retransmis), plus grande est la responsabilité découlant d'une telle décision »[407].

Enfin, la responsabilité des entreprises est renforcée lorsque leur domaine d'activité est relié aux services informatiques ou lorsqu'elles sont familiarisées avec les processus de

---

[403] J.-L. BAUDOUIN et P. DESLAURIERS, « La responsabilité des commettants », préc., note 268, n° 2-754.

[404] *Loi concernant le cadre juridique des technologies de l'information*, préc., note 50, art. 22, 36 et 37 (relatifs à la responsabilité des intermédiaires des communications électroniques).

[405] Voir *infra*, Partie 2, Chapitre 1, Section 1, 1.4, p. 147.

[406] P. TRUDEL et al., préc., note 255, p. 5-3.

[407] *Id.*, p. 5-3.

vérification et de sécurisation des informations : l'attentisme ou l'approximation sont, en effet, difficilement justifiables lorsqu'il s'agit de spécialistes[408]. Ainsi, on demeure perplexe lorsque l'on apprend qu'il a fallu plus d'un mois et demi pour découvrir qu'un CD, égaré dans un avion par un salarié du cabinet *Deloitte & Touche*, contenait en fait les données personnelles de 9 000 salariés de la société *McAfee*. Le salarié fautif avait attendu 3 semaines avant d'avertir la direction de son groupe, qui avait elle-même attendu 3 jours avant d'en informer *McAfee*. Cette dernière avait, de son côté, mis 20 jours avant de déterminer le contenu du CD et le type d'informations qui y étaient stockées. Pour couronner le tout, ces données – pourtant sensibles – n'avaient fait l'objet d'aucun codage ou cryptage! De tels manquements, provenant de deux sociétés considérées comme des chefs de file dans leurs domaines, tels que *Deloitte & Touche*, spécialisée dans les audits et les processus de vérification et *McAfee*, dans la sécurité des systèmes d'information, sont tout simplement édifiants[409]. Et cela d'autant plus qu'en vertu des dispositions relatives à la sous-traitance, la société *McAfee* était tenue de donner des directives précises à *Deloitte & Touche* sur la manière de protéger les données hébergées[410]. L'affaire n'a pas été portée devant un tribunal, mais au vu de cette succession d'erreurs grossières, l'on peut supposer que les différents protagonistes n'auraient certainement pas été épargnés.

Pour tenter de limiter sa responsabilité ou de s'en exonérer, l'employeur va principalement exploiter les moyens de défense suivants : son absence de contrôle sur le préposé (3.1.), l'absence de lien entre la faute du préposé et l'exécution de ses fonctions (3.2.) et l'existence d'une politique d'utilisation des ressources informatiques.

---

[408] C. CRÉPIN, préc., note 107.

[409] *Id.*

[410] *Id.*

3.1. L'absence de contrôle du commettant

Le contrôle du commettant implique le « pouvoir de donner des ordres, des instructions ou des directives précises sur la manière dont le préposé doit exécuter la tâche »[411], mais également la maîtrise que l'employeur exerce sur les outils qu'il met à la disposition de ses salariés. Ce second aspect a une grande importance lorsque l'on sait que le contrôle de l'activité sur les réseaux numériques n'est pas toujours aisé. La question peut devenir encore plus complexe lorsque l'entreprise a recours à des télétravailleurs. Un nombre croissant d'organisations confient, en effet, une partie de leurs travaux à des personnes travaillant à distance, parfois dans le cadre d'un contrat de travail. L'entreprise pourra alors tenter de démonter que l'auteur des actes dommageables n'est pas son préposé, mais plutôt un travailleur autonome auquel il est, par exemple, lié par un contrat d'entreprise[412]. Dans un tel contexte, les juges chercheront certainement, dans un premier temps à qualifier, si nécessaire, la relation contractuelle existant entre l'entreprise et le travailleur auteur des actes dommageables. Ensuite, si le lien de préposition est établi, la question se ramènera sans doute alors, à déterminer, conformément à la jurisprudence constante, « si, quel que soit le moment ou le lieu où l'acte a été posé, le préposé agissait ou non pour le compte du patron »[413].

Un premier moyen de défense pourra consister pour l'employeur à invoquer son ignorance des agissements illicites du salarié, pour tenter de s'exonérer de sa responsabilité, puisque « le facteur qui déclenche [la] responsabilité [des intermédiaires] est la connaissance qu'ils ont ou qu'ils acquièrent de la nature délictueuse de l'information circulant dans le réseau »[414]. Ce sera notamment le cas lorsque le salarié a recours à des stratagèmes pour contourner les contrôles existants, par exemple, en demandant à ses interlocuteurs de compresser leurs messages ou de leur attribuer des noms anodins (ceux de fournisseurs de

---

[411] J.-L. BAUDOUIN et P. DESLAURIERS, « La responsabilité des commettants », préc., note 268, n° 1-780.

[412] *Id.*, n° 1-797, 1-798, 1-799, 1-800 et 1-801.

[413] *Id.*, n° 1-834.

[414] P. TRUDEL, « La responsabilité des acteurs du commerce électronique », préc., note 313, n° 54, p. 631.

l'entreprise, par exemple) afin qu'ils ne soient pas bloqués par le système de filtrage, en raison de leur taille ou de leur intitulé[415].

De plus, puisque c'est le degré de contrôle exercé sur un document qui détermine les droits et responsabilités à son égard[416], l'employeur pourra tenter de limiter sa responsabilité en minimisant l'intensité de son contrôle sur les contenus circulant dans son réseau ou soutenant qu'il n'avait aucune maîtrise sur les activités reprochées. Il devra, notamment, s'attacher à démontrer que les actes visés résultaient de la seule activité du salarié[417]. Il pourra exploiter le fait que les actes dommageables ont été commis par un employé ayant accédé à distance à son réseau. La question se pose, en effet, de savoir si et comment l'employeur peut contrôler l'activité d'un salarié qui accède à distance à son système informatique. Là encore, tout dépendra de l'acception du rôle de l'employeur par le juge. En effet, si l'on considère que l'employeur est responsable de son système informatique, on pourra difficilement admettre la thèse de l'absence de contrôle, puisqu'il existe des solutions techniques permettant d'accéder à distance au disque dur du salarié et donc de contrôler son activité[418]. La Cour de cassation française a ainsi admis que la responsabilité de l'employeur pouvait être engagée en raison des agissements frauduleux commis par ses salariés avec des outils de communication se trouvant dans ses locaux, mais sur lesquels il n'avait pas de contrôle technique direct[419]. S'agissant du salarié travaillant à distance, s'il est certain que les moyens de communication mis à sa disposition ne se trouvent pas dans les locaux de l'employeur (et donc sous son contrôle physique direct), on pourrait, en revanche, considérer qu'ils sont sous son contrôle technique, dans la mesure où c'est lui qui définit les conditions d'accès au réseau de son entreprise. Certains auteurs sont d'ailleurs d'avis que le lieu du télétravail devrait être considéré comme une « extension des lieux

---

[415] Pour une illustration, voir *Blais* c. *Société des Loteries Vidéos du Québec Inc*., préc., note 239.

[416] V. GAUTRAIS et P. TRUDEL, préc., note 318, p. 71.

[417] *Id.*, p. 74-75.

[418] V. ROQUES, préc., note 34, p. 24.

[419] Civ. 2e, 19 juin 2003, préc., note 346.

physiques normalement sous le contrôle et la supervision de l'établissement »[420]. De la sorte, quel que soit l'endroit où il se trouve, l'utilisateur « qui amorce une session d'accès distant avec les réseaux informationnels de l'établissement agira dans le cadre de ses fonctions, comme s'il ou elle était sur les lieux physiques de l'établissement »[421]. La responsabilité de l'employeur en serait donc encore renforcée.

L'employeur pourra également tenter de faire valoir qu'il n'avait aucun pouvoir d'action sur le document litigieux[422]. Toutefois, il pourra s'agir d'un fardeau difficile à supporter lorsque l'entreprise dispose d'un système d'information lui permettant d'effectuer une surveillance plus ou moins constante des communications électroniques de ses salariés. Il exerce alors, en effet, un « contrôle accru » sur les contenus circulant dans son réseau[423] qui lui donne la possibilité de sélectionner ou de modifier l'information des documents (par exemple, lorsqu'il supprime des pièces jointes en raison d'un contenu suspect)[424], de ne pas délivrer le message à son destinataire (par exemple, en cas de contenu inapproprié)[425] ou de le conserver pendant quelque temps, pour examen[426]. Il pourra donc difficilement justifier son inaction ou son incapacité à agir promptement pour empêcher ou mettre fin aux activités illicites se déroulant sur son réseau.

L'employeur devra, en outre, démontrer qu'il a fait preuve d'un minimum de diligence pour pouvoir bénéficier d'une limitation de responsabilité[427]. Il pourra, par exemple, pour témoigner de sa bonne foi, tenter de prouver que[428] :

---

[420] M. DUBOIS, préc., note 51, p. 6.

[421] *Id.*, p. 7.

[422] V. GAUTRAIS et P. TRUDEL, préc., note 318, p. 79-81.

[423] *Id.*, p. 82.

[424] P. TRUDEL, « La responsabilité des acteurs du commerce électronique », préc., note 313, n° 85, p. 641.

[425] *Id.*, n° 86, p. 641.

[426] *Id.*, n° 87, p. 642.

[427] *Loi concernant le cadre juridique des technologies de l'information*, préc., note 50, art. 22, 36 et 37.

[428] P. TRUDEL et al., préc., note 255, p. 5-6.

- il a retiré les informations dommageables ou pris les mesures nécessaires pour faire cesser le préjudice dès qu'il en a eu connaissance[429]; ou
- il a prévenu les destinataires que des informations dommageables pouvaient être contenues dans les messages ou les contenus diffusés[430]; ou
- il a enjoint aux intéressés de s'abstenir de porter intentionnellement atteinte aux droits des tiers, notamment grâce à des politiques claires[431].

De plus, la rapidité de la réaction de l'employeur sera un facteur déterminant, puisque la responsabilité du prestataire n'est pas engagée s'il prend promptement les mesures appropriées afin de corriger la situation[432]. L'empressement de l'employeur sera évalué à compter du moment où il prend connaissance des faits illicites et sera « fonction des circonstances, des moyens nécessaires et des efforts consentis afin de passer à l'action »[433]. Les actions ou omissions de l'employeur seront examinées selon les critères du droit commun de la responsabilité civile[434].

3.2. L'absence de lien entre la faute du préposé et l'exécution de ses fonctions

L'un des moyens de défense le plus souvent invoqués par l'employeur, pour tenter de s'exonérer de sa responsabilité, est que l'acte fautif n'a pas été commis par le préposé dans le cadre de l'exécution de ses fonctions. L'employeur pourra, par exemple, prétendre que le salarié a délibérément désobéi à des directives patronales claires ou qu'il a agi en dehors de ses heures normales de travail. Il existe une abondante jurisprudence autour de la notion « de l'exécution des fonctions » et, au fil des décisions, il semble se dégager un principe

---

[429] *Id*., p. 5-5, citant Eric SCHLACHTER, « Cyberspace, the Free Market and the Free Marketplace of Ideas: Recognizing Legal Differences in Computer Bulletin Board Functions », (1993) 16 *Hastings Comm/Ent L.J.* 87, 118.

[430] *Id.*, 134.

[431] *Id.*

[432] P. TRUDEL, « La responsabilité des acteurs du commerce électronique », préc., note 313, n^{os} 78 et 79 p. 638-639.

[433] *Id.*

[434] *Id.*

selon lequel c'est la finalité des agissements du préposé qui est déterminante[435]. En conséquence, les facteurs liés au lieu et au temps n'auront qu'une influence limitée[436]. Ainsi, il a été jugé que la responsabilité de l'employeur n'était pas engagée si son préposé, obligé par ses fonctions d'être disponible vingt-quatre heures par jour, avait causé un préjudice en utilisant, à des fins personnelles, un camion mis à sa disposition pour son travail[437]. En effet, comme l'avait relevé le juge en première instance :

> « Le fait qu'il devait être en disponibilité vingt-quatre heures par jour […] n'implique pas qu'il était vingt-quatre heures par jour dans l'exécution des fonctions auxquelles il était employé et qu'il ne lui était pas loisible de vaquer à des activités personnelles – telle la nécessité d'aller prendre ses repas – n'entrant pas dans la sphère des fonctions à l'exécution desquelles il était employé ».
>
> […] on a reconnu que l'employé qui va prendre son repas agit pour lui-même, dans son intérêt, et que le fait qu'il utilise le véhicule de son employeur pour ce faire ne suffit pas *per se* pour conclure qu'il était alors dans l'exécution de ses fonctions »[438].

En revanche, une municipalité a vu sa responsabilité engagée par les agissements d'un de ses policiers qui, pendant son jour de congé, avait causé un accident avec l'automobile de son patron, alors qu'il était en train de raccompagner un indicateur de police à qui il venait de soutirer des renseignements[439].

En définitive, dans leur analyse pour délimiter le cadre de l'exercice des fonctions de l'employé, les juges rechercheront :

> « si, malgré le contexte tout à fait inusité de la faute dommageable commise par l'employé, malgré la nature de son geste et en dépit des

---

[435] J.-L. BAUDOUIN et P. DESLAURIERS, « La responsabilité des commettants », préc., note 268, n° 1-826.

[436] *Id.*

[437] *R.* c. *Tremblay*, [1964] R.C.S. 601.

[438] *Id.*, 604 et 605.

[439] *Comtois* c. *Montreal (City of),* [1954] C.S. 416.

> circonstances de temps et de lieu inhabituelles, ce dernier agissait tout de même ultimement au bénéfice de son employeur »[440].

Lorsque, selon cette analyse, il y a poursuite d'un intérêt personnel pour le préposé, en même temps que l'intérêt du commettant, les tribunaux ont nettement tendance à conclure que l'activité fautive du préposé s'est effectuée dans le cadre de l'exécution de ses fonctions[441]. Par contre, lorsque le préposé est le seul qui pouvait trouver un intérêt dans l'activité qu'il poursuivait au moment des faits dommageables, les juges estimeront que le salarié était sorti du cadre de ses fonctions et le commettant sera dégagé de toute responsabilité[442]. Ainsi, dans *Lemay* c. *Dubois*[443], pour conclure que la préposée n'était pas dans l'exécution de ses fonctions lorsqu'elle avait choisi de publier les informations privées de sa collègue sur Internet, le Tribunal a relevé qu'elle avait justifié sa conduite par son souci de révéler la vraie personnalité de la plaignante aux autres membres de l'entreprise.

Finalement, pour que la responsabilité de l'employeur soit exclue, il ne suffit pas que les actes du préposé soient délictuels ou qu'ils aient été commis en désobéissant aux ordres de l'employeur : il faut également qu'ils aient été commis en dehors du cadre normal de l'exécution de ses fonctions[444]. Cependant, la jurisprudence n'a pas encore développé de test adéquat permettant de déterminer de façon sûre si le préposé était dans l'exécution de ses fonctions, aussi Messieurs Baudouin et Deslauriers proposent de s'inspirer du test en quatre étapes proposé par un auteur et selon lequel, les juges, dans leur analyse, devraient rechercher si[445] :

1. la faute a été commise dans l'exécution ou simplement à l'occasion de l'exécution des fonctions;

---

[440] A. SOLDEVILA, préc., note 263, p. 21.

[441] *Id.*, p. 22.

[442] *Id.*

[443] Préc., note 278.

[444] J.-L. BAUDOUIN et P. DESLAURIERS, « La responsabilité des commettants », préc., note 268, n° 1-834.

[445] *Id*., n° 1-823; Voir également Philippe G. HÉBERT, *Pour une interprétation renouvelée du critère de l'exécution des fonctions de l'article 1463 C.C.Q.*, mémoire de maîtrise, Québec, Faculté de droit, Université Laval, 2005.

2. la faute a profité en totalité ou en partie au commettant;
3. le commettant ignorait que la faute profitait au préposé ou que celui-ci recherchait exclusivement son bénéfice personnel;
4. le commettant a pris toutes les mesures raisonnables pour éviter la faute de son préposé.

L'avantage de ce test est que « [c]es questions sont séquentielles et une réponse positive à l'une ou l'autre suffirait à retenir la responsabilité du commettant »[446]. Cela permettrait donc de rechercher la responsabilité du commettant de façon beaucoup plus large que si l'analyse porte seulement sur le point de savoir si le salarié agissait ou non pour le compte de son patron.

Rappelons, pour terminer sur ce point, que dans certains pays comme la France, les juges semblent déterminés à rechercher très largement la responsabilité de l'entreprise lorsqu'il s'agit de l'utilisation des moyens de communication électroniques mis à la disposition des salariés. La Cour de Cassation a ainsi, dans l'arrêt précité du 19 juin 2003, admis la responsabilité de l'employeur en raison des agissements frauduleux perpétrés par une salariée au moyen d'outils informatiques dont il n'avait même pas le contrôle technique direct[447]. Les faits mettaient en cause une employée d'un agent général d'une compagnie d'assurance qui avait commis différentes escroqueries en déclarant de faux sinistres pour payer ses dettes personnelles, le tout en utilisant les moyens informatiques fournis par la compagnie d'assurance (et non l'agent général). Les magistrats ont jugé que le seul fait que ce soit l'employeur qui ait mis lesdits moyens informatiques à la disposition de la préposée et que cette dernière ait

> « agi au temps et au lieu de son travail, à l'occasion des fonctions auxquelles elle était employée et avec le matériel mis à sa disposition,

---

[446] J.-L. BAUDOUIN et P. DESLAURIERS, « La responsabilité des commettants », préc., note 268, n° 1-823.

[447] Civ. 2e, 19 juin 2003, préc., note 346.

> […] excluait qu'elle ait commis des détournements en dehors de ses fonctions »[448].

Il s'agit d'un arrêt important et de portée générale, puisque les juges, sans se préoccuper de savoir qui avait mis le matériel à la disposition du salarié, affirment que l'employeur doit être en mesure de contrôler l'activité de ses salariés sur les outils informatiques se trouvant dans ses locaux et de sanctionner toute conduite inappropriée, sous peine de voir sa responsabilité engagée[449].

Il semble donc se dégager un consensus sur le fait que, non seulement l'employeur a le pouvoir de surveiller l'utilisation des moyens de communication électroniques qu'il met à la disposition de ses salariés, mais qu'il en a aussi le devoir[450]. Cette volonté de responsabiliser les entreprises est particulièrement évidente en matière de harcèlement sexuel où la « tolérance zéro » est généralement requise[451]. Aussi est-il fortement conseillé aux entreprises d'encadrer en amont l'utilisation de leur système d'information, notamment en adoptant une politique claire. L'employeur pourra ainsi minimiser les coûts et les risques juridiques et informatiques. De plus, il disposera, le cas échéant, de solides arguments en faveur d'une limitation ou d'une exonération de responsabilité.

Conclusion de la première partie

La question de la responsabilité de l'employeur du fait de ses préposés oblige à se poser la question de son pouvoir de contrôle. Comment l'employeur peut-il, en effet, engager sa responsabilité s'il n'a pas, en contrepartie, le pouvoir de contrôler l'activité des salariés et notamment l'utilisation que ceux-ci font des outils de communication électroniques[452]? De

---

[448] *Id.*

[449] I. RENARD, « Les droits et devoirs des entreprises », préc., note 309.

[450] *Id.*; J.-P. DE LONGEVIALLE, préc., note 1.

[451] *Strauss* v. *Microsoft Corp*., préc., note 359; *Blakey* v. *Continental Airlines Inc.*, préc., note 347, *Davison* v. *Nova Scotia Safety Association*, préc., note 369.

[452] FORUM DES DROITS SUR L'INTERNET, *Relations du travail et internet. Panorama législatif et jurisprudentiel*, préc., note 289, p. 10.

nombreux auteurs partagent l'idée que le contrôle de l'usage de ces outils est, de fait, devenu une obligation pour l'entreprise[453]. Du coup, un nombre croissant d'entreprises adoptent des politiques d'utilisation des moyens informatiques pour clarifier les droits et obligations de chacun, tout en tentant de limiter leur propre responsabilité.

Le problème de la responsabilité patronale met également en lumière une contradiction fondamentale entre l'obligation pour l'entreprise de garantir le respect de la vie privée de ses salariés et de l'autre le régime de la responsabilité du commettant en vertu duquel elle doit endosser des agissements qui lui sont tout à fait étrangers. Là encore, c'est également le droit commun qui permettra de déterminer dans quelles limites l'entreprise peut exercer une surveillance de l'utilisation des ressources informatiques qu'elle met à la disposition de ses salariés sans se montrer trop intrusive dans la vie de ces derniers[454].

---

[453] I. RENARD, « Les droits et devoirs des entreprises », préc., note 309; Ian J. TURNBULL, « Identity Theft and Surveillance in the Workplace », dans Ian J. TURNBULL, Shari SIMPSON CAMPBELL, Donald F. HARRIS et Brian KIMBALL, *Privacy in the workplace: the employment perspective*, Canadian Privacy Institute, CCH Canadian, Toronto, 2004, p. 30.

[454] I. RENARD, « Les droits et devoirs des entreprises », préc., note 309.

Partie 2 : Les conditions de la cybersurveillance

S'interroger sur le droit de l'employeur de surveiller ses salariés revient à s'interroger sur la nature des pouvoirs que l'on reconnaît au premier sur les seconds. La question fait débat, notamment sur le terrain disciplinaire où elle se pose avec le plus d'acuité. Le pouvoir patronal est souvent décrit comme la réunion de trois prérogatives : le pouvoir de direction (faculté de diriger et d'organiser l'activité de l'entreprise), le pouvoir de règlement (droit de fixer les règles de vie en commun au sein de la collectivité du travail) et le pouvoir de discipline (possibilité de sanctionner les salariés pour leurs comportements fautifs). Le pouvoir de direction, en raison de sa nature économique, semble avoir une prépondérance : c'est en effet lui qui permet à l'employeur de prendre des mesures appropriées face aux évolutions de l'organisation, aux mutations technologiques ou aux restructurations et, ultimement, de décider la cessation définitive des activités de l'entreprise. Cependant, il est difficile de dissocier le pouvoir de direction de l'employeur de ses autres prérogatives dans la mesure où chaque décision prise par ce dernier a pour objectif le bon fonctionnement de l'entreprise. Aussi doit-on considérer que « le pouvoir patronal est un »[455]. Il se décline simplement sous plusieurs facettes assez complémentaires et trouve sa source dans le rapport de subordination qui fonde le contrat de travail[456].

Plusieurs théories ont été développées, notamment en France, relativement à la question du fondement du pouvoir patronal. Au XIX^{e} siècle, la justification avancée était de nature patrimoniale. L'employeur étant propriétaire des moyens de production, il était admis qu'il pouvait en faire l'usage qu'il souhaitait, sans restriction, sauf hypothèse d'abus[457]. Cependant, certains auteurs ont relevé que si cette analyse cadrait parfaitement avec l'exercice des prérogatives de gestion au sens économique, elle échouait à expliquer le pouvoir de direction exercé sur les individus, si bien qu'« un détour par le contrat » était

---

[455] A. MAZEAUD, préc., note 223, p.82.

[456] François DUQUESNE, *Droit du travail*, Gualino, coll. Universités, Série manuel, Paris, 2004, p. 91.

[457] *Id.*

nécessaire[458]. En effet, à partir du moment où la discipline en général est en jeu, « seule la volonté du salarié peut expliquer la soumission à l'autorité et à la sanction »[459]. C'est ce qui a donné naissance à la thèse contractuelle selon laquelle le pouvoir patronal résulte du contrat de travail par lequel le salarié, en s'engageant, accepte de se placer sous la subordination et l'autorité du chef d'entreprise et adhère tacitement à la réglementation[460]. Cependant, une partie de la doctrine a reproché à cette thèse d'être purement « individualiste » et de ne pas tenir compte de la dimension collective des relations. Et surtout, les auteurs cherchaient à identifier un fondement qui ouvrirait la voie à un contrôle effectif de l'exercice du pouvoir patronal sur les personnes[461]. Aussi a-t-on avancé une autre thèse, découverte en transposant la « théorie de l'institution » à la réalité de l'entreprise. Il s'agit de la thèse institutionnelle, selon laquelle l'entreprise est une institution à la tête de laquelle il faut un responsable, le chef d'entreprise, qui ne disposerait de pouvoirs qu'en raison de la fonction qu'il occupe. Ces prérogatives seraient accordées à l'employeur en vue de la satisfaction d'un intérêt allant bien au-delà de ses propres préoccupations, liées au capital, et qui intègreraient les intérêts des salariés. L'avantage de cette thèse est de tenir compte de la dimension essentiellement collective de la problématique des pouvoirs, puisqu'il est ici question de finalité commune[462]. Par ailleurs, avec la théorie institutionnelle, l'employeur devient titulaire d'un pouvoir et non d'un droit à l'égard des salariés et des outils de production[463]. Le contrôle du pouvoir patronal par le juge devient alors possible, puisque les décisions de l'employeur peuvent être mesurées à l'aune de l'intérêt commun[464]. Ce contrôle permet, grâce au concept de détournement de pouvoir emprunté au droit public, de limiter les risques d'abus de l'employeur[465]. La

---

[458] *Id.*

[459] *Id.*

[460] *Id.*

[461] *Id.*

[462] *Id.*

[463] *Id.*

[464] *Id.*

[465] A. MAZEAUD, préc., note 223, p.84.

théorie institutionnelle a cependant subi quelques critiques, notamment parce qu'elle projetait une vision tronquée de l'entreprise en laissant supposer l'existence d'un consensus gommant les contradictions et antagonismes[466].

La jurisprudence française a, dans un premier temps, semblé adopter la théorie contractuelle. Ainsi, dans l'arrêt Brinon rendu en 1956, la Cour de cassation déclarait que « l'employeur qui porte la responsabilité de l'entreprise est seul juge » de ses choix de gestion[467]. Par la suite, elle a modifié sa jurisprudence et décidé qu'il

> « n'appartient ni aux salariés ni aux juges de substituer leur appréciation à celle de l'employeur quant à la conduite de l'entreprise, à moins qu'un détournement de pouvoir ne soit allégué »[468].

Le juge était alors invité à contrôler la conformité des décisions patronales au regard de « l'intérêt de l'entreprise », notion empruntée à la thèse institutionnelle[469]. Cependant, il régnait une certaine incertitude, car dans le même temps, certaines décisions fondaient plutôt le pouvoir disciplinaire sur le contrat[470]. Le législateur a opéré une clarification avec la réforme du règlement intérieur qui a consacré l'existence du pouvoir réglementaire de l'employeur, tout en l'encadrant de limites strictes[471]. Parallèlement, l'exercice du pouvoir de sanction était désormais soumis au contrôle du juge[472]. Le mouvement semblait alors s'orienter en faveur de l'analyse fonctionnelle[473].

Toutefois, il faut nuancer cette analyse, car la Cour de cassation s'appuie en réalité tant sur la thèse institutionnelle que sur la thèse contractuelle pour justifier le pouvoir de direction[474]. D'ailleurs, pour certains auteurs, ces deux thèses « se complètent, même si leur

---

[466] *Id.*

[467] Soc. 31 mai 1956, D. 1958.21, note Levasseur.

[468] A. MAZEAUD, préc., note 223, p.84.

[469] *Id.*

[470] F. DUQUESNE, préc., note 456, p. 93.

[471] *Loi n° 82-689 relative aux libertés des travailleurs dans l'entreprise*, J.O. 6 août 1982, p. 2518.

[472] F. DUQUESNE, préc., note 456, p. 93-94.

[473] *Id.*, p. 94.

[474] A. MAZEAUD, préc., note 223, p.85.

angle d'attaque diffère »[475], aussi faudrait-il plutôt évoquer une articulation des différents fondements du pouvoir, au lieu d'analyser les choix jurisprudentiels en termes de « préférence »[476]. Le droit du travail a en effet évolué et doit notamment s'exercer dans le respect des libertés et des droits fondamentaux. Mais, en définitive, le pouvoir patronal est assez large, notamment lorsqu'il s'agit de questions d'ordre économique où il « ne rencontre d'autre limite que celles que pose le Code du travail »[477].

Ce débat théorique n'a pas eu lieu au Québec où le droit du travail est appréhendé uniquement sous un aspect « contractualiste » qui ne laisse aucune place à la notion de liberté publique[478]. Le contrat individuel de travail constitue en effet « le substrat du rapport de travail »[479], même s'il est indéniable que les lois en matière de droit du travail viennent, de plus en plus souvent, restreindre les effets juridiques du contrat de travail, par exemple, pour suppléer au silence des parties ou imposer des dispositions impératives[480]. Par ailleurs, le droit de propriété bénéficie d'une place prépondérante qui confère au chef d'entreprise des droits très larges confirmés par les articles 2085 et 2088 du *Code civil du Québec* qui lui reconnaissent le droit de gérer son entreprise et de diriger les personnes qui y travaillent, notamment, en contrôlant la quantité et la qualité de leurs prestations de travail[481]. Comme l'indique Juliette Lenfant, ce droit de propriété omnipotent forme avec le contrat de travail un

> « couple inséparable permettant une maîtrise juridique des biens de l'entreprise et une domination des personnes y travaillant. Il va en découler une confusion entre les différents pouvoirs : si la propriété peut conférer exclusivement à l'employeur les pouvoirs de direction

---

[475] *Id.*, p. 83; F. DUQUESNE, préc., note 456, p. 94.

[476] F. DUQUESNE, préc., note 456, p. 94.

[477] *Id.*

[478] Juliette LENFANT, *Le droit à la vie privée s'étend-il à l'utilisation du courriel par un employé dans le cadre de ses fonctions? Analyse de la doctrine, législation, jurisprudence et autres normes*, Montréal, Faculté des études supérieures, Université de Montréal, 2000, p. 14-15, en ligne : <http://www.juriscom.net/uni/etd/04/priv01.pdf> (site consulté le 29 juillet 2010).

[479] Robert P. GAGNON, *Le droit du travail du Québec*, 5e éd., Cowansville, Québec, Éditions Yvon Blais, 2003, p. 63.

[480] *Id.*

[481] *Id.*

> économique de son entreprise, la propriété, par un effet "tâche d'huile", va fonder l'ensemble des pouvoirs patronaux à l'égard du salarié. »[482]

Dans ce contexte, la surveillance des salariés va être justifiée comme étant l'exercice du droit de propriété pour assurer la sécurité et la productivité. Une telle justification sera considérée comme légitime dans la mesure où les questions liées à « la protection des lieux, des biens ou des personnes […] ne relèvent pas seulement des intérêts de l'employeur, mais aussi de l'ordre public »[483].

Ce besoin de contrôle va être largement satisfait avec les NTIC qui offrent à l'employeur la possibilité de surveiller discrètement ses salariés et d'affiner sa surveillance en fonction de ce qu'il cherche à vérifier ou à protéger. Il peut ainsi brider l'accès aux sites illicites ou contraires aux bonnes mœurs ou filtrer les messages afin, notamment, de bloquer l'envoi d'informations confidentielles vers la concurrence et l'importation de contenus à risque. L'employeur a même la possibilité de suivre ses salariés « à la trace »[484], puisque chaque mouvement électronique laisse systématiquement des traces qui sont mémorisées par les ordinateurs : l'employeur peut ainsi connaître la date et l'heure de connexion (et déconnexion) d'un salarié au système informatique, l'usage qu'il fait de la messagerie ou de l'Internet, les saisies ou les différents traitements de données qu'il effectue, ainsi que tous ses « déplacements » à travers les divers réseaux de l'entreprise[485].

Cette intrusion dans les activités des employés peut être encore plus étendue, dans la mesure où le travail s'invite de plus en plus souvent à la maison : grâce à l'ordinateur portable et au *BlackBerry*, on peut rapporter du travail pour le soir, le week-end … et même les vacances! Par la même occasion, le salarié fournit à l'employeur l'opportunité de pénétrer encore davantage dans sa sphère privée. Ce nouveau risque d'intrusion dans l'intimité de la vie privée des salariés ne manque pas d'aviver les tensions entre employés

---

[482] J. LENFANT, préc., note 478, p. 14-15.

[483] Diane VEILLEUX, « Le droit à la vie privée – sa portée face à la surveillance de l'employeur », (2000) *R. du B.* 60, 37.

[484] D. SERIO et C. MANARA, préc., note 7.

[485] *Id.*

et employeurs. L'un des principaux points de friction est de savoir jusqu'à quel point un patron peut surveiller ses salariés sans porter atteinte à leurs droits fondamentaux. Car si l'on reconnaît à l'employeur le droit de contrôler ses employés en vertu de son pouvoir de direction, la question de sa responsabilité en cas d'utilisation de techniques trop intrusives peut, toutefois, se poser. Et cela d'autant plus que les salariés peuvent réclamer leur droit à des conditions de travail justes et raisonnables, tel que le prévoient les articles 46 de la *Charte des droits et libertés de la personne*[486] et 2087 du *Code civil du Québec*. Ils peuvent également invoquer le droit à la vie privée de l'article 5 de la *Charte des droits et libertés de la personne*[487] et des articles 35 et 36 C.c.Q., ce qui soulève quelques questionnements, notamment sur l'existence d'un tel droit sur le lieu de travail ou sur l'opportunité de préserver un « espace privé » aux salariés, même au bureau.

Quoi qu'il en soit, la surveillance patronale ne peut pas reposer uniquement sur le désir de l'entreprise de contrôler ce que font les salariés : l'employeur doit avoir un motif sérieux et légitime pour contrôler les activités informatiques de ses salariés (Chapitre 2) et il doit avoir donné à ces derniers des directives claires quant à l'utilisation des NTIC mises à leur disposition (Chapitre 1).

Chapitre 1. L'existence de directives d'utilisation des ressources informatiques claires

La principale préoccupation des entreprises, face aux NTIC, est leur capacité à conserver la maîtrise des flux sur leur réseau informatique, avec la faculté de limiter ou d'interdire certains usages que les salariés pourraient faire des outils mis à leur disposition. Aussi un nombre croissant d'organisations régulent-elles l'utilisation de leurs équipements informatiques, de façon à pouvoir sanctionner les comportements déviants, tout en se préconstituant de solides preuves. Cette régulation, de nature juridique et/ou technique, peut

---

[486] Préc., note 361.

[487] *Id.*

aller de l'interdiction pure et simple de tout usage personnel de ces outils (avec un blocage systématique de tout accès aux sites non reliés aux activités des employés) à l'aménagement de règles plus souples permettant une utilisation à des fins autres que professionnelles, sous certaines conditions. Les entreprises sont confrontées à un autre défi : celui de devoir sans cesse s'ajuster à l'évolution des techniques et de trouver, souvent dans l'urgence, des solutions aux problématiques complexes liées à ces technologies.

La régulation technique consiste généralement à brider les communications électroniques afin, notamment, d'éviter les chutes de productivité ou l'inoccupation inutile de la bande passante ou encore de « retracer »[488] l'activité électronique du salarié.

Quant à la régulation juridique, elle permet à l'employeur de définir et sanctionner les comportements qu'il juge inappropriés. La surveillance patronale est, en effet, souvent exercée à des fins disciplinaires. Or, il découle de la jurisprudence québécoise récente que l'employeur qui souhaite sanctionner ses salariés relativement à leur utilisation des outils de communication électroniques doit avoir préalablement émis des directives claires définissant précisément les modalités et limites de l'utilisation de ces ressources. Les tribunaux sont en effet venus préciser que les politiques Internet devaient indiquer clairement les attentes de l'employeur, ainsi que les conséquences découlant de la violation de leur contenu. L'employeur qui respecte ces impératifs pourra sanctionner les employés dès lors qu'ils auront contrevenu à cette politique : il lui suffira alors, par exemple, de simplement produire une liste de titres des messages électroniques échangés par le salarié concerné ou le relevé de ses connexions Internet, pour démontrer son utilisation abusive ou inappropriée des outils informatiques de l'entreprise[489]. Il ne sera même pas nécessaire que l'employeur accède au contenu des fichiers et des messages personnels du salarié pour

---

[488] D. SERIO et C. MANARA, préc., note 7.

[489] *Syndicat canadien des communications, de l'énergie et du papier, section locale 522* c. *CAE Électronique Ltée*, préc., note 159.

prouver la faute. En revanche, en l'absence de directives claires, le pouvoir de l'employeur de discipliner ou de congédier un employé risque d'être fortement limité[490].

Le fait pour l'employeur d'adopter des directives claires en matière d'utilisation des ressources informatiques permet également à l'employeur de régler la délicate question de la vie privée. Il existe, en effet, une certaine incertitude autour de l'attente que les salariés peuvent raisonnablement avoir quant au respect de leur vie privée lorsqu'ils utilisent les technologies de l'information fournies par l'employeur[491]. Aussi, l'un des moyens les plus sûrs pour éviter les éventuels conflits est que l'employeur indique clairement ses attentes dans ce domaine, en précisant dans quelle mesure il reconnaît éventuellement l'existence d'une vie privée à ses salariés[492].

De plus, comme indiqué en première partie, l'employeur se donne ainsi une solide occasion de limiter, voire de s'exonérer de sa responsabilité éventuelle vis-à-vis des tiers, en cas d'utilisation non appropriée des salariés.

La régulation juridique peut prendre la forme de clauses contractuelles (section 2); toutefois, une majorité d'employeurs optent plutôt pour la mise en place d'un instrument collectif règlementant l'usage des ressources informatiques dans l'entreprise (section 1).

Section 1. Les politiques Internet

De nombreuses entreprises se sont dotées de politiques Internet, suivant ainsi les conseils de plusieurs auteurs, qui avaient très tôt souligné l'intérêt, pour les employeurs, d'adopter des directives en matière d'utilisation des ressources informatiques et spécialement

---

[490] *Fiset* c. *Service d'administration P.C.R. Ltée*, préc., note 174; *Commission des normes du travail* c. *Bourse de Montréal Inc.*, préc., note 164.

[491] F. CÔTÉ, préc., note 251.

[492] Ian J. TURNBULL « Privacy Management Plan and Policies », dans Ian J. TURNBULL, Shari SIMPSON CAMPBELL, Donald F. HARRIS et Brian KIMBALL, *Privacy in the workplace: the employment perspective*, Canadian Privacy Institute, CCH Canadian, Toronto, 2004, p. 242.

d'Internet et, surtout, de l'urgence qu'ils avaient à le faire[493]. Ce mouvement s'est accru avec les récentes décisions jurisprudentielles[494]. Dans la foulée, de nombreux organismes offrant des services informatiques non seulement à leurs employés, mais aussi à d'autres groupes d'utilisateurs (par exemple, les universités à leurs étudiants), ont également emboîté le pas[495]. Les politiques Internet s'avèrent, en effet, indispensables dans le mesure où ces utilisateurs disposent de comptes personnels et ont, généralement, libre accès aux ordinateurs et aux réseaux numériques de ces organismes. Il est donc tout à fait normal que ces organisations souhaitent encadrer les activités en ligne des personnes utilisant leurs réseaux et les sensibiliser aux risques liés à une utilisation inappropriée des ressources mises à leur disposition. Certains auteurs soutiennent d'ailleurs que ces organismes devraient aller au-delà d'une simple sensibilisation et que leur action devrait s'étendre à la surveillance des activités de leurs utilisateurs[496].

Une « politique Internet » est un document qui vise généralement à réguler l'usage des outils informatiques au sein de l'entreprise (à savoir : l'Internet, la messagerie électronique, l'Intranet et l'ensemble des ressources informatiques). À cet effet, elle définit les droits et obligations de chacun, de façon à éviter les abus, à informer les employés sur les modalités d'usage des moyens mis à leur disposition et à circonscrire le contrôle de l'employeur sur un tel usage. Toutefois, ces instruments ont une fonction beaucoup plus large, puisqu'ils visent aussi à préserver la sécurité des systèmes d'information.

---

[493] F. CÔTÉ, préc., note 251; Christopher DEEHY, « Cyberespace en milieu de travail : politiques d'entreprise », Lapointerosenstein.com, Été 1999, en ligne : <http://www.lapointerosenstein.com/fichier/listelibrary/37/Cde-cyberespace.pdf> (site consulté le 19 août 2010).

[494] *Fiset* c. *Service d'administration P.C.R. Ltée*, préc., note 174; *Commission des normes du travail* c. *Bourse de Montréal Inc.*, préc., note 164; *Syndicat canadien des communications, de l'énergie et du papier, section locale 522* c. *CAE Électronique Ltée*, préc., note 159; *Alliance de la fonction publique du Canada* et *Musée des beaux-arts du Canada*, préc., note 155.

[495] Voir notamment *Politique de sécurité informatique et d'utilisation des ressources informatiques de l'Université de Montréal*, Recueil officiel (Règlements, directives, politiques et procédures) de l'Université de Montréal, n° *40.28*, qui concerne « la sécurité du réseau informatique de l'Université de Montréal, des équipements informatiques appartenant à l'Université, de tous les équipements informatiques qui utilisent son réseau, ainsi que des données qui y résident ou y transitent ».

[496] Blandine POIDEVIN, « L'usage du système informatique par les employés : quel risque pour l'employeur? », Jurisexpert.net, 10 novembre 2006, en ligne : <http://www.jurisexpert.net/l_usage_du_systeme_informatique_par_les/> (site consulté le 19 août 2010).

Afin de s'assurer que sa politique Internet sera valide et efficace, l'employeur doit veiller à en définir le contenu de la façon la plus précise possible (1.1.) et à respecter certains critères (1.2.).

1.1. Le contenu des politiques Internet

Le fait de disposer de directives claires et précises en matière d'utilisation des outils informatiques permet à l'entreprise de verrouiller toute interprétation face à des situations ambigües que les employés ne manqueraient pas d'exploiter à leur avantage. L'un des points de discorde concerne l'usage des équipements de l'employeur en dehors des heures de travail. Ainsi que le souligne Ian J. Turnbull, cette question suscite des réponses variées :

> « We wonder: may an employee travelling overnight on organization business use the organization's laptop for personal use after hours? Some would say yes with no conditions. Others would say that the use has to meet legal, and perhaps behavioural, standards (no navel-gazing), while still others would say absolutely not, pointing out that the employee would still be using the employer's network to access the Net. »[497]

Une clarification en matière d'utilisation des ressources informatiques de l'entreprise est donc souhaitable, voire incontournable. Et cela d'autant plus qu'une bonne information sur le contenu des droits et obligations de chacun permet une plus grande responsabilisation des employés et une utilisation plus rationnelle des ressources informatiques.

Le contenu des directives patronales varie d'une entreprise à l'autre, en fonction des préoccupations propres à chacune, et peut aller du simple catalogue de conseils et règles de savoir-vivre à l'édiction de véritables obligations assorties de sanctions pouvant aller jusqu'au congédiement. En fait, ni la loi ni la jurisprudence ne donnent d'indications quant à la teneur des politiques Internet, aussi c'est à la doctrine qu'est revenu le soin d'en déterminer le contenu « idéal ». À cet égard, une majorité d'auteurs s'accordent pour dire qu'il n'y a pas de contenu standard et figé et que ce dernier devrait être évolutif et

---

[497] I. J. TURNBULL, « Identity Theft and Surveillance in the Workplace », préc., note 453, p. 31.

déterminé en fonction de facteurs propres à l'entreprise[498]. En réalité, le contenu de la politique Internet sera souvent fonction, pour une large part, de la taille de l'entreprise, de son domaine d'activité, de l'utilisation des ressources électroniques qu'elle attend de ses employés[499] et de son degré de familiarisation avec l'Internet. Toutefois, les pistes de solutions fournies par la doctrine tournent autour d'un contenu « minimal » regroupant les quatre rubriques suivantes : la raison d'être de la politique Internet et de la surveillance patronale, les usages permis ou interdits, les conséquences auxquelles les employés s'exposent et les attentes en matière de vie privée[500]. L'annexe I fournit une liste des principales clauses à prendre en compte lors de l'élaboration d'une politique Internet.

1.1.1. La raison d'être de la politique Internet et de la surveillance patronale

Idéalement, la première chose que l'employeur devrait s'attacher à faire est d'informer les employés des raisons de la mise en place d'une politique Internet et de la surveillance patronale[501]. Une telle initiative est souhaitable afin de maintenir un climat de travail sain et de permettre une meilleure compréhension des enjeux liés à l'utilisation des technologies de l'information[502]. À cet effet, l'employeur doit informer les employés sur les risques encourus et les sensibiliser aux problèmes juridiques, ainsi qu'aux risques liés à la sécurité, la confidentialité, la productivité, etc.

La politique Internet doit également contenir un volet consacré aux contrôles mis en place par l'entreprise. À cet égard, des procédures de sécurité strictes devraient être adoptées, notamment vis-à-vis de la transmission de fichiers et des téléchargements, afin de vérifier

---

[498] C. DEEHY, préc., note 493.

[499] *Id.*

[500] F. CÔTÉ, préc., note 251; Karl DELWAIDE, « L'Internet en milieu de travail et les politiques et directives relatives à l'utilisation des nouvelles technologies », Fasken.com, 2001, p. 47-52, en ligne : <http://www.fasken.com/files/Publication/2bdfed9a-a187-4755-abc3-04fd5e0c6bb1/Presentation/PublicationAttachment/6bed511b-6037-4345-a9f6-09760d937b45/L_INTERNET_EN_MILIEU_DE_TRAVAIL.pdf> (site consulté le 19 août 2010).

[501] I. LAUZON et L. BERNIER, préc., note 363, p. 103.

[502] I. J. TURNBULL « Privacy Management Plan and Policies », préc., note 492, p. 242.

que les messages et contenus échangés ne violent aucune loi[503]. L'employeur devrait, par exemple, indiquer la taille maximale autorisée pour les fichiers, ainsi que les provenances ou destinations autorisées. Les salariés devraient également être informés des conditions d'accès à l'Internet, au courrier électronique et au système d'information en général : ils devraient notamment savoir si tous les réseaux et programmes sont indifféremment accessibles à tous ou si l'accès à certains d'entre eux est restreint et soumis à une autorisation spéciale[504]. En cas d'accès limité, l'entreprise peut prévoir un message d'avertissement avisant l'utilisateur que tel programme ou site auquel il souhaite accéder lui est interdit et que toute utilisation non-autorisée l'expose à des poursuites. L'employeur serait aussi avisé de préciser si et à quelles conditions les salariés sont autorisés à accéder aux réseaux de l'entreprise en dehors de ses locaux[505]. Si l'entreprise protège ses équipements avec des mots de passe, il serait également judicieux qu'elle mette en place des procédures obligeant les employés à garder leur mot de passe personnel confidentiel et à s'abstenir d'accéder, sans permission ou sans raison légitime, aux fichiers des autres employés ou aux programmes non-autorisés[506]. Il serait également nécessaire de centraliser les informations[507] afin que l'employeur dispose d'une liste complète et à jour des mots de passe et des autorisations qui y sont attachés, de façon à toujours être en mesure d'identifier l'utilisateur qui ouvre une session ou, à tout le moins, de savoir quel est l'utilisateur dont le mot de passe est utilisé. Cela permettrait, en cas de discorde, de rapprocher les heures de présence du salarié sur lequel pèsent les soupçons avec les connexions litigieuses.

1.1.2. Les usages autorisés ou interdits

En second lieu, l'employeur devrait indiquer sa position quant à l'utilisation attendue des outils électroniques mis à la disposition des salariés en décrivant les droits et obligations de

---

[503] I. LAUZON et L. BERNIER, préc., note 363, p. 104.

[504] John B. LEWIS, « I know what you e-mailed last summer (Legal Update Employee Monitoring) », *Security Management* 93, January, 2002, en ligne : <http://www.entrepreneur.com/tradejournals/article/82015917.html> (site consulté le 19 août 2010).

[505] C. DEEHY, préc., note 493.

[506] I. LAUZON et L. BERNIER, préc., note 363, p. 103.

[507] C. DEEHY, préc., note 493.

chacun. À cet effet, il serait judicieux qu'il fournisse une explication très détaillée sur les modalités d'utilisation. Il est impossible de donner une liste exhaustive des comportements potentiellement dangereux pour l'entreprise; cependant, la doctrine s'accorde pour dire que plus le contenu de la politique est détaillé et précis, mieux l'entreprise est armée pour prévenir les risques et abus liés à l'utilisation des outils électroniques par les salariés[508]. L'employeur devrait donc définir de façon la plus précise possible le périmètre des comportements souhaités en indiquant ce qui est interdit et ce qui est autorisé. Il peut, notamment, préciser qui est autorisé à accéder à l'Internet ou à utiliser le courrier électronique, quand et à quelles fins[509]. À cet égard, il pourrait rappeler aux employés que les ressources électroniques mises à leur disposition, ainsi que les droits qui s'y rattachent, sont la propriété exclusive de l'entreprise[510] et qu'elles doivent donc, sauf autorisation expresse, n'être utilisées qu'à des fins professionnelles. Bref, il faudrait que l'employeur définisse clairement la limite entre l'utilisation personnelle et l'utilisation à des fins professionnelles. Et lorsqu'il autorise l'utilisation à des fins personnelles d'Internet et du courriel, il devrait alors souligner qu'il s'agit d'un privilège accordé aux employés ou à certaines catégories d'entre eux et qu'il ne tolère une telle utilisation que dans la mesure où elle demeure raisonnable et occasionnelle et ne cause aucun préjudice à l'entreprise[511]. Il ne faut, en effet, pas oublier que l'utilisation en dehors des horaires habituels n'élimine pas la responsabilité juridique de l'entreprise. Cette dernière devrait donc informer de manière précise ses employés sur ce qu'ils sont autorisés à faire pendant et en dehors des horaires de travail : par exemple, peuvent-ils créer des pages personnelles ou encore participer à des chaînes de messages du style « envoyez ce message à tous vos amis et connaissances »? Même lorsque l'usage à des fins autres que professionnelles est interdit, l'employeur doit

---

[508] I. LAUZON et L. BERNIER, préc., note 363, p. 103-104.

[509] F. CÔTÉ, préc., note 251.

[510] *Id.*

[511] J. B. LEWIS, préc., note 504.

néanmoins préciser les modalités d'utilisation et dire si, par exemple, les employés pourront télécharger ou installer des logiciels gratuits utiles à l'accomplissement de leurs tâches[512].

Enfin, la politique Internet doit, dans la mesure du possible, prévoir des règles pour gérer certaines situations particulières, comme, par exemple, la question des fenêtres intempestives : les salariés seront-ils autorisés à ouvrir celles qui n'auront pas été bloquées par le système de filtrage de l'entreprise? De même, pourront-ils lire les pourriels qui auront réussi à passer à travers les mailles du filet? Etc.

Bref, l'employeur a intérêt à balayer autant que possible tous les éventuels sujets de discorde, en incluant, notamment, les éléments suivants dans sa politique Internet[513] :

- une interdiction de se livrer à des actes de discrimination, harcèlement, diffamation ou de tenir des propos injurieux envers autrui. À cet égard, l'employeur devrait rappeler aux employés les règles applicables en matière de protection des droits des personnes;
- des dispositions relatives aux fuites de confidentialité : la politique devrait interdire toute diffusion d'informations confidentielles ou privilégiées concernant l'entreprise ou ses clients. La diffusion des renseignements personnels des employés ou de tiers en relation d'affaires avec l'entreprise, sans leur consentement, devrait également être interdite[514]. Il serait judicieux, lorsque le secret professionnel est en jeu, d'insister auprès des employés qui y sont soumis sur les responsabilités découlant de cette obligation[515]. Pour garantir la confidentialité de ses documents, l'entreprise peut prévoir des mesures de cryptage lors de la transmission par voie électronique de fichiers sensibles[516];

---

[512] C. DEEHY, préc., note 493.

[513] I. LAUZON et L. BERNIER, préc., note 363, p. 103-104.

[514] F. CÔTÉ, préc., note 251.

[515] K. DELWAIDE, préc., note 500, à la page 50.

[516] F. CÔTÉ, préc., note 251.

- l'interdiction d'accéder, de détenir ou de diffuser du matériel pornographique et, de façon générale d'accéder à des sites illicites ou de diffuser des contenus interdits;
- un rappel des règles applicables en matière de propriété intellectuelle, avec une interdiction faite aux salariés d'utiliser de façon inappropriée le matériel protégé par le droit d'auteur et l'obligation de ne faire usage que des programmes pour lesquels l'employeur détient une licence en bonne et due forme[517]. À cet égard, il faudrait non seulement rappeler que le téléchargement de logiciels est interdit, mais aussi préciser que cette interdiction concerne même les logiciels utiles au salarié dans son travail. Par conséquent, avant d'installer quelque programme que ce soit, les employés devraient préalablement obtenir l'approbation de l'employeur[518]. Cette précaution, qui vise à préserver les droits des tiers, constitue également une mesure de sécurité supplémentaire contre les éventuels programmes malveillants.

1.1.3. Les conséquences du non-respect de la politique Internet

Pour une meilleure efficacité, la politique Internet devrait contenir des clauses prévoyant les procédures et sanctions en cas d'usage non conforme des ressources électroniques : les employés doivent, en effet, être informés qu'en cas de comportement fautif, ils s'exposent à des mesures disciplinaires pouvant aller jusqu'au congédiement[519]. De plus, l'employeur peut les poursuivre en dommages, voire en injonction[520].

Certaines entreprises disposent de politiques décrivant de façon très détaillée les sanctions encourues en cas de non-respect, ainsi que les procédures et méthodes d'évaluation des mesures disciplinaires[521]. L'avantage de telles politiques est qu'elles sont susceptibles de favoriser une meilleure adhésion des salariés aux valeurs véhiculées, puisque l'employeur y

---

[517] I. LAUZON et L. BERNIER, préc., note 363, p. 104.

[518] *Id.*, p. 103-104.

[519] F. CÔTÉ, préc., note 251; I. J. TURNBULL « Privacy Management Plan and Policies », préc., note 492, p. 242.

[520] K. DELWAIDE, préc., note 500, à la page 14.

[521] Voir, par exemple, *Gilles* et *Ciba Spécialités chimiques Canada Inc.,* 2008 QCCRT 134 (CanLII).

liste des obligations qu'il s'engage à respecter. La politique leur paraîtra alors moins arbitraire et pourra même être perçue comme un véritable contrat entre les parties.

1.1.4. Les attentes en matière de vie privée

Un autre volet de la politique devrait être consacré à la délicate question de la vie privée. Les salariés devraient être avisés que leur utilisation des ressources informatiques de l'employeur les expose à la surveillance et au contrôle de ce dernier[522]. Pour éviter les conflits, l'employeur devrait, dès le départ, circonscrire son contrôle en en précisant les modalités[523], ainsi que sa conception de l'expectative de vie privée des salariés[524]. L'entreprise devrait, notamment, indiquer ce qui sera contrôlé (utilisation du courrier électronique? navigation sur Internet?), dans quelles circonstances et à quelle fréquence (par exemple, sur une base régulière ou uniquement en cas de soupçons sur les agissements d'un employé particulier?)[525]. De plus, l'employeur devrait préciser ce qu'il adviendra de l'information découlant de la surveillance effectuée[526].

Lorsqu'il expose ses attentes en matière de vie privée, l'employeur pourra en profiter pour réduire au minimum toute expectative des salariés dans ce domaine. À cet égard, certains auteurs invitent les entreprises à inclure dans leur politique Internet une clause avisant les employés qu'en utilisant les outils électroniques mis à leur disposition par l'employeur, ils acceptent implicitement la surveillance patronale[527]. Une telle clause pourra, par exemple, prévoir que l'utilisation de l'Internet ou du courrier électronique ne pourra en aucun être reconnue comme « confidentielle » et que les employés renoncent, en conséquence, à invoquer leur droit à la protection de la vie privée lorsqu'ils utilisent ces outils[528]. Toutefois, s'il est préférable que l'employeur prenne les devants pour délimiter la « sphère

---

[522] F. CÔTÉ, préc., note 251.

[523] C. DEEHY, préc., note 493.

[524] F. CÔTÉ, préc., note 251.

[525] C. DEEHY, préc., note 493.

[526] K. DELWAIDE, préc., note 500, p. 51.

[527] I. J. TURNBULL, « Privacy Management Plan and Policies », préc., note 492, p. 242, F. CÔTÉ, préc., note 251.

[528] J. B. LEWIS, préc., note 504.

de protection de la vie privée » qu'il souhaite accorder à ses employés, il faudra néanmoins qu'il évite d'accéder au courrier électronique d'un employé sans son consentement[529]**.** À cet égard, il serait judicieux que l'entreprise avise les tiers que les messages électroniques échangés avec les employés peuvent être conservés par l'employeur à des fins de contrôle et de surveillance et que, par conséquent, d'autres personnes que leur correspondant peuvent y avoir accès[530].

Il ne suffit pas à l'employeur d'adopter une politique Internet pour pouvoir valablement s'en prévaloir contre ses employés : la question de l'opposabilité de ces documents et, plus généralement, de leur validité peut, en effet, se poser.

1.2. Les critères de validité des politiques Internet

À ce jour, la valeur juridique des politiques Internet demeure incertaine, car elles sont relativement récentes, ne sont pas obligatoires et ne sont réglementées par aucun texte. Ce sont donc la doctrine et la jurisprudence qui se sont chargées de dire si et dans quelles conditions elles peuvent produire des effets juridiques.

Au Québec, l'employeur a la possibilité de définir unilatéralement ses attentes dans une politique d'entreprise[531]. Cependant, précisément en raison de ce caractère unilatéral, les tribunaux ne sont aucunement liés par l'intégralité d'une politique patronale et peuvent donc en réviser le contenu[532]. La jurisprudence, notamment avec *Lumber & Sawmill Workers' Union, Local 2537 and K.V.P.* Co. *Ltd.*[533], a dégagé les six critères suivants pour

---

[529] K. DELWAIDE, préc., note 500, p. 14.

[530] *Id.*

[531] I. LAUZON et L. BERNIER, préc., note 363, p. 7.

[532] *Association des professionnels de la Régie régionale de la santé et des services sociaux 002 (C.S.N.)* c. *Régie régionale de la santé et des services sociaux du Saguenay-Lac-St-Jean*, [2002] R.J.D.T. 990 (T.A.); I. LAUZON et L. BERNIER, préc., note 363, p. 7.

[533] [1965] O.L.A.A. No. 2 (L.A.) (QL/LN), [1965] 16 L.A.C. 730 (Ont. L.A.) : dans cette affaire, l'employeur avait mis en place une politique d'entreprise sans avoir préalablement obtenu l'accord du syndicat des employés. La validité de celle-ci fut ultérieurement examinée par un arbitre, lorsqu'un employé fut sanctionné pour l'avoir enfreinte. L'arbitre conclut qu'un employeur pouvait adopter une politique de façon unilatérale, à condition, toutefois, que celle-ci fût raisonnable. Il énuméra six critères permettant d'apprécier la validité d'une politique patronale. Ces principes, toujours en vigueur,

apprécier la validité d'une politique d'entreprise : ce règlement doit être connu des employés (1.2.1.); il doit être clair et non équivoque (1.2.2.); il doit être appliqué de façon constante et uniforme (1.2.3.); les salariés doivent connaître les conséquences de sa violation (1.2.4); il doit être raisonnable (1.2.5.) et, enfin, il doit être conforme à la législation (1.2.6.)[534].

1.2.1. La connaissance de la politique par les employés

La politique doit être connue des employés qui doivent avoir été avisés de son existence et son contenu. Le cas échéant, les salariés pris en défaut pourront toujours prétendre que les obligations qu'ils auraient prétendument violées ne leur sont pas opposables puisqu'elles ne leur ont pas été communiquées[535]. L'employeur doit donc diffuser sa politique Internet de façon formelle, par exemple, par la remise à main propre d'un exemplaire à chaque employé, la publication d'avis dans les lieux d'affichage habituels au sein de l'entreprise ou la diffusion grâce au courrier électronique ou l'Intranet. En l'absence de remise individuelle de ce document ou en cas de diffusion restreinte, les tribunaux pourront conclure que les employés n'en ont pas eu connaissance[536]. L'employeur peut se ménager un bon moyen de preuve s'il obtient la signature de ses employés accusant réception de la politique Internet et confirmant leur engagement à s'y conformer. Il peut prendre des précautions supplémentaires pour rappeler aux employés leurs obligations, notamment grâce à un mécanisme se déclenchant automatiquement chaque fois qu'ils tenteraient d'accéder à l'Internet ou au courrier électronique, et qui afficherait un message les avisant que leur

---

servent régulièrement de fondement aux décisions des tribunaux : voir, par exemple, *Travailleurs et travailleuses unis de l'alimentation et du commerce, local 502* c. *Canon Canada Inc.*, 2008 CanLII 56025 (QC A.G.), qui s'y réfère.

[534] C. Gordon SIMMONS, « Arbitral Stare Decisis: An Unheralded but Important Doctrine in Canadian Arbitral Jurisprudence Labour Law », (1985-1986) 11 *Queen's L.J.* 347, 350.

[535] *Fiset* c. *Service d'administration P.C.R. Ltée*, préc., note 174; *Briar* c. *Canada (Conseil du Trésor)*, 2003 CRTFP 3 (CanLII) : dans cette décision de la Commission des relations de travail dans la fonction publique rejette l'argumentation des plaignants, car l'employeur avait communiqué sa politique aux employés au moins cinq fois dans un laps de temps inférieur à un an. De plus, ces derniers recevaient un avertissement avec demande d'accusé de réception chaque fois qu'ils se connectaient à la messagerie électronique.

[536] *Fiset* c. *Service d'administration P.C.R. Ltée*, préc., note 174; J. B. LEWIS, préc., note 504.

utilisation est soumise au contrôle et à la surveillance de l'employeur[537]. En principe, cet avis requiert de l'employé un geste positif, soit d'acceptation pour indiquer qu'il a bien lu l'avis et qu'il en accepte la teneur, soit de refus[538], auquel cas il serait automatiquement déconnecté du système[539].

1.2.2. L'utilisation d'un langage clair et sans équivoque

Le simple fait de communiquer la politique aux employés ne suffit, en effet, pas à établir sa connaissance : il faudrait en plus s'assurer que les employés en ont bien compris les objectifs[540]. Il s'agit là d'un point essentiel, car les salariés fautifs seront souvent tentés d'exploiter les situations ambigües[541]. L'employeur a donc intérêt, pour éviter tout problème d'interprétation, à rédiger sa politique Internet dans des termes simples et accessibles à tous. En cas de doute, les tribunaux devront déterminer si la politique est suffisamment claire. Ils seront enclins à conclure positivement si les employés en ont reçu une copie lors de leur embauche ou en cours d'emploi, surtout lorsque cette remise s'est accompagnée de la signature d'un formulaire dans lequel ils reconnaissaient formellement avoir reçu ce document[542].

1.2.3. L'application constante et uniforme de la politique

La politique doit être appliquée de façon uniforme et constante, et ce, dès son entrée en vigueur. Les tribunaux sont en effet enclins à interpréter toute tolérance en faveur des salariés[543]. Aussi, l'employeur doit-il « prendre les moyens raisonnables » pour s'assurer que sa politique Internet sera suivie et appliquée[544] et éviter toute situation qui pourrait être interprétée par les employés comme les autorisant à s'écarter des lignes directrices de ce

---

[537] I. LAUZON et L. BERNIER, préc., note 363, p. 102; J. B. LEWIS, préc., note 504.

[538] *Briar* c. *Canada (Conseil du Trésor)*, préc., note 535; K. DELWAIDE, préc., note 500, p. 48.

[539] I. LAUZON et L. BERNIER, préc., note 363, p. 102

[540] *Id.*, p. 7.

[541] *Fiset* c. *Service d'administration P.C.R. Ltée*, préc., note 174.

[542] *Martel* c. *Fédération des caisses Desjardins du Québec*, 2006 QCCRT 300 (CanLII).

[543] *Fiset* c. *Service d'administration P.C.R. Ltée*, préc., note 174.

[544] K. DELWAIDE, préc., note 500, p. 6.

règlement. L'employeur doit également veiller à rester cohérent dans l'application de ses directives, les mêmes décisions devant être prises par rapport à des situations identiques[545].

Bien entendu, l'employé qui invoque la tolérance ou la disparité des sanctions infligées par l'employeur pour des comportements similaires doit être en mesure d'établir l'inconsistance patronale. À cet égard, on peut s'interroger sur la portée du principe de tolérance lorsque le salarié a fait l'objet de plusieurs mesures disciplinaires réprimant les mêmes violations de la politique d'entreprise, sans pour autant avoir été congédié. Peut-on considérer que l'on se trouve face à une tolérance de l'employeur face à l'inconduite répétée de son employé? C'est en tout cas ce que prétendait un salarié dans *Backman* c. *Maritime Paper Products Limited, corps constitué*[546]. Le plaignant avait reçu deux avertissements, deux années de suite, pour avoir consulté des sites pornographiques et prétendait que l'employeur avait, par la suite, fermé les yeux sur une conduite ultérieure similaire et lui avait même accordé des augmentations de salaire, puis l'avait sommairement congédié, plus de trois ans après le deuxième avertissement, pour d'autres nouvelles navigations sur des sites interdits. La Cour d'appel du Nouveau-Brunswick n'a pas suivi l'argumentation du salarié. Elle a plutôt conclu que l'employeur n'avait aucunement toléré ces écarts de conduite qui avaient été systématiquement réprimandés, notamment, par deux avertissements officiels, dont le dernier avisait l'employé qu'il encourrait le congédiement en cas de récidive. Et, bien que la politique d'entreprise, qu'il connaissait et avait signée, prohibe de tels comportements, il avait délibérément choisi, à au moins deux reprises, de ne pas prendre cet avertissement au sérieux. La première récidive n'avait fait l'objet d'aucune réprimande, la direction ayant estimé ne pas disposer de preuve suffisante pour engager une procédure disciplinaire; quant à la deuxième, elle avait eu lieu un an plus tard. La Cour a donc conclu que l'employé avait été congédié en raison d'une nouvelle violation de la politique d'entreprise, constituée par la dernière série de visites sur des sites pornographiques au travail. Ce sont ces agissements qui avaient irrémédiablement

---

[545] *Fiset* c. *Service d'administration P.C.R. Ltée*, préc., note 174; I. LAUZON et L. BERNIER, préc., note 363, p. 9-10.

[546] 2009 NBCA 62 (CanLII).

entraîné une perte de confiance de l'employeur en la capacité du salarié à exercer ses fonctions de supervision. Dans de telles conditions, le principe de la tolérance ne pouvait être retenu au profit du salarié.

1.2.4. L'information des salariés sur les conséquences du non-respect de la politique

Les employés doivent, en effet, savoir qu'ils s'exposent à des sanctions pouvant aller jusqu'au congédiement, en cas de comportement inapproprié. Le fait d'avoir une indication de l'échelle des sanctions encourues et d'être informés que leurs écarts de conduite peuvent leur coûter leur emploi peut constituer un excellent moyen de dissuasion pour les salariés.

Pour cette raison, les tribunaux pourront se monter particulièrement sévères vis-à-vis des salariés qui ont participé à la mise en place de la politique concernant Internet et qui, par conséquent, ne devraient pas s'étonner d'être sanctionnés, même pour des écarts de conduite plutôt minimes. C'est ce qu'a conclu l'arbitre dans l'affaire *Centre de réadaptation Lethbridge* c. *Syndicat des physiothérapeutes et des thérapeutes en réadaptation physique du Québec*[547], au sujet d'un salarié qui contestait une suspension de 5 jours, infligée en raison de navigations sur des sites pornographiques. L'arbitre a maintenu cette sanction, malgré la relative faiblesse de la faute du plaignant (les navigations s'étaient déroulées sur une journée), la qualité de son dossier (qui était alors vierge) et son ancienneté (27 ans), après avoir relevé que la politique d'entreprise, que salarié connaissait parfaitement, puisqu'il avait siégé au comité qui l'avait adoptée, interdisait la consultation de sites pornographiques. Dans ce contexte, il était important pour l'employeur d'imposer une sanction exemplaire au plaignant, afin d'indiquer à tous les employés le sérieux qu'il accordait au respect de sa politique.

D'un autre côté, lorsque l'employeur décrit les procédures disciplinaires et les sanctions applicables dans sa politique d'entreprise, il est tenu de respecter ces règles qu'il a lui-

---

[547] *Centre de réadaptation Lethbridge* et *Syndicat des physiothérapeutes et des thérapeutes en réadaptation physique du Québec*, D.T.E. 2004T-755 (T.A.).

même établies. Comme le souligne le Tribunal dans *Gilles* et *Ciba Spécialités chimiques Canada Inc.*, si l'employé a des obligations, l'employeur en a également[548]. Dans cette affaire, l'employeur avait mis en place un règlement d'entreprise qui décrivait de façon très précise et détaillée les comportements acceptables, ainsi que les règles encadrant le déroulement des procédures disciplinaires. Or, en l'espèce, il avait ignoré les critères ainsi fixés et avait sommairement congédié le salarié, à qui il reprochait d'innombrables consultations de sites pornographiques, sans lui avoir donné la possibilité de s'expliquer sur les faits qui lui étaient reprochés et alors même que son dossier disciplinaire était vierge[549]. Le salarié n'avait même pas été informé de la nature disciplinaire de l'entretien auquel il était convié!

1.2.5. Le caractère raisonnable de la politique

La politique Internet doit être raisonnable, c'est-à-dire qu'elle ne doit être ni arbitraire, ni abusive ou discriminatoire. Ainsi, dans l'affaire *Association des professionnels de la Régie régionale de la santé et des services sociaux 002 (C.S.N.)* c. *Régie régionale de la santé et des services sociaux du Saguenay-Lac-St-Jean*[550], l'arbitre invalide les dispositions d'une politique Internet exigeant que les salariés complètent un formulaire de demande d'autorisation d'utilisation d'Internet au motif qu'elles pouvaient avoir pour effet de priver un ensemble de salariés d'un outil de travail essentiel pour l'exécution de leurs tâches. Il en conclut qu'une telle exigence rendait la politique patronale déraisonnable et inappropriée. De plus, elle affectait les conditions de travail des salariés, puisque le consentement du syndicat était requis selon les termes de la convention collective alors en vigueur. L'arbitre modifia donc la politique de façon à la rendre « raisonnablement acceptable et compatible avec la convention collective »[551].

---

[548] Préc., note 521, par 34.

[549] Voir également *Alberta Union of Provincial Employees v. Alberta*, préc., note 234, qui annule le congédiement d'un employé non pas pour absence de cause juste et sérieuse, mais plutôt en raison du non-respect par l'employeur des règles fixées par la convention collective pour les procédures disciplinaires.

[550] Préc., note 532.

[551] Y. SAINT-ANDRÉ, préc., note 122, p. 9.

1.2.6. La conformité de la politique aux dispositions législatives et règlementaires

Le politique doit, enfin, être conforme aux lois, à l'équité et à la convention collective éventuellement applicables. L'employeur doit, notamment, respecter les dispositions relatives à la protection des renseignements personnels et à la vie privée[552].

Les six critères de validité qui viennent d'être énoncés sont évalués par les tribunaux comme un ensemble et peuvent contribuer à grandement diminuer la portée de la politique lorsqu'ils ne sont pas satisfaits[553]. La quête de satisfaction de ces critères doit être combinée à d'autres facteurs susceptibles d'augmenter l'efficacité de la politique Internet.

1.3. Les autres facteurs de réussite de l'implantation de la politique Internet

En plus de porter une attention particulière à la rédaction de sa politique Internet, l'entreprise doit prendre les moyens appropriés pour que celle-ci soit effectivement appliquée par les employés.

Pour y parvenir, elle doit d'abord s'attacher à obtenir l'adhésion du personnel aux valeurs que la politique véhicule. En effet, si certains employés comprennent parfaitement qu'il est normal que l'employeur limite ou interdise l'usage de l'Internet et du courrier électronique, tous n'en saisissent pas toujours les enjeux. Une partie d'entre eux interprètent ces restrictions comme résultant d'une mauvaise gestion des ressources humaines. Il faut dire qu'il existe parfois un décalage générationnel entre les dirigeants des entreprises, qui sont généralement peu familiarisés avec les NTIC, et une grosse majorité de salariés pour qui ces outils font partie de leur mode de vie. Les premiers sont généralement partisans d'un usage uniquement professionnel de ces outils, tandis que les seconds revendiquent le droit à un usage personnel. L'employeur a donc intérêt à instaurer un climat de confiance, par

---

[552] Pour une illustration, *Section locale 143 du Syndicat canadien des communications, de l'énergie et du papier* c. *Goodyear Canada inc.*, D.T.E. 2008T-27 (C.A.), par.18, statuant qu'une « politique, qui prévoit des tests de dépistage d'alcool et de drogues doit franchir le test de l'article 9.1 de la *Charte*, une disposition justificative dont l'application est soumise aux critères de l'objectif poursuivi et du moyen adopté (lien rationnel, atteinte minimale et effet de la mesure) »; Voir également K. DELWAIDE, préc., note 500, p. 51.

[553] I. LAUZON et L. BERNIER, préc., note 363, p. 8.

exemple, en associant les employés à l'élaboration de la politique Internet : ces derniers seront, en effet, plus enclins à appliquer une politique qu'ils ont contribué à créer[554]. De plus, celle-ci aura une force morale encore plus grande si sa mise en place résulte d'une concertation entre l'employeur et les employés ou leurs représentants[555]. Tous les corps de métiers, notamment les services juridique, informatique et de ressources humaines – qui sont en première ligne pour gérer les difficultés juridiques, techniques ou disciplinaires – devraient, autant que possible, y participer. L'entreprise peut également mettre en place, sur une base régulière, des actions pour informer les salariés et les responsables sur les risques liés à l'utilisation des outils électroniques et les former à une utilisation plus rationnelle des ces ressources[556]. L'employeur pourra désigner une personne chargée d'assurer la bonne application de la politique, de répondre aux interrogations des employés, de coordonner la formation continue et d'effectuer les éventuelles mises à jour. Pour un résultat optimal, l'employeur devrait s'adjoindre les services de professionnels avant la mise en place de sa politique Internet : ceux-ci seront en effet mieux outillés pour identifier toutes les contraintes et doter l'entreprise des règles et procédures appropriées[557]. Ainsi, pour ne mentionner que l'aspect juridique, les règles applicables sont souvent si peu lisibles et contradictoires que le recours à un juriste spécialisé est presqu'incontournable.

Toujours dans un souci d'efficacité, l'employeur doit veiller à ce que sa politique Internet soit adaptée aux particularités de l'entreprise, de son personnel, etc.[558], et reflète ses préoccupations (volonté d'éviter le « *surf* » ludique et improductif des salariés, de protéger l'entreprise contre les menaces extérieures, de prévenir les risques liés à une utilisation inappropriée de l'Internet, etc.). À cet effet, il dispose d'une large palette d'interdictions ou de limitations d'inégale importance : blocage systématique interdisant tout accès aux sites illicites; aménagement de plages horaires permettant une utilisation modérée à des fins

---

[554] I. J. TURNBULL, « Privacy Management Plan and Policies », préc., note 492, p. 243.

[555] I. LAUZON et L. BERNIER, préc., note 363, p. 8.

[556] F. CÔTÉ, préc., note 251; W. G. PORTER II, M. C. GRIFFATON, préc., note 354.

[557] I. J. TURNBULL, « Privacy Management Plan and Policies », préc., note 492, p. 242.

[558] C. DEEHY, préc., note 493.

personnelles en dehors des heures de bureau ou selon un système de « quota » d'heures allouées aux salariés sur une base hebdomadaire ou mensuelle pour la navigation sur des sites non professionnels; système de déblocage permettant à l'utilisateur d'accéder à un site non professionnel sur autorisation d'un supérieur[559]. Il pourrait, cependant, être opportun que la politique ne comporte pas que des interdictions et que l'employeur prenne en compte les préoccupations et intérêts des employés. Ainsi, l'entreprise pourrait autoriser un usage raisonnable du courrier électronique pour les salariés distants (télétravailleurs ou salariés situés sur des sites éloignés géographiquement) afin de maintenir un lien social avec les autres employés de l'entreprise[560]. Elle pourrait également permettre une utilisation de l'Internet à des fins personnelles en dehors des heures de travail, à condition que celle-ci soit modérée et conforme aux lois et aux valeurs de l'entreprise[561]. Certains employeurs aménagent même des espaces dédiés aux salariés et disposant d'ordinateurs reliés à un réseau indépendant, où les salariés peuvent, en dehors de leurs heures de travail, utiliser l'Internet et le courrier électronique pour leurs propres besoins[562]. Toutefois, cette stratégie, qui repose en fait sur le bon jugement des employés, peut se révéler dangereuse pour l'employeur; aussi certaines entreprises sont-elles tentées d'interdire toute utilisation à des fins personnelles des moyens de communication. Cependant, un tel radicalisme convient mal au contexte actuel de banalisation des NTIC : l'ordinateur et l'Internet font désormais partie du quotidien d'une grande majorité d'individus, si bien que certains militent plutôt pour un usage personnel « raisonnable » des ces outils au bureau[563]. Par ailleurs, il est fréquent que les employés effectuent des appels personnels pendant les heures de travail (par exemple, pour prévenir le service de garde que l'on sera en retard pour récupérer les

---

[559] W. G. PORTER II, M. C. GRIFFATON, préc., note 354.

[560] I. DE BENALCÁZAR, préc., note 28, p. 69.

[561] I. LAUZON et L. BERNIER, préc., note 363, p. 103; J. B. LEWIS, préc., note 504.

[562] *Martel* c. *Fédération des caisses Desjardins du Québec*, préc., note 542.

[563] Charles MORGAN, « Monitoring Employee, Electronic Mail and Internet Use: Balancing Competing Rights », dans Vincent GAUTRAIS (dir.), *Droit du commerce électronique*, Montréal, Éditions Thémis, 2002, p. 171, n° 94 à la page 209; COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, *22ème Rapport d'activité 2001*, 2002, p. 58, en ligne : <http://lesrapports.ladocumentationfrancaise.fr/BRP/024000377/0000.pdf> (site consulté le 26 juillet 2010); S. LEFEBVRE, « Naviguer sur Internet au travail: et si on nageait en eaux troubles? », préc., note 254, p. 53.

enfants), si bien que, même en présence d'une politique, l'employeur devrait s'attendre à ce que les moyens de communication électroniques soient utilisés pour les mêmes fins[564]. Il a même été jugé, dans l'affaire *Bell Canada*, qu'une interdiction absolue de l'usage personnel de ces outils n'était pas raisonnable en milieu de travail[565]. Aussi de nombreux auteurs conseillent-ils aux entreprises non pas d'interdire toute utilisation personnelle mais plutôt d'aviser les employés qu'un tel usage devrait rester raisonnable et ne pas avoir d'impact négatif dans l'accomplissement de leur travail[566]. En France, par exemple, la CNIL a également indiqué qu'« une interdiction générale et absolue de toute utilisation d'Internet à des fins autres que professionnelles ne paraît pas réaliste dans une société de l'information et de la communication »[567]. Il faut souligner que les tribunaux français ont tendance à interpréter restrictivement toute restriction des libertés et, en cas de litige, le juge sera enclin à appliquer le principe de proportionnalité indépendamment du contenu de la politique Internet[568].

1.4. L'impact juridique de la politique Internet

La jurisprudence, notamment avec l'affaire *Commission des normes du travail* c. *Bourse de Montréal*[569], a confirmé, au cours des dernières années, qu'il était indispensable que les entreprises se dotent d'une politique Internet. De nombreuses conséquences juridiques sont en effet rattachées à l'existence ou non d'une telle politique au sein de l'entreprise. De plus, l'impact juridique d'une politique Internet dépend étroitement de sa validité. En effet, comme indiqué précédemment, le défaut de validité des six critères énoncés ci-dessus peut

---

[564] C. MORGAN, préc., note 563, n° 94, p. 209.

[565] *Bell Canada* c. *Association Canadienne des Employés de Téléphone*, préc., note 238.

[566] C. MORGAN, préc., note 563, n° 94, p. 203.

[567] COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, *22ème Rapport d'activité 2001*, préc., note 563, p. 58.

[568] COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, *Rapport d'étude et de consultation publique. La cybersurveillance des salariés dans l'entreprise*, Mars 2001, p. 17 et suiv., en ligne : <http://www.cnil.fr/fileadmin/documents/approfondir/rapports/cybersurveillance.pdf> (site consulté le 19 août 2010).

[569] Préc., note 164; *Fiset* c. *Service d'administration P.C.R. Ltée*, préc., note 174; *Syndicat canadien des communications, de l'énergie et du papier, section locale 522* c. *CAE Électronique Ltée*, préc., note 159; *Alliance de la fonction publique du Canada* et *Musée des beaux-arts du Canada*, préc., note 155.

considérablement affaiblir la portée de la politique[570]. Toutefois, il est préférable d'en rédiger une, car ces documents constituent un premier niveau de protection de l'entreprise contre les dangers liés à l'utilisation des outils de communication informatiques. Ils demeurent également une solide ressource sur laquelle l'employeur pourra s'appuyer pour régler les questions concernant, par exemple, la vie privée, qui pourraient surgir[571]. Bref, ils permettent à l'entreprise de prendre les devants et de se prononcer sur de nombreuses questions controversées.

Les principales conséquences juridiques rattachées aux politiques Internet sont les suivantes : la possibilité, pour l'entreprise, d'exercer efficacement son pouvoir de discipline; de limiter sa responsabilité pour les activités en ligne de ses salariés et de réduire l'expectative de vie privée de ces derniers.

1.4.1. La possibilité de discipliner efficacement les salariés

Le non-respect de la politique Internet peut engager la responsabilité de l'employé et justifier des sanctions disciplinaires pouvant aller jusqu'au congédiement[572]. En effet, la politique Internet constitue une extension du contrat de travail et sa violation délibérée et répétée peut irrémédiablement détruire la relation entre l'employé et l'employeur[573]. Toutefois, l'employeur ne doit pas trop tarder à réprimander l'employé : le cas échéant, il pourrait se voir opposer le principe de la tolérance de l'inconduite du salarié et voir sa sanction annulée ou réduite.

L'employeur sera autorisé à sanctionner ses salariés, notamment, si la politique est claire et largement diffusée au sein de l'entreprise[574]. Ces directives auront l'avantage de fixer le

---

[570] Voir *supra*, Partie 2, Chapitre 1, Section 1, 1.2., p. 138.

[571] I. J. TURNBULL, « Privacy Management Plan and Policies », préc., note 492, p. 236.

[572] Voir *Syndicat canadien des communications, de l'énergie et du papier, section locale 522* c. *CAE Électronique Ltée*, préc., note 159; *Alliance de la fonction publique du Canada* et *Musée des beaux-arts du Canada*, préc., note 155; *Blais* c. *Société des Loteries Vidéos du Québec Inc*., préc., note 239.

[573] *Backman* c. *Maritime Paper Products Limited, corps constitué*, préc., note 546.

[574] N.-A. BÉLIVEAU, K. BOUTIN et N. ST-PIERRE, préc., note 177, p. 10; *Syndicat canadien des communications, de l'énergie et du papier, section locale 522* c. *CAE Électronique Ltée*, préc., note 159; *Syndicat des spécialistes et professionnels d'Hydro-Québec* c. *Hydro-Québec*, préc., note 229.

seuil de tolérance de l'entreprise, car, comme l'énonce l'arbitre dans *Fiset* c. *Services d'administration P.C.R. Ltée* :

> « à défaut de directive, qui peut prétendre que le ou la salariée qui rédige une lettre personnelle, fait un appel personnel ou en reçoit un, à partir d'un équipement de l'employeur pose un geste fautif? »[575]

En effet, sauf politique connue de tous et explicite de l'employeur à l'effet contraire, il est d'usage de tolérer que le salarié fasse, à des fins personnelles et que la morale ne réprouve pas, un usage modéré et raisonnable de certains biens de l'entreprise, tels le téléphone[576], l'ordinateur, le courrier électronique ou l'Internet[577]. Par conséquent, en l'absence de politique claire au sein de l'entreprise[578] ou si la politique n'était pas connue des salariés[579] ou n'était pas appliquée de façon uniforme par l'employeur[580], l'employeur risque d'être limité dans sa capacité à discipliner ses salariés et à les congédier. La conséquence sera souvent la modification ou l'annulation de la sanction disciplinaire prise à la suite d'une utilisation inappropriée des outils de communication[581], le congédiement, sauf circonstances aggravantes, n'étant alors pas fondé[582].

L'existence d'une politique Internet connue des employés pourra, dans certaines circonstances, justifier le congédiement sans que l'employeur ait à respecter le principe de la progressivité des sanctions. Ainsi, dans *Bourassa* et *Ville de La Tuque*[583], la Commission a confirmé le congédiement, sans gradation des sanctions disciplinaires, d'un salarié en raison de son utilisation excessive de l'Internet. Il avait, en effet, consulté plus de 25 000 sites en l'espace de trente mois, essentiellement à des fins personnelles. L'employé avait

---

[575] *Fiset* c. *Service d'administration P.C.R. Ltée*, préc., note 174, par. 35.

[576] *Srivastava* c. *Hindu Mission of Canada (Québec) Inc.*, REJB 2001-23958 (C.A.).

[577] M.-F. BICH, préc., note 199, p. 7 (commentaires sous la note 19).

[578] *Commission des normes du travail* c. *Bourse de Montréal Inc.*, préc., note 164.

[579] *Fiset* c. *Service d'administration P.C.R. Ltée*, préc., note 174.

[580] *Id.*

[581] *Commission des normes du travail* c. *Bourse de Montréal Inc.*, préc., note 164; *Belisle* c. *Rawdon (Municipalité)*, préc., note 204.

[582] N.-A. BÉLIVEAU, K. BOUTIN et N. ST-PIERRE, préc., note 177, p. 10.

[583] 2009 QCCRT 322 (CanLII).

reconnu les faits, mais contestait la sévérité de la sanction qui, selon lui, ne respectait pas le principe de proportionnalité, puisqu'il n'avait préalablement reçu aucun avertissement relativement à son utilisation de l'Internet. Il avançait également que ses visites ne s'effectuaient pas sur des sites pornographiques et que ses transgressions n'avaient pas eu d'impact négatif sur son rendement ni sur l'image de l'employeur. Il proposait donc de substituer au congédiement une suspension de 6 mois. La Commission a rejeté son argumentation en raison de la gravité des faits reprochés : en effet, non seulement le salarié était cadre et avait même, antérieurement, occupé la fonction de responsable du réseau informatique pendant 3 ans, mais en plus, l'entreprise disposait d'une politique claire en matière d'utilisation du système informatique dont il connaissait l'existence, puisqu'il avait signé un formulaire en accusant réception. En outre, 96 % de ses navigations étant de nature personnelle, certains contenus visités étant de nature sexuelle ou d'un goût douteux. Enfin, ces activités constituaient un vol de 50 à 75 % de son temps de travail.

Pour conclure sur ce point, il convient de souligner que c'est à l'entreprise de déterminer les comportements acceptables, ainsi que son seuil de tolérance. C'est ce qu'a rappelé la Cour d'appel de l'Alberta dans *Poliquin* v. *Devon Canada Corporation*[584] lorsqu'elle a confirmé le congédiement d'un salarié qui avait enfreint le Code de conduite de l'entreprise, notamment en utilisant son ordinateur professionnel pour recevoir, visionner et transmettre des messages électroniques à caractère sexuel, pornographique ou raciste, le tout pendant ses heures de travail[585]. Les expéditeurs ou destinataires des contenus ainsi échangés étaient aussi bien ses collègues que des fournisseurs et des partenaires d'affaires de l'employeur. Le salarié soutenait, entre autre, qu'il était rarement celui qui entreprenait les échanges, son rôle se bornant à recevoir les messages. De plus, il avançait qu'il existait une culture de tolérance vis-à-vis de contenus sexuels ou à caractère pornographique tant au sein de l'entreprise que de l'industrie pétrolière : ses collègues et lui recevaient, en effet, de nombreux courriels au contenu discutable provenant, pour la plupart, de contacts d'affaires

---

[584] *Poliquin* v. *Devon Canada Corporation*, préc., note 355.

[585] *Id.*

de l'employeur. Pour la Cour, peu importait que le salarié ait jugé son comportement acceptable, puisqu'il était conforme aux normes tolérées par l'industrie en général : c'était à l'employeur de déterminer les standards qu'il entendait exiger de ses employés[586]. Il faut, en effet, garder à l'esprit que l'employeur a l'obligation d'assurer un environnement de travail sain et exempt de toute forme de harcèlement psychologique et doit donc prendre les mesures optimales pour y parvenir.

1.4.2. La limitation de la responsabilité de l'employeur

À ce jour, les tribunaux québécois ne semblent pas s'être prononcés sur l'impact de l'existence d'une politique Internet sur le régime de responsabilité de l'employeur, les jugements existants ayant été rendus dans le cadre de litiges entre employeurs et salariés. Cependant, il ne fait pas de doute que la situation de l'employeur qui a mis en place une politique détaillée des comportements interdits sera considérée avec plus de faveur que celui qui ne s'en est pas préoccupé. Ainsi, si

> « l'employeur prouve que l'utilisation fautive d'Internet s'est faite sans son autorisation, du fait, par exemple qu'il avait mis en place une politique de l'utilisation de l'Internet qui interdisait l'utilisation à des fins personnelles, l'exercice n'aura été que l'occasion, le support ou le soutien fortuit de l'acte fautif, mais ne l'ayant pas directement provoqué »[587].

Finalement, si les directives définies dans une politique Internet ne garantissent pas forcément l'exonération pour les entreprises, elles peuvent, néanmoins, constituer un moyen de prévention très efficace : si elles sont bien rédigées et surtout largement divulguées et appliquées de façon uniforme, elles peuvent épargner à l'entreprise, mais aussi aux salariés, bien des poursuites.

---

[586] *Id*.

[587] S. ROMPRÉ, préc., note 180, p. 22.

1.4.3. La limitation de l'expectative de vie privée des salariés

De nombreuses entreprises adoptent des politiques précisant explicitement qu'aucun utilisateur ne pourra prétendre à l'aspect « privé » des échanges qu'il effectue grâce à leur système informatique[588]. À cet égard, la jurisprudence, généralement peu encline à reconnaître l'existence d'une expectative de vie privée lors de l'utilisation des outils informatiques de l'employeur, accorde leur plein effet aux politiques d'entreprise qui contiennent de telles clauses. Les tribunaux estiment souvent que la seule existence de la politique autorise l'employeur à contrôler l'utilisation de l'ordinateur d'employé et à vérifier le contenu de son historique de navigations et de ses courriels. Ainsi, dans *Alliance de la fonction publique du Canada* et *Musée des beaux-arts du Canada*, l'arbitre reconnaît à l'employeur le droit d'accéder au contenu de l'ordinateur d'un salarié afin de s'assurer du respect du règlement de l'entreprise, et cela d'autant plus que l'employé avait transgressé la politique de l'entreprise à de nombreuses reprises[589].

Dans une autre affaire, l'employeur ne contrôlait pas l'utilisation individuelle de son réseau; toutefois, il était expressément prévu dans le Code de conduite de l'entreprise qu'il se réservait le droit de le faire en cas de violation ou de suspicion de violation de la loi ou d'utilisation abusive grave[590]. Les employés avaient donc une indication claire qu'ils devaient s'attendre à voir leurs activités surveillées étroitement.

Finalement, si les politiques Internet permettent à l'entreprise de régler de nombreux problèmes, elles se révèlent, néanmoins, parfois inappropriées face à certaines préoccupations patronales, notamment en raison de leur contenu uniforme et peu propice

---

[588] Voir, par exemple, *Blais* c. *Société des Loteries Vidéos du Québec Inc*., préc., note 239.

[589] Préc., note 155; Voir également *Ghattas* c. *École nationale de théâtre du Canada*, EYB 2006-102226 (C.S.) [ci-après Ghattas]; *R*. c. *Tremblay*, REJB 2001-23521 (C.Q.) (résumé du jugement sur la requête en exclusion de preuve et en arrêt des procédures, C.Q., 29-03-2001, 400-01-019056-001) et REJB 2001-25375 (C.Q.) (jugement statuant sur les accusations) [ci-après « Tremblay »]; *Syndicat des travailleuses et travailleurs de Resto-Casino de Hull (F.E.E.S.P.-C.S.N.) (section Hilton Lac Leamy)* et *Hilton Lac Leamy*, D.T.E. 2004T-811 (T.A.).

[590] *Gilles* et *Ciba Spécialités chimiques Canada Inc., p*réc., note 521.

aux aménagements. Aussi certains employeurs peuvent être tentés de recourir à la technique des clauses contractuelles qui offre davantage de souplesse.

Section 2. Les clauses contractuelles

Les clauses contractuelles permettent à l'employeur de prédéfinir les comportements de ses salariés qu'il considère comme fautifs et justifiant le congédiement pour faute grave[591]. Elles offrent donc un attrait indéniable, notamment en France où les entreprises qui souhaitent mettre en place une politique (ou « charte ») Internet sont tenues au respect de la vie privée et des principes de proportionnalité et de transparence[592], tout en étant confrontées aux contraintes liées au règlement intérieur[593]. La validité des chartes Internet en France semble en effet être liée à leur contenu : si elles édictent des interdictions assorties de sanctions disciplinaires, elles doivent être annexées au règlement intérieur et respecter les formalités relatives au règlement (consultation du comité d'entreprise, contrôle de l'inspection du travail sur la licéité de certaines clauses et information des salariés par un affichage visible de la charte dans les locaux de l'entreprise); au contraire, si elles se bornent à énoncer des règles générales et à donner des conseils techniques ou des règles de savoir-vivre, elles n'auront pas de valeur juridique[594]. En effet, selon le Code du travail, c'est le règlement intérieur de l'entreprise qui fixe le cadre disciplinaire, si bien que toute obligation nouvelle dont l'employeur souhaite sanctionner les éventuels manquements doit être annexée à ce règlement[595]. Toutefois, ce principe a semblé remis en question à la suite d'un arrêt du Conseil d'État[596] qui reconnaissait l'existence d'un pouvoir normatif de

---

[591] D. SERIO et C. MANARA, préc., note 7.

[592] Le principe de transparence correspond à l'obligation d'information préalable et de loyauté et découle de l'article L 121-8 du Code du Travail, selon lequel les salariés doivent avoir été informés préalablement sur tout dispositif et collecte de données les concernant personnellement. Quant au principe de proportionnalité, elle résulte de l'article L 120-2 : « Nul ne peut apporter aux droits des personnes et aux libertés individuelles et collectives de restrictions qui ne seraient pas […] proportionnées au but recherché ».

[593] B. POIDEVIN, « L'usage du système informatique par les employés : quel risque pour l'employeur? », préc., note 496.

[594] M. CAHEN, préc., note 12.

[595] COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, *Rapport d'étude et de consultation publique. La cybersurveillance des salariés dans l'entreprise*, préc., note 568, p. 16.

[596] Cons. d'Ét. 11 juin 1999, *Chicard*, D. 2000.somm.com.88, obs. Girodet.

l'employeur en dehors de ce cadre. En l'espèce, la haute juridiction administrative française avait jugé fondé le licenciement d'un salarié qui avait violé une note de service édictant une règle déontologique qui n'avait pourtant pas été annexée au règlement intérieur de l'entreprise. Cependant, cette décision reste isolée et la force du principe selon lequel l'employeur ne peut apporter de restrictions aux libertés que dans le cadre normal du règlement intérieur ne semble pas entamée.

Dans ce contexte, il peut-être tentant pour l'employeur désireux de contourner ces contraintes encadrant si strictement son pouvoir de direction, de recourir à des clauses contractuelles lui permettant de moduler les obligations des salariés en fonction, par exemple, de leur statut ou des circonstances, tout en conservant son droit de sanctionner leurs éventuels manquements. Toutefois, une telle stratégie comporte un risque élevé face à l'arsenal juridique érigé, dans un souci de protection du salarié, par le législateur et la jurisprudence, qui lors de l'examen des clauses insérées dans les contrats de travail, exerce un contrôle très serré des critères de la nécessité et de la proportionnalité, au détriment de l'autonomie de la volonté[597].

Au Québec, l'employeur dispose d'une marge de manœuvre plus large, puisqu'il n'est pas soumis aux exigences du règlement intérieur évoquées ci-dessus. Le besoin d'enserrer des obligations des salariés dans des contrats de travail individuels, pour contourner les contraintes légales, est donc moins pressant. On note, néanmoins, que de nombreux employeurs ne se contentent plus de distribuer leur politique Internet aux salariés et obligent de plus en plus souvent ces derniers à s'engager formellement. Ils leur feront, par exemple, signer une lettre et/ou un formulaire confirmant qu'ils se conformeront aux dispositions de la politique et renoncent à invoquer leur droit à la vie privée lorsqu'ils utilisent les ressources informatiques de l'entreprise[598]. Les salariés sont d'ailleurs généralement invités à renouveler la procédure lors de chaque modification des diverses

---

[597] F. FÉVRIER, préc., note 21, p. 58.

[598] *Sirois* c. *Sodema*, préc., note 161.

politiques d'entreprise, par exemple, grâce à la signature d'un avenant au contrat de travail ou d'un nouveau formulaire.

Parfois, de tels engagements seront pris dans le cadre d'un contrat individuel de travail, lors de l'embauche d'un salarié. Cela permet à l'employeur de s'assurer formellement que les nouveaux employés prennent connaissance des règlements internes relatifs à l'usage du système informatique, ainsi que de l'ensemble des politiques de l'entreprise, et s'engagent, par écrit, à les respecter. Ces divers documents sont généralement mentionnés dans une clause du contrat de travail et annexés à ce dernier.

La technique contractuelle est utilisée par de nombreux employeurs pour obtenir une renonciation formelle des employés à la protection de leur vie privée. Cela est notamment le cas depuis que l'arrêt *Syndicat des travailleuses et travailleurs de Bridgestone/Firestone de Joliette (C.S.N.)* c. *Trudeau*[599] a clairement rejeté le principe de « renonciation implicite » [600] selon lequel le salarié, en acceptant le lien de subordination découlant du contrat de travail, consent implicitement à toute atteinte de son droit à la vie privée et à la dignité. Selon la Cour d'appel, en effet, pour qu'une renonciation à un droit – et par conséquent à la protection à la vie privée – soit valide, en vertu de l'article 35 C.c.Q., elle doit être « précise » et « explicite »[601]. De plus, la renonciation ne doit pas constituer une dénégation complète du droit en question[602] et doit être conforme à l'ordre public[603]. À cet égard, il importe de préciser que si les renonciations à la protection de la vie privée sont

---

[599] Préc., note 8.

[600] Mario ÉVANGÉLISTE, « Les affaires Bridgestone/Firestone et Ville de Mascouche : la Cour d'appel rompt avec la jurisprudence du travail et fixe des balises. Mais où en sommes-nous? », dans *Développements récents en droit du travail (2000)*, Service de la formation permanente du Barreau du Québec, 2000, *Droit civil en ligne* (DCL), EYB2000DEV859, p. 4-5.

[601] *Syndicat des travailleuses et travailleurs de Bridgestone/Firestone de Joliette (C.S.N.)* c. *Trudeau*, préc., note 8, par. 68.

[602] France ALLARD, « Les droits de la personnalité », dans Collection de droit 2009-2010, École du Barreau du Québec, vol. 3, *Personnes, famille et successions*, Cowansville, Yvon Blais, 2009, p. 59, à la page 59.

[603] Christian BRUNELLE, « Les limites aux droits et libertés », dans Collection de droit 2009-2010, École du Barreau du Québec, vol.7, *Droit public et administratif*, Cowansville, Éditions Yvon Blais, 2009, p. 77, à la page 77.

valides, les clauses renonçant à la protection de la dignité (autorisant, par exemple des traitements discriminatoires) ne le sont pas, car la dignité humaine est inaliénable[604].

Les tribunaux analysent avec un soin particulier le contenu des renonciations aux droits fondamentaux, ainsi que les circonstances dans lesquelles elles sont faites. Aussi, dans leur évaluation de la validité de ces clauses, ils prennent généralement en compte les cinq facteurs suivants, notamment identifiés par Christian Brunelle :

1. la nature du droit ou de la liberté en cause;
2. la possibilité, pour le demandeur, de renoncer à ce droit ou à cette liberté;
3. la manière selon laquelle le demandeur y a renoncé;
4. la mesure dans laquelle le demandeur pouvait y renoncer;
5. l'effet de la renonciation[605].

Finalement, la renonciation à un droit fondamental « semble affaire de "contexte" », et pourra aussi bien découler d'une manifestation positive de sa part que de son inaction ou omission[606]. Toutefois, elle ne peut être présumée[607]. En définitive, pour être valable, la « renonciation devra être claire, non équivoque, éclairée, libre et volontaire »[608].

On peut s'interroger, avec certains auteurs, sur la réalité du caractère volontaire du consentement donné par le salarié dans le cadre d'une relation de subordination qui l'oblige à se placer sous la surveillance de l'employeur. En effet, comme le souligne Sophie Rompré, dans un tel contexte, le consentement de l'employé « équivaut à l'acceptation d'un contrat d'adhésion »[609] et sa renonciation ne pourra être qualifiée de volontaire que s'il a

---

[604] *Id.*, p. 77-78.
[605] *Id.*, p. 77.
[606] *Id.*, p. 78.
[607] *Id.*
[608] *Id.*, p. 78-79.
[609] S. ROMPRÉ, préc., note 180, p. 89.

« la possibilité de négocier de gré à gré avec l'employeur quant à l'étendue de la surveillance »[610].

Finalement, si l'efficacité du pouvoir de sanction de l'employeur dépend étroitement de l'existence ou non d'une politique Internet claire et précise[611], le défaut de directives explicites ne le paralyse pas complètement[612]. Les tribunaux lui ont, dans certains cas, reconnu le droit de sanctionner les abus, malgré l'absence de politique Internet[613] : ce fut le cas, notamment en cas de baisse appréciable de la productivité liée à l'utilisation du matériel informatique à des fins personnelles pendant les heures de travail[614] ou de transmission par courriel de fichiers à contenu obscène ou pornographique[615]. Toutefois, lorsqu'il existe un règlement d'entreprise, l'employeur pourra plus facilement établir la légitimité de sa surveillance, puisqu'il est reconnu qu'il a le droit de contrôler l'utilisation des ressources informatiques par un salarié, afin de s'assurer que ce dernier respecte les prescriptions patronales[616].

Chapitre 2. L'existence d'un intérêt sérieux et légitime

L'employeur, dans l'exercice de son pouvoir de direction, doit donc tenir compte des droits des employés. Ceux-ci, en tant qu'individus, disposent, en effet, du droit à la vie privée

---

[610] *Id.*, p. 90.

[611] *Commission des normes du travail* c. *Bourse de Montréal Inc.*, préc., note 164.

[612] Y. SAINT-ANDRÉ, préc., note 122, p. 9.

[613] *Id.*

[614] *Syndicat des fonctionnaires municipaux de Montréal (S.C.F.P.)* c. *Ville de Montréal*, D.T.E. 99T-478 (T.A.) : cette décision confirme une suspension de dix jours en raison, notamment, des nombreux avertissements adressés antérieurement au salarié.

[615] Voir, par exemple, *Bell Canada* c. *Association Canadienne des Employés de Téléphone*, préc., note 238; Voir également *Consumers Gas* v. *Communications, Energy and Paperworkers Union* (Primiani Grievance), [1999] O.L.A.A. No. 649 (L.A.) (QL/LN), où l'arbitre accueille le moyen de défense d'une employée affirmant ne pas avoir été informée de l'existence de la politique sur l'utilisation de l'Internet et ignorer que la détention et la distribution de contenus pornographiques étaient interdites par la politique d'entreprise. L'arbitre conclut, toutefois, que cette ignorance ne pouvait pas disculper la plaignante dans la mesure où le simple bon sens lui interdisait d'utiliser la messagerie électronique de l'employeur pour stocker et distribuer des contenus à caractère sexuel. Au vu de l'ensemble des circonstances, le congédiement a finalement été remplacé par une suspension d'un mois.

[616] *Syndicat canadien des communications, de l'énergie et du papier, section locale 522* c. *CAE Électronique Ltée*, préc., note 159; *Alliance de la fonction publique du Canada* et *Musée des beaux-arts du Canada*, préc., note 155.

protégé, notamment, par l'article 5 de la *Charte des droits et libertés de la personne*[617], les articles 3 et 35 à 41 du *Code civil du Québec*, ainsi que les articles 4 et 5 de la *Loi sur la Protection des renseignements personnels dans le secteur privé*[618].

Toutefois, ce droit à la vie privée n'est pas absolu et pourra être limité lorsqu'il s'oppose à d'autres droits fondamentaux ou à des considérations d'ordre public ou de nécessité. À cet égard, les tribunaux rappellent régulièrement que l'article 9.1 de la *Charte des droits et libertés de la personne*[619] autorise des aménagements au droit à la vie privée et permet des restrictions, limites ou intrusions lorsqu'elles :

1. répondent à un objectif légitime et important;
2. sont rationnellement liées à cet objectif; et
3. constituent une atteinte minimale au droit protégé[620].

De son côté, l'article 4 de la *Loi sur la Protection des renseignements personnels dans le secteur privé*[621] requiert « un intérêt sérieux et légitime » pour toute personne exploitant une entreprise qui souhaite constituer un dossier sur autrui.

Le problème est de savoir à partir de quel moment la surveillance patronale pourra être considérée comme répondant à ces critères. En d'autres termes, jusqu'où les intrusions de l'employeur dans la vie privée des travailleurs peuvent-elles aller? La question est pour le moins délicate, car pour l'employeur, le contrôle est toujours légitime, tandis que pour les salariés il constitue une atteinte intolérable à leur vie privée.

La jurisprudence québécoise a, au fil du temps, élaboré des principes pour encadrer la surveillance patronale. Selon ces principes, toute intrusion de l'employeur dans la vie privée du salarié doit, pour être légitime, être fondée sur l'existence de « motifs

---

[617] Préc., note 361.

[618] Préc., note 10.

[619] Préc., note 361.

[620] Pour une illustration, voir *Godbout* c. *Ville de Longueuil*, préc., note 724, p. 916; Voir également *Section locale 143 du Syndicat canadien des communications, de l'énergie et du papier* c. *Goodyear Canada inc.*, préc., note 552, par. 18.

[621] Préc., note 10.

raisonnables »[622]. Ces règles, élaborées dans le cadre de la surveillance vidéo et des écoutes téléphoniques[623], sont reconnues par une majorité d'auteurs comme pertinentes et parfaitement transposables à la surveillance des outils de communication informatiques[624]. Ainsi, dans l'affaire *Syndicat canadien des communications, de l'énergie et du papier, section locale 522* c. *CAE Électronique Ltée*, l'arbitre compare l'Internet au téléphone et conclut, en vertu des principes établis en matière de surveillance électronique, que la surveillance de l'employeur devait nécessairement être justifiée par des motifs sérieux[625]. Condition remplie en l'espèce, puisque le plaignant avait utilisé Internet à des fins personnelles pour un total de 329 heures en l'espace de quatre mois et demi, la majorité du temps pour visiter des sites de nature pornographique. L'arbitre en conclut que l'employeur était fondé à imposer une sanction sévère et confirme le congédiement[626].

Toutefois, certaines voix s'élèvent contre cette assimilation et avancent que les principes dégagés en matière de surveillance vidéo ne seraient pas « intégralement » applicables à la surveillance des technologies de l'information[627], notamment parce qu'une telle surveillance est réalisée grâce à des logiciels préinstallés dans les ordinateurs et ayant d'autres fins que la seule surveillance[628]. De plus, ces outils sont moins intrusifs que les caméras[629], par exemple, et offrent une surveillance plus discrète, puisqu'il suffit d'accéder à la mémoire de l'ordinateur pour contrôler l'activité d'un salarié, contrairement aux

---

[622] *Syndicat des travailleuses et travailleurs de Bridgestone/Firestone de Joliette (C.S.N.)* c. *Trudeau*, préc., note 8.

[623] *Id.* (à propos de la surveillance vidéo); *Srivastava* c. *Hindu Mission of Canada (Québec) Inc.*, préc., note 576 (à propos de l'interception de conversations téléphoniques).

[624] I. LAUZON et L. BERNIER, préc., note 363, p. 101; Emmanuel TANI-MOORE, « *L'appréciation en droit québécois de l'arrêt Nikon: même résultat?* », (2002) 8-1 *Lex Electronica*, en ligne : <http://www.lex-electronica.org/articles/v8-1/tani-moore.htm> (site consulté le 30 juillet 2010).

[625] *Syndicat canadien des communications, de l'énergie et du papier, section locale 522* c. *CAE Électronique Ltée*, préc., note 159, par. 45.

[626] Voir également *Blais* c. *Société des loteries vidéo du Québec Inc*., préc., note 239.

[627] Louis BARIBEAU, « Internet et le milieu du travail », (2001) 33-19 *J. du Bar.*

[628] *Id.*

[629] *Id.*

écoutes téléphoniques ou à la surveillance vidéo qui nécessitent d'enregistrer ou d'épier ce dernier[630].

Tous s'accordent cependant sur le fait que la surveillance patronale ne peut s'exercer que s'il existe un intérêt sérieux[631]. Cette exigence s'apprécie en tenant compte de la finalité de la surveillance (Section 1), de son efficacité (Section 2) ainsi que de l'étendue de l'atteinte à la vie privée (Section 3).

Section 1. La finalité de la surveillance

La cybersurveillance répond à divers objectifs qui ont été, pour la plupart, développés dans la première partie. Il s'agit maintenant d'étudier le contrôle exercé par les tribunaux sur les motifs de surveillance habituellement invoqués par les employeurs.

L'arrêt de principe souvent cité, à cet égard, est *Syndicat des travailleurs et travailleuses de Bridgestone/Firestone de Joliette (CSN)* c. *Trudeau*[632], rendu le 30 août 1999, qui est venu poser les balises en matière de surveillance patronale. L'un de ses principaux apports est d'imposer le « test de la justification » [633] en vertu de l'article 9.1 de la *Charte des droits et libertés de la personne*[634], en exigeant un lien entre la surveillance et les nécessités du bon fonctionnement de l'entreprise ou de l'établissement, ainsi que la justification préalable de l'employeur pour surveiller ses salariés. Jusqu'à lors, l'examen des tribunaux portait uniquement sur la « raisonnabilité » des motifs de la surveillance de l'employeur, c'est-à-dire le droit, dans le cadre d'une relation de travail, pour ce dernier de s'immiscer dans des limites raisonnables, dans la vie privée des employés[635].

Dans cette affaire, la Cour d'appel du Québec devait déterminer si la surveillance vidéo effectuée par un employeur sur un salarié était licite eu égard à la protection de la vie privée

---

[630] F. CÔTÉ, préc., note 251.

[631] Y. SAINT-ANDRÉ, préc., note 122, p. 7 et suiv.

[632] Préc., note 8.

[633] M. ÉVANGÉLISTE, préc., note 600, p. 5-8.

[634] Préc., note 361.

[635] M. ÉVANGÉLISTE, préc., note 600, p. 5.

prévue aux articles 5 de la *Charte des droits et libertés de la personne*[636] et 35 et 36 du *Code civil du Québec*. L'employeur avait congédié cet employé pour faute disciplinaire grave résultant de ses mensonges et simulations destinés à prolonger son absence à la suite d'un accident du travail. L'employeur avait décidé de mettre le salarié sous surveillance vidéo après avoir relevé des contradictions entre les affirmations de ce dernier (il prétendait être très souffrant sans pour autant être capable de situer la douleur à un point précis), le diagnostic de son médecin traitant et les observations du médecin de la partie patronale. Ces filatures, réalisées à des dates différentes, montraient le salarié accomplissant, sans douleur apparente, des gestes incompatibles avec les symptômes allégués (il était notamment capable de faire une petite course avec son fils, en courant à petits pas sur une courte distance, de transporter une chaudière de poids moyen ou d'effectuer des travaux de jardinage devant chez lui). L'employeur avait alors estimé que ces mensonges avaient irrémédiablement brisé le lien de confiance et justifiaient le renvoi de l'employé. C'est ce congédiement, confirmé par un arbitre, puis la Cour supérieure du Québec, qui était porté en appel par le syndicat qui contestait l'admissibilité en preuve des bandes vidéo déposées par l'employeur. L'arbitre avait rejeté ces objections et conclu que ces bandes ne portaient pas atteinte à la vie privée du salarié, notamment parce qu'elles avaient été captées dans des lieux publics.

Au-delà de l'admissibilité ou non des bandes vidéo, la Cour d'appel devait trancher la question relative au droit de l'employeur de surveiller un employé en dehors des lieux de travail, comme le précisait alors le juge Lebel dans les termes suivants :

> « La question en litige doit être bien comprise : elle n'est pas un problème de captation d'image, mais plutôt de surveillance. La réalisation des films ne constitue que la résultante de la filature ou surveillance décidée par l'employeur. »[637]

---

[636] Préc., note 361.

[637] *Syndicat des travailleuses et travailleurs de Bridgestone/Firestone de Joliette (C.S.N.)* c. *Trudeau*, préc., note 8, par. 62.

La Cour a confirmé que la surveillance patronale, même effectuée en dehors du lieu de travail, peut être admise, malgré l'apparente atteinte à la vie privée, lorsqu'elle « est justifiée par des motifs rationnels et conduite par des moyens raisonnables »[638]. L'employeur doit donc apporter la preuve concrète que ses motifs répondent à une exigence de « rationalité » et de « proportionnalité »[639]. Le critère de « rationalité » implique que le motif doit exister avant que l'employeur décide de procéder à la surveillance du poste informatique d'un salarié[640]; quant à la proportionnalité, elle signifie que l'employeur doit veiller à ce que la mesure de surveillance constitue une atteinte minimale à la vie privée du salarié[641]. En outre, la surveillance doit être « nécessaire pour la vérification du comportement du salarié »[642].

En somme, l'employeur a le droit de surveiller ses employés, à condition qu'il démontre l'importance de l'intérêt qu'il souhaite protéger (1.1.) et l'antériorité du motif de la surveillance (1.2.).

1.1. La nature de l'intérêt protégé

La surveillance doit être mise en place pour faire face à un problème important, réel et précis (1.1.1.) et en lien avec les exigences du bon fonctionnement de l'entreprise (1.1.2.). Il faut également tenir compte de l'impact des facteurs aggravants et atténuants (1.1.3.), puisque, comme nous le verrons ultérieurement, l'existence de facteurs aggravants peut, à elle seule, justifier le congédiement du salarié fautif, sans qu'il soit nécessaire de respecter le principe de progressivité des sanctions[643].

---

[638] *Id.,* par. 73.

[639] Y. SAINT-ANDRÉ, préc., note 122, p. 3, 10 et 15; D. VEILLEUX, préc., note 483, 44.

[640] *Syndicat des travailleuses et travailleurs de Bridgestone/Firestone de Joliette (C.S.N.)* c. *Trudeau*, préc., note 8.

[641] Y. SAINT-ANDRÉ, préc., note 122, p. 10.

[642] *Syndicat des travailleuses et travailleurs de Bridgestone/Firestone de Joliette (C.S.N.)* c. *Trudeau*, préc., note 8, par. 75.

[643] Voir, par exemple, *Syndicat des employés municipaux de Beloeil (SCFP)* et *Beloeil (Ville de)*, préc., note 173, qui confirme le congédiement, sans gradation des sanctions, d'un salarié pour usage abusif de l'Internet. Dans cette affaire, l'employeur accordait certaines permissions, malgré l'existence d'une politique réglementant l'usage de l'Internet. Toutefois, le plaignant avait abusé de ce privilège, puisque son utilisation s'élevait à 3 heures par jour et occupait 40% de son temps de travail. Voir également *Bourassa* et *Ville de La Tuque,* préc., note 583.

1.1.1. L'existence d'un problème important, réel et précis

Il découle des articles 9.1 de la *Charte des droits et libertés de la personne*[644] et 4 de la *Loi sur la Protection des renseignements personnels dans le secteur privé*[645] que l'employeur ne peut pas se contenter d'invoquer un simple doute relativement au comportement d'un salarié pour vérifier le contenu de son ordinateur : « [l]'objectif visé doit être clairement identifié et doit être sérieux et important en vue de régler un problème important »[646]. Or, il n'est pas toujours possible pour l'entreprise de prouver que la surveillance répondait à une exigence particulière, car bien souvent, il s'agit d'un besoin abstrait[647]. Certes, dans certaines circonstances, le risque hypothétique pourra suffire[648]. Ce sera le cas, par exemple, dans les industries sensibles où le risque de fuite d'informations est si élevé et « évident » qu'il est inutile que l'employeur étaye son argumentation[649]. Cependant, dans la plupart des cas, l'employeur devra concrètement démontrer l'existence d'un « problème réel et précis »[650].

À cet égard, on peut se demander si le droit de propriété des équipements informatiques, souvent invoqué par les employeurs, constitue un motif suffisant. Les jugements rendus en matière d'écoute téléphonique fournissent de précieux enseignements ce point. Ainsi, il ressort de l'arrêt *Srivastava* c. *Hindu Mission of Canada (Québec) Inc.*[651] que ce qui est déterminant,

---

[644] Préc., note 361.

[645] Préc., note 10.

[646] Lyette DORÉ, « Surveillance vidéo vs respect du droit à la vie privée », *dans Développements récents en droit de l'accès à l'information (2005)*, Service de la formation permanente du Barreau du Québec, 2005, *Droit civil en ligne* (DCL), EYB2005DEV1087, p. 31.

[647] Georges RADWANSKI, (COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA), *Décisions récentes et questions émergentes en vertu de la nouvelle loi sur la protection de la vie privée*, discours à la Conférence annuelle sur les droits de la personne et la vie privée au travail, Lancaster House, Toronto, 2002, en ligne : <http://www.privcom.gc.ca/speech/02_05_a_020503_f.asp> (site consulté le 25 juillet 2010).

[648] *Id.*

[649] *Id.*

[650] *Id.*

[651] Préc., note 576.

> « ce n'est pas la propriété de la ligne téléphonique […] mais plutôt la nature de l'information ainsi que l'identité des interlocuteurs qui permettent de vérifier si la conversation téléphonique est protégée par l'article 5 de la Charte »[652].

En l'espèce, un temple hindou avait décidé d'effectuer des écoutes sur sa ligne téléphonique afin de vérifier les soupçons de liaison entre le prêtre et l'une des fidèles. Ces derniers avaient alors intenté une action en diffamation et pour atteinte à leur vie privée. Pour les débouter, le juge de première instance s'était, notamment, fondé sur le droit de propriété de l'employeur sur le téléphone, ainsi que sur le fait que, historiquement, la ligne téléphonique était réservée aux affaires professionnelles reliées au temple. La Cour d'appel rejeta cette argumentation au motif que la question fondamentale, en l'espèce, n'était pas savoir si le téléphone était protégé, mais plutôt si la conversation entre les deux plaignants l'était. Dans une espèce proche, jugée quelques années plus tôt[653], la Cour d'appel du Québec avait toutefois conclu différemment, considérant que l'enregistrement d'une conversation téléphonique effectuée par une employée soupçonnée de concurrencer son employeur ne constituait pas une atteinte à la vie privée de cette dernière, dans la mesure où l'appareil téléphonique utilisé appartenait à l'employeur et était réservé aux affaires du commerce. De plus, le contenu des conversations interceptées portait uniquement sur des matières relevant d'affaires commerciales et non de la vie privée de l'employée.

Finalement, comme le souligne Charles Morgan:

> « the fact that an employer owns the computer equipment used by employees dos no, *per se*, provide an unfettered right to monitor use »[654].

La seule invocation par l'employeur de son droit de propriété sur les équipements (téléphoniques ou informatiques) n'est donc pas suffisante pour justifier sa surveillance.

---

[652] Y. SAINT-ANDRÉ, préc., note 122, p. 11.

[653] *Roy* c. *Saulnier*, préc., note 8.

[654] C. MORGAN, préc., note 563, n° 5, p. 175.

D'autres facteurs, propres à chaque circonstance, seront pris en compte dans l'évaluation de la légalité de la surveillance patronale.

De même, le souhait de l'employeur de s'assurer la loyauté du salarié et son exécution correcte des obligations lui incombant ne constitue pas automatiquement l'intérêt « légitime, important, voire urgent » [655] requis par l'article 9.1 de la *Charte des droits et libertés de la personne*[656]. Aussi, l'employeur doit-il démontrer que son objectif présente ces qualités. C'est ce qu'énonce la Cour d'appel dans *Syndicat des travailleuses et travailleurs de Bridgestone/Firestone de Joliette (C.S.N.)* c. *Trudeau* :

> « 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. »[657]

Dans *Fiset* c. *Service d'administration P.C.R. Ltée*[658], l'employeur échoua à établir le caractère sérieux de ses motifs en raison de l'absence de directives quant à l'utilisation d'Internet à des fins personnelles et de l'existence, au sein de l'entreprise, d'une certaine tolérance de l'usage à des fins personnelles. En revanche, dans *Syndicat canadien des communications, de l'énergie et du papier, section locale 522* c. *CAE Électronique Ltée*[659], l'employeur a pu démontrer la légitimité de la surveillance de l'ordinateur d'un salarié en établissant le vol de temps (en raison de l'utilisation excessive de l'Internet à des fins personnelles pendant le temps de travail) et la violation des règles et politiques de l'entreprise interdisant, notamment, l'utilisation du matériel sexiste ou pornographique.

---

[655] M. ÉVANGÉLISTE, préc., note 600, p. 6.

[656] Préc., note 361.

[657] *Syndicat des travailleuses et travailleurs de Bridgestone/Firestone de Joliette (C.S.N.)* c. *Trudeau*, préc., note 8, par. 74.

[658] Préc., note 174.

[659] Préc., note 159.

En conséquence, lorsque l'employeur est dans l'incapacité d'identifier clairement son besoin et se contente d'hypothèses ou de généralisations pour justifier sa surveillance, il faut conclure à l'absence de caractère « sérieux » de ses motifs.

1.1.2. Le lien avec les exigences du bon fonctionnement de l'entreprise

Outre son caractère grave, l'objectif visé par l'employeur doit avoir un lien avec le travail et le bon fonctionnement de l'entreprise[660]. La loyauté et le respect, de bonne foi, des obligations contractuelles et des directives patronales sont les motifs qui viennent immédiatement à l'esprit. Il faut y ajouter la productivité, la sécurité et la prévention des faits illicites, contraires aux bonnes mœurs, diffamatoires ou susceptibles de porter atteinte à la dignité d'autrui.

Dans *Syndicat des travailleuses et travailleurs de Resto-Casino de Hull (F.E.E.S.P.-.S.N.) (section Hilton Lac Leamy)* et *Hilton Lac Leamy*[661], l'arbitre a reconnu à l'employeur un droit d'intervention dans un conflit privé, après avoir conclu à l'existence d'un lien direct entre ce conflit et le travail. Dans cette affaire, l'employeur avait congédié un salarié de sexe masculin qui avait proféré des menaces à caractère sexuel envers une collègue dans le cadre de séances de « clavardages » privées. Ces échanges avaient pourtant été effectués par les employés depuis leurs domiciles respectifs et en dehors de leurs heures de travail. Pour justifier la sanction, l'employeur avançait que le salarié avait également agressé physiquement et verbalement cette même salariée sur les lieux de travail, allant même jusqu'à proférer des menaces de mort à son encontre. L'arbitre jugea que les événements intervenus dans les locaux de l'entreprise conféraient à l'affaire un caractère hybride qui justifiait l'intrusion de l'employeur. Il confirma le congédiement, après avoir pris en compte l'ensemble des gestes commis par le plaignant et leur gravité.

---

[660] *Syndicat des travailleuses et travailleurs de Bridgestone/Firestone de Joliette (C.S.N.)* c. *Trudeau*, préc., note 8; *Srivastava* c. *Hindu Mission of Canada (Québec) Inc.*, préc., note 576, par. 57 et 78 : dans cette décision, la Cour d'appel fait référence à un « lien logique » entre le motif invoqué par l'employeur pour surveiller un employé et la mesure de surveillance.

[661] Préc., note 589.

La jurisprudence sur ce dernier point est assez abondante, les tribunaux ayant toujours admis qu'un usage des équipements de l'employeur à des fins autres que l'accomplissement de son travail pouvait justifier le congédiement du salarié. Ainsi, dans *Alliance de la fonction publique du Canada* et *Musée des beaux-arts du Canada*[662], l'arbitre indique que le fait pour un employeur de consulter le rapport d'utilisation de l'ordinateur d'un salarié et de vérifier le contenu de ses courriels, afin de s'assurer qu'il respecte le règlement de l'entreprise, n'est pas constitutif d'un abus, dans la mesure où l'on ne reconnaît pas de droit à la vie privée à un employé lorsqu'il utilise l'ordinateur fourni pour l'exécution de son travail. Il en conclut qu'en l'espèce, la surveillance particulière visant le salarié était justifiée, en raison de ses nombreuses transgressions de la politique de l'entreprise et de son défaut à respecter les avertissements antérieurs[663].

Cette affaire apporte la confirmation que l'une des meilleures façons d'établir le caractère sérieux du motif demeure l'existence d'une politique Internet valide avisant, notamment, les salariés qu'une surveillance de leur utilisation des outils informatiques sera effectuée selon les modalités bien précises indiquées[664].

1.1.3. L'impact des facteurs aggravants ou atténuants

Les divers manquements du salarié à l'égard de ses obligations seront, notamment, évalués en fonction de ses responsabilités ou de l'activité de l'entreprise (1.1.3.1.), de l'état de son dossier et de son attitude générale face aux événements (1.1.3.2.), ainsi que des pratiques[665] ayant cours dans l'entreprise. Ces facteurs pourront, bien entendu, parfois se cumuler dans le cadre d'une même affaire.

---

[662] Préc., note 155.

[663] Voir également *Syndicat canadien des communications, de l'énergie et du papier, section locale 522* c. *CAE Électronique Ltée*, préc., note 159; *Blais* c. *Société des loteries Vidéo du Québec Inc.*, préc., note 239.

[664] I. LAUZON et L. BERNIER, préc., note 363, p. 101.

[665] Voir *supra*, Partie 2, Chapitre 1, Section 1, 1.4, p. 147.

1.1.3.1. La nature de l'emploi ou de l'activité de l'entreprise

Il est certain que les manquements à la loyauté de certains professionnels, tels les salariés travaillant dans les services informatiques, seront appréciés avec plus de sévérité que s'ils émanaient d'un employé n'ayant qu'une connaissance très limitée de l'informatique[666] : les premiers sont, en effet, tenus à une obligation de loyauté renforcée et leurs agissements pourront être assimilés à des « manquements graves à l'éthique »[667].

De même, l'obligation de confidentialité sera renforcée pour certains salariés en raison de leurs fonctions ou d'une clause de leur contrat de travail[668]. On pense, par exemple, au personnel du service financier ou celui de la recherche et développement qui manipulent des informations hautement stratégiques. De même, les employés qui traitent les informations personnelles de tiers seront également tenus à une obligation plus lourde et ils ne peuvent, notamment, pas se servir de ces renseignements pour leur propre profit ou celui d'un tiers. Ainsi, dans l'affaire *Syndicat de la Fonction Publique du Québec (SFPQ)* c. *Québec (Ministère du Revenu)*[669], le congédiement d'un employé du Ministère du Revenu, qui avait profité de sa fonction pour consulter les renseignements personnels concernant des membres de sa famille ainsi que des contribuables avec lesquels il faisait affaire, a été confirmé. Les dossiers de ces personnes avaient été consultés sans autorisation, à plusieurs reprises. L'employé avait même apporté des corrections au dossier fiscal de son fils, se plaçant ainsi en situation de conflit d'intérêts.

Dans *Bolduc* c. *Collège de Montréal*[670], l'employeur avait également congédié une employée en raison de son usage inapproprié de l'information confidentielle obtenue dans le cadre de sa fonction. L'intéressée occupait un poste d'agente aux services administratifs de l'employeur et était la seule à avoir accès à des informations financières très précises qui

---

[666] *Syndicat des spécialistes et professionnels d'Hydro-Québec* c. *Hydro-Québec*, préc., note 229; *Syndicat des spécialistes et professionnels d'Hydro-Québec, (SCFP-FTQ, section locale 4250)* c. *Hydro-Québec*, préc., note 193.

[667] *Syndicat des spécialistes et professionnels d'Hydro-Québec, (SCFP-FTQ, section locale 4250)* c. *Hydro-Québec*, préc., note 193.

[668] V. ROQUES, préc., note 34, p. 21.

[669] 2005 IIJCan 43078 (QC A.G.).

[670] 2010 QCCRT 130 (CanLII).

avaient été divulguées à un journaliste. Or, à son arrivée ce poste, elle avait signé une entente de non-divulgation par laquelle elle s'interdisait de divulguer ou d'utiliser l'information confidentielle qu'elle pourrait obtenir dans le cadre de son travail. De plus, l'employée avait d'abord nié toute participation à ces faits. Toutefois, l'employeur disposait de nombreux courriels qui prouvaient son implication dans cette fuite d'informations. Le Tribunal a confirmé le congédiement, estimant que les fonctions syndicales de l'employée ne la dispensaient pas de respecter son obligation de s'abstenir de participer à toute action susceptible de porter atteinte à la réputation de l'entreprise, comme ne manquerait pas de le faire une divulgation d'informations sur des aspects controversés de la situation financière de l'employeur.

Il faut également tenir compte du niveau hiérarchique du poste du salarié : plus son niveau de responsabilité sera élevé, plus l'employeur sera en droit d'exiger un « plus grand dévouement et une plus grande loyauté » de sa part[671]. En revanche, l'absence de supervision appropriée peut être interprétée en faveur du salarié puisqu'il est de la responsabilité du superviseur de s'assurer que ses subordonnés utilisent adéquatement leur temps. Ceux qui occupent des postes de direction dans l'entreprise seront donc tenus à une obligation plus lourde, proche, parfois, d'une obligation de résultat[672]. Ainsi, dans l'affaire *Potvin* c. *Ville de Malartic*, l'employeur a congédié un gestionnaire au motif que tant la nature de son poste que l'obligation de loyauté de l'article 2088 C.c.Q., imposaient à l'intéressé « [d']agir avec loyauté, intégrité et honnêteté »[673]. Outre la mauvaise gestion du club de golf municipal dont il avait la charge, la ville lui reprochait un usage inapproprié de son ordinateur professionnel. Les vérifications effectuées sur ce dernier avaient permis de découvrir plus de 170 photographies à caractère sexuel et pornographique, ainsi que des « clavardages » de la même nature. Le gestionnaire avait nié les faits. Cependant, bien que

---

[671] *Syndicat canadien des communications, de l'énergie et du papier, section locale 522* c. *CAE Électronique Ltée*, préc., note 159; N.-A. BÉLIVEAU, K. BOUTIN et N. ST-PIERRE, préc., note 177, p. 17.

[672] *Syndicat canadien des communications, de l'énergie et du papier, section locale 522* c. *CAE Électronique Ltée*, préc., note 159; R. P. GAGNON, « Le contrat de travail », préc., note 158, p. 9.

[673] Préc., note 159, par. 9; Voir également *Arpin* c. *Grenier*, préc., note 243; *Syndicat canadien des communications, de l'énergie et du papier, section locale 522* c. *CAE Électronique Ltée*, préc., note 159.

l'employeur n'ait pas pu prouver les téléchargements des images pornographiques (d'autres personnes avaient, en effet, accès à l'ordinateur), il avait néanmoins démontré que le salarié en avait forcément eu connaissance et n'avait rien fait pour retirer les photographies compromettantes ou exiger que cela soit fait. Quant aux « clavardages » qui s'étendaient sur des périodes passablement longues, leur transcription avait permis de conclure nettement qu'il en était l'auteur. Le congédiement a donc été confirmé.

Dans le même ordre d'idées, on peut citer l'affaire *Persechino* c. *Flint Ink North America Corporation*[674] relative au congédiement pour harcèlement sexuel d'un cadre. Ce dernier envoyait constamment des messages électroniques à connotation sexuelle à une employée travaillant sous son autorité ou faisait des allusions verbales devant elle. Face à son refus persistant, il avait essayé d'obtenir son congédiement. Or, comme le relevait la Commission des relations du travail, il n'avait rien fait pour la congédier, comme il aurait dû le faire si elle était aussi incompétente qu'il le prétendait. Bien au contraire, il avait plutôt proposé sa candidature pour un poste plus élevé. De plus, tout en reconnaissant ses sentiments pour l'employée, il niait l'avoir harcelée et prétendait ne pas se souvenir des propos prononcés ou écrits. Il avait même soutenu que c'était plutôt elle qui le harcelait. Pourtant, il lui avait, entre autres, envoyé un mémorable courriel contenant plus de 9500 points d'interrogation! On pouvait difficilement oublier un tel message ou soutenir qu'il ne constituait pas du harcèlement. La Commission a donc maintenu le congédiement, en se fondant, notamment, sur le fait que le salarié occupait une fonction élevée au sein de l'entreprise (il était « le grand patron au Québec ») [675] et était, à ce titre, tenu à un niveau plus élevé d'obligations et à un comportement exemplaire.

---

[674] 2007 QCCRT 354 (CanLII).

[675] Id., par. 5; Voir également *Poliquin* v. *Devon Canada Corporation*, préc., note 355, où la Cour d'appel de l'Alberta souligne qu'un salarié qui occupe un poste de superviseur sénior (il cumule plus de 23 ans d'expérience sur des fonctions d'encadrement et dirige 20 à 25 employés au moment de son congédiement) est tenu à une obligation de loyauté renforcée et doit, notamment, s'abstenir de participer à la distribution de contenus à caractère sexuel, pornographique ou raciste avec ses collègues et – pire – les contacts d'affaires de son employeur.

Le facteur aggravant pourra découler de la structure de l'entreprise ou de la spécificité de son activité[676]. Ainsi, la situation d'un préposé au nettoyage d'une entreprise de produits alimentaires, qui se vante sur Internet de jouer aux cartes pendant la moitié de son quart de travail, sera examinée avec beaucoup plus de sévérité que s'il s'agissait d'un employé d'une usine dont l'activité n'est pas reliée à la sécurité alimentaire[677]. Il en ira de même lorsque l'employeur est un centre d'hébergement pour personnes malades et âgées[678] ou s'il s'agit d'un établissement d'enseignement secondaire accueillant de jeunes élèves, à une étape de leur vie où ils sont particulièrement vulnérables[679].

Il existe d'autres situations particulières dans lesquelles le salarié sera tenu à une obligation de loyauté renforcée. Ce sera, par exemple, le cas pour le salarié qui est en période d'essai et qui doit être particulièrement précautionneux : il doit en effet, pendant cet intervalle, démontrer à son employeur qu'il peut bénéficier de sa confiance. Il ne peut donc pas, comme l'a souligné l'arbitre dans l'affaire *Martel* c. *Fédération des caisses Desjardins du Québec*[680], s'autoriser à envoyer et recevoir des courriels en contravention du règlement de l'entreprise. Le salarié avait, en l'espace d'à peine un mois, reçu 616 courriels et en avait expédié 454, alors même que les différentes politiques de l'entreprise, qu'il avait reçues et signées lors de son embauche, interdisaient l'utilisation des outils de communication à des fins personnelles. Confronté par l'employeur sur ses agissements, l'employé indélicat avait admis avoir envoyé quelques courriels personnels, et cela dès son premier jour de travail, mais en avait cependant minimisé le nombre. Il avait justifié ses agissements par le manque de travail, précisant que son usage personnel des outils de communication avait diminué dès qu'il avait eu plus d'activité. Il avait ajouté que les courriels privés qu'il échangeait avec l'extérieur ne surchargeaient pas le réseau et qu'il y avait une tolérance à cet égard.

---

[676] *Syndicat des cols bleus regroupés de Montréal (SCFP), section locale 301 (S.C.F.P.)* et *La Ronde (Six Flags)*, D.T.E. 2004T-1124 (T.A.) : dans cette affaire, l'arbitre conclut que le caractère familial et la nature des activités de l'entreprise, spécialisée dans le divertissement familial, constitue un facteur aggravant.

[677] *Montour Limitée* c. *Syndicat des employé-e-s de la Cie Montour (CSN)*, préc., note 245.

[678] *Ordre des infirmières et infirmiers du Québec* c. *Léveillé*, 2008 CanLII 47548 (QC C.D.O.I.I.).

[679] *Addy* c. *Commission scolaire Eastern Township*, 2010 QCCS 1708 (CanLII).

[680] Préc., note 542.

Ces arguments n'ont pas convaincu l'arbitre qui a conclu que les dispositions des règlements étaient claires. De plus, l'employé avait été avisé que toute utilisation inappropriée des outils informatiques entraînerait des sanctions. L'arbitre a estimé que ce qui avait provoqué la perte de confiance de l'employeur c'était la suppression par l'employé de tous les courriels litigieux de son ordinateur. Cette suppression avait eu lieu à l'issue de l'entrevue que l'employé avait eue avec sa responsable concernant, entre autres, son usage inapproprié du courrier électronique. Le congédiement fut donc confirmé.

Enfin, un niveau supérieur de confiance est également exigé des employés qui, sans forcément occuper une fonction hiérarchique, sont tenus d'obéir à des standards éthiques plus élevés. Ce sera notamment le cas pour les enseignants de qui l'on exige une norme de conduite plus élevée, surtout lorsqu'ils sont au contact de jeunes enfants ou d'adolescents[681]. Il en ira de même pour les infirmiers qui, tout comme les médecins, doivent particulièrement éviter de s'engager dans des actes indécents[682]. En effet, les patients doivent pouvoir avoir une confiance absolue dans les personnes qui s'occupent d'eux.

1.1.3.2. Le dossier disciplinaire du salarié, le niveau de gravité de son inconduite et son comportement après la découverte des faits

L'examen du dossier disciplinaire du salarié et de son comportement après la découverte des faits pourra être décisif lors de la détermination de la mesure disciplinaire applicable. Il faudra également prendre en compte le niveau de gravité de ses gestes ainsi que les circonstances entourant les faits.

---

[681] Voir notamment *Addy* c. *Commission scolaire Eastern Township*, préc., note 679, qui confirme le congédiement d'un aspirant enseignant pour avoir, à des nombreuses reprises, consulté des sites pornographiques sur un ordinateur de l'école secondaire où il effectuait son stage de fin d'études universitaires. L'établissement accueille des élèves âgés de 11 à 17 ans et dispose d'une politique d'utilisation des ordinateurs interdisant spécifiquement la consultation de sites pornographiques.

[682] Voir *Ordre des infirmières et infirmiers du Québec* c. *Léveillé*, préc., note 678, par. 32, où les gestes obscènes de l'employé sont qualifiés d' « atteinte à l'honneur et à la dignité de la profession d'infirmier ».

Ainsi, dans *Ordre des infirmières et infirmiers du Québec* c. *Léveillé*[683], le facteur aggravant résultait, notamment, de la nature des actes reprochés au salarié et des circonstances entourant les faits. Lors d'une modification de son système informatique, l'employeur, un centre d'hébergement pour personnes âgées et malades, avait découvert qu'un ordinateur abritait une importante activité vers des sites Internet pornographiques. Grâce à une surveillance vidéo, il avait rapidement découvert qu'un employé consultait des sites pornographiques pendant son quart de travail en se livrant à des actes de grossière indécence devant l'écran de l'ordinateur. Ces agissements ont valu à leur auteur une radiation temporaire du Tableau de l'Ordre des infirmières et infirmiers en raison de l'extrême gravité des faits reprochés. En effet, ces activités avaient lieu alors que l'employé avait un poste de nuit auprès d'une population âgée et vulnérable. Ensuite, les gestes reprochés s'étaient étalés sur une longue période (environ deux ans) et avaient lieu à chaque quart de travail. De plus, ces activités se déroulaient pendant les heures de travail de l'employé, ce qui constituait un vol de temps. Le tout avait lieu dans une aire ouverte et passante, où l'employé aurait facilement pu être surpris par un collègue, un patient ou encore un membre de la famille d'un patient. Sans compter que pendant ce temps, le bien-être de ses patients était compromis, puisque les faits reprochés avaient lieu pendant la pause et l'heure de repas de l'infirmière auxiliaire qui travaillait avec lui. De plus, l'employé avait précédemment fait l'objet d'une enquête à la suite d'allégations de certains employés relativement à son utilisation de l'Internet, mais aucune procédure ne s'en était suivie, faute de preuve suffisante. En outre, l'employé avait nié les faits et n'avait reconnu sa responsabilité qu'après avoir été confronté avec les preuves vidéo. Il avait également tenté de minimiser les conséquences de ses activités en soutenant qu'elles n'avaient causé aucun préjudice aux patients sous sa responsabilité. Enfin, l'employé n'avait jamais suivi de thérapie, ni même consulté un professionnel du comportement, alors ses actes répétitifs appelaient peut-être un suivi spécialisé. Finalement, comme le salarié n'exerçait plus la fonction d'infirmier lors du jugement (il occupait alors un poste sans lien avec ses

[683] Préc., note 678.

occupations précédentes dans une institution financière), il a reçu une sanction suspendue qui ne deviendrait exécutoire que lorsqu'il se réinscrirait au Tableau de l'Ordre de cette profession.

L'aggravation des sanctions pourra aussi résulter de certains comportements particuliers, comme le fait, pour le salarié, de dissimuler les traces de ses activités ou d'effacer son historique de navigation[684] ou encore de refuser de reconnaître les faits[685]. Il en ira de même lorsque l'employé persiste dans son comportement, malgré les remarques ou réprimandes de l'employeur[686].

Au contraire, la qualité de son dossier disciplinaire ou son ignorance de l'interdiction des activités reprochées peuvent jouer en faveur du salarié, et doivent donc être prises en compte lors de l'évaluation de la sanction. Ainsi, dans *Gilles* et *Ciba Spécialités chimiques Canada Inc.*[687], la Commission des relations du travail a annulé le congédiement d'un salarié après avoir relevé plusieurs circonstances atténuantes en sa faveur. L'employeur reprochait au salarié d'avoir mis en péril la sécurité du système informatique, utilisé par ses 19 000 employés à travers le monde, en téléchargeant et sauvegardant des images et des vidéos à caractère pornographique, contrairement aux directives claires en vigueur dans l'entreprise. L'employeur considérait que la faute de l'employé était d'autant plus grave qu'il disposait d'une grande liberté d'action et sa fonction de directeur de comptes responsable d'une région incluant plusieurs villes exigeait un plus grand niveau de confiance. L'employé, de son côté, tout en admettant avoir commis une faute sérieuse, soutenait que la sanction imposée était trop sévère compte tenu, notamment, de la qualité de

---

[684] *Syndicat du personnel de soutien de la Seigneurie des Mille-Îles* (CSN) et *Commission scolaire de la Seigneurie des Mille-Îles*, D.T.E. 2008T-149 (T.A.).

[685] *Di Vito* v. *MacDonald Dettwiler and Associates*, 1996 CanLII 3165 (BC S.C.) : la Cour suprême de Colombie-Britannique confirme le congédiement de deux employés accusés de harcèlement et de distribution de matériel à caractère sexuel et qui, malgré les preuves, nient les faits de façon répétée; Voir également *Syndicat des spécialistes et professionnels d'Hydro-Québec* c. *Hydro-Québec*, préc., note 229.

[686] Voir, par exemple, *Backman* c. *Maritime Paper Products Limited, corps constitué*, préc., note 546, qui confirme le congédiement d'un employé pour consultations répétées de sites pornographiques, en violation de la politique de l'entreprise relative à l'utilisation du système informatique dont il avait pris connaissance lors de son embauche, et malgré deux avertissements sanctionnant formellement son inconduite répétée. La dernière sanction l'avisait d'ailleurs qu'il encourait le congédiement en cas de récidive.

[687] Préc., note 521.

son dossier disciplinaire et de son ancienneté dans l'entreprise. Le Tribunal a accueilli sa demande, principalement en raison du non-respect par l'employeur du principe de la gradation des sanctions, ainsi que des dispositions du règlement d'entreprise relatives aux procédures disciplinaires. Ces règles prévoyaient notamment le droit pour l'employé de s'expliquer sur sa conduite et la prise en compte de son dossier disciplinaire. Or, l'employeur s'était simplement contenté de convoquer l'employé à une entrevue et l'avait congédié sur-le-champ, après l'avoir sommé de rendre les équipements appartenant à l'entreprise. En rompant la relation de travail de façon aussi sommaire, sans donner à l'employé la possibilité de s'expliquer, l'employeur avait méconnu ses propres obligations. De plus, l'examen des faits révélait que l'employé travaillait souvent de chez lui, sur un équipement que l'entreprise l'autorisait, sauf certaines exceptions, à utiliser à des fins personnelles. Et il avait accumulé les fichiers litigieux pendant 9 ans, les transférant d'ordinateur à ordinateur à chaque changement de poste. Ces actes étaient commis en dehors des heures de travail et n'avaient fait l'objet d'aucune remarque de l'employeur pendant cette longue période, si bien que l'employé en avait déduit qu'il y avait une tolérance de l'employeur à l'égard de son utilisation personnelle. De plus, l'employé avait un dossier disciplinaire vierge et aurait pu facilement cesser les activités reprochées si on lui en avait fourni l'occasion. En outre, malgré leur gravité, ces actes n'avaient pas eu de conséquences directes sur les clients ou sur les autres employés. Par ailleurs, bien que l'employeur ait fait référence à un salarié qui avait été congédié pour des faits similaires, aucune précision n'était donnée quant au pays ou la province où ces événements se seraient déroulés. Finalement, même si le Tribunal conclut à l'absence de tolérance de l'employeur et constate l'existence d'un facteur aggravant lié à la durée des activités reprochées, il juge que le congédiement constituait une sanction trop sévère au vu de la faute et des circonstances, et le remplace donc par une suspension de 3 mois sans solde.

En définitive, l'affaire *Gilles* et *Ciba Spécialités chimiques* Canada *Inc.*[688] présente un intérêt particulier dans la mesure où elle énumère quelques facteurs déterminants à prendre

---

[688] *Id*.

en compte lors de l'évaluation du comportement de l'employé dans le cadre d'une procédure disciplinaire. Ces facteurs atténuants ou aggravants sont les suivants :

- le niveau de gravité de l'inconduite de l'employé;
- son dossier disciplinaire;
- sa capacité à corriger la situation;
- l'existence de mesures prises pour des cas similaires touchant d'autres employés;
- les conséquences pour les clients (et, plus généralement, les partenaires d'affaires de l'entreprise et les tiers);
- l'impact sur les autres employés;
- les circonstances entourant l'incident.

Bien entendu, d'autres facteurs, mis en évidence dans l'annexe II, pourront, selon les cas, être pris en compte, tels :

- la nature des fonctions, ainsi que le degré d'autonomie et le niveau de confiance accordés par l'employeur;
- la nature des activités de l'employeur;
- la durée des manquements;
- le caractère isolé des faits reprochés ou leur répétition;
- l'existence ou non d'un risque de récidive;
- la responsabilité de l'employeur (liée, notamment, à sa tolérance face aux manquements ou à l'absence de directives claires);
- l'attitude de l'employé après la découverte des faits (refus d'admettre sa responsabilité ou ses aveux et remords sincères, etc.);
- l'existence ou non d'un profit, pour le salarié, lié à ses actes,
- les éléments liés à la situation personnelle de l'employé (dont l'âge, l'ancienneté et la situation familiale).

1.2. L'antériorité du motif de la surveillance

Il ressort de l'arrêt *Brigdestone/Firestone* que le motif de surveillance doit exister avant la mise en œuvre de cette dernière[689]. C'est ce qu'indique clairement la Cour d'appel dans les termes suivants :

> « 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. »[690]

Le défaut d'antériorité du motif rend donc, en principe, la surveillance patronale invalide. Le problème c'est que bien souvent, les ordinateurs de l'employeur sont dotés de logiciels de surveillance préinstallés. L'employeur risque donc d'éprouver quelques difficultés s'il doit démonter qu'il a initié la surveillance informatique pour répondre à un besoin précis et préexistant, alors que les outils de surveillance existaient bien avant l'achat des équipements informatiques[691].

De plus, il arrive parfois que les actes reprochés à un salarié soient découverts à l'occasion d'une surveillance effectuée, à titre préventif, pour un tas de raisons plus ou moins avouables. Les motifs « préventifs » évidents sont la sécurité et le bon fonctionnement du matériel informatique, ainsi que les risques de responsabilité. À cet égard, les tribunaux ont précisé que l'installation de caméras vidéo dans un but purement préventif, sans que l'employeur soit en mesure d'établir qu'il était victime de vols, n'était pas justifiée[692]. Toutefois, dans une autre affaire, il a été jugé que la surveillance vidéo ne constituait pas une condition de travail déraisonnable dans la mesure où elle visait seulement à protéger les

---

[689] *Syndicat des travailleuses et travailleurs de Bridgestone/Firestone de Joliette (C.S.N.)* c. *Trudeau*, préc., note 8 par. 73.

[690] *Id.*

[691] Georges RADWANSKI, préc., note 647.

[692] *Garaga Inc.* c. *Syndicat des salariés de garage (C.S.D.)*, D.T.E. 2002T-1100 (T.A.).

secrets industriels et l'équipement de l'entreprise tout en assurant la sécurité des lieux de travail[693].

La surveillance préventive peut également avoir pour objectif de resserrer le lien de subordination. Ce besoin devient d'autant plus impérieux que les salariés travaillent de plus en plus souvent hors des locaux de l'entreprise[694]. Avec les NTIC, le « travail nomade » connaît, en effet, une croissance exponentielle[695]. Et, contrairement à ce qui se passe dans l'entreprise « intra-muros », l'employeur se retrouve alors dans l'impossibilité de contrôler physiquement la présence du salarié à son poste de travail et de s'assurer qu'il remplit bien ses obligations contractuelles. Grâce aux possibilités de traçabilité ou de mise en réseau des activités de l'entreprise offertes par les NTIC, l'employeur peut étendre son pouvoir de direction et de surveillance hors des murs de l'entreprise[696]. Il peut ainsi retrouver une partie du contrôle qui lui échappe face à cette autonomie, qui n'est pas toujours souhaitée, du salarié. Finalement, malgré l'indéniable liberté que les NTIC offrent aux employés, ces dernières constituent également un excellent outil de subordination dont la traçabilité est le « support »[697].

On peut, enfin, signaler que la surveillance peut être effectuée à des fins de gestion comportementale pour établir le « profil professionnel, intellectuel ou psychologique du salarié virtuel »[698] à partir, par exemple, de ses préférences et habitudes de navigation.

L'employeur peut donc se retrouver dans une position délicate, si, dans les circonstances qui viennent d'être évoquées, il lui faut prouver que la découverte des actes indésirables d'un salarié est survenue à l'occasion d'une surveillance justifiée. Les tribunaux ont, en

---

693 *Poulies Maska Inc.* c. *Syndicat des employés de Poulies Maska Inc.,* préc., note 126.

694 Xavier BISEUL, « Cybersurveillance : les nouvelles technologies ravivent les vieilles peurs », 01net.com, 19 juillet 2004, en ligne : <http://www.01net.com/article/248848.html> (site consulté le 18 août 2010).

695 FORUM DES DROITS SUR L'INTERNET, *Rapport final. Relations du travail et internet*, 2002, p. 8, en ligne : <http://www.foruminternet.org/telechargement/documents/rapp-RTI-20020917.pdf> (site consulté le 26 juillet 2010).

696 V. ROQUES, préc., note 34, p. 26.

697 D. SERIO et C. MANARA, préc., note 7.

698 COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, *La cybersurveillance sur les lieux de travail*, 2004, p. 4, en ligne : <http://www.cnil.fr/fileadmin/documents/approfondir/rapports/Rcybersurveillance-2004-VD.pdf> (site consulté le 26 juillet 2010).

effet, tendance à invalider les décisions patronales lorsqu'elles découlent d'une « expédition de pêche », effectuée sans but précis, pour trouver des faits incriminants permettant, par exemple, de se débarrasser d'un salarié « gênant »[699]. Dans *Martel* c. *Fédération des caisses Desjardins du Québec*[700], le plaignant plaidait que le motif de son congédiement était un prétexte et que la véritable raison de son renvoi était, non pas son usage inapproprié des outils informatiques, comme le prétendait l'employeur, mais plutôt son refus de recourir aux services bancaires de l'employeur. Il avançait que son congédiement était intervenu juste quelques jours après qu'il a fermé le compte initialement ouvert pour recevoir les virements de salaires effectués par l'employeur, et demandé à être payé par chèque à l'avenir. L'employeur, de son côté, arguait que l'incident relatif à la paie était sans lien avec le congédiement et que la vérification du profil d'utilisation du courrier électronique du plaignant n'avait été effectuée qu'après la découverte sur une imprimante d'un courriel qui lui était destiné. La Commission des relations du travail a conclu que le motif allégué par l'employeur n'était pas un prétexte, puisque le plaignant, alors même qu'il était en période d'essai, s'était autorisé à utiliser la messagerie électronique à des fins personnelles. Pour la Commission, le fait que plaignant ait souhaité être payé par chèque était étranger à la décision de l'employeur.

Dans *Syndicat des spécialistes et professionnels d'Hydro-Québec, (SCFP-FTQ, section locale 4250)* c. *Hydro-Québec*[701], c'est également un document oublié sur l'imprimante qui avait éveillé les soupçons de l'employeur. Ce dernier avait, en effet, découvert une vingtaine d'exemplaires de la page d'accueil du site Internet d'une association sur l'imprimante. Cet organisme ne faisait pas affaire avec l'entreprise et une visite sur ce site avait permis à l'employeur de constater une différence de qualité entre le document imprimé – qui en représentait une version très améliorée – et le visuel qui apparaissait à l'écran. Sachant que le plaignant s'était spécialisé dans la conception de sites Internet et

---

[699] *Mascouche (Ville)* c. *Houle*, [1999] R.J.Q. 1894 (C.A.); *Srivastava* c. *Hindu Mission of Canada (Québec) Inc.*, préc., note 576.

[700] Préc., note 542.

[701] Préc., note 193.

Intranet, il avait alors procédé à l'examen de l'ordinateur de ce dernier, afin de vérifier si ces améliorations étaient le fruit de ses travaux. Les vérifications avaient permis de répondre par l'affirmative et de conclure que ces travaux avaient été réalisés par le salarié, pour son propre compte, avec les outils de l'entreprise et pendant ses heures de travail.

De même, dans *Bolduc* c. *Collège de Montréal*[702], la question se posait de savoir si la fonction syndicale de la plaignante ne constituait pas le véritable motif de son congédiement. Le Tribunal a conclu que cette mesure s'appuyait sur une autre cause juste et suffisante. En effet, l'employeur avait mis son enquête en œuvre à la suite de la publication d'informations confidentielles le concernant dans un journal. De plus, la plaignante était la seule à avoir accès à ces informations financières précises et, dans le contexte particulier de cette affaire, il aurait été inutile d'effectuer une enquête coûteuse sur tous les employés pour faire croire à une fausse neutralité. D'ailleurs, l'enquête s'était concentrée sur la plaignante et un groupe restreint de personnes et n'avait finalement porté que sur les courriels échangés dans le système interne de messagerie. Ce contrôle avait permis à l'employeur d'accéder à une foule d'informations qui l'avaient rapidement convaincu de l'implication de la plaignante dans les événements. L'employée avait d'ailleurs fini par avouer être la source de la fuite de l'information.

En définitive, l'employeur doit à chaque fois démontrer que sa surveillance n'était pas basée sur de simples soupçons, mais reposait sur des motifs raisonnables et probables. Tout sera alors une question de preuve qu'il devra positivement rapporter, la surveillance étant considérée, le cas échéant, comme illégale[703]. Toutefois, le défaut d'antériorité du motif de la surveillance ne constitue pas une entrave absolue à l'exercice du pouvoir de sanction de l'employeur, dans la mesure où les preuves recueillies dans ce contexte sont admissibles en Cour, tel qu'il ressort de l'opinion complémentaire du juge Beaudoin dans l'arrêt *Syndicat des travailleuses et travailleurs de Bridgestone/Firestone de Joliette (C.S.N.)* c. *Trudeau* :

---

[702] Préc., note 670.

[703] M. ÉVANGÉLISTE, préc., note 600, p. 6-7.

> « 81 Pour qu'une preuve du genre de celle qui a été présentée à l'arbitre puisse être exclue en raison d'une violation de la vie privée, aux termes de l'article 2858 C.c.Q., il faut démontrer (et le fardeau repose sur la partie qui en réclame l'exclusion) que son admission soit de nature à déconsidérer l'administration de la justice civile.
>
> […]
>
> 83 Nous nous trouvons ici devant un cas de fraude caractérisée, volontairement ou involontairement soutenue par une complicité médicale.
>
> 84 Refuser d'admettre en preuve les éléments dont disposait l'arbitre dans les circonstances que relate mon collègue, me paraîtrait, à l'inverse, déconsidérer l'administration de la justice civile en permettant indirectement à un fraudeur d'invoquer (selon le terme consacré par l'adage latin «nemo auditur...») sa propre turpitude. »[704]

Cette position semble majoritairement suivie par la jurisprudence arbitrale qui a tendance à admettre les preuves obtenues illégalement, à moins que leur admission soit de nature à déconsidérer l'administration de la justice[705]. Les tribunaux semblent en effet soucieux de laisser à l'employeur, lorsque ce dernier n'est pas en mesure de justifier au préalable sa surveillance, la possibilité de prouver les comportements fautifs des salariés et d'établir, après coup, grâce au produit de la vidéosurveillance, que son intrusion était bel et bien justifiée. Le critère généralement utilisé par la jurisprudence pour recevoir ou exclure un élément de preuve obtenu en violation d'un droit fondamental est celui de la gravité de la violation, combiné à d'autres facteurs, tels que la nature du litige ou l'importance de la preuve[706]. Lorsque la preuve est obtenue en violation d'un droit fondamental, le tribunal décidera, au cas par cas, s'il doit faire primer la recherche de la vérité ou la protection du droit bafoué[707]. Les éléments de preuve ne seront généralement rejetés que lorsque la

---

[704] *Syndicat des travailleuses et travailleurs de Bridgestone/Firestone de Joliette (C.S.N.)* c. *Trudeau*, préc., note 8, par. 81, 83 et 84.

[705] S. LEFEBVRE, *Nouvelles technologies et protection de la vie privée en milieu de travail en France et au Québec*, préc., note 70, n° 252 et suiv. p. 102-103.

[706] Jean-Claude ROYER, « La preuve obtenue par des moyens illégaux », dans *La Preuve civile*, 3e éd., 2003, *Droit civil en ligne* (DCL), EYB2003PRC35, p. 23-24.

[707] *Id.*, p. 24.

violation est si grave qu'il serait inacceptable de faire profiter celui qui en est l'auteur de preuves obtenues dans de telles circonstances[708]. En fait, en matière de surveillance informatique, le constat est que, bien souvent, l'employeur n'est pas en mesure de justifier au préalable la surveillance et c'est généralement la preuve recueillie qui va permettre, après coup, d'en établir la légitimité.

En plus de prouver la réalité et l'importance du problème auquel il était confronté, l'employeur doit démontrer que la surveillance mise en œuvre était nécessaire et efficace pour le régler.

Section 2. L'efficacité de la cybersurveillance

Une fois la finalité établie, l'employeur doit démontrer que son intrusion dans la vie privée de l'employé était nécessaire et constituait le moyen le plus efficace pour vérifier le comportement du salarié[709]. L'employeur a donc un double fardeau, puisqu'il doit à la fois prouver la faute de son employé et l'efficacité de la surveillance pour obtenir cette preuve. À cet égard, la pertinence de recours à la cybersurveillance comme moyen de contrôle de l'utilisation des ressources informatiques ne semble pas sérieusement discutable, sauf à se poster physiquement derrière chaque salarié ou à « braquer » en continu une caméra vidéo sur chaque écran d'ordinateur. Toutefois, l'employeur doit être en mesure de justifier l'utilisation de tel outil particulier comme étant le seul moyen efficace pour parvenir au but recherché. Ce point sera examiné ultérieurement dans la section réservée à l'étendue de la surveillance.

Quant à l'efficacité de la surveillance, elle repose sur la capacité de l'employeur à recueillir la preuve des comportements fautifs des salariés et d'en identifier le coupable. En effet, si la surveillance peut révéler l'existence d'une activité inappropriée sur un ordinateur, elle ne permet pas toujours de la relier avec certitude à un salarié. Par ailleurs, l'employeur doit

---

[708] *Id.*, p. 22; *Mascouche (Ville)* c. *Houle*, préc., note 699, 1906.

[709] D. VEILLEUX, préc., note 483, 42.

démontrer que les preuves ainsi recueillies sont fiables et n'ont fait l'objet d'aucune manipulation.

Les données numériques sont extrêmement volatiles, et cela d'autant plus que les salariés, pour peu qu'ils soient familiers avec l'informatique, disposent d'une large gamme d'outils leur permettant d'effacer ou dissimuler efficacement leurs traces informatiques. L'ordinateur se manipule et il est très facile de créer, modifier ou effacer totalement ou partiellement les données numériques. Aussi l'employeur doit-il mettre en œuvre des outils capables de recueillir et de conserver intacte la preuve des comportements fautifs de ses salariés. Pour un meilleur résultat, il aura souvent recours à des experts en informatique pour mener les enquêtes appropriées. Ceux-ci disposent généralement d'outils capables de retracer les activités des employés et de reconstituer les documents et fichiers supprimés.

La recherche des preuves et leur préservation conduisent de plus en plus d'entreprises à recourir à des ordonnances Anton Piller prononcées par un tribunal. Il s'agit de mesures préliminaires qui permettent au demandeur d'obtenir, avant l'exercice d'une poursuite, la perquisition et la saisie d'un bien afin que ce dernier ne puisse être détruit ou modifié. En matière informatique, l'ordonnance Anton Piller peut concerner tout matériel susceptible de contenir des informations numériques (serveurs informatiques, ordinateurs, assistants numériques, clés USB, DVD, etc.). La saisie peut s'effectuer aussi bien sur le lieu de travail qu'au domicile du salarié soupçonné de malversations.

Outre la préservation de la preuve, l'ordonnance Anton Piller constitue l'un des meilleurs moyens de s'assurer que la preuve demeure fiable et authentique. Son exécution est, en effet, réalisée sous le contrôle de l'autorité judiciaire et répond à des exigences strictes. La collecte et la conservation des éléments de preuve sont encadrées de façon à garantir, en tout temps, que la preuve originale n'est pas modifiée.

Il s'agit là d'un point important, car les possibilités de manipulation sont réelles pour les preuves numériques. La jurisprudence a, dans l'ensemble, pris la mesure des difficultés probatoires liées à l'outil informatique. Un tribunal a ainsi été amené à conclure qu'un contrat avait été antidaté après avoir relevé des incohérences entre la date du contrat et la

date de sauvegarde indiquée sur les fichiers informatiques[710]. Dans cette affaire, l'une des parties prétendait que le contrat était antidaté et la Cour avait ordonné que le fichier informatique et l'horloge de l'ordinateur sur lequel le contrat avait été préparé soient produits. La preuve révélait que la date de préparation du contrat indiquée sur l'horloge concordait avec celle figurant sur le contrat, toutefois, l'heure de sauvegarde indiquée par cette même horloge était incompatible avec le témoignage des parties. La Cour, après avoir relevé qu'il était extrêmement facile de trafiquer l'horloge d'un système informatique, avait finalement conclu que les indications de l'horloge n'étaient pas fiables et que le contrat avait été antidaté.

Dans un tel contexte, il est permis de croire que certains patrons peuvent être tentés de manipuler les données de navigation ou les fichiers de leurs salariés afin de se constituer la preuve de leurs prétendues fautes professionnelles. Aussi l'employeur qui souhaite exhiber des preuves numériques est-il tenu de respecter les règles relatives à l'authenticité et à la fiabilité prévues aux articles 2837 à 2839 C.c.Q.

Parce que la preuve numérique n'est pas toujours fiable, le tribunal doit souvent prendre en compte la preuve circonstancielle. Dans *R.* c. *Crevier*, la Cour indique que le seul examen d'un texte de courriel ne permet pas de tirer des conclusions quant à son auteur ou même son contenu, mais que les juges peuvent se forger une opinion lorsqu'ils disposent d'une preuve testimoniale complémentaire[711]. Le tribunal rendra souvent sa décision en se basant sur les témoignages ou attestations qui viennent ou non corroborer la preuve matérielle produite en Cour. Bien entendu, il rejettera tous les éléments qui ne lui semblent pas suffisamment clairs ou crédibles. Ainsi, dans une affaire où l'employeur reprochait à un employé d'avoir voulu pirater l'ordinateur de son supérieur hiérarchique afin de recueillir des informations qui le concernaient, l'arbitre rejette les allégations de l'employeur pour manque de crédibilité. Les tentatives d'intrusion non autorisée alléguées avaient, en effet, duré moins de cinq secondes. L'arbitre énonce clairement qu'il est « quasiment de

---

[710] *Technologie Labtronix Inc*. c. *Technologie Micro contrôle Inc*., J.E. 97-228 (C.S.).

[711] *R.* c. *Crevier*, EYB 2006-113697, par. 69 (C.Q.).

connaissance judiciaire » qu'il est impossible d'accéder au compte d'une personne et de s'introduire dans ses fichiers en si peu de temps, puisqu'un simple clic sur une icône pour ouvrir un logiciel dure bien plus que quelques secondes[712].

Il est également primordial d'apporter une preuve établissant de manière fiable que le salarié visé est bien l'auteur du comportement inapproprié. À cet égard, les tribunaux doivent examiner les preuves qui leur sont soumises avec la plus grande circonspection. Il n'est, en effet, pas toujours aisé de déterminer qui est l'auteur des actes inappropriés au sein d'une organisation, dans la mesure où les entreprises utilisent généralement une seule adresse IP pour tout leur parc informatique. En cas d'activité inappropriée, il est alors difficile de déterminer avec certitude quel ordinateur l'a abritée. Certains auteurs approuvent fortement cette approche et estiment que les tribunaux ne devraient admettre les preuves numériques qu'avec beaucoup de réserves[713].

La prudence est particulièrement de mise lorsque les actes frauduleux sont commis grâce à la messagerie électronique. En effet, même lorsqu'un message porte la mention de l'adresse électronique d'un salarié, il faut demeurer prudent. Il existe, en effet, un tas de virus capables d'« usurper » des adresses de courriel, et de les utiliser pour diffuser toutes sortes de messages à des tiers[714]. Sans avoir recours à des solutions aussi extrêmes, les salariés peuvent profiter d'autres opportunités pour accéder à la messagerie électronique d'un collègue à son insu. Ce sera le cas, par exemple, lorsque des employés partagent le même bureau, voire le même poste de travail, et ne disposent pas de comptes d'utilisateurs séparés. La jurisprudence a ainsi dû statuer sur des cas de salariés contestant être l'auteur de courriels qui, en apparence, émanaient d'eux. Ainsi, dans *R.* c. *Crevier*[715], une employée niait être l'auteur d'un courriel demandant le transfert d'une vingtaine d'ordinateurs appartenant à son employeur et qui s'étaient finalement retrouvés en la possession de son conjoint, qui les avait revendus à des tiers. L'employée prétendait qu'elle était en vacances

---

[712] *Roy* c. *Produits Vitafoam Canada limitée (Les fabrications Ultra inc.)*, 2006 QCCRT 371 (CanLII), par 44.

[713] H. PESCHAUD, préc., note 303.

[714] *Id.*

[715] Préc., note 711.

avec ses enfants le jour où le courriel litigieux avait été envoyé. Le Tribunal n'a pas été convaincu par ces affirmations, car l'accusée avait pendant des années été incapable de fournir la moindre preuve pour confirmer ses dires. Toutefois, elle avait, soudainement, été en mesure d'exhiber son agenda professionnel lors du procès, soit près de quatre ans plus tard. Cette preuve n'avait pas été jugée suffisamment fiable, car les annotations indiquant la date de l'envoi du courriel comme jour de congé avaient été rédigées par l'accusée elle-même. De plus, l'agenda était demeuré en sa possession et sous son contrôle pendant toutes ces années. Le Tribunal a, en revanche, accueilli favorablement les affirmations de l'employeur qui avait fourni une preuve circonstanciée reposant, notamment, sur le témoignage de l'employé qui avait préparé la commande. Ce dernier avait téléphoné à l'accusée lors de la réception du courriel, afin de confirmer la commande et d'obtenir des informations complémentaires. Et, après l'exécution et l'expédition de celle-ci, il avait à nouveau confirmé le tout par un courriel envoyé à l'accusée. Ce courriel, qui faisait partie des messages reçus par l'ordinateur de l'accusée, n'avait provoqué aucune réaction chez cette dernière, comme si le déroulement des faits était parfaitement normal. Le Tribunal en est donc arrivé à la conclusion que le bon de commande par courriel émanait bien de l'accusée.

Les salariés peuvent aussi profiter de l'absence temporaire d'un collègue, ayant malencontreusement laissé sa session ouverte, pour envoyer des courriels compromettants à des tiers, manipuler des fichiers ou consulter des sites interdits. Dans *Dosanjh* c. *Conseil du Trésor*[716], le Tribunal accueille les allégations d'un employeur qui reprochait à un salarié d'avoir profité du fait qu'un collègue avait, par mégarde, laissé l'ordinateur sur lequel il venait de travailler allumé, pour accéder à son compte d'utilisateur et détruire des fichiers, après en avoir transféré certains sur sa messagerie électronique personnelle. Trois employés avaient utilisé l'ordinateur dans les minutes suivant le transfert de fichiers et pouvaient avoir commis les actes reprochés. Le Tribunal était convaincu que le salarié désigné par l'employeur était bien le coupable, car il était le seul à avoir un intérêt à détruire les

[716] 2003 CRTFP 16 (CanLII).

fichiers, puisque ceux-ci contenaient un compte rendu le mettant directement en cause. De plus, les relevés d'utilisation n'indiquaient à aucun moment qu'il ait utilisé l'ordinateur, alors que, selon les témoignages, il s'en était servi et avait même été le premier des trois à s'installer sur le poste de travail. Le système informatique de l'employeur ne permettait pas de connaître les heures de déconnexion d'un utilisateur; toutefois, il était impossible d'entamer une nouvelle session tant que la session en cours n'était pas terminée. Le Tribunal en a conclu que l'ordinateur étant resté allumé, l'employé n'avait pas eu besoin d'ouvrir une nouvelle session : il avait ainsi pu commettre les actes reprochés dans les deux ou trois minutes qui avaient précédé les connexions de ses deux collègues dont les heures de début de connexion apparaissaient sur les relevés d'utilisation.

Finalement, les éléments de preuve recueillis par l'employeur doivent non seulement permettre de désigner un salarié comme étant l'auteur probable des faits allégués, mais également de prouver que ces actes n'ont pas pu être commis par quelqu'un d'autre. Lorsqu'il y a un doute sur l'identité de l'auteur des faits reprochés, le tribunal doit écarter la responsabilité du salarié. Ainsi, dans *Beslile* c. *ville de Rawdon*[717], le Tribunal rejette les accusations de l'employeur qui reprochait à l'un de ses cadres d'avoir téléchargé près de 1 600 fichiers à caractère pornographique dans le disque dur de son ordinateur professionnel, au motif, notamment, que plusieurs employés pouvaient facilement accéder à cet ordinateur. Dans ce contexte, il était permis d'avoir des doutes quant à l'implication du salarié relativement à l'enregistrement et à l'usage des fichiers.

Les précautions entourant l'analyse des preuves numériques sont autant de garanties pour les salariés, puisque cette phase peut conduire au rejet d'éléments de preuve qui avaient pourtant été accueillis et que le tribunal juge finalement insuffisamment fiables. Cette protection des salariés est encore renforcée lors de l'examen de l'étendue de la surveillance patronale.

---

[717] Préc., note 204.

Section 3. L'étendue de l'atteinte à la vie privée

La légitimité de la surveillance patronale ne pourra être confirmée que si, outre l'existence d'un motif sérieux, il est établi, que cette intrusion dans la sphère intime du salarié est juste et raisonnable, à la fois quant aux finalités poursuivies qu'aux moyens utilisés pour sa réalisation. Il s'agit ici d'un point important, car l'employeur a, techniquement, la possibilité de contrôler les activités des salariés, même à leur insu. Cette possibilité d'ingérence dans leur vie privée n'est pas sans inquiéter les salariés qui redoutent, entre autres, que l'employeur en profite pour collecter des informations parfois sans aucun lien avec la recherche de preuves de comportements fautifs. De plus, la surveillance patronale peut être constante et s'étendre sur une durée assez longue. Bref, leur préoccupation centrale est alors de savoir jusqu'où l'employeur peut aller dans sa surveillance.

Pour déterminer l'étendue de la surveillance patronale, il est nécessaire de faire un bref rappel sur la notion de vie privée au travail (3.1.), avant de s'étendre davantage sur la prise en compte concrète de l'expectative de vie privée au travail lors de l'accès à l'ordinateur de l'employé (3.2.).

3.1. La notion de vie privée au travail

Aucun texte de loi ne définit la notion de vie privée. Toutefois, l'on s'accorde généralement aujourd'hui pour rattacher cette notion à la tranquillité et à l'isolement, qui, comme l'indiquait le juge Lebel dans *Syndicat des travailleuses et travailleurs de Bridgestone/Firestone de Joliette (C.S.N.)* c. *Trudeau*, « comporte des composantes telles que le droit à l'anonymat et à l'intimité, au secret et à la confidentialité, dont la fonction ultime est la préservation du droit de chaque personne à son autonomie »[718]. Or, cette idée même s'accommode mal avec et le lien de subordination issu du contrat de travail : si le salarié accepte de travailler pour l'employeur et sous son contrôle, il peut ensuite difficilement revendiquer le droit à être laissé tranquille. Pour cette raison, auteurs et

[718] *Syndicat des travailleuses et travailleurs de Bridgestone/Firestone de Joliette (C.S.N.)* c. *Trudeau*, préc., note 8, par. 64.

tribunaux ont longtemps nié l'existence d'un droit des salariés à la protection de leur vie privée dans le cadre du travail. Ainsi, en dehors de certains endroits, tels les lieux d'aisance, où l'on peut légitimement s'attendre à voir sa sphère privée protégée, la vie privée du salarié était plutôt restreinte[719].

L'occultation des droits des salariés était encore renforcée lorsque l'utilisation des outils de communication de l'employeur, notamment le téléphone, le courriel ou l'Internet, était en jeu, en raison de l'aspect patrimonial qui s'y rajoutait. Le droit à la vie privée des salariés était alors perçu comme devant s'effacer face au droit de propriété de l'employeur qui, par conséquent, était autorisé à contrôler l'utilisation qui était faite de ces moyens.

Cette position était et demeure majoritairement appliquée par la jurisprudence aux États-Unis où les tribunaux affirment régulièrement qu'en matière d'emploi, le travailleur ne peut prétendre à aucune attente raisonnable quant au respect de sa vie privée lorsqu'il utilise les outils de communication de l'employeur[720].

Au Québec, de nombreux jugements ont tranché dans le même sens. On peut notamment citer deux décisions importantes dans ce domaine, qui identifient clairement les échanges effectués grâce aux outils de communication de l'employeur comme ne relevant pas de la vie privée du salarié. Dans *Société des alcools du Québec* c. *Syndicat des employés de magasins et bureaux de la SAQ.*, l'arbitre souligne que « [l]e salarié, dans l'exécution de ses fonctions, a des agissements qui n'appartiennent pas à sa vie privée, sauf exception»[721]. De même, dans *Roy* c. *Saulnier*[722], l'arbitre indique qu'une salariée ne peut s'attendre à ce que ses communications aient un caractère privée alors même qu'elle utilise le téléphone de l'employeur, outil normalement réservé aux affaires de l'entreprise, et qu'elle est payée pour effectuer des appels.

---

[719] Claude D'AOUST, Louis LECLERC et Gilles TRUDEAU, *Les mesures disciplinaires : étude jurisprudentielle et doctrinale*, Montréal, École des relations industrielles, Université de Montréal, 1982, p. 219.

[720] Voir notamment *Ontario* v. *Quon*, 177 L. Ed. 2d 216 (2010); *Smyth* v. *Pillsbury Co.*, 914 F. Supp. 97 (E.D. Pa. 1996).

[721] [1983] T.A. 335.

[722] Préc., note 8.

Toutefois, la jurisprudence a évolué et prend désormais en compte les droits des salariés, conformément aux principes de la *Charte des droits et libertés de la personne*[723] et à ceux dégagés par la jurisprudence de la Cour suprême du Canada qui a apporté une contribution majeure dans la définition des contours de la notion d'expectative de vie privée. Ainsi, dans l'arrêt *R*. c. *Wong*, le juge La Forest indiquait que :

> « la vie privée serait mal protégée si le caractère raisonnable de notre attente en matière de respect de la vie privée dépendait de la question de savoir si nous nous sommes exposés à la surveillance électronique »[724].

Transposés au milieu du travail, ces principes dégagés dans le cadre de la surveillance électronique exercée par l'État, impliquent que l'attente raisonnable de vie privée du salarié ne peut être fondée sur le risque d'être surveillé par l'employeur, puisque ce dernier a généralement la possibilité de se doter de moyens technologiques pour surveiller ses salariés[725].

Dans une autre affaire, relative à la captation et à l'utilisation d'une image, la Cour suprême du Canada précise que les intérêts de vie privée ne sont pas sujets à une limitation géographique stricte se confinant aux murs du foyer : ils peuvent continuer d'exister et d'être protégés avec des intensités diverses, même dans les lieux où un individu peut être vu du public[726].

De son côté, la Cour d'appel du Québec, notamment avec les arrêts *Syndicat des travailleuses et travailleurs de Bridgestone/Firestone de Joliette (C.S.N.)* c. *Trudeau*[727], *Mascouche (Ville)* c. *Houle*[728] et *Srivastava* c. *Hindu Mission of Canada (Québec) Inc.*[729], a

---

[723] Préc., note 361.

[724] *R.* c. *Wong*, [1990] 3 R.C.S. 36; *Godbout* c. *Ville de Longueuil*, [1997] 3 R.C.S. 844.

[725] D. VEILLEUX, préc., note 483, 21.

[726] *Éditions Vice-Versa* c. *Aubry*, [1998] 1 R.C.S. 591.

[727] Préc., note 8.

[728] Préc., note 699.

[729] Préc., note 576.

également clairement pris position en faveur d'une reconnaissance du droit des salariés au respect de leur vie privée, même sur les lieux de travail.

Dans la première affaire, la Cour précise qu'en dehors du travail, le salarié dispose d'une « sphère d'autonomie intrinsèquement personnelle » et peut donc espérer être à l'abri des indiscrétions de l'employeur[730]. Dans ces circonstances, l'attente subjective raisonnable de vie privée demeure malgré le lien de subordination juridique. La Cour indique, cependant, que tout est question de circonstances et que l'employeur peut, dans certains cas, surveiller un salarié, même en dehors du lieu de travail.

Dans *Mascouche (Ville)* c. *Houle*[731], la Cour juge que l'interception, par un tiers, des conversations téléphoniques d'une employée à son domicile constitue une violation des droits fondamentaux de cette dernière. La Cour estime, de plus, que les éléments de preuve ainsi recueillis sont totalement inadmissibles et que leur utilisation aurait pour effet de déconsidérer l'administration de la justice en vertu de l'article 2858 C.c.Q. Il faut préciser qu'en l'espèce, l'interception avait été effectuée par un individu particulièrement fouineur, qui avait utilisé un scanner pour capter et enregistrer les conversations privées de sa voisine qu'il soupçonnait de comploter contre son propre employeur. Les enregistrements ainsi obtenus avaient été transmis à l'employeur qui avait alors congédié la salariée pour violation de son devoir de loyauté.

Dans *Srivastava* c. *Hindu Mission of Canada (Québec) Inc.*[732], la Cour conclut que l'enregistrement clandestin des conversations entre un salarié prêtre et une de ses fidèles constitue une violation du droit à la vie privée de ces deux personnes, car certaines de ces conversations étaient susceptibles d'être protégées par les dispositions relatives au secret professionnel. En effet, en tant que prêtre, le salarié pouvait être appelé à recevoir les confidences des fidèles.

---

[730] *Syndicat des travailleuses et travailleurs de Bridgestone/Firestone de Joliette (C.S.N.)* c. *Trudeau*, préc., note 8.

[731] Préc., note 699.

[732] Préc., note 576.

Cependant, tout en reconnaissant le droit à la vie privée, la jurisprudence a toujours répété, de manière constante, que ce droit n'était pas absolu et devait être évalué à l'aune des droits fondamentaux avec lesquels il pourrait entrer en conflit. Ainsi, la Cour suprême du Canada, dans l'affaire *Hunter* c. *Southam*, précise que :

> « La garantie de protection contre les fouilles, les perquisitions et les saisies abusives ne vise qu'une attente raisonnable. Cette limitation du droit garanti par l'art. 8 [*de la Charte canadienne des droits et libertés*[733]], qu'elle soit exprimée sous la forme négative, c'est-à-dire comme une protection contre les fouilles, les perquisitions et les saisies «abusives», ou sous la forme positive comme le droit de s'attendre «raisonnablement» à la protection de la vie privée, indique qu'il faut apprécier si, dans une situation donnée, le droit du public de ne pas être importuné par le gouvernement doit céder le pas au droit du gouvernement de s'immiscer dans la vie privée des particuliers afin de réaliser ses fins et, notamment, d'assurer l'application de la loi. »[734]

Les tribunaux québécois rappellent régulièrement les mêmes principes et précisent que le droit à la vie privée peut être restreint ou limité par des clauses contractuelles – à condition qu'elles soient « précises et explicites »[735] – ou encore par l'inexistence d'une attente raisonnable quant au respect de la vie privée[736].

Pour ce qui concerne le droit du travail, il ressort de la jurisprudence que l'expectative de vie privée des salariés est beaucoup plus réduite que celle à laquelle les salariés pourraient s'attendre lorsqu'ils sont chez eux. D'ailleurs, le simple bon sens nous oblige à nier à certaines activités un quelconque caractère privé : il est, par exemple, difficilement concevable qu'un employé qui navigue sur des sites pornographiques, tout en se livrant à des actes indécents devant son écran d'ordinateur, puisse invoquer le droit au respect de sa vie privée, alors que le poste de travail est situé dans un espace ouvert où il peut facilement être surpris. Comme le soutenait la plaignante dans *Ordre des infirmières et infirmiers du*

---

[733] Partie I de la *Loi constitutionnelle de 1982* [annexe B de la *Loi de 1982 sur le Canada*, 1982, c. 11 (R.-U.)].

[734] [1984] 2 R.C.S. 145, 159-160.

[735] *Syndicat des travailleuses et travailleurs de Bridgestone/Firestone de Joliette (C.S.N.)* c. *Trudeau*, préc., note 8, par. 68.

[736] *Godbout* c. *Ville de Longueuil*, préc., note 724.

Québec c. *Léveillé*, dans une telle hypothèse, ce n'est pas la vie privée de l'employé qui est en cause, mais bien sa vie professionnelle[737].

Par conséquent, l'employeur peut surveiller les activités de ses employés, à condition, comme indiqué dans la section précédente, de disposer de motifs légitimes pour le faire. En outre, il faut que la surveillance soit proportionnelle au but recherché, qu'elle soit réalisée avec des moyens raisonnables et pertinents et que cette intrusion dans l'intimité des salariés cause une atteinte minimale dans leur vie privée[738]. De plus, la surveillance d'un employeur privé ne semble pas soumise aux mêmes conditions qu'un employeur gouvernemental[739]. En effet, les employeurs du secteur privé sont tenus de respecter les dispositions de la *Charte canadienne des droits et libertés*,[740] si bien que leurs employés pourraient devoir effectuer leurs renonciations au droit à la protection de leur vie privée selon les critères constitutionnels[741]. Les employeurs privés n'étant pas soumis à cette Charte, les renonciations au droit à la vie privée de leurs employés ne seraient donc pas soumises aux mêmes standards[742].

La surveillance de l'utilisation des outils informatiques se manifeste, généralement, par l'accès au contenu de l'ordinateur du salarié. Pour évaluer concrètement les droits en présence, il sera essentiel de se poser les questions suivantes :

1. l'intrusion dans la vie privée de l'employé était-elle proportionnelle à l'objectif poursuivi par l'employeur? En d'autres termes, l'atteinte à la vie privée du salarié était-elle raisonnable et appropriée, compte tenu des circonstances[743]? On pourra, notamment, se demander si les modalités de la surveillance portent le moins

---

[737] *Ordre des infirmières et infirmiers du Québec* c. *Léveillé*, préc., note 678.

[738] *Syndicat des travailleuses et travailleurs de Bridgestone/Firestone de Joliette (C.S.N.)* c. *Trudeau*, préc., note 8; *Syndicat des employées et employés professionnels et de bureau, section locale 57* c. *Caisse populaire St-Stanislas de Montréal*, D.T.E. 99T-59 (T.A.).

[739] François BLANCHETTE, *L'expectative raisonnable de vie privée et les principaux contextes de communications dans Internet*, mémoire de maîtrise, Montréal, Faculté des études supérieures, Université de Montréal, 2001, p. 79.

[740] Préc., note 733.

[741] F. BLANCHETTE, préc., note 739, p. 79.

[742] *Id.*

[743] D. VEILLEUX, préc., note 483, 43.

possible atteinte à la dignité, à l'intégrité ou à la liberté des salariés ou encore si ces derniers ont été préalablement avertis de la surveillance. On pourra aussi s'interroger sur la destination finale des informations recueillies dans ce cadre : seront-elles utilisées uniquement pour prouver les comportements fautifs des salariés ou à d'autres fins, comme l'analyse de leurs habitudes, préférences ou méthodes de travail, afin, par exemple, de dresser leur profil intellectuel, psychologique ou professionnel; et

2. existait-il un autre moyen moins envahissant qui aurait permis à l'employeur d'atteindre son objectif ? Ainsi, s'il est nécessaire d'accéder au contenu des messages électroniques échangés par un salarié, pour vérifier l'existence d'un harcèlement sexuel, est-il pertinent de le faire pour prouver le vol de temps ? Un simple contrôle du nombre de connexions Internet ou de messages non reliés au travail ne serait-il pas suffisant dans cette deuxième hypothèse ?

3.2. La prise en compte concrète de l'expectative de vie privée lors de l'accès au contenu de l'ordinateur de l'employé

La mise en œuvre de la protection de la vie privée du salarié nécessite, notamment, une prise en compte des modalités de réalisation de l'intrusion dans la vie privée du salarié. L'évaluation du degré de protection doit, entre autres, s'attacher à l'intensité de la surveillance et au choix des moyens qui doivent être pertinents au regard du but poursuivi. À cet égard, il a été jugé que la surveillance devait demeurer raisonnable et ne pas être exercée de façon constante et continue, afin de ne pas porter atteinte à la dignité du salarié[744]. Ainsi, dans *Société des alcools du Québec* c. *Syndicat des employés de magasins et bureaux de la S.A.Q.*[745], l'arbitre précise que la protection du salarié au regard de ce point particulier est garantie non par l'article 5 de la *Charte des droits et libertés de la*

---

[744] *Association des techniciennes et techniciens en diététique du Québec* c. *Centre hospitalier Côte-des-Neiges*, D.T.E. 93T-1329 (T.A.).

[745] [1983] T.A. 335.

personne[746], mais plutôt par l'article 46 de cette Charte relatif au droit à des conditions de travail justes et raisonnables.

La question de loyauté de la surveillance peut également se poser. À cet égard, il est généralement admis que l'employeur peut recourir à une surveillance électronique temporaire et à l'insu du salarié pour des motifs de discipline industrielle. Ce principe a été énoncé dans l'arrêt *Société des alcools du Québec* c. *Syndicat des employés de magasins et bureaux de la S.A.Q.*[747]. Toutefois, il est conseillé à l'employeur d'aviser les salariés, notamment dans le cadre d'une politique d'utilisation des ressources informatiques, que leurs activités pourraient faire l'objet de contrôles.

L'accès au contenu de l'ordinateur du salarié peut être effectué sur des outils appartenant à l'employeur, directement sur le lieu de travail, en présence du salarié ou même à son insu. Mais l'employeur peut également, grâce à une ordonnance Anton Piller, accéder, en dehors de ses locaux, au contenu de disques durs ou d'autres supports informatiques qui ne lui appartiennent parfois même pas[748].

Or, ces intrusions peuvent permettre à l'employeur d'accéder à des informations considérées par l'intéressé comme purement personnelles, empiétant ainsi sur son droit à la vie privée. Les deux arguments généralement exploités par les salariés à l'appui d'une revendication de la protection de leurs droits sont : l'accès, à leur insu, au contenu de leur ordinateur et l'interception de leurs communications personnelles. Par conséquent, le contentieux relatif à la protection de la vie privée des salariés dans le cadre de l'utilisation des technologies de l'information et de la communication porte majoritairement sur la nature des informations à protéger. C'est sur ce point que vont porter les prochains développements.

---

[746] Préc., note 361.

[747] Préc., note 746; *Service d'entretien Montcalm-Complexe Desjardins* c. *Syndicat canadien des officiers de la marine marchande*, D.T.E. 93T-950 (T.A.).

[748] *Sherelco Inc.* c. *Laflamme*, préc., note 210; *Shermag Inc.* c. *Zelnicker*, préc., note 210.

Les tribunaux québécois ont, à de nombreuses reprises, eu à trancher sur la question de la délimitation du caractère privé des informations contenues dans l'ordinateur du salarié. Ainsi, dans *Syndicat des travailleuses et travailleurs de Resto-Casino de Hull (F.E.E.S.P.-C.S.N.) (section Hilton Lac Leamy)* c. *Hilton Lac Leamy*[749], le plaignant soumettait que l'intervention de l'employeur dans les échanges qu'il avait eus avec une collègue, sur un site de « clavardage » privé, constituait purement et simplement une intrusion dans leur vie privée. Au vu des circonstances, l'arbitre a estimé que la situation présentait un caractère propre et unique, puisqu'elle mêlait des faits survenus aussi bien sur les lieux de travail qu'en dehors de ceux-ci. Et, il a conclu que l'intrusion de l'employeur était justifiée dans la mesure où, malgré sa nature privée, cette querelle était néanmoins en lien avec le travail.

Trois autres décisions nous semblent particulièrement intéressantes, car les salariés y développent des arguments différents pour contester l'accès de l'employeur au contenu de leur ordinateur : *R.* c. *Tremblay*[750], *Ghattas* c. *École nationale de théâtre du Canada*[751] et *Blais* c. *Société des Loteries Vidéos du Québec Inc.*[752].

Dans *Tremblay*, le service de police d'une municipalité avait mis l'ordinateur d'un salarié sous surveillance, à la suite d'une dénonciation anonyme alléguant qu'il visionnait régulièrement de la pornographie juvénile sur son poste de travail. Le salarié faisait parallèlement l'objet d'une surveillance vidéo grâce à une caméra branchée en permanence et dirigée vers l'écran de son ordinateur. Finalement, à la suite d'une perquisition et d'une fouille de son bureau et de son ordinateur, son disque dur, ainsi que des dossiers et disquettes abritant des contenus prohibés avaient été saisis. Ces preuves, ainsi que les enregistrements vidéo, avaient été déposées dans le cadre d'une poursuite criminelle contre le salarié pour possession de pornographie infantile.

---

[749] Préc., note 589.

[750] Préc., note 589.

[751] Préc., note 589.

[752] Préc., note 239.

Le salarié avait exploité deux moyens de défense. Dans un premier temps, il avait contesté la validité de la preuve qui, selon lui, avait été recueillie en violation de son droit à la vie privée garanti par l'article 8 de la *Charte canadienne des droits et libertés*[753]. Puis il avait affirmé que la poursuite criminelle n'était pas fondée, car le téléchargement et la détention des contenus litigieux avaient été réalisés dans le cadre d'une enquête de police qu'il effectuait.

Concernant l'argument relatif à la violation de la vie privée du salarié, la Cour du Québec, dans son jugement sur la requête en exclusion de preuve et en arrêt des procédures, rejette ce moyen, car, en l'espèce, il ne pouvait y avoir d'attente raisonnable en ce sens[754]. La Cour commence par rappeler que dans le cadre du travail, l'expectative de vie privée est réduite et est fonction des circonstances. Elle souligne également qu'il est évident que lorsqu'un employé reçoit un ordinateur dans le cadre de son emploi, il doit s'en servir pour le travail. De plus, l'accusé était censé avoir pris connaissance de la directive de l'employeur relative à l'usage des ordinateurs fournis dans le cadre du travail. En outre, la preuve établissait que l'accusé permettait à d'autres employés de se servir de son ordinateur ouvert en permanence, et ce, même en son absence. Enfin, il était de notoriété que le gestionnaire du système informatique pouvait accéder aux ordinateurs de tous les salariés depuis son propre ordinateur. La Cour en conclut donc que, dans de telles circonstances, il était clair qu'il n'y avait aucune place pour une expectative raisonnable de vie privée lors de l'utilisation de l'ordinateur. Par conséquent, l'article 8 de la Charte ne pouvait trouver application.

La Cour admet donc la preuve. Elle ajoute que, même en tenant pour acquis qu'une expectative raisonnable de vie privée existait et que la perquisition avait été effectuée en violation de l'article 8 de la Charte, cette violation était plus que mineure et ne devait pas entraîner l'exclusion de la preuve. De plus, l'employeur disposait de motifs raisonnables et probables et avait agi en toute honnêteté en faisant procéder à la surveillance.

---

[753] Préc., note 733.

[754] *R.* c. *Tremblay*, préc., note 589.

Pour ce qui est des accusations portées contre le salarié, la Cour rejette les contestations de ce dernier et conclut plutôt qu'il a été prouvé, hors de tout doute, qu'il était le seul à avoir pu télécharger le matériel stocké dans son ordinateur[755]. Plusieurs témoignages allaient en effet en ce sens. De plus, la surveillance vidéo établissait que le poste de travail du salarié était occupé et utilisé à 97 % par lui-même. Enfin, il y avait une convergence entre les nombreux témoignages et preuves sur le fait que le salarié n'avait concrètement participé à aucune enquête sur la pornographie juvénile. La Cour en conclut que les activités reprochées résultaient d'actes volontaires, effectués par le salarié dans un but purement personnel et non dans le cadre de son travail, comme il le prétendait.

Dans l'affaire *Blais* c. *Société des Loteries Vidéos du Québec*[756], le salarié invoquait le *Code criminel* qui interdit les interceptions de communications privées. Dans cette affaire, le plaignant avait été congédié, notamment, en raison d'une utilisation inappropriée du courrier électronique et de l'Internet dans le but d'obtenir, puis distribuer, du matériel pornographique. L'employé soutenait que la preuve fournie par l'employeur devait être exclue, car elle avait été obtenue en contravention, notamment, avec les articles 183 et 184 du *Code criminel* qui interdisent d'intercepter une communication privée. Et, en accédant ainsi à son courrier électronique, l'employeur avait violé son droit au respect de la vie privée, garantis par l'article 5 de la *Charte des droits et libertés de la personne*[757] et par les articles 35 et 36 du *Code civil du Québec*. La Commission des relations du travail devait donc déterminer, d'une part, s'il y avait eu interception de communications privées et, d'autre part, s'il y avait eu violation de la vie privée du salarié.

À la première question, la Commission répond par la négative et refuse de qualifier l'accès au courrier électronique du salarié d'« interception », car :

> « Contrairement à ce qui est nécessairement le cas lors d'une conversation téléphonique, [l'employeur] n'a pas ici intercepté une communication en cours. Plutôt, alertée par un fichier qui se butait au

---

[755] *Id.*

[756] Préc., note 239.

[757] Préc., note 361.

> firewall en raison de sa taille – dispositif de sécurité dont l'existence est connue de tous –, elle en a tout simplement vérifié le contenu, comme cela est la pratique, afin d'apprécier si le fichier pouvait être accepté malgré son volume important. Cet incident a bien sûr permis d'identifier le destinataire du courriel et d'effectuer des vérifications plus poussées. Mais l'essentiel de la preuve provient de la récupération d'informations stockées, étant acquis que l'entreprise procède, tous les jours, à la copie et à l'archivage sur disque compact du contenu des disques durs de tous les ordinateurs. On ne peut certes pas parler, dans ces circonstances, d'une « communication » au sens strict du terme, encore moins d'une « interception »[758].

Pour ce qui concerne l'argument relatif à la violation de la vie privée, la Commission conclut que, pour plusieurs raisons, le salarié ne pouvait raisonnablement s'attendre à ce que ses courriels et le contenu de son ordinateur restent privés. En premier lieu, l'employeur lui avait fourni l'ordinateur, les logiciels et l'accès Internet à des fins professionnelles, même si une utilisation personnelle minimale et limitée de ces outils était tolérée, au même titre que l'usage du téléphone. Le salarié ne pouvait donc pas ignorer que le contenu de l'ordinateur ainsi mis à sa disposition relevait davantage de sa vie professionnelle que de sa vie privée. De plus, tous les salariés de l'entreprise savaient que tout message électronique transitait d'abord par le serveur de l'entreprise où il subissait différents contrôles, dont le filtrage du pare-feu, avant d'être acheminé dans les boîtes individuelles des salariés. D'ailleurs, les salariés étaient informés, grâce à la politique Internet de l'entreprise, de l'existence de mesures de suivi et de contrôle assurées par les gestionnaires du réseau. Le plaignant ne pouvait donc pas non plus ignorer que ces derniers avaient accès au contenu de ses courriels. Ils l'avaient d'ailleurs avisé, à plusieurs reprises, que ses courriels ou les sites Internet qu'il visitait étaient inappropriés. Enfin, la politique de l'entreprise précisait explicitement, qu'aucun utilisateur ne pouvait prétendre à l'aspect « privé » de ses échanges.

Cette affaire est intéressante dans la mesure où la Commission non seulement confirme les décisions antérieures affirmant que l'interception de communications secrètes du salarié

---

[758] *Blais* c. *Société des Loteries Vidéos du Québec*, préc., note 239, par. 92.

effectuées sur le lieu au travail, ne constitue pas toujours une violation de sa vie privée[759], mais aussi parce que cette instance rejette la terminologie habituellement utilisée pour qualifier l'accès sans autorisation à la messagerie électronique d'autrui.

Dans l'arrêt *Ghattas*[760], une salariée contestait son congédiement pour insubordination et reprochait, entre autres, à son supérieur immédiat d'avoir violé sa vie privée en interceptant un courriel personnel, après avoir accédé, à son insu, au contenu de son ordinateur. Cette intrusion avait permis à l'employeur de prendre connaissance d'un projet de réponse à une lettre de réprimande que la salariée avait transmise, pour commentaires, à ses amis. La Cour supérieure du Québec a rejeté la réclamation de la plaignante au motif que tout employeur a le droit de vérifier que ses employés exécutent leurs tâches pendant leurs heures de travail. En l'espèce, l'employée avait utilisé son temps de travail pour rédiger et transmettre, grâce à l'ordinateur fourni pour l'exécution de ses tâches, des brouillons d'une lettre qu'elle s'apprêtait à remettre à son supérieur immédiat. De tels agissements étaient inadmissibles aux yeux de la Cour. L'employeur avait donc un motif légitime pour surveiller les échanges que l'employée effectuait à partir de son ordinateur. De plus, tous les employés avaient été informés, lors d'une réunion, de l'interdiction de tout usage personnel des technologies de l'information et de la communication. La Cour a refusé de prendre en compte le fait que l'employée était en congé lors de la tenue de cette réunion : pour elle, la salariée aurait dû s'enquérir des questions et sujets abordés pendant ses vacances et ne devait s'en prendre qu'à elle-même pour avoir omis de le faire.

Finalement, les trois décisions évoquées dans les paragraphes précédents confirment que les employés ont une expectative de vie privée extrêmement réduite lorsqu'ils utilisent les outils informatiques de l'employeur, surtout si l'employeur a mis en place une politique Internet indiquant explicitement que cette utilisation serait soumise à la surveillance patronale. À cet égard, l'affaire *Ghattas* nous enseigne qu'il incombe certes à l'employeur d'informer individuellement chaque salarié de l'existence et du contenu de sa politique en

---

[759] *Roy* c. *Saulnier*, préc., note 8; *Mascouche (Ville)* c. *Houle*, préc., note 699.

[760] Préc., note 589.

la matière, mais que ceux-ci ont également la responsabilité, surtout lorsqu'ils occupent des postes de niveau élevé, de s'informer sur les dossiers et décisions importants concernant leur entreprise.

Ces trois décisions montrent la difficulté à tracer une frontière nette entre les informations relevant de la vie privée du salarié et celles de nature professionnelle. Comme le note le juge La Forest dans l'arrêt *Thomson Newspapers Ltd.* c. *Canada (Directeur des enquêtes et recherches, Commission sur les pratiques restrictives du commerce)* :

> « […] un bureau peut s'avérer plus privé que le domicile en ce qui concerne les relations familiales. Peu importe la raison, il est effectivement probable que l'on trouvera dans un bureau des lettres personnelles, des répertoires d'adresses et de numéros de téléphone privés et bien d'autres indices de la vie personnelle de son occupant. L'obligation de subir la perquisition des lieux de l'entreprise par des fonctionnaires de l'État peut donc revenir à obliger le particulier à révéler des aspects de sa vie privée au regard froid de fonctionnaires. Cela porte sérieusement atteinte au droit d'être protégé contre les fouilles, les perquisitions et les saisies abusives. »[761]

En cas d'accès au contenu de l'ordinateur d'un salarié, la détermination de la nécessité de protéger certaines informations au titre du droit à la vie privée variera en fonction des circonstances et de la nature de l'information en cause[762]. Par conséquent, on ne devrait pas forcément exclure une information uniquement parce qu'elle est identifiée comme « personnelle » par le salarié. De même, l'employeur n'a pas un droit absolu à accéder au contenu d'un ordinateur sous prétexte que c'est lui qui a fourni cet outil au salarié pour aux fins son travail.

L'arrêt *Thomson Newspapers*[763] est particulièrement significatif pour le droit du travail, puisqu'il pose le principe selon lequel les tribunaux, lorsqu'ils sont amenés à se prononcer

---

[761] *Thomson Newspapers Ltd.* c. *Canada (Directeur des enquêtes et recherches, Commission sur les pratiques restrictives du commerce)*, [1990] 1 R.C.S. 425, 521-522 [ci-après : Thomson Newspapers].

[762] *Srivastava* c. *Hindu Mission of Canada (Québec) Inc.*, préc., note 576; *Ste-Marie* c. *Placements J.P.M. Marquis Inc.*, EYB 2005-88296, (C.A.); Voir également F. BLANCHETTE, préc., note 739, p. 79, qui souligne que la détermination du caractère privé de telles informations devra se faire en fonction d'une « multitude de facteurs spécifiques aux environnements de travail ».

[763] Préc., note 761.

sur une question relative à la fouille et à la vie privée en milieu de travail, doivent opérer une distinction entre les aspects personnels et les autres aspects contenus dans les informations concernant les salariés. Dans cette décision, la Cour devait se prononcer sur le pouvoir d'un tribunal administratif de contraindre une personne à témoigner et à produire des documents provenant de son entreprise. Le juge La Forest, dans son analyse estime que, traditionnellement, la revendication du droit à la vie privée repose sur la conviction qu'il appartient à chacun de déterminer la façon dont il veut mener sa vie privée. Or, les dossiers et documents appartenant à une entreprise

> « […] 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. »[764]

Par conséquent, la garantie constitutionnelle relative à la vie privée ne s'applique pas à ces documents. Il semblerait donc que l'information à protéger dans le cadre de la vie privée soit celle qui se rattache aux caractéristiques personnelles de l'individu et qui est constituée de renseignements relatifs au mode de vie d'une personne, à ses relations intimes ou à ses convictions politiques ou religieuses.

Conclusion de la deuxième partie

L'employeur semble jouir d'un droit de surveillance parfois très étendu lorsqu'il s'agit de l'usage des outils électroniques lui appartenant, tandis que le droit à la vie privée reste, en fait, l'exception. Cependant, les salariés peuvent bénéficier, même dans le cadre du travail, d'une sphère de protection certes très réduite, mais bien réelle. Cette protection leur est accordée au titre du droit à des conditions justes et raisonnables qui permet, par exemple, de réviser une politique Internet si celle-ci est déraisonnable ou de censurer une surveillance constante et continue. De plus, les principes dégagés par la jurisprudence

---

[764] *Id.*, 518.

tendent à garantir la protection des informations privées des salariés, même sur le lieu du travail, puisqu'ils affirment que ce qui est protégé c'est la nature de l'information susceptible d'être divulguée et non le lieu de sa divulgation ou de son stockage.

Finalement, la jurisprudence québécoise en la matière se situe dans une position intermédiaire entre le modèle américain, qui ne laisse place à aucune expectative de vie privée, et la situation française qui privilégie la protection des droits fondamentaux[765], au risque parfois de placer l'employeur dans l'impasse. En effet, en France, la jurisprudence issue du fameux arrêt Nikon[766] affirme que la règle du secret des correspondances s'applique aux messages électroniques dès lors qu'ils sont qualifiés de « personnels » par le salarié. Par conséquent, il est interdit à l'employeur d'en prendre connaissance. Dans cette affaire, un salarié avait été licencié pour faute grave, au motif qu'il entretenait une activité parallèle pendant ses heures de travail en vendant illégalement du matériel de la société. L'employeur avait obtenu la preuve de ces faits en accédant à des messages expédiés, reçus et enregistrés par le salarié sur le disque dur de son ordinateur, dans un fichier intitulé « Personnel ». La Cour de cassation indique, dans son attendu de principe que :

> « […] le salarié a droit, même au temps et au lieu de travail, au respect de l'intimité de sa vie privée; que celle-ci implique en particulier le secret des correspondances; que l'employeur ne peut dès lors sans violation de cette liberté fondamentale prendre connaissance des messages personnels émis par le salarié et reçus par lui grâce à un outil informatique mis à sa disposition pour son travail et ceci même au cas où l'employeur aurait interdit une utilisation non professionnelle de l'ordinateur. »[767]

Ces principes, qui pouvaient laisser croire que les salariés bénéficient d'un espace privé, juridiquement inaccessible à l'employeur, sur le disque de l'ordinateur fourni par ce dernier, ont, toutefois, été tempérés par un arrêt du 17 mai 2005, dans lequel la Cour de cassation conclut que :

---

[765] J. LENFANT, préc., note 478, p. 31.

[766] Soc. 2 oct. 2001, *Bull. civ.* V, n° 291.

[767] *Id.*

> « sauf risque ou événement particulier, l'employeur ne peut ouvrir les fichiers identifiés par les salariés comme personnels contenus sur le disque dur de l'ordinateur mis à sa disposition qu'en présence de ce dernier ou celui-ci dûment appelé. »[768]

En l'espèce, un salarié avait été licencié pour faute grave à la suite de la découverte de photographies érotiques dans un tiroir de son bureau. L'employeur avait alors accédé au disque dur de son ordinateur, pour en contrôler le contenu, et avait découvert un ensemble de dossiers, totalement étrangers à ses fonctions, et qui étaient classés dans un fichier intitulé « perso ». En l'espèce, pour la Cour de cassation, la découverte de ces photos ne semble pas constituer ce « risque ou événement particulier » justifiant l'accès, hors la présence du salarié, à ses fichiers personnels. Toutefois, l'employeur semble disposer d'une marge de manœuvre plus large qu'antérieurement, puisque la haute instance française indique clairement qu'il peut accéder au contenu de l'ordinateur du salarié, à condition, cependant, que cette opération ne se fasse pas à l'insu de l'intéressé.

---

[768] Soc. 17 mai 2005, *Bull. civ.* V, n° 165.

Conclusion

Le fait que l'employeur dispose d'une marge de manœuvre assez étendue quant à l'usage des NTIC qu'il entend tolérer au sein de son entreprise est, dans une très large mesure, généralement souhaitable, car les activités personnelles du salarié ne doivent avoir aucun impact sur la qualité ou le temps effectif de son travail. Elles ne doivent pas non plus représenter de coûts ni de risques pour l'entreprise.

Cependant, l'employeur doit également composer avec des technologies en constante évolution et des salariés toujours plus exigeants qu'il faut conserver. Ces derniers acceptent de plus en plus souvent de travailler en dehors de leur lieu de travail ou de leurs horaires normaux, pour accommoder l'employeur. De plus, un nombre croissant d'employés sont dotés d'outils permettant de les joindre à tout moment et en tout lieu. En contrepartie de ces sacrifices, ils s'attendent, généralement, à ce que leur patron fasse preuve de souplesse quant à l'usage personnel de ces outils. En effet, à partir du moment où l'on accepte l'idée que le travail s'invite dans la vie des salariés, on devrait aussi admettre qu'ils puissent, parfois, avoir envie de se détendre au travail. Et cela d'autant plus que certaines études démontrent qu'un usage raisonnable de l'Internet à des fins personnelles peut avoir des effets positifs sur la motivation des salariés et que ces derniers montrent généralement un regain d'énergie au travail après un échange en ligne avec leurs amis et proches ou tout simplement après avoir effectué leurs courses ou payé leurs factures sur Internet. Ainsi, une étude effectuée par des neuropsychologues du laboratoire *Mind Lab International*, à la demande de *Hewlett-Packard*, révèle que le fait de naviguer sans contraintes sur ses sites préférés ne serait-ce que 10 minutes par jour procure des bénéfices émotionnels et intellectuels considérables[769]. Cette « pause Internet » contribue à diminuer le stress, améliorer la capacité de concentration et augmenter les performances au travail. Les

---

[769] HEWLETT-PACKARD FRANCE, « Une étude démontre que les femmes qui surfent régulièrement sur leurs sites Web favoris sont moins stressées, stimulent leur activité cérébrale et augmentent leur productivité », 2008, en ligne : <http://h41131.www4.hp.com/fr/fr/press/une--tude-d-montre-que-les-femmes-qui-surfent-r-guli-rement-sur-leurs-sites-web-favoris-sont-moins-stress-es--stimulent-leur-activit--c-r-brale-et-augmentent-leur-productivit--.html?jumpid=reg_R1002_FRFR> (site consulté le 18 août 2010).

responsables des services de ressources humaines pourraient donc avoir un intérêt à aménager cette possibilité d'évasion en favorisant la navigation – raisonnable – à des fins personnelles, et tout particulièrement le réseautage social en ligne, en raison de sa grande capacité à développer et maintenir les liens sociaux.

L'étude du *Mind Lab*, en raison de son caractère scientifique (utilisation de divers capteurs pour mesurer les variations de l'activité cérébrale et enregistrer le rythme cardiaque), constitue un argument de taille pour ceux qui affirment qu'il est socialement souhaitable que l'employeur prenne en compte l'aspect ludique et récréatif lorsqu'il établit les règles relatives à l'usage des NTIC. La tolérance de l'utilisation de ces technologies à des fins personnelles permettrait ainsi à l'employeur de conserver un degré suffisant de motivation chez ses salariés. Le tout est que l'usage personnel demeure raisonnable et n'affecte pas la productivité du travailleur. De plus, ces activités doivent rester conformes aux lois et aux valeurs de l'entreprise. En effet, en cas d'usage abusif, les tribunaux jugeront presque toujours les contrôles de l'employeur justifiés, surtout si ce dernier a mis en place une politique d'utilisation des outils électroniques claire.

Les salariés sont donc invités, dans leur propre intérêt, à faire preuve d'un minimum de bon sens, puisqu'il est relativement connu que chaque mouvement informatique laisse des traces et que, les entreprises possèdent généralement les moyens techniques pour savoir qui fait quoi. Ils ne peuvent donc pas, dans ces conditions, réellement s'attendre à ce que leurs activités en ligne demeurent secrètes. Ils peuvent juste espérer que l'employeur s'abstiendra de les surveiller. Toutefois, le recours accru aux technologies de l'information et de la communication mobiles, tels le *BlackBerry* ou l'ordinateur portable, constitue une nouvelle source de préoccupation pour les employeurs. Il faut dire que le contexte actuel d'explosion du réseautage social s'y prête grandement : il faut absolument être vu et échanger avec le plus de monde, le tout si possible en temps réel! Du coup, les entreprises peuvent craindre, entre autres, que l'utilisation des nouveaux téléphones « intelligents » ne fasse grimper le coût de leurs communications ou que les salariés s'en servent pour communiquer en tout

temps et lieu avec leurs nombreux « amis » ou pour échanger des contenus inappropriés ou communiquer, volontairement ou non, des informations stratégiques de l'entreprise.

Ces nouveaux outils peuvent également soulever des questionnements quant à l'expectative de vie privée des salariés lorsqu'ils les utilisent : les risques de collusion entre activités professionnelles et privées sont presqu'inévitables avec ces technologies, ce qui vient compliquer encore davantage la délimitation des informations à protéger au titre de la vie privée.

En somme, on se retrouverait devant les mêmes problématiques rencontrées avec l'usage personnel du téléphone, puis de l'Internet. Si bien que les principes dégagés par la jurisprudence dans le cadre de la surveillance de ces moyens de communications devraient pouvoir trouver application dans ce nouveau contexte.

Bibliographie

Table de législation et réglementation

Textes fédéraux

Charte canadienne des droits et libertés, partie I de la Loi *constitutionnelle de 1982* [annexe B de la Loi de 1982 sur le Canada, 1982, c. 11 (R.-U.)]

Code criminel, L.R.C. 1985, c. C-46

Loi sur la Protection des renseignements personnels et les documents électroniques, L.C. 2000, c. 5

Textes québécois

Charte des droits et libertés de la personne, L.R.Q., c. C-12

Code civil du Bas-Canada

Code civil du Québec, L.Q. 1991, c. 64.

Loi concernant le cadre juridique des technologies de l'information, L.R.Q. 2001, c. C-1.1

Loi modifiant la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels et d'autres dispositions législatives, L.Q. 2006, c. 22

Loi sur la Protection des renseignements personnels dans le secteur privé, L.R.Q. 1993, c. P-39.1

Loi sur les normes de travail, L.R.Q. 1979, c. N-1.1

Loi sur les valeurs mobilières, L.R.Q. 1982, c. V-1.1

Politique de sécurité informatique et d'utilisation des ressources informatiques de l'Université de Montréal, Recueil officiel (Règlements, directives, politiques et procédures) de l'Université de Montréal, n° 40.28

Textes américains

California Database Breach Act, CAL. CIV. CODE § 1798.82 (West 2003)

Civil Rights Act, Pub. L. No. 88-352, 78 Stat. 241 (1964)

Communication Decency Act, 47 U.S.C. (1996)

Digital Millennium Copyright Act, 17 U.S.C. (1998)

Textes français

Code civil

Code pénal

Loi n° 82-689 relative aux libertés des travailleurs dans l'entreprise (1ère Loi Auroux), J.O. 6 août 1982, p. 2518

Loi n° 92-597 relative au code de la propriété intellectuelle, J.O. 3 juil. 1992, p. 8801

Loi n° 2004-575 pour la confiance dans l'économie numérique, J.O. 22 juin 2004, p. 11168

Loi n° 2006-961 relative au droit d'auteur et aux droits voisins dans la société de l'information, J.O. 3 août 2006, p. 11529

Table des jugements

Jurisprudence québécoise

124670 Canada Ltée (Clinique de médecine industrielle et préventive du Québec) c. *Remmouche*, EYB 2004-69859 (C.S.)

Addy c. *Commission scolaire Eastern Township*, 2010 QCCS 1708 (CanLII)

Alliance de la fonction publique du Canada et *Musée des beaux-arts du Canada*, D.T.E. 2003T-89 (T.A.)

Arpin c. *Grenier*, REJB 2004-65808 (C.Q.)

Association des professionnels de la Régie régionale de la santé et des services sociaux 002 (C.S.N.) c. *Régie régionale de la santé et des services sociaux du Saguenay-Lac-St-Jean*, [2002] R.J.D.T. 990 (T.A.)

Association des techniciennes et techniciens en diététique du Québec c. *Centre hospitalier Côte-des-Neiges*, D.T.E. 93T-1329 (T.A.)

Belisle c. *Rawdon (Municipalité)*, 2005 QCCRT 453 (IIJCan)

Bell Canada c. *Association Canadienne des Employés de Téléphone*, D.T.E. 2000-254 (T.A.)

Blais c. *Société des Loteries Vidéos du Québec Inc.*, D.T.E. 2003T-178 (C.R.T.)

Bolduc c. *Collège de Montréal*, 2010 QCCRT 130 (CanLII)

Bourassa et *Ville de La Tuque*, 2009 QCCRT 322 (CanLII)

Carrier c. *Centre local de développement (CLD) des Etchemins*, 2005 QCCRT 183 (CanLII)

Centre de réadaptation Lethbridge et *Syndicat des physiothérapeutes et des thérapeutes en réadaptation physique du Québec*, D.T.E. 2004T-755 (T.A.)

Chambre de l'assurance de dommages c. *Kotliaroff*, 2008 CanLII 19078 (QC C.D.C.H.A.D.)

Cogeco Câble Canada Inc. et *Syndicat canadien de la fonction publique, section locale 3624*, D.T.E. 2001T- 1039 (T.A.)

Collège Ahuntsic et *Syndicat du personnel de soutien du Collège Ahuntsic*, D.T.E. 2007T-889 (T.A.)

Commission des normes du travail c. *Bourse de Montréal Inc.*, REJB 2002-31243 (C.Q.)

Comtois c. Montreal (City of), [1954] C.S. 416

D'Astous c. *Sesno*, REJB 2000-22668 (C.Q.)

Dufresne c. *Pratt & Whitney Canada Inc*., D.T.E. 94T-405 (C.T.)

Fiset c. *Service d'administration P.C.R. Ltée*, D.T.E. 2003T-41 (C.R.T.), conf. par *Services d'administration P.C.R. Ltée* c. *Daigle*, D.T.E. 2003T-177 (C.S.)

Garaga Inc. c. *Syndicat des salariés de garage (C.S.D.)*, D.T.E. 2002T-1100 (T.A.)

Ghattas c. *École nationale de théâtre du Canada*, EYB 2006-102226 (C.S.)

Gilles et *Ciba Spécialités chimiques Canada Inc.*, 2008 QCCRT 134 (CanLII)

Glopak Inc. c. *Métallurgistes unis d'Amérique, section locale 7625*, D.T.E. 2000T-998 (T.A.)

Lemay c. *Dubois*, 2005 CanLII 15315 (QC C.Q.)

Manufacture de Lambton Ltée c. *Syndicat des employés de Manufacture Lambton (CSD)*, D.T.E. 2003T-997 (T.A.)

Martel c. *Fédération des caisses Desjardins du Québec*, 2006 QCCRT 300 (CanLII)

Mascouche (Ville) c. *Houle*, [1999] R.J.Q. 1894 (C.A.)

Montour Limitée c. *Syndicat des employé-e-s de la Cie Montour (CSN)*, 2006 IIJCan 43801 (QC A.G.)

Ordre des infirmières et infirmiers du Québec c. *Léveillé*, 2008 CanLII 47548 (QC C.D.O.I.I.)

Perreault c. *Syndicat des employés de soutien de l'Université de Sherbrooke*, 2004 CanLII 14513 (QC T.T.)

Persechino c. *Flint Ink North America Corporation*, 2007 QCCRT 354 (CanLII)

Potvin c. *Ville de Malartic*, REJB 2003-46527 (C.S.)

Poulies Maska Inc. c. *Syndicat des employés de Poulies Maska Inc.*, D.T.E. 2001T-620 (T.A.)

Québec (Commission des droits de la personne et des droits de la jeunesse) c. *Québec (Procureur général)*, 1998 CanLII 30 (QC T.D.P.)

R. c. *Chassé*, REJB 2002-33523 (C.Q.)

R. c. *Crevier*, EYB 2006-113697 (C.Q.)

R. c. *Martineau*, REJB 2003-48758 (C.Q.)

R. c. *Tremblay*, REJB 2001-23521 (C.Q.); REJB 2001-25375 (C.Q.)

Refplus Inc. c. *Kehar*, EYB 2006-104760 (C.S.)

Roy c. *Produits Vitafoam Canada limitée (Les fabrications Ultra inc.)*, 2006 QCCRT 371 (CanLII)

Roy c. Saulnier, [1992] R.J.Q. 2419 (C.A.)

Section locale 143 du Syndicat canadien des communications, de l'énergie et du papier c. *Goodyear Canada inc.*, D.T.E. 2008T-27 (C.A.)

Séguin c. *Général Motors Acceptance Corporation du Canada ltée*, 2007 QCCQ 14509 (CanLII)

Service d'entretien Montcalm-Complexe Desjardins c. *Syndicat canadien des officiers de la marine marchande*, D.T.E. 93T-950 (T.A.)

Sherelco Inc. c. *Laflamme*, EYB 1992-75301 (C.S.)

Shermag Inc. c. *Zelnicker*, REJB 2004-69078 (C.S.)

Sirois c. *Sodema*, 2005 QCCRT 91 (CanLII)

Société des alcools du Québec c. *Syndicat des employés de magasins et bureaux de la S.A.Q.*, [1983] T.A. 335

Société des alcools du Québec c. *Syndicat des travailleuses et travailleurs de la Société des alcools du Québec (SCFP), section locale 3535T*, D.T.E. 2005T-229 (T.A.)

Srivastava c. *Hindu Mission of Canada (Québec) Inc.*, REJB 2001-23958 (C.A.)

Stacey c. *Sauvé Plymouth Chrysler (1991) Inc.*, J.E. 2002-1147 (C.Q.)

Ste-Marie c. *Placements J.P.M. Marquis Inc.*, EYB 2005-88296, (C.A.)

Syndicat canadien des communications, de l'énergie et du papier, Section locale 145 c. *Québec-livres (Division de : Communications Québécor Inc.)*, 2006 CanLII 27316 (QC A.G.)

Syndicat canadien des communications, de l'énergie et du papier, section locale 522 c. *CAE Électronique Ltée*, REJB 2000-16857 (T.A.)

Syndicat de la Fonction Publique du Québec (SFPQ) c. *Québec (Ministère du Revenu)*, 2005 IIJCan 43078 (QC A.G.)

Syndicat des cols bleus regroupés de Montréal (SCFP), section locale 301 (S.C.F.P.) et *La Ronde (Six Flags)*, D.T.E. 2004T-1124 (T.A.)

Syndicat des employées et employés professionnels et de bureau, section locale 57 c. *Caisse populaire St-Stanislas de Montréal*, D.T.E. 99T-59 (T.A.)

Syndicat des employés municipaux de Beloeil (SCFP) et *Beloeil (Ville de)*, D.T.E. 2007T-874 (T.A.)

Syndicat des fonctionnaires municipaux de Montréal (S.C.F.P.) c. *Ville de Montréal,* D.T.E. 99T-478 (T.A.)

Syndicat des spécialistes et professionnels d'Hydro-Québec c. *Hydro-Québec*, 2003 CanLII 20475 (QC A.G.)

Syndicat des spécialistes et professionnels d'Hydro-Québec, (SCFP-FTQ, section locale 4250) c. *Hydro-Québec*, 2007 CanLII 20291 (QC A.G.)

Syndicat des travailleurs de Mométal (C.S.N.) c. *Mométal Inc.*, [2001] R.J.D.T. 1967 (T.A.)

Syndicat des travailleuses et travailleurs de Bridgestone/Firestone de Joliette (C.S.N.) c. *Trudeau*, REJB 1999-14156 (C.A.)

Syndicat des travailleuses et des travailleurs de la Fabrique Notre-Dame (CSN) c. *Fabrique de la paroisse Notre-Dame*, D.T.E. 2006T-56 (T.A.)

Syndicat des travailleuses et travailleurs de Resto-Casino de Hull (F.E.E.S.P.-C.S.N.) (section Hilton Lac Leamy) et *Hilton Lac Leamy*, D.T.E. 2004T-811 (T.A.)

Syndicat du personnel de soutien de la Seigneurie des Mille-Îles (CSN) et *Commission scolaire de la Seigneurie des Mille-Îles*, D.T.E. 2008T-149 (T.A.)

Syndicat national de l'automobile, de l'aérospatiale, du transport et des autres travailleuses et travailleurs du Canada c. *BMW Canbec*, D.T.E. 2007T-697 (T.A.)

Technologie Labtronix Inc. c. *Technologie Micro contrôle Inc.*, J.E. 97-228 (C.S.)

Télébec ltée c. *Association canadienne des employés de téléphone*, [2000] R.J.D.T. 1869 (T.A.).

Travailleurs et travailleuses unis de l'alimentation et du commerce, local 502 c. *Canon Canada Inc.*, 2008 CanLII 56025 (QC A.G.)

Union des consommateurs c. *Procureur général du Canada*, 2006 QCCS 448 (CanLII)

Jurisprudence canadienne

Briar c. *Canada (Conseil du Trésor)*, 2003 CRTFP 3 (CanLII)

Commissaire à la protection de la vie privée c. *Conseil canadien des relations de travail*, 2000 CanLII 15487 (C.A.F.)

Dosanjh c. *Conseil du Trésor*, 2003 CRTFP 16 (CanLII)

Éditions Vice-Versa c. *Aubry*, [1998] 1 R.C.S. 591

Frezza et *Réseau CP Rail*, [1997] D.A.T.C. no 389, (C.L.A.) (QL/LN)

Godbout c. *Ville de Longueuil*, [1997] 3 R.C.S. 844

Hunter c. *Southam*, [1984] 2 R.C.S. 145

Janzen c. *Platy enterprises Ltd*., [1989] 1 R.C.S. 1252

R. c. *Canadian Dredge and Dock Co.*, [1985] 1 R.C.S. 662

R. c. *Tremblay*, [1964] R.C.S. 601

R. c. *Wong*, [1990] 3 R.C.S. 36

Robichaud c. *Canada (Conseil du Trésor)*, [1987] 2 R.C.S. 84

Thomson Newspapers Ltd. c. *Canada (Directeur des enquêtes et recherches, Commission sur les pratiques restrictives du commerce)*, [1990] 1 R.C.S. 425

Union des consommateurs c. *Procureur général du Canada*, C.F. Ottawa, n° T-1869-07, 23 juin 2008, j. Martineau, en ligne : <http://recours-collectifs.ca/Wdocs/562008517102ULL.pdf> (site consulté le 25 juillet 2010)

Jurisprudence des provinces canadiennes de common law

Alberta v. *Alberta Union of Provincial Employees* (R. Grievance), [2008] A.G.A.A. No. 20 (G.A.) (QL/LN), [2008] 174 L.A.C. (4th) 371 (Alta. G.A.), inf. par *Alberta Union of Provincial Employees v. Alberta*, 2009 ABQB 208 (CanLII)

Backman c. *Maritime Paper Products Limited, corps constitué*, 2009 NBCA 62 (CanLII)

Consumers Gas v. *Communications, Energy and Paperworkers Union* (Primiani Grievance), [1999] O.L.A.A. No. 649 (L.A.) (QL/LN)

Davison v. *Nova Scotia Safety Association*, 2005 NSHRC 4 (CanLII)

Dhont c. *Minister of Education et al*, 2008 NWTSC 40

Di Vito v. *MacDonald Dettwiler and Associates*, 1996 CanLII 3165 (BC S.C.)

EV Logistics v. *Retail Wholesale Union, Local 580* (Discharge Grievance), [2008] B.C.C.A.A.A. No. 22 (Coll. Agr. Arb.) (QL/LN)

Inform Cycle Ltd. v. *Rebound Inc.*, 2007 ABQB 319 (CanLII)

International Association of Bridge, Local Union No. 97, and Structural and Ornamental Ironworkers (the "Employer") and *Office and Technical Employees' Union, Local 15 (the "Union")*, [1997] B.C.C.A.A.A. No. 630 (Coll. Agr. Arb.) (QL/LN)

Lumber & Sawmill Workers' Union, Local 2537 and K.V.P. Co. *Ltd.*, [1965] O.L.A.A. No. 2 (L.A.) (QL/LN), [1965] 16 L.A.C. 730 (Ont. L.A.)

Poliquin v. *Devon Canada Corporation*, 2009 ABCA 216 (CanLII)

Jurisprudence américaine

Blakey v. *Continental Airlines Inc.*, 751 A.2d 538 (N.J. 2000)

Ontario v. *Quon*, 177 L. Ed. 2d 216 (2010)

People v. *Eubanks*, 927 P.2d 310 (Cal. 1996)

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

Strauss v. *Microsoft Corp.*, 856 F. Supp. 821 (S.D.N.Y. 1994)

Jurisprudence française

Soc. 31 mai 1956, D. 1958.21, note Levasseur

Trib. gr. inst. Mans, 16 févr. 1998, J.C.P. 1999.II.10011

Cons. d'Ét. 11 juin 1999, *Chicard*, D. 2000.somm.com.88, obs. Girodet

Trib. gr. inst. Lyon, 20 févr. 2001, *Gaz. Pal***.**, 2001.2.somm.1686, note Alain Blanchot

Soc. 3 av. 2001, *Dr. ouvrier*, 2002.204

Soc. 2 oct. 2001, *Bull. civ.* V, n° 291

Paris, 17 déc. 2001, J.C.P. 2002.éd. Entr.1336, note J. Deveze et M. Vivant

Soc. 1er oct. 2002, *Gaz. Pal.* 2003.33, note Tessalonikos

Paris, 30 oct. 2002, *Gaz.Pal*.2003.205

Trib. gr. inst. Marseille, 11 juin 2003, en ligne : <http://www.legalis.net/jurisprudence-decision.php3?page=breves-article&id_article=234> (site consulté le 30 juillet 2010)

Civ. 2e, 19 juin 2003, *Bull civ.* II, n° 202

Trib. gr. inst. Mans, 7 nov. 2003 : Juritel n° JTL OGH711TGI–Internet, en ligne : <http://www.juritel.com/Ldj_html-941.html> (site consulté le 30 juillet 2010)

Soc. 2 juin 2004, *Bull. civ.* V, n° 152

Aix-en-Provence, 17 janv. 2005, en ligne : <http://www.foruminternet.org/telechargement/documents/ca-aix20050117.pdf> (site consulté le 30 juillet 2010)

Paris, 5 févr. 2005, en ligne : <http://www.foruminternet.org/telechargement/documents/ca-par20050204.pdf> (site consulté le 30 juillet 2010)

Trib. gr. inst. Paris, 19 av. 2005, en ligne : <http://www.legalis.net/jurisprudence-decision.php3?id_article=1433> (site consulté le 30 juillet 2010)

Soc. 17 mai 2005, *Bull. civ.* V, n° 165

Aix-en-Provence, 13 mars 2006, en ligne : <http://www.legalis.net/jurisprudence-decision.php3?page=jurisprudence-decision&id_article=1611> (site consulté le 30 juillet 2010)

Trib. gr. inst. Carcassonne, 16 juin 2006, en ligne : <http://www.legalis.net/breves-article.php3?id_article=1645> (site consulté le 30 juillet 2010)

Paris, 4 mai 2007, en ligne : <http://www.legalis.net/spip.php?page=jurisprudence-decision&id_article=2096> (site consulté le 30 juillet 2010)

Civ. 1re, 14 janv. 2010, Bull. civ. I, n° 8

Paris, 14 av. 2010 : Juritel n° JTL KTK421CA–Internet, en ligne : <http://www.juritel.com/Ldj_html-1478.html> (site consulté le 30 juillet 2010)

Doctrine

Monographies et ouvrages collectifs

Canadiens

BAUDOUIN, J.-L., *La responsabilité civile délictuelle*, 3e éd., Cowansville, Éditions Yvon Blais, 1990

BAUDOUIN, J.-L. et P. DESLAURIERS, « Introduction générale », dans *La responsabilité civile, Volume I – Principes généraux*, 7e édition, 2007, *Droit civil en ligne* (DCL), EYB2007RES1

BAUDOUIN, J.-L. et P. DESLAURIERS, « La responsabilité des commettants », dans *La responsabilité civile, Volume I – Principes généraux*, 7e édition, 2007, *Droit civil en ligne* (DCL), EYB2007RES10

BAUDOUIN, J.-L. et P. DESLAURIERS, « La responsabilité du fait des autres - Schéma général », dans *La responsabilité civile, Volume I – Principes généraux*, 7e édition, 2007, *Droit civil en ligne* (DCL), EYB2007RES7

D'AOUST, C., L. LECLERC et G. TRUDEAU, *Les mesures disciplinaires : étude jurisprudentielle et doctrinale*, Montréal, École des relations industrielles, Université de Montréal, 1982

GAGNON, R. P., *Le droit du travail du Québec*, 5e éd., Cowansville, Québec, Éditions Yvon Blais, 2003

GAUTRAIS, V. (dir.), *Droit du commerce électronique*, Montréal, Éditions Thémis, 2002

GAUTRAIS, V. et P. TRUDEL, *Circulation des renseignements personnels et Web 2.0*, Montréal, Éditions Thémis, 2010

LAUZON, I. et L. BERNIER, *Manuel d'employés et politiques d'entreprise : tout ce que l'employeur doit savoir*, Nouv. éd., Cowansville, Éditions Yvon Blais, 2004

LLUELLES, D. avec la collab. de J. RINGUETTE, *Guide des références pour la rédaction juridique*, 7e éd., Montréal, Éditions Thémis, 2008

ROMPRÉ S., *La surveillance de l'utilisation d'Internet au travail*, Montréal, Éditions Yvon Blais, 2009

ROYER, J.-C., « La preuve obtenue par des moyens illégaux », dans *La Preuve civile*, 3e éd., 2003, *Droit civil en ligne* (DCL), EYB2003PRC35

TRUDEL, P., F. ABRAN, K. BENYEKHLEF et S. HEIN avec la collab. de M. BEAUPRÉ, L. BOUCHER, M. MICHAUD, F. OUELLETTE, S. PARISIEN, F. THÉMENS et V. WATTIEZ-LAROSE, *Droit du cyberespace*, Montréal, Éditions Thémis, 1997

TURNBULL, I. J., S. SIMPSON CAMPBELL, D. F. HARRIS et B. KIMBALL, *Privacy in the workplace: the employment perspective*, Canadian Privacy Institute, CCH Canadian, Toronto, 2004

Français

DE BENALCÁZAR, I., *Droit du travail et nouvelles technologies : collecte des données, Internet, cybersurveillance, télétravail*, coll. B business, Paris, Montchrestien : Gualino, 2003

DUQUESNE, F., *Droit du travail*, coll. Universités, Série manuel, Paris, Gualino, 2004

LEFEBVRE, S., *Nouvelles technologies et protection de la vie privée en milieu de travail en France et au Québec*, coll. Droit social, Aix-en-Provence, Presses universitaires d'Aix-Marseille, 1998

MAZEAUD, A., *Droit du travail*, 5e éd., Paris, Montchrestien, 2006

Articles de revue et études d'ouvrages collectifs

Canadiens

ALLARD, F., « Les droits de la personnalité », dans Collection de droit 2009-2010, École du Barreau du Québec, vol. 3, *Personnes, famille et successions*, Cowansville, Yvon Blais, 2009, p. 59

BARIBEAU, L., « Internet et le milieu du travail », (2001) 33-19 *J. du Bar.*

BARIL, A., « Chronique – L'obligation de loyauté, de diligence et de discrétion d'un salarié après la cessation de son emploi », dans *Repères*, Septembre 1999, *Droit civil en ligne* (DCL), EYB1999REP109

BÉLIVEAU, N.-A., K. BOUTIN et N. ST-PIERRE, « Les "motifs sérieux" et la "cause juste et suffisante" de congédiement », dans *Un abécédaire des cessations d'emploi et des indemnités de départ (2005)*, Service de la formation permanente du Barreau du Québec, 2005, *Droit civil en ligne* (DCL), EYB2005DEV866

BICH, M.-F., « La viduité post-emploi : loyauté, discrétion et clauses restrictives », dans *Développements récents en droit de la propriété intellectuelle (2003*), Service de la formation permanente du Barreau du Québec, 2003, *Droit civil en ligne* (DCL), EYB2003DEV358

BISEUL, X., « Cybersurveillance : les nouvelles technologies ravivent les vieilles peurs », 01net.com, 19 juillet 2004, en ligne : <http://www.01net.com/article/248848.html> (site consulté le 18 août 2010)

BRUNELLE, C., « Les limites aux droits et libertés », dans Collection de droit 2009-2010, École du Barreau du Québec, vol.7, *Droit public et administratif*, Cowansville, Éditions Yvon Blais, 2009, p. 77.

CÔTÉ, F., « Surveillance des technologies de l'information », Ogilvyrenault.com, Décembre 1999, en ligne : <http://www.ogilvyrenault.com/fr/centreDeResources_1665.htm> (site consulté le 18 août 2010)

DEEHY, C., « Cyberespace en milieu de travail : politiques d'entreprise », Lapointerosenstein.com, Été 1999, en ligne :

<http://www.lapointerosenstein.com/fichier/listelibrary/37/Cde-cyberespace.pdf> (site consulté le 19 août 2010)

DELWAIDE, K., « L'Internet en milieu de travail et les politiques et directives relatives à l'utilisation des nouvelles technologies », Fasken.com, 2001, en ligne : <http://www.fasken.com/files/Publication/2bdfed9a-a187-4755-abc3-04fd5e0c6bb1/Presentation/PublicationAttachment/6bed511b-6037-4345-a9f6-09760d937b45/L_INTERNET_EN_MILIEU_DE_TRAVAIL.pdf> (site consulté le 19 août 2010)

DELWAIDE, K. et A. AYLWIN, « Leçons tirées de dix ans d'expérience : la Loi sur la protection des renseignements personnels dans le secteur privé du Québec », Commissariat à la protection de la vie privée du Canada, en ligne : <http://www.priv.gc.ca/information/pub/dec_050816_f.pdf> (site consulté le 19 août 2010)

DESCHAMPS, P., « L'exonération et le partage de responsabilité », dans *Responsabilité*, Collection de droit 2007-2008, École du Barreau du Québec, vol. 4, 2007, *Droit civil en ligne* (DCL), EYB2007CDD90

DORÉ, L., « Surveillance vidéo vs respect du droit à la vie privée », *dans Développements récents en droit de l'accès à l'information (2005)*, Service de la formation permanente du Barreau du Québec, 2005, *Droit civil en ligne* (DCL), EYB2005DEV1087

DUBOIS, M., « Nouvelles technologies de l'information et des communications et sécurité informationnelle », dans *Développements récents en droit de l'accès à l'information (2002)*, Service de la formation permanente du Barreau du Québec, 2002, *Droit civil en ligne* (DCL), EYB2002DEV565

ÉVANGÉLISTE, M., « Les affaires Bridgestone/Firestone et Ville de Mascouche : la Cour d'appel rompt avec la jurisprudence du travail et fixe des balises. Mais où en sommes-nous? », dans *Développements récents en droit du travail (2000)*, Service de la formation permanente du Barreau du Québec, 2000, *Droit civil en ligne* (DCL), EYB2000DEV859

GAGNON, R. P., « Le contrat de travail », dans *Droit du travail*, Collection de droit 2006-2007, vol. 8, École du Barreau du Québec, 2006, *Droit civil en ligne* (DCL), EYB2006CDD196

LEFEBVRE, S., « Naviguer sur Internet au travail: et si on nageait en eaux troubles? », dans Service de la formation permanente du Barreau du Québec, *Développements récents en droit du travail 2008*, Cowansville, Éditions Yvon Blais, 2008, p. 51

LÉVESQUE, G. et S. FOREST, « L'atteinte à la réputation dans le cadre des rapports collectifs de travail », dans *Développements récents en droit du travail (2002),* Service de la formation permanente du Barreau du Québec, 2002, *Droit civil en ligne* (DCL), EYB2002DEV618

LEWIS, J. B., « I know what you e-mailed last summer (Legal Update Employee Monitoring) », *Security Management* 93, January, 2002, en ligne : <http://www.entrepreneur.com/tradejournals/article/82015917.html> (site consulté le 19 août 2010)

MORGAN, C., « Monitoring Employee, Electronic Mail and Internet Use: Balancing Competing Rights », dans GAUTRAIS, V. (dir.), *Droit du commerce électronique*, Montréal, Éditions Thémis, 2002, p. 171

PINNINGTON, D., « Beware the Dangers of Metadata », *Lawpro.ca*, Juin 2004, en ligne : <http://www.lawpro.ca/LawPRO/metadata.pdf> (site consulté le 19 août 2010)

SAINT-ANDRÉ, Y., « Le respect du droit à la vie privée au travail : mythe ou réalité?, dans *Développements récents en droit du travail (2004)* », Service de la formation permanente du Barreau du Québec, 2004, *Droit civil en ligne* (DCL), EYB2004DEV408

SIMMONS, C. G. « Arbitral Stare Decisis: An Unheralded but Important Doctrine in Canadian Arbitral Jurisprudence Labour Law », (1985-1986) 11 *Queen's L.J.* 347

SOLDEVILA, A., « La responsabilité pour le fait ou la faute d'autrui et pour le fait des biens », dans *Responsabilité*, Collection de droit 2007-2008, vol. 4, École du Barreau du Québec, 2007, *Droit civil en ligne* (DCL), EYB2007CDD89

TANI-MOORE, E., « *L'appréciation en droit québécois de l'arrêt Nikon: même résultat?* », (2002) 8-1 *Lex Electronica*, en ligne : <http://www.lex-electronica.org/articles/v8-1/tani-moore.htm> (site consulté le 30 juillet 2010)

TRUDEL, P., « La responsabilité des acteurs du commerce électronique » dans Vincent GAUTRAIS (dir.), *Droit du commerce électronique*, Montréal, Éditions Thémis, 2002, p. 607

TRUDEL, P., « La responsabilité civile : qui répond de l'information? », dans RACICOT M., M. S. HAYES, A. R. SZIBBO et P. TRUDEL, *L'espace cybernétique n'est pas une terre sans loi. Étude des questions relatives à la responsabilité à l'égard du contenu circulant sur Internet*, Ottawa, Industrie Canada, 1997, p. 135.

VEILLEUX, D., « Le droit à la vie privée – sa portée face à la surveillance de l'employeur », (2000) *R. du B.* 60

VERMEYS, N. W., « Chronique – Responsabilité civile et Web 2.0 », dans *Repères*, Juillet 2007, *Droit civil en ligne* (DCL), EYB2007REP607

Américains

HARRIS, D. P., D. B. GARRIE, M. J. ARMSTRONG, « Sexual Harassment: Limiting the Affirmative Defense in the Digital Workplace », 39 *U. MICH. J.L. REFORM* 73 (2005-2006)

PERRITT JR., H. H., « Tort Liability, the First Amendment and Equal Access to Electronic Networks », (1992) 5 *Harvard J. of L. & Tech.* 65

PORTER, W. G. II, M. C. GRIFFATON, « Between the Devil and the Deep Blue Sea: Monitoring the Electronic Workplace», 70 *DEF. COUNSEL. J.* 65 (2003)

SCHLACHTER, E., « Cyberspace, the Free Market and the Free Marketplace of Ideas: Recognizing Legal Differences in Computer Bulletin Board Functions », (1993) 16 *Hastings Comm/Ent L.J.* 87

Belges

SCHMIDT, H., « E-mail, internet et le lieu de travail : une relation difficile? », Avcb-vsgb.be, Mai 2006, en ligne : <http://www.avcb-

vsgb.be/documents/documents/personnel/email-internet-travail.pdf> (site consulté le 19 août 2010)

Français

AKDENIZ Y. et J. BELL, « La vie privée et l'Internet : perspectives du Royaume Uni », dans TABATONI, P., *La protection de la vie privée dans la société d'information*, t. 3, coll. « Cahiers Académie des Sciences morales et politiques », Paris, Les Presses Universitaires de France, 2002, p. 152

CAHEN, M., « La validité des chartes Internet », Legalbiznext.com, 10 novembre 2005, en ligne : <http://www.legalbiznext.com/droit/La-validite-des-chartes-Internet> (site consulté le 19 août 2010)

CAPRIOLI, E. A., « La qualité de fournisseur d'accès à l'internet : un nouveau risque juridique pour l'entreprise », Caprioli-avocats.com, Juin 2005, en ligne : <http://www.caprioli-avocats.com/donnees-perso/88-fournisseur-acces-internet> (site consulté le 19 août 2010)

CAPRIOLI, E. A., « Les contrats informatiques face à la jurisprudence récente. Gare au surf incontrôlé des salariés », Caprioli-avocats.com, Première publication : Avril 2008, en ligne : <http://www.caprioli-avocats.com http://www.caprioli-avocats.com/securite-informatique/146-surf-incontrole-des-salaries> (consulté le 19 août 2010)

CRÉPIN, C., « Pertes de données : à quand une politique d'entreprise responsabilisante », Droit-tic.com, 6 mars 2006, en ligne : <http://www.droit-ntic.com/news/afficher.php?id=347> (site consulté le 19 août 2010)

GOLVERS, L., « L'informatique et la protection de la vie privée », Droit-technologie.org, 11 janvier 2001, en ligne : <http://www.droit-technologie.org/upload/dossier/doc/33-1.pdf> (site consulté le 19 août 2010)

GRIGUER, D., « Le débat sur l'utilisation, à titre privé, du courrier électronique au sein de l'entreprise serait-il dépassé? », Legalbiznext.com, 28 juillet 2004, en ligne :

<http://www.legalbiznext.com/droit/Le-debat-sur-l-utilisation-a-titre> (site consulté le 19 août 2010)

IVALDI, N. et P. VINCENT, « Cybersurveillance des salariés et chartes informatiques », Caprioli-avocats.com, Septembre 2005, en ligne : <http://www.caprioli-avocats.com/donnees-perso/87-cybersurveillance> (site consulté le 19 août 2010)

LANDAT, C. et M. DELAWARI, « Les enjeux du développement d'Internet au regard de la relation salariale et pré-salariale », Droit-ntic.com, 2001, en ligne : <http://www.droit-ntic.com/pdf/cybersurv.pdf> (site consulté le 29 juillet 2010)

MAITROT DE LA MOTTE, A., « Le droit au respect de la vie privée », dans TABATONI, P., *La protection de la vie privée dans la société d'information*, t. 3, coll. « Cahiers Académie des Sciences morales et politiques », Paris, Les Presses Universitaires de France, 2002, p. 255.

PESCHAUD, H., « Cyberpreuve de l'identité de l'auteur d'un courriel antisémite », Legalbiznext.com, 05 juillet 2004, en ligne : <http://www.legalbiznext.com/droit/Cyberpreuve-de-l-identite-de-l> (site consulté le 19 août 2010)

POIDEVIN, B., « Quelle responsabilité lors de la diffusion de virus? », Jurisexpert.net, 20 décembre 2001, en ligne : <http://www.jurisexpert.net/quelle_responsabilit_lors_de_la_diffusio/> (site consulté le 19 août 2010)

POIDEVIN, B., « Quelle responsabilité en matière de sécurité informatique? », Jurisexpert.net, 8 avril 2002, en ligne : <http://www.jurisexpert.net/quelle_responsabilit_en_mati_re_de_s_cur/> (consulté le 19 août 2010)

POIDEVIN, B., « L'usage du système informatique par les employés : quel risque pour l'employeur? », Jurisexpert.net, 10 novembre 2006, en ligne : <http://www.jurisexpert.net/l_usage_du_systeme_informatique_par_les/> (site consulté le 19 août 2010)

RENARD, I., « Responsabilité de l'entreprise et de ses dirigeants du fait de la perte de données informatiques », Lejournaldunet.com, 23 janvier 2003, en ligne : <http://www.journaldunet.com/solutions/0301/030123_chro_juridique.shtml> (site consulté le 19 août 2010).

RENARD, I., « Les droits et devoirs des entreprises », Lejournaldunet.com, Mars 2004, en ligne : <http://www.journaldunet.com/management/dossiers/040331acces/renard.shtml> (site consulté le 19 août 2010)

RENARD, I., « Les DSI et les RSSI sont ils responsables pénalement? », Lejournaldunet.com, 02 février 2005, en ligne : <http://www.journaldunet.com/solutions/0502/050202_juridique.shtml> (site consulté le 19 août 2010)

SÉDALLIAN, V., « Légiférer sur la sécurité informatique : la quadrature du cercle? », Juriscom.net, 08 décembre 2003, en ligne : <http://www.juriscom.net/documents/secu20031208.pdf> (site consulté le 19 août 2010)

SERIO, D. et C. MANARA, « Traçabilité et responsabilité dans les relations de travail », Caprioli-avocats.com, Première publication : *Les premières journées internationales du droit du commerce électronique, Actes du colloque de Nice des 23, 24 et 25 octobre 2000, coll. Actualités de droit de l'entreprise, dirigée par J. RAYNARD*, Litec, 2002, p. 149 s., Date de la mise à jour : janvier 2001, en ligne : <http://www.caprioli-avocats.com/tracabilite/74-tracabilite-responsabilite-relations-travail> (consulté le 19 août 2010)

Thèses de doctorat et mémoires de maîtrise

Canadiens

BLANCHETTE, F., *L'expectative raisonnable de vie privée et les principaux contextes de communications dans Internet*, mémoire de maîtrise, Montréal, Faculté des études supérieures, Université de Montréal, 2001

HÉBERT, P. G., *Pour une interprétation renouvelée du critère de l'exécution des fonctions de l'article 1463 C.C.Q.*, mémoire de maîtrise, Québec, Faculté de droit, Université Laval, 2005

LENFANT, J., *Le droit à la vie privée s'étend-il à l'utilisation du courriel par un employé dans le cadre de ses fonctions? Analyse de la doctrine, législation, jurisprudence et autres normes*, Montréal, Faculté des études supérieures, Université de Montréal, 2000, en ligne : <http://www.juriscom.net/uni/etd/04/priv01.pdf> (site consulté le 29 juillet 2010)

VERMEYS, N. W., *Qualification et quantification de l'obligation de sécurité informationnelle dans la détermination de la faute civile, thèse de doctorat*, Montréal, Faculté des études supérieures, Université de Montréal, 2009

VICENTE, A. I., *La convergence de la sécurité informationnelle et la protection des données à caractère personnel. Vers une nouvelle approche juridique,* mémoire de maîtrise, Montréal, Faculté des études supérieures, Université de Montréal, 2003

Français

FÉVRIER, F., *Pouvoir de contrôle de l'employeur et droits des salariés à l'heure d'Internet. Les enjeux de la cybersurveillance dans l'entreprise*, mémoire de D.E.A., Nanterre, Faculté de droit, Université de Nanterre – Paris X, 2003

LEMARTELEUR, X., *L'employeur : un fournisseur d'accès à l'internet comme les autres? Implications juridiques de la fourniture d'accès à l'internet par l'entreprise*, mémoire de DESS, Paris, Faculté de droit, Université Paris II Panthéon-Assas, 2003

ROQUES, V., *La sécurité des données d'entreprises en réseau*, mémoire de DEA, Montpellier, Institut de Recherche et d'Étude pour le Traitement de l'Information Juridique, Université Montpellier I, 2002

Documents ou rapports d'organismes publics

Canadiens

COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Les risques associés aux métadonnées. Fiche d'information*, en ligne : <http://www.priv.gc.ca/fs-fi/02_05_d_30_f.cfm> (site consulté le 25 juillet 2010)

COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Résumé de conclusions d'enquête en vertu de la LPRPDÉ n° 289. Le vol d'un ordinateur portatif met en cause la responsabilité d'une banque*, 3 février 2005, 2005 IIJCan 15488 (C.V.P.C.), en ligne : <http://www.canlii.org/>

COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA, *Résumé de conclusions d'enquête en vertu de la LPRPDÉ n° 346. Un courriel soulève des questions concernant les motifs, la crédibilité et la responsabilisation*, 15 juin 2006, 2006 CanLII 37531 (C.V.P.C.), en ligne : <http://www.canlii.org/>

COMMISSION DE L'ÉTHIQUE DE LA SCIENCE ET DE LA TECHNOLOGIE, *L'utilisation des données biométriques à des fins de sécurité : questionnement sur les enjeux éthiques. Document de réflexion*, Québec, Conseil de la science et de la technologie, 2005, en ligne : <http://www.cst.gouv.qc.ca/IMG/pdf/Biometrie-reflexion.pdf> (site consulté le 25 juillet 2010)

RADWANSKI, G. (COMMISSARIAT À LA PROTECTION DE LA VIE PRIVÉE DU CANADA), *Décisions récentes et questions émergentes en vertu de la nouvelle loi sur la protection de la vie privée*, discours à la Conférence annuelle sur les droits de la personne et la vie privée au travail, Lancaster House, Toronto, 2002, en ligne : <http://www.privcom.gc.ca/speech/02_05_a_020503_f.asp> (site consulté le 25 juillet 2010)

STATISTIQUE CANADA, *Enquête canadienne sur l'utilisation d'Internet*, 2010, en ligne : <http://www.statcan.gc.ca/daily-quotidien/100510/dq100510a-fra.htm> (site consulté le 28 juillet 2010)

Américains

COMPUTER SECURITY INSTITUTE, FEDERAL BUREAU OF INVESTIGATION, *2005 CSI/FBI Computer Crime and Security Survey*, 2005, en ligne: <http://www.cpppe.umd.edu/Bookstore/Documents/2005CSISurvey.pdf> (site consulté le 22 août 2010)

Français

COMMISSION DES OPÉRATIONS DE BOURSE, *Communiqué à l'attention des sociétés disposant d'un site ou d'un accès internet sur les possibilités d'utilisation du réseau*, Paris, 2000, en ligne : <http://www.amf-france.org/documents/general/3390_1.pdf> (site consulté le 25 juillet 2010)

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, *Rapport d'étude et de consultation publique. La cybersurveillance des salariés dans l'entreprise*, Mars 2001, en ligne : <http://www.cnil.fr/fileadmin/documents/approfondir/rapports/cybersurveillance.pdf> (site consulté le 19 août 2010)

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, *Communication de la CNIL relative à la mise en œuvre de dispositifs de reconnaissance par empreinte digitale avec stockage dans une base de données*, 2007, en ligne : <http://www.cnil.fr/fileadmin/documents/approfondir/dossier/CNI-biometrie/Communication-biometrie.pdf> (site consulté le 26 juillet 2010)

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, *La cybersurveillance des salariés en entreprise*, *20ème rapport d'activité 1999*, 2000, en ligne : <http://lesrapports.ladocumentationfrancaise.fr/BRP/004001043/0000.pdf> (site consulté le 26 juillet 2010)

COMMISSION NATIONALE INFORMATIQUE ET LIBERTÉS, *21ème rapport d'activité 2000*, 2001, en ligne : <http://lesrapports.ladocumentationfrancaise.fr/BRP/014000460/0000.pdf > (site consulté le 26 juillet 2010)

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, *22ème Rapport d'activité 2001*, 2002, en ligne :

<http://lesrapports.ladocumentationfrancaise.fr/BRP/024000377/0000.pdf> (site consulté le 26 juillet 2010)

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, *La cybersurveillance sur les lieux de travail*, 2004, en ligne : <http://www.cnil.fr/fileadmin/documents/approfondir/rapports/Rcybersurveillance-2004-VD.pdf> (site consulté le 26 juillet 2010)

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, *Délibération 2005-023. Délibération portant autorisation de la mise en œuvre par la Banque de France d'un traitement automatisé de données à caractère personnel ayant pour finalité de contrôler l'accès aux locaux sensibles*, 17 février 2005, en ligne : <http://www.legifrance.gouv.fr> (site consulté le 26 juillet 2010)

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, *Délibération 2005-206. Délibération portant autorisation de mise en œuvre d'un traitement automatisé de données à caractère personnel reposant sur la reconnaissance de l'empreinte digitale et ayant pour finalité de contrôler l'accès logique à un service d'informations financières de la société Bloomberg L.P.*, 22 septembre 2005, en ligne : <http://www.legifrance.gouv.fr> (site consulté le 26 juillet 2010)

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, *Délibération 2005-281. Délibération portant autorisation de la mise en œuvre par la Cité des Sciences et de l'Industrie d'un traitement automatisé de données à caractère personnel reposant sur l'utilisation d'un dispositif biométrique de reconnaissance de l'empreinte digitale et ayant pour finalité le contrôle de l'accès aux locaux*, 22 novembre 2005, en ligne : <http://www.legifrance.gouv.fr> (site consulté le 26 juillet 2010)

COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS, *Délibération 2006-132. Délibération portant autorisation de la mise en œuvre par la société Atos Worldline d'un traitement automatisé de données à caractère personnel reposant sur la reconnaissance des empreintes digitales et ayant pour finalité le contrôle de l'accès aux locaux*, 09 mai 2006, en ligne : <http://www.legifrance.gouv.fr> (site consulté le 26 juillet 2010)

DIRECTION DE L'ANIMATION DE LA RECHERCHE, DES ÉTUDES ET DES STATISTIQUES (DARES), *Conditions de travail : une pause dans l'intensification du travail. Premières Synthèses*, Paris, Publications Dares, 2007, n° 01.2, en ligne : <http://www.travail-solidarite.gouv.fr/IMG/pdf/2007.01-01.2.pdf> (site consulté le 25 juillet 2010)

DE LONGEVIALLE, J.-P. (COMMISSION NATIONALE DE L'INFORMATIQUE ET DES LIBERTÉS), *Intervention à la 26ème conférence internationale sur la vie privée et la protection des données personnelles. Session sur le thème de « La protection de la vie privée de l'employé et les intérêts de l'employeur »*, Wroclaw, 2004, en ligne : <http://26konferencja.giodo.gov.pl/data/resources/LongevialleJP_paper.pdf> (site consulté le 26 juillet 2010)

Documents internationaux

EUROPEAN INDUSTRIAL RELATIONS OBSERVATORY (EIRO), *New technology and respect for privacy at the workplace*, Février 2007, en ligne: <http://www.eurofound.europa.eu/eiro/2007/02/articles/ee0702079i.htm> (site consulté 25 juillet 2010)

WIKIPEDIA, « Spam », 2010, en ligne: <http://fr.wikipedia.org/wiki/Pourriel> (site consulté 30 juillet 2010)

Documents ou rapports d'organismes privés ou paragouvernementaux

AMERICAN MANAGEMENT ASSOCIATION, THE EPOLICY INSTITUTE, *2007 Electronic Monitoring & Surveillance Survey. Over Half of All Employers Combined Fire Workers for E-Mail & Internet Abuse*, 2008, résumé en ligne : <http://press.amanet.org/press-releases/177/2007-electronic-monitoring-surveillance-survey/> (site consulté le 27 juillet 2010)

CEFRIO et SOM RECHERCHES ET SONDAGES, *NetQuébec 2008. Portrait de l'utilisation des TI et d'Internet au Québec*, 2008, en ligne : <https://www.cefrio.qc.ca/index.php?eID=tx_nawsecuredl&u=4818&file=fileadmin

/doc_bloc_achat/DEPnestquebecwebSECUR.pdf&t=1280345975&hash=c6efb88e785aabb676a1ccb9a91acd79> (site consulté le 27 juillet 2010)

CEFRIO et SOM RECHERCHES ET SONDAGES, *NetPME 2009. Utilisation des TI par les entreprises québécoises : plus de 1800 PME sondées. Faits saillants*, 2009, en ligne : <https://www.cefrio.qc.ca/index.php?eID=tx_nawsecuredl&u=4818&file=fileadmin/doc_bloc_achat/netpmefaitssaillants2009secur.pdf&t=1280346654&hash=65ef29f39fc1033a7bc8174925ff7363> (site consulté le 27 juillet 2010)

FORUM DES DROITS SUR L'INTERNET, *Rapport final. Relations du travail et internet*, 2002, en ligne : <http://www.foruminternet.org/telechargement/documents/rapp-RTI-20020917.pdf> (site consulté le 26 juillet 2010)

FORUM DES DROITS SUR L'INTERNET, *Relations du travail et internet. Panorama législatif et jurisprudentiel*, 2006, en ligne : <http://www.foruminternet.org/telechargement/documents/dossier-travail-20060126.pdf> (site consulté le 26 juin 2010)

GFI SOFTWARE, *Echantillon de politique d'usage de l'internet*, <http://www.gfsfrance.com/internet-monitoring-software/sample-internet-usage-policy> (site consulté le 25 juillet 2010)

GFI SOFTWARE, *White paper. Archiving technologies*, p. 6, en ligne : <http://www.gfsfrance.com/whitepapers/stubbingwp.pdf> (site consulté le 28 juillet 2010)

GFI, *White Paper. The Importance of an Acceptable Use Policy*, 2010, en ligne: <http://www.gfi.com/whitepapers/acceptable_use_policy.pdf> (site consulté le 28 juillet 2010)

GUIDE DES DROITS SUR INTERNET, *Politique sur l'utilisation du courriel-Éléments d'une politique*, en ligne : <http://www.droitsurinternet.ca/section_135.html> (site consulté le 25 juillet 2010)

HEWLETT-PACKARD FRANCE, *Une étude démontre que les femmes qui surfent régulièrement sur leurs sites Web favoris sont moins stressées, stimulent leur activité cérébrale et augmentent leur productivité*, 2008, en ligne :

<http://h41131.www4.hp.com/fr/fr/press/une--tude-d-montre-que-les-femmes-qui-surfent-r-guli-rement-sur-leurs-sites-web-favoris-sont-moins-stress-es--stimulent-leur-activit--c-r-brale-et-augmentent-leur-productivit--.html?jumpid=reg_R1002_FRFR> (site consulté le 18 août 2010)

JURIFAX, *Politique courrier électronique*, extrait en ligne : <http://www.orhri.org/_Externe.aspx?l=http%3a%2f%2fstore.yahoo.com%2fjurifaxstore%2f3244f.html%3fp%3d241248> (site consulté le 28 juillet 2010)

JURIFAX, *Politique Internet*, extrait en ligne : <http://www.orhri.org/_Externe.aspx?l=http%3a%2f%2fstore.yahoo.com%2fjurifaxstore%2f3244f.html%3fp%3d241248> (site consulté le 28 juillet 2010)

KPMG, *Les vols d'information liés à la malveillance interne ont augmenté de plus de 50% au premier semestre 2009. Selon le Baromètre KPMG du vol et de la perte d'informations*, Paris, 2009, en ligne : <http://www.kpmg.fr/fr/Press/documents/cp-it-dataloss-dec09.pdf> (site consulté le 22 août 2010)

MELISON, D., *Charte d'utilisation du système d'information et de communication*, dans *Formulaire commenté Lamy Droit de l'immatériel*, Éditions Lamy, Décembre 2006, extrait, en ligne : <http://www.journaldunet.com/management/dossiers/040331acces/modele-charte-internet.shtml> (consulté le 13 juillet 2010)

PRICEWATERHOUSECOOPERS, *IT security survey*, Décembre 2009, résumé en ligne : <http://www.pwc.fr/securite-informatique-les-attaques-ciblant-les-donnees-de-lentreprise-ont-presque-double-en-2009-dans-le-monde.html> (site consulté le 22 août 2010)

Conférences

DELWAIDE, K., *Internet et contrat de travail : Enjeux et solutions*, Conférence « Droit civil + technologies », Chaire en droit de la sécurité et des affaires électroniques, Université de Montréal, 2010, acétates PowerPoint, fichier mp3 et vidéo en ligne :

<http://www.gautrais.com/Les-videos-sont-en-ligne> (site consulté le 22 juillet 2010)

Articles anonymes et communiqués en ligne

LCN CANOE, « Internet au travail. Une autre enquête à la Ville de Québec », 20 avril 2010, Lcn.canoe.ca, en ligne : <http://lcn.canoe.ca/lcn/infos/regional/archives/2010/04/20100402-170342.html> (site consulté le 18 août 2010)

LEGALIS.NET, « Virus le client responsable d'être allé sur des sites étrangers à son activité », 04 décembre 2007, en ligne : <http://www.legalis.net/article.php3?id_article=2098> (site consulté le 30 juillet 2010)

LEGALIS.NET, « Fraude informatique : 5 mois de prison », 09 juillet 1998, en ligne : <http://www.legalis.net/spip.php?page=archives&id_rubrique=60> (site consulté le 30 juillet 2010)

LE JOURNAL DU MANAGEMENT, « Réguler l'accès Internet des salariés. Contrôle technique contrôle éthique », Mars 2004, en ligne : Lejournaldunet.com : <http://www.journaldunet.com/management/dossiers/040331acces/lead.shtml> (site consulté le 30 juillet 2010)

LEMONDE.FR, « Selon son ancien chef, Jérôme Kerviel "mentait" mais était "crédible" », 21 juin 2010, en ligne : <http://www.lemonde.fr/economie/article/2010/06/21/selon-son-ancien-chef-jerome-kerviel-mentait-mais-etait-credible_1376141_3234.html> (site consulté le 30 juillet 2010)

Annexe I – Exemple de guide pour l'élaboration de la politique d'utilisation de l'Internet et du courrier électronique

Contenu de la politique d'utilisation de l'Internet et du courrier électronique	
Thèmes	**Contenu des clauses**
Préambule	Titre de la politique; présentation de la politique.
Objectifs	Objectifs; contexte.
Champ d'application	Utilisateurs, activités et outils de communication concernés; définition des mots et expressions utilisés.
Règles de sécurité informatique	Gestion des mots de passe; règles générales de sécurité et de bon usage; protection du matériel et des fichiers.
Règles d'utilisation de l'Internet	Personnes autorisées à accéder à Internet; périodes d'accès autorisées; usages permis; usages et sites interdits; règles spécifiques à l'usage personnel; accès à distance; utilisation du matériel portatif; indication des contrôles mis en place.
Règles d'utilisation du courrier électronique	Personnes autorisées à utiliser le courrier électronique; usages autorisés; usages interdits et contenus interdits; règles spécifiques à l'usage personnel; accès à distance; gestion des fichiers joints et des expéditeurs douteux; confidentialité des adresses de courriel; indication des contrôles mis en place et de l'absence de caractère confidentiel des contenus en circulation.

Contenu de la politique d'utilisation de l'Internet et du courrier électronique	
Thèmes	**Contenu des clauses**
Dispositions relatives à la responsabilité	Obligation de confidentialité (règles de protection des renseignements personnels, protection des données de l'entreprise); respect de la propriété intellectuelle; respect des droits des personnes (droit à la vie privée, droit à la réputation, droit à l'image, règles concernant le harcèlement); respect des lois d'ordre public (propagande haineuse, pornographie, pornographie juvénile).
Droits de l'entreprise	Droit de propriété sur les informations circulant dans le réseau; droit de contrôle et de surveillance du système d'information; clause exonératoire de la responsabilité de l'entreprise; rappel des autres politiques de l'entreprise.
Non-respect de la politique	Sanctions; recours en justice de l'entreprise.
Publicité, entrée en vigueur et évolution	Modalités de diffusion; date d'entrée en vigueur; durée d'application; dispositions relatives à l'évolution de la politique (modification, annulation); application et suivi.
Engagement du salarié	Déclarations, engagements et renonciations de l'employé (notamment à son droit à la protection de la vie privée).

Annexe II – Tableau des manquements liés à l'usage de l'Internet et de la messagerie électronique de l'employeur et mesures appliquées

Décisions jurisprudentielles relatives à l'usage abusif de l'Internet et de la messagerie électronique et mesures appliquées				
Nom des parties	**Manquements de l'employé**	**Facteurs aggravants**	**Facteurs atténuants**	**Décision du Tribunal**
Addy c. *Commission scolaire Eastern Township*, 2010 QCCS 1708 (CanLII)	Utilisation des ordinateurs de l'employeur pour naviguer sur des sites pornographiques pendant les heures de travail.	Aspirant enseignant en stage; établissement scolaire accueillant de jeunes élèves; existence d'une politique claire.		Congédiement confirmé.
Alberta v. *Alberta Union of Provincial Employees* (R. Grievance), [2008] (Alta. G.A.), inf. par *Alberta Union of Provincial Employees v. Alberta*, (2009 Alt. Q.B.)	Insultes et propos dénigrants vis-à-vis de l'employeur, de collègues et de clients de l'entreprise postés sur le blogue personnel de la salariée; les personnes visées sont aisément identifiables.	Absence de remords de la part de l'employée; aucune mesure n'a été prise pour bloquer l'accès aux contenus litigieux.		Congédiement confirmé, mais annulé en appel pour non-respect de la procédure disciplinaire prévue dans la convention collective.
Alliance de la fonction publique du Canada et *Musée des beaux-arts du Canada*, (2003/ T.A.)	« Clavardages » et navigation sur des sites pornographiques et de jeux; réinstallation des logiciels de jeux chaque fois que l'employeur les supprime du poste de travail.	Existence d'une politique d'entreprise claire; persistance du salarié dans l'insubordination, malgré diverses réprimandes et mesures disciplinaires prises à son encontre.		Suspension de deux mois confirmée.
Arpin c. *Grenier*, REJB	Publication d'un texte offensant et	Le salarié est Adjoint au		Condamnation au paiement de

Décisions jurisprudentielles relatives à l'usage abusif de l'Internet et de la messagerie électronique et mesures appliquées				
Nom des parties	**Manquements de l'employé**	**Facteurs aggravants**	**Facteurs atténuants**	**Décision du Tribunal**
2004-65808 (C.Q.)	à caractère diffamant dans un forum de discussion sur Internet; le salarié signe de son nom et ajoute son adresse électronique professionnelle, laquelle comporte le nom de l'employeur.	président, responsable du marketing : il aurait dû savoir que ses actes auraient des conséquences dommageables, notamment pour l'obtention de financements.		3 000 $ de dommages-intérêts à l'employeur devenu ex-employeur).
Backman c. *Maritime Paper Products Limited, corps constitué*, 2009 NBCA 62 (CanLII)	Consultation de sites pornographiques avec le matériel de l'employeur.	Politique Internet connue du salarié; 2 avertissements formels au dossier du salarié (le dernier l'avertissait qu'il encourait le congédiement en cas de la récidive).		Congédiement confirmé.
Belisle c. *Rawdon (Municipalité)*, 2005 QCCRT 453 (IIJCan)	Utilisation de l'ordinateur à des fins personnelles; téléchargement et stockage de près de 1 600 fichiers à caractère pornographique sur le disque dur; insubordination; incivilité et manque de respect vis-à-vis des collègues et de la hiérarchie.	Le salarié est un haut cadre, avec 21 ans d'ancienneté; il persiste dans son insubordination, malgré des rappels à l'ordre effectués à au moins deux reprises.	Poste de travail du salarié accessible à d'autres salariés; absence de politique claire quant à l'usage du matériel informatique; aucun préjudice démontré par l'employeur.	Congédiement sans progressivité des sanctions confirmé.
Bell Canada c. *Association Canadienne des Employés de Téléphone*, D.T.E. 2000-	Utilisation de la messagerie électronique pour transmettre des fichiers à caractère	Étalement des faits sur plusieurs mois; majorité des envois effectués pendant les heures de travail.	Ancienneté de 9 ans; dossier disciplinaire vierge; coopération et franchise du salarié	Congédiement annulé et remplacé par une suspension de trois mois.

Décisions jurisprudentielles relatives à l'usage abusif de l'Internet et de la messagerie électronique et mesures appliquées				
Nom des parties	**Manquements de l'employé**	**Facteurs aggravants**	**Facteurs atténuants**	**Décision du Tribunal**
254 (T.A.)	pornographique à des collègues et à des tiers hors de l'entreprise; atteinte à l'image de l'entreprise du fait de ces envois.		lors de l'enquête; reconnaissance des faits et de sa responsabilité	
Blais c. *Société des Loteries Vidéos du Québec Inc*., D.T.E. 2003T-178 (C.R.T.)	Téléchargement et distribution de matériel obscène et offensant; vol d'une somme de 400 $ dans les caisses de l'employeur.	Politique d'utilisation des outils informatiques claire et connue du salarié; utilisation de manœuvres pour contourner le système de pare-feu.		Congédiement confirmé.
Bolduc c. *Collège de Montréal*, 2010 QCCRT 130 (CanLII)	Atteinte à la réputation de l'employeur consécutivement à la publication d'informations confidentielles le concernant dans un journal; l'employée est agente aux services administratifs et est la seule à avoir accès aux informations financières divulguées; de nombreux courriels prouvent son implication dans les faits.	Entente de non-divulgation (et de non-utilisation) de l'information confidentielle obtenue dans le cadre de son travail signée par la salariée; refus de reconnaître sa participation à la fuite des informations et d'assumer sa responsabilité.		Congédiement confirmé.
Bourassa et *Ville de La Tuque,* 2009 QCCRT 322 (CanLII)	Utilisation abusive de l'Internet : 25 000 sites visités en trente mois, à	Existence d'une politique Internet dont le plaignant a connaissance; le salarié est cadre; il		Congédiement sans progression des sanctions.

Décisions jurisprudentielles relatives à l'usage abusif de l'Internet et de la messagerie électronique et mesures appliquées				
Nom des parties	**Manquements de l'employé**	**Facteurs aggravants**	**Facteurs atténuants**	**Décision du Tribunal**
	raison de 90 minutes en moyenne par jour, 96% de cette utilisation est à des fins personnelles.	a déjà occupé des fonctions de responsable informatique; vol de temps allant, pour certaines périodes, de 50 à 75 % de son temps de travail.		
Briar c. *Canada (Conseil du Trésor)*, 2003 CRTFP 3 (CanLII)	Distribution d'images offensantes à caractère sexuel par plusieurs salariés grâce au courrier électronique de l'employeur.	Existence d'une politique interdisant les activités illégales ou inacceptables; certains salariés ont un dossier disciplinaire et/ou nient les faits.	Certains employés ont un dossier disciplinaire vierge et/ou assument leur responsabilité.	Diverses retenues sur salaire valant avertissement versé au dossier.
Carrier c. *Centre local de développement (CLD) des Etchemins*, 2005 QCCRT 183 (CanLII)	Complot contre un salarié cadre afin de le contraindre à démissionner : adhésion, sous une fausse identité, d'une employée à un site de rencontres fréquenté par la victime en vue d'initier une relation virtuelle avec lui et lui soutirer des informations compromettantes; subtilisation, détention et utilisation de divers documents confidentiels de la victime et de l'employeur.	Préméditation et implication de plusieurs salariés; poursuite d'intérêts personnels et syndicaux (les salariés sont représentants syndicaux); absence de remords des salariés; refus d'admettre leur responsabilité.		Congédiement confirmé.

Décisions jurisprudentielles relatives à l'usage abusif de l'Internet et de la messagerie électronique et mesures appliquées				
Nom des parties	**Manquements de l'employé**	**Facteurs aggravants**	**Facteurs atténuants**	**Décision du Tribunal**
Centre de réadaptation Lethbridge et *Syndicat des physiothérapeutes et des thérapeutes en réadaptation physique du Québec*, D.T.E. 2004T-755 (T.A.)	Consultation de sites pornographiques sur l'ordinateur de l'employeur.	Existence d'une politique d'entreprise claire et parfaitement connue du salarié qui a siégé au comité l'ayant adoptée.	27 ans d'ancienneté; dossier vierge; les navigations se sont déroulées sur une journée.	Suspension de cinq jours maintenue.
Cogeco Câble Canada Inc. et *Syndicat canadien de la fonction publique, section locale 3624*, D.T.E. 2001T- 1039 (T.A.)	Utilisation d'une adresse IP appartenant à l'employeur pour s'introduire dans le système informatique d'un concurrent de l'employeur; divulgation aux média d'une faille de sécurité constatée dans ce système d'information.	Les actes auraient pu avoir des conséquences néfastes pour l'employeur, en raison de la compétition entre les deux entreprises.	Absence de politique d'entreprise sur l'utilisation d'Internet.	Suspension de 10 jours substituée à celle de 33 jours imposée par l'employeur.
Collège Ahuntsic et *Syndicat du personnel de soutien du Collège Ahuntsic*, D.T.E. 2007T-889 (T.A.)	Utilisation du téléphone et de l'équipement informatique de l'employeur à des fins personnelles, notamment au profit de l'entreprise du salarié; utilisation de son adresse de courriel chez l'employeur sur les cartes de visite de son entreprise personnelle.	Le salarié réclame pourtant le paiement d'heures supplémentaires pour le temps consacré à ses activités personnelles.	Vol de temps négligeable; aucune mise au point préalable effectuée par l'employeur quant aux activités personnelles de l'employé; aucun impact négatif sur la réputation de l'employeur.	Suspension de trois semaines substituée à celle de 3 mois imposée par l'employeur.

Décisions jurisprudentielles relatives à l'usage abusif de l'Internet et de la messagerie électronique et mesures appliquées				
Nom des parties	**Manquements de l'employé**	**Facteurs aggravants**	**Facteurs atténuants**	**Décision du Tribunal**
Commission des normes du travail c. *Bourse de Montréal Inc.*, REJB 2002-31243 (C.Q.)	Conservation d'un fichier contenant un virus; visite d'un site de piratage et réalisation d'une opération sur ce site.	Aggravation liée à la fonction d'analyste en informatique du salarié et à sa faible ancienneté (1 an).	Règles concernant l'utilisation des outils informatiques peu claires et ambiguës et insuffisantes à couvrir la faute de l'employé; aucun préjudice subi par l'employeur.	Indemnité correspondant au préavis de cessation de travail accordée au salarié (3 084 $).
Consumers Gas v. *Communications, Energy and Paperworkers Union* (Primiani Grievance), [1999] O.L.A.A. No. 649 (L.A.) (QL/LN)	Réception et distribution de contenus à caractère sexuel et pornographique *via* la messagerie de l'employeur; l'un des messages endommage le système informatique.	Le simple bon sens interdisait à l'employée d'utiliser la messagerie électronique de l'employeur pour stocker et distribuer des contenus à caractère sexuel.	Ignorance de l'existence de la politique d'entreprise alléguée par l'employée; laxisme de l'employeur vis-à-vis de l'usage de ses outils électroniques.	Suspension d'un mois substituée au congédiement.
D'Astous c. *Sesno*, REJB 2000-22668 (C.Q.)	Création d'un site Internet reproduisant textuellement celui créé pour l'employeur. Insertion d'un lien sur le site de l'employeur redirigeant les visiteurs vers le site du salarié; maintien de la situation bien après la rupture du contrat de travail.	L'homonymie des deux sites accentue les risques de confusion pour la clientèle de l'entreprise.		Condamnation de l'ex-salarié à 3 000 $ de dommages-intérêts.
Davison v. *Nova Scotia Safety Association*, 2005 NSHRC 4	La salariée se plaint de harcèlement sexuel constant,	Facteurs aggravants pour l'employeur : carence de l'employeur à		Condamnation à des dommages-intérêts d'un

Décisions jurisprudentielles relatives à l'usage abusif de l'Internet et de la messagerie électronique et mesures appliquées				
Nom des parties	**Manquements de l'employé**	**Facteurs aggravants**	**Facteurs atténuants**	**Décision du Tribunal**
(CanLII)	notamment de la part de son supérieur hiérarchique qui fait incessamment des blagues et allégations à connotation sexuelle en sa présence et celles d'autres employés; la salariée le surprend une fois en train de visionner une photo de femme nue qu'il imprime et distribue, devant la plaignante, à des collègues.	prendre les mesures appropriées pour mettre fin à la situation dénoncée; actes de représailles de la part des membres du comité de direction envers l'employée qui est finalement congédiée.		montant total de 13 000 $ pour l'employeur et les directeurs, plus 7 000 $ de dommages exemplaires pour l'employeur.
Di Vito v. *MacDonald Dettwiler and Associates*, 1996 CanLII 3165 (BC S.C.)	Utilisation des outils de l'employeur pour télécharger, stocker, et distribuer du matériel à caractère sexuel	Refus répété d'admettre les faits.		Congédiement confirmé.
Dosanjh c. *Conseil du Trésor*, 2003 CRTFP 16 (CanLII)	Accès au compte d'utilisateur d'un collègue ayant oublié de se déconnecter; destruction de fichiers; transfert de fichiers sur sa messagerie électronique personnelle.	Réprimande écrite et une amende de 90 $ déjà inscrites au dossier.	51 ans; 27 ans d'ancienneté; plusieurs citations, dont une pour bravoure; incident isolé; actes accomplis sous le coup de l'impulsion; aucune preuve de profit pour le salarié.	Suspension de trois mois substituée au congédiement.
Dufresne c.	Intimidation et	Existence d'une	Absence de	Congédiement

Décisions jurisprudentielles relatives à l'usage abusif de l'Internet et de la messagerie électronique et mesures appliquées				
Nom des parties	**Manquements de l'employé**	**Facteurs aggravants**	**Facteurs atténuants**	**Décision du Tribunal**
Pratt & Whitney Canada Inc., D.T.E. 94T-405 (C.T.)	harcèlement de collègues *via* la messagerie; échange de contenus érotiques avec 2 employées avec lesquelles l'employé a une liaison amoureuse.	plainte antérieure pour harcèlement sexuel, qui a donné lieu à un rappel des règles en la matière.	contenus de nature sexuelle dans les messages envoyés à la plaignante	est annulé.
EV Logistics v. *Retail Wholesale Union, Local 580* (Discharge Grievance), [2008] B.C.C.A.A.A. No. 22 (Coll. Agr. Arb.) (QL/LN)	Exploitation d'un blogue contenant des propos racistes; le site fait référence à l'employeur qui est clairement identifié.		Ni l'employeur (ou ses produits) ni les clients ni même un salarié en particulier ne sont visés directement; dossier vierge; remords exprimés dans une lettre d'excuses.	Congédiement annulé; période entre la date du congédiement et la réintégration transformée en suspension disciplinaire.
Fiset c. *Service d'administration P.C.R. Ltée*, D.T.E. 2003T-41 (C.R.T.), conf. par *Services d'administration P.C.R. Ltée* c. *Daigle*, D.T.E. 2003T-177 (C.S.)	Utilisation du matériel informatique de l'employeur à des fins personnelles; entretien d'une liaison amoureuse virtuelle durant les heures de travail.	Mensonges et refus du salarié d'admettre les faits; réprimandes antérieures à la suite d'une utilisation abusive des appels interurbains dont le salarié avait dû rembourser le coût.	Absence de directives d'utilisation claires de l'Internet; laxisme de l'employeur quant à l'usage personnel; absence de preuve d'un impact négatif sur la prestation de travail du salarié ou de préjudice subi par l'employeur.	Congédiement annulé.
Ghattas c. *École nationale de théâtre du Canada*, EYB 2006-102226	Utilisation de l'ordinateur de l'employeur pour rédiger et transmettre, par	Existence d'une politique interdisant tout usage personnel des outils de communication;		Rejet de la demande de dommages moraux pour atteinte à la vie

Décisions jurisprudentielles relatives à l'usage abusif de l'Internet et de la messagerie électronique et mesures appliquées				
Nom des parties	**Manquements de l'employé**	**Facteurs aggravants**	**Facteurs atténuants**	**Décision du Tribunal**
(C.S.)	courriel, à des tiers, des brouillons d'une lettre qu'elle s'apprête à remettre à son supérieur à la suite d'une réprimande pour insubordination.	la salariée était en vacances lors de l'adoption de cette politique, cependant, sa fonction lui commandait de s'informer sur les dossiers traités en son absence, ce qu'elle a omis de faire.		privée de la salariée, après l'accès, à son insu, de l'employeur à son ordinateur.
Gilles et *Ciba Spécialités chimiques Canada Inc.,* 2008 QCCRT 134 (CanLII)	Téléchargement et stockage de matériel à caractère pornographique sur l'ordinateur portable remis par l'employeur aux fins du travail.	Interdiction claire de tels contenus par la politique; étalement des faits dans le temps (9 ans); conséquences potentiellement très graves pour le système d'information de l'entreprise qui compte 19 000 salariés à travers le monde.	9 ans d'ancienneté; dossier vierge; aucune réprimande ou remarque antérieure de l'employeur quant à l'usage de l'ordinateur par le salarié; non-respect par l'employeur de la procédure de licenciement prévue dans la politique de l'entreprise.	Suspension de 3 mois substituée au congédiement.
Inform Cycle Ltd. v. *Rebound Inc.*, 2007 ABQB 319 (CanLII)	Utilisation de la connexion Internet de l'employeur pour enregistrer le nom de l'ex-employeur comme nom de domaine; site ensuite redirigé vers un site de pornographie homosexuelle.	Absence de politique relative à l'utilisation d'Internet; grande autonomie accordée au salarié; fermeture du site litigieux uniquement cinq jours après le signalement des faits.		Rejet de l'action en responsabilité de l'ex-employeur contre le nouvel employeur : le salarié agissait pour son propre compte et dans son seul intérêt.

Décisions jurisprudentielles relatives à l'usage abusif de l'Internet et de la messagerie électronique et mesures appliquées				
Nom des parties	**Manquements de l'employé**	**Facteurs aggravants**	**Facteurs atténuants**	**Décision du Tribunal**
International Association of Bridge, Local Union No. 97, and Structural and Ornamental Ironworkers (the "Employer") and *Office and Technical Employees' Union, Local 15 (the "Union")*, [1997] B.C.C.A.A.A. No. 630 (Coll. Agr. Arb.) (QL/LN)	Utilisation du téléphone et de l'ordinateur de l'employeur à des fins personnelles durant les heures de travail; transmission, sans autorisation, et à l'insu de sa hiérarchie, d'informations à des tiers (cette tâche fait partie des attributions d'un autre salarié); suppression des courriels et fichiers relatifs à ces échanges du disque dur.	Violation des règles de confidentialité de la politique d'entreprise; politique claire de l'employeur imposant aux salariés de ne pas outrepasser leurs attributions et d'informer en tout temps leur hiérarchie sur leurs activités; deux avertissements pour usage à des fins personnelles des outils de l'employeur et insubordination figurent déjà au dossier.	Absence de remords et refus de l'employée d'assumer sa responsabilité.	Suspension de 15 jours maintenue.
Lemay c. *Dubois*, 2005 CanLII 15315 (QC C.Q.)	Communication, sur le babillard public d'un site Internet, de la date de diffusion d'un reportage sur l'entreprise, en même temps que d'informations jugées de nature privée par la plaignante; ces informations ont été postées grâce au matériel informatique de l'employeur.			Rejet de la responsabilité de l'employeur : l'employée n'a pas respecté les directives patronales et n'a pas agi dans l'intérêt de l'employeur.
Martel c. *Fédération des caisses Desjardins du*	454 courriels personnels envoyés et 616 reçus en à peine	Salarié en période d'essai; existence d'un règlement d'entreprise		Congédiement confirmé.

Décisions jurisprudentielles relatives à l'usage abusif de l'Internet et de la messagerie électronique et mesures appliquées				
Nom des parties	**Manquements de l'employé**	**Facteurs aggravants**	**Facteurs atténuants**	**Décision du Tribunal**
Québec, 2006 QCCRT 300 (CanLII)	un mois.	interdisant clairement l'usage à des fins personnelles; le salarié nie les faits, minimise sa responsabilité et tente de dissimuler les actes en supprimant les courriels.		
Montour Limitée c. *Syndicat des employé-e-s de la Cie Montour (CSN)*, 2006 IIJCan 43801 (QC A.G.)	Participation à un forum de discussion où l'employé se vante de jouer aux cartes pendant son quart de travail et de ne pas « travailler très fort », tout en étant bien payé; le nom de l'employeur est indiqué; les écrits ont été postés 2 ans plus tôt.	Entreprise spécialisée dans la fabrication de produits alimentaires où le respect de normes élevées de qualité est crucial; elle bénéficie d'une certification internationale dans ce domaine qu'elle souhaite conserver; l'employé est préposé au lavage et a suivi une formation de sensibilisation sur les exigences en matière d'hygiène.		Congédiement confirmé.
Ordre des infirmières et infirmiers du Québec c. *Léveillé*, 2008 CanLII 47548 (QC C.D.O.I.I.)	L'employé consulte des sites pornographiques sur le lieu de travail et se livre à des actes de grossière indécence devant l'écran.	Infirmier travaillant de nuit dans un centre d'hébergement pour personnes malades et âgées; actes accomplis à chaque quart de travail; étalement des faits sur 2 ans; actes se déroulant devant un		Radiation du Tableau de l'Ordre des infirmiers du Québec pour un an (sanction suspendue et exécutoire uniquement lors de la réinscription

Décisions jurisprudentielles relatives à l'usage abusif de l'Internet et de la messagerie électronique et mesures appliquées				
Nom des parties	**Manquements de l'employé**	**Facteurs aggravants**	**Facteurs atténuants**	**Décision du Tribunal**
		ordinateur situé dans une aire ouverte et passante où le risque d'être surpris est élevé; refus d'admettre les et réticence à admettre sa responsabilité et la gravité des actes; le salarié ne fait l'objet d'aucun suivi.		de l'employé au Tableau.
Persechino c. *Flint Ink North America Corporation*, 2007 QCCRT 354 (CanLII)	Harcèlement sexuel consistant, notamment, en l'envoi de messages électroniques à connotation sexuelle à une employée.	Le salarié est cadre (il est « le grand patron au Québec ») et la victime travaille sous sa supervision. Le salarié nie les faits et minimise ses actes.		Congédiement confirmé.
Poliquin v. *Devon Canada Corporation*, 2009 ABCA 216 (CanLII)	Réception et distribution de messages à caractère sexuel, pornographique ou raciste pendant les heures de travail; les expéditeurs et destinataires des contenus sont des collègues, ainsi que des fournisseurs et contacts d'affaires de l'employeur.	Existence d'une politique d'entreprise interdisant de tels contenus; cadre sénior; 23 ans d'ancienneté; le salarié admet sa faute, mais en minimise les conséquences.		Congédiement maintenu.
Potvin c. *Ville de Malartic*, REJB 2003-46527 (C.S.)	Mauvaise gestion du club de golf municipal sous la responsabilité du salarié; usage	Le salarié n'utilise jamais son ordinateur aux fins pour lesquelles il a été fourni	D'autres personnes ont accès à l'ordinateur et ont pu effectuer les	Congédiement maintenu.

Décisions jurisprudentielles relatives à l'usage abusif de l'Internet et de la messagerie électronique et mesures appliquées				
Nom des parties	**Manquements de l'employé**	**Facteurs aggravants**	**Facteurs atténuants**	**Décision du Tribunal**
	inapproprié de son ordinateur professionnel, notamment pour des "clavardages" de nature sexuelle; téléchargement et stockage de plus de 170 photographies à caractère sexuel et pornographique sur le disque dur.	(communiquer avec ses collègues éloignés géographiquement) ; il nie les faits, alors que les preuves établissent qu'il est bien l'auteur des « clavardages »; il n'a rien fait pour mettre fin aux téléchargements, alors qu'il en avait forcément connaissance, ni pour détruire les fichiers compromettants.	téléchargements.	
R. c. *Crevier*, EYB 2006-113697 (C.Q.)	Utilisation du courriel pour effectuer une commande d'ordinateurs qui sont ensuite détournés au profit de l'entreprise du conjoint de la salariée; la commande a été passée depuis la messagerie de cette dernière qui nie cependant en être l'auteur.			Maintien des accusations de vol et de fabrication et usage de faux documents : des échanges, notamment téléphoniques, ont été faits pour confirmer la commande.
R. c. *Tremblay*, REJB 2001-23521 (C.Q.); REJB 2001-25375 (C.Q.)	Navigation sur des sites de pornographie juvénile et téléchargement de matériel de la même nature sur	Mensonges du salarié sur sa prétendue participation à une enquête de police sur la pornographie juvénile justifiant		Maintien des accusations de détention de pornographie juvénile.

Décisions jurisprudentielles relatives à l'usage abusif de l'Internet et de la messagerie électronique et mesures appliquées				
Nom des parties	**Manquements de l'employé**	**Facteurs aggravants**	**Facteurs atténuants**	**Décision du Tribunal**
	le disque dur de l'ordinateur du salarié; le salarié occupe son poste de travail à 97%.	ses activités; le salarié laisse d'autres employés utiliser son poste de travail.		
Syndicat canadien des communications , de l'énergie et du papier, section locale 522 c. *CAE Électronique Ltée*, REJB 2000-16857 (T.A.)	Utilisation excessive de l'Internet (329 heures sur une période de cinq mois); navigation essentiellement sur des sites pornographiques; le salarié déclare parallèlement plus de 466 heures supplémentaires sur la même période.	Demande de paiement d'heures supplémentaires; cadre autonome; 14 ans d'ancienneté; existence d'une politique Internet claire; l'usage de l'Internet est un privilège réservé à certains employés, sous certaines conditions; le salarié nie et tente de minimiser ses actes.		Congédiement confirmé.
Syndicat des cols bleus regroupés de Montréal (SCFP), section locale 301 (S.C.F.P.) et *La Ronde (Six Flags)*, D.T.E. 2004T-1124 (T.A.)	Navigation sur des sites pornographiques pendant les pauses et les heures de travail.	Aggravation liée à la nature des activités de l'entreprise (un parc d'attractions à caractère familial); création d'un risque de contamination du système informatique interne et international de l'entreprise.	Aucune perte occasionnée ni d'impact sur le travail du salarié (agent de sécurité dont les attributions consistent à effectuer des rondes et veiller à la sécurité des bâtiments).	Congédiement annulé et remplacé par une suspension dont la durée est à déterminer par les parties ou, à défaut, par le Tribunal.
Syndicat des employés municipaux de Beloeil (SCFP) et *Beloeil (Ville de)*, D.T.E. 2007T-874 (T.A.)	Navigation sur Internet à raison de 3 heures par jour (soit 40% du temps de travail du salarié), à des fins essentiellement personnelles.	La politique d'entreprise accorde des permissions, mais le salarié a dépassé les limites; refus d'admettre les faits et sa responsabilité; tentative de		Congédiement sans progression des sanctions confirmé.

Décisions jurisprudentielles relatives à l'usage abusif de l'Internet et de la messagerie électronique et mesures appliquées				
Nom des parties	**Manquements de l'employé**	**Facteurs aggravants**	**Facteurs atténuants**	**Décision du Tribunal**
		dissimulation des gestes en débranchant un dispositif installé la veille sur son ordinateur afin de permettre à l'employeur de suivre ses activités sur Internet		
Syndicat des fonctionnaires municipaux de Montréal (S.C.F.P.) c. *Ville de Montréal*, D.T.E. 99T-478 (T.A.)	Utilisation des équipements de l'employeur à des fins personnelles, notamment pour naviguer sur Internet pendant les heures de travail.	Baisse appréciable de la productivité de l'employé.	Absence de politique sur l'usage de l'Internet.	Suspension de dix jours confirmée.
Syndicat des spécialistes et professionnels d'Hydro-Québec c. *Hydro-Québec*, 2003 CanLII 20475 (QC A.G.)	Navigation sur des sites à caractère sexuel et pornographique; distribution de tels contenus par courriel au sein de l'entreprise et à des tiers en dehors; utilisation de l'adresse électronique de l'employeur, ainsi que le numéro de pagette, pour promouvoir sa propre entreprise et solliciter des clients pour son propre compte.	Existence d'une politique claire et largement diffusée au sein de l'entreprise; aggravation liée à la fonction de spécialiste en informatique (Analyste support informatique) bénéficiant d'une grande autonomie; faible ancienneté (4 ans); réticence à admettre les faits et refus de collaborer durant l'enquête de l'employeur.	Dossier disciplinaire vierge.	Congédiement maintenu.
Syndicat des spécialistes et professionnels d'Hydro-	Utilisation du réseau informatique de l'employeur pour	Existence d'une politique d'entreprise claire; destruction de	L'employé admet la plupart des faits qui lui sont reprochés; pas	Suspension de 9 mois substituée au congédiement.

Décisions jurisprudentielles relatives à l'usage abusif de l'Internet et de la messagerie électronique et mesures appliquées				
Nom des parties	**Manquements de l'employé**	**Facteurs aggravants**	**Facteurs atténuants**	**Décision du Tribunal**
Québec, (SCFP-FTQ, section locale 4250) c. *Hydro-Québec*, 2007 CanLII 20291 (QC A.G.)	effectuer des travaux au profit d'une association à but non lucratif; installation, sans autorisation, d'un logiciel permettant l'accès direct au site Internet de l'association depuis le poste de travail du salarié.	fichiers sur son poste de travail, sous le coup de la frustration, après avoir subi une entrevue de nature disciplinaire de 2 heures relativement à son utilisation des ressources informatiques.	d'impact négatif sur l'image de l'entreprise; absence de supervision adéquate; le salarié est souvent désœuvré et dispose de beaucoup de temps libre.	
Syndicat des travailleuses et travailleurs de Resto-Casino de Hull (F.E.E.S.P.-C.S.N.) (section Hilton Lac Leamy) et *Hilton Lac Leamy*, D.T.E. 2004T-811 (T.A.)	Menaces à caractère sexuel proférées envers une collègue dans le cadre de séances de « clavardages » privées effectuées en dehors des heures de travail et hors des locaux de l'entreprise.	Le salarié agresse également physiquement et verbalement sa collègue sur les lieux de travail, allant même jusqu'à la menacer de mort		Congédiement confirmé. (L'intrusion de l'employeur dans ce conflit privé est justifiée, en raison des agressions qui se sont déroulées sur le lieu de travail.)
Syndicat du personnel de soutien de la Seigneurie des Mille-Îles (CSN) et *Commission scolaire de la Seigneurie des Mille-Îles*, D.T.E. 2008T-149 (T.A.)	Téléchargement, à partir des ordinateurs de l'employeur, d'une centaine de vidéos de nature pornographique (adulte et juvénile) contenant parfois des scènes de bestialité; surveillance non autorisée d'un collègue au moyen d'une webcaméra.	Mensonges et réponses délibérément évasives; tentative de dissimuler les faits en effaçant les traces des activités reprochées dans l'historique de navigation.	Le salarié vit une situation difficile en raison de la maladie de son fils. (L'arbitre ne tient pas compte de ce facteur qu'il juge sans lien avec les fautes de l'employé).	Congédiement confirmé.