La cybersurveillance sur les lieux de travail

Montero, Etienne

Published in:
Droits et obligations du travailleur en droit congolais

Publication date:
2003

Document Version
le PDF de l'éditeur

La cybersurveillance sur les lieux de travail

Etienne Montero*

Propos liminaires

Dans l'entreprise, les employés (tout comme les fonctionnaires au sein des administrations publiques) utilisent de plus en plus couramment les technologies de l'information : en particulier, le courrier électronique, pour communiquer au sein de l'entreprise ou avec l'extérieur, et l'Internet, pour consulter des sites *web* en quête d'informations de toute nature ou pour participer à des forums de discussion.

Ces outils de communication modernes peuvent être utilisés non seulement à des fins professionnelles, mais également à des fins privées ou récréatives.

Ainsi, au départ de son ordinateur, un employé pourra prendre part à un forum de discussion pour défendre la politique de son entreprise, mais aussi pour un échange de points de vue avec d'autres internautes à propos d'un thème à caractère privé qui leur tient à cœur. Il pourra pareillement adresser des *e-mails* à ses collègues sur des questions de travail, mais aussi à ses amis ou à des membres de sa famille pour des échanges à caractère privé. Enfin, il pourra surfer sur le *net* pour y recueillir des données de nature [non seulement] professionnelle, mais aussi à des fins strictement personnelles (réservation d'un lieu de vacances, recherche bibliographique pour le travail d'un enfant, recherche d'informations sur des biens de consommation privés...).

* Professeur aux Facultés Universitaires Notre-Dame de la Paix à Namur et à la Faculté de droit de l'Université catholique de Louvain, membre de l'Observatoire des droits de l'Internet (organisme consultatif installé près le ministère des Affaires économiques) et Directeur de la collection des Cahiers du CRID (Centre de Recherches Informatique et droit).

De son côté, l'employeur entend mettre ces technologies à la disposition de ses employés aux fins d'amélioration de leur rendement et, partant, de la rentabilité et des performances de l'entreprise. Il s'opposera à un usage privé abusif, qui pourrait dégénérer en des pertes de temps et d'énergie intolérables, et nuire à la prospérité de l'entreprise. Il sera également attentif à ce que les moyens de communication mis à la disposition de ses employés ne soient pas utilisés par l'un d'eux à des fins « honteuses » ou pour communiquer à l'extérieur des informations confidentielles ou préjudiciables à l'entreprise. A cet égard, il aura, en particulier, le souci légitime de se mettre à l'abri d'éventuelles mises en cause de sa responsabilité, pénale ou civile, du fait d'une utilisation de l'Internet ou du courrier électronique par l'un de ses travailleurs à des fins illicites (postage de messages à caractère raciste, violent ou pornographique...dans des groupes de discussion, téléchargement d'images à caractère pédophile, diffusion malveillante de virus, faits de *hacking*, violation d'un accord de confidentialité, etc.).

C'est dans ce contexte que se généralisent les techniques de surveillance de l'usage de l'Internet et du courrier électronique au sein des entreprises. Si les technologies représentent un facteur de risques pour l'entreprise, elles facilitent aussi les contrôles de la part de l'employeur. On observe, en Amérique du Nord et en Europe, une tendance de plus en plus marquée des entreprises à utiliser des moyens électroniques pour contrôler l'usage que les employés font de l'Internet et du courrier électronique.

Il ne fait pas de doute que l'usage des moyens de communication peut se révéler abusif dans le chef des employés, et préjudiciable pour l'entreprise. Mais, à l'inverse, il saute aux yeux que les formes nouvelles de contrôle que les technologies induisent et facilitent peuvent pareillement donner lieu à des abus de la part des employeurs. On recense, d'ores et déjà, par dizaines, les cas de licenciement d'employés au motif qu'ils ont été surpris en train de consulter des sites pornographiques pendant les heures de bureau, ou que l'on a découvert sur le disque dur de leur ordinateur des *e-mails* estimés diffamatoires pour l'entreprise.

Les moyens de contrôle électroniques dont disposent les entreprises sont diversifiés[1]. Certaines entreprises utilisent des logiciels de filtrage permettant de bloquer l'accès aux sites « indésirables ». D'autres suivent une politique de surveillance plus ou moins étroite des sites consultés. A cet égard, les techniques sont multiples. La plus simple consiste à opérer des vérifications aléatoires sur la machine du travailleur, dès lors que le navigateur installé sur celle-ci conserve automatiquement en mémoire les derniers sites visités. Certains employeurs font usage de logiciels spécifiques (tel « *Little Brother* ») qui scrutent les connexions des employés à l'Internet (sites visités, temps de consultation, types de fichiers téléchargés...). D'autres procèdent à l'enregistrement et à la conservation temporaire, sur le serveur central de l'entreprise, des pages *web* consultées.

Pareils contrôles sont également possibles en ce qui concerne le courrier électronique, qu'ils interviennent au niveau du serveur de l'entreprise ou de la machine de l'employé.

Ces considérations conduisent à s'interroger sur la légitimité et les limites du contrôle par l'employeur de l'utilisation privée de l'Internet et du courrier électronique sur le lieu de travail. Avant d'envisager les principes d'une bonne politique juridique en la matière, visant à l'équilibre entre les droits et intérêts des deux parties (II.), il convient de prendre la mesure exacte de leurs droits et intérêts respectifs (I.).

I. Un "apparent" conflit d'intérêts

Il est clair que, selon le point de vue adopté – celui de l'employé ou de l'employeur –, les valeurs mises en avant s'inscriront dans des ordres de préoccupations de signe opposé.

[1] A ce sujet, voy. Th. VERBIEST, « La surveillance de l'usage de l'internet dans l'entreprise : quelle légalité ?, *L'Echo*, 20 janvier 2000.

D'une part, en effet, le travailleur doit exécuter son travail conformément aux ordres et instructions de l'employeur, avec soin, intégrité et compétence, au lieu, dans les temps et aux conditions convenus. Il en résulte que l'employeur peut légitimement s'attendre à ce que, pendant les heures où il est à son service en échange d'une rémunération, son employé consacre ses meilleures énergies à son travail. Il escompte aussi que les moyens de communication mis à sa disposition, aux frais de l'employeur, soient utilisés dans un cadre professionnel, à l'exclusion de tout détournement à des fins privées ou récréatives.

D'autre part, l'employé conserve, sur son lieu de travail, des droits inaliénables, inhérents à sa condition de personne, et qu'il appartient à l'employeur de respecter. Parmi ces droits, on mentionne le droit à la vie privée, à l'intégrité physique, à l'honneur... Qui ne voit que des mesures de contrôle excessives pourraient mener à un énervement de ces droits fondamentaux ?

Comment concilier ces points de vue apparemment antagonistes ? Pour répondre à cette question, il apparaît nécessaire d'affiner l'analyse, en se plaçant tantôt du côté du travailleur, tantôt du côté de l'employeur. Dans la conception et la mise en œuvre d'un régime juridique approprié, l'idéal est évidemment, *in fine*, de trouver le juste point d'équilibre où les droits et intérêts des deux parties se trouvent préservés dans une égale mesure.

A. Côté travailleur – un droit à la vie privée

La Déclaration universelle des droits de l'homme dispose, en son article 12, que « Nul ne sera l'objet d'immixtions arbitraires dans *sa vie privée*, sa famille, son domicile ou *sa correspondance* [...] ». Le Pacte international relatif aux droits civils et politiques, fait à New York le 19 décembre 1966, contient une disposition similaire (art. 17). Le droit au respect de la vie privée et de la correspondance est également consacré par d'autres conventions internationales, parmi lesquelles la plus illustre est la Convention de sauvegarde des droits de l'homme et des libertés fondamentales, signée à Rome le 4 novembre 1950 (art. 8). Dans de

nombreux Etats de par le monde, ce droit est encore confirmé et précisé par des dispositions constitutionnelles, légales et réglementaires. En particulier, la plupart des Etats occidentaux se sont dotés d'une législation tatillonne relative à la protection de la vie privée à l'égard des traitements automatisés des données à caractère personnel.

Il est incontestable que le travailleur continue de bénéficier, sur le lieu de travail, d'une sphère d'autonomie, et du régime de protection de la vie privée mis en place. En d'autres termes, la situation de subordination n'entraîne aucune renonciation de principe à son droit à la vie privée. Le travailleur n'est nullement sommé de mettre sa vie privée au vestiaire dès l'instant où il pénètre dans son lieu de travail. Des espaces de vie privée doivent lui être ménagés tant il est vrai, d'une part, qu'il demeure un être privé sur son lieu de travail, avec une part d'intimité que l'on ne saurait ignorer et bafouer, d'autre part, que le travail remplit une fonction sociale singulière au sens où celui-ci représente un espace-temps dans lequel se tissent, pour une bonne part, les liens humains.

Dans et à travers leurs occupations professionnelles, les hommes et les femmes trouvent une occasion irremplaçable de se rencontrer et de s'estimer, même si leurs relations s'épanouiront et s'approfondiront naturellement en dehors de celles-ci. A cet égard, dans l'affaire Niemitz c. Allemagne, la Cour européenne des droits de l'homme s'est exprimée en des termes particulièrement heureux :

> *« Le respect de la vie privée doit aussi englober, dans une certaine mesure, le droit pour l'individu de nouer et de développer des relations avec ses semblables. Il paraît en outre n'y avoir aucune raison de principe de considérer cette manière de comprendre la notion de 'vie privée' comme excluant les activités professionnelles ou commerciales : après tout, c'est dans leur travail que la majorité des gens ont beaucoup, voire le maximum d'occasions, de resserrer leurs liens avec le monde extérieur. Un fait, souligné par la Commission le confirme, dans les occupations de quelqu'un, on ne peut pas toujours démêler ce qui relève du domaine professionnel de ce qui en sort »*[2].

[2] Arrêt du 16 déc. 1992, *Recueil*, série A, n° 251/B, par. 30 ; *J.T.T.*, 1994, p. 65, également disponible sur Internet (www.echr.coe.int).

Cette décision de principe est sans doute d'une application plus délicate à l'heure des technologies de l'information. Néanmoins, le précédent du téléphone constitue un premier jalon permettant de penser la protection des travailleurs à l'égard des techniques de surveillance électroniques. Ainsi, la Cour des droits de l'homme a-t-elle qualifié expressément d'ingérence dans la vie privée les écoutes téléphoniques de communications commerciales. Cette jurisprudence a été confirmée dans l'affaire Halford c. Royaume-Uni :

> *« (...) les appels téléphoniques émanant de locaux professionnels, tout comme ceux provenant du domicile, peuvent se trouver compris dans les notions de 'vie privée' et de 'correspondance privée' visées à l'article 8, § 1er [de la Convention européenne des droits de l'hommes] ».*

Dans un arrêt du 10 avril 1990, la Cour de cassation de Belgique a eu l'occasion de poser un principe analogue[3].

Il est clair que l'on ne saurait exclure tout usage du téléphone à des fins privées dès lors que les heures d'ouverture de nombreux services coïncident avec les heures de bureau des intéressés : comment éviter l'utilisation du téléphone, pendant les heures de travail, pour prendre contact avec son dentiste ou son garagiste, ou encore pour convenir avec sa femme du moment de rendez-vous pour regagner ensemble le lieu de résidence ? Et comment frustrer les travailleurs dans leur besoin de s'échanger, au cours du travail, des messages à caractère personnel, sans rapport direct avec les dossiers du moment ? Qui ne voit que la teneur de l'ensemble des communications est soit d'ordre essentiellement privé, soit d'ordre professionnel, mais où se mêlent inévitablement des considérations à caractère privé ?

En clair et en substance, il y a lieu de tenir que « toutes les communications passées par un travailleur, depuis l'entreprise, sont des communications privées (...) et, à ce titre, il est interdit à l'employeur d'écouter ces communications et de les enregistrer, sauf si son travailleur l'y autorise » (Ballarin, 1997, 24). Plus précisément, on s'avisera d'un paradoxe : l'employeur ne peut prendre connaissance du contenu des

[3] Cass., 10 avril 1990, *Pas.*, 1990, p. 932.

courriers privés (droit au secret de la correspondance), mais comment faire le départ entre ces derniers et les communications professionnelles, si ce n'est en lisant les messages ? Seules les parties à la communication ont le droit de déterminer son caractère privé ou public. Mais alors, la porte est ouverte aux comportements illicites sous le couvert de « communications privées ». On aura l'occasion de revenir sur cette difficulté.

B. Côté employeur – un droit au contrôle

On ne saurait ignorer les inconvénients que l'utilisation privée de l'Internet et du courrier électronique fait courir aux entreprises.

Une série de vicissitudes d'ordre purement factuel viennent spontanément à l'esprit. Le *surf*, le téléchargement fréquent de fichiers et la réception d'*e-mails* accroissent le risque d'infection du système informatique par des virus, avec leur cortège de désagréments (destruction de dossiers informatisés, paralysie du système informatique, etc.). L'envoi de messages volumineux et le téléchargement de gros fichiers peuvent entraîner une saturation du réseau et un ralentissement, sinon la paralysie, des communications professionnelles. Outre les pertes de temps, liées à une utilisation excessive des moyens de communication à des fins étrangères aux occupations professionnelles, on songe aussi aux risques de nuisances portées à l'image et à la bonne réputation de l'entreprise et, bien sûr, à l'augmentation des coûts à charge de celle-ci.

Les risques juridiques liés à une mise en cause de la responsabilité des employeurs, au titre de commettants, du fait (fautif) de leurs préposés inquiètent également les premiers. Si ce risque n'est pas nouveau, il s'accroît néanmoins à mesure de l'augmentation du volume des communications électroniques. A cet égard, on se borne à évoquer la phobie des employeurs en ce qui concerne l'utilisation du courrier électronique à des fins de harcèlement sexuel ou de diffusion d'images à caractère pornographique. A juste titre, les entreprises s'inquiètent de voir engagée leur responsabilité pour ne pas avoir fait diligence en vue d'empêcher ce genre de pratiques.

La responsabilité de l'employeur pour une faute commise par un employé dans l'exercice de ses fonctions peut encore être engagée dans d'autres hypothèses multiples : communication de renseignements erronés à l'origine d'un préjudice commercial ou financier pour leur destinataire, transmission d'un virus par *e-mail*, propos diffamatoires tenus dans un groupe de discussions ou diffusés *via* l'adresse *e-mail* professionnelle, etc.

Selon la jurisprudence (belge à tout le moins), cette responsabilité pourra d'autant plus facilement être mise en œuvre qu'il n'est pas nécessaire que l'acte illicite commis par le préposé rentre dans les fonctions assignées à celui-ci : il suffit qu'il ait été accompli *pendant la durée du service* et qu'il soit en relation avec celui-ci, fût-ce indirectement ou occasionnellement[4].

Ces risques et responsabilités impliquent un certain droit-devoir de regard et de contrôle par l'employeur sur l'utilisation des outils de communication mis à la disposition des employés. Les législations sur le contrat de travail prévoient d'ordinaire, d'une façon générale, un pouvoir de contrôle de l'employeur. Celui-ci se trouve enserré, on l'aura compris, dans les limites tracées par le droit à la vie privée reconnu à toute personne.

Selon quels critères peut-on conjuguer, au quotidien et très concrètement, ces deux valeurs de signe apparemment contraire ? C'est ce qu'il convient à présent d'examiner.

II. Principes de politique juridique

Il nous apparaît que toute bonne politique juridique en la matière devrait être guidée par quatre principes fondamentaux : les principes de transparence, de légalité, de finalité et de proportionnalité. Nous les commentons tour à tour.

[4] Cass., 19 juin 1986, *Pas.*, 1986, p. 1296.

A. Principe de transparence

Il importe tout d'abord que les travailleurs soient informés, non pas nécessairement du contrôle proprement dit, mais de l'existence ou de la possibilité d'un contrôle et, plus généralement, des caractéristiques et modalités de la politique de contrôle de l'employeur. A cet égard, un dialogue doit se nouer avec le personnel ou ses représentants. Il est préférable, en outre, que le travailleur ait eu l'occasion de marquer son accord. Cette information visera notamment :

- les modalités d'utilisation du courrier électronique et de l'Internet qui sont conseillées, permises, tolérées ou interdites ;
- les finalités et modalités du contrôle de cette utilisation (nature des données recueillies, étendue et circonstances des contrôles, personnes ou catégories de personnes assujetties aux procédures de contrôle) ;
- l'existence d'un enregistrement des données de communication et la durée de conservation de ces données, par exemple sur un serveur central ;
- la nature des décisions pouvant être prises par l'employeur à l'égard de l'employé (sanctions disciplinaires : de l'avertissement au licenciement, en passant par le blâme...) et les critères justifiant pareilles décisions (faute lourde, faute légère habituelle, seuil de fréquence des transgressions ou des volumes...) ;
- le droit d'accès de l'employé aux données à caractère personnel le concernant.

On souligne l'intérêt que ces divers éléments d'information soient repris dans une sorte de « charte des bons usages » des technologies de l'information dans l'entreprise, et que cette charte soit portée à la connaissance des employés, idéalement au moment de leur engagement. En toute hypothèse, on veillera à mettre en œuvre les moyens appropriés pour que les employés connaissent cette charte ou aient au moins la possibilité d'en prendre connaissance (affichage sur les murs ou sur les écrans d'ordinateur, annexe au contrat de travail...).

B. Principe de légalité

Le contrôle réalisé par l'employeur de l'utilisation que font les travailleurs des moyens de communication sur les lieux de travail suppose une forme d'ingérence dans la vie privée de ces derniers. Or, on considère généralement qu'une telle ingérence doit être prévue par une loi. Cependant, selon la jurisprudence de la Cour européenne des droits de l'homme, ni une loi formelle, ni même une loi matérielle n'est requise. Il suffit que la restriction apportée à la vie privée soit prévue par une règle *claire, précise* et *aisément accessible au travailleur*, de sorte qu'il puisse prévoir les possibles suites attachées au contrôle et adapter son comportement en conséquence. Un règlement de travail, une simple fiche d'instructions ou charte des bons usages peut satisfaire à cette condition.

Encore faut-il que les règles édictées soient claires et précises (à cet égard, aux principes vagues, à caractère trop général, on préférera des dispositions concrètes visant des hypothèses bien déterminées), et aisément accessibles (on évitera que les règles figurent dans des dispositions statutaires ou autres textes largement méconnus : si elles figurent dans ce genre de documents, elles seront avantageusement reprises dans des documents directement accessibles aux travailleurs).

C. Principe de finalité

En aucun cas, l'ingérence dans la vie privée ne peut constituer un but en soi. Pour pouvoir instituer un contrôle, l'employeur doit poursuivre un but précis. A cet égard, il doit décliner les valeurs jugées plus essentielles qu'il entend protéger : ainsi, la prévention des infractions pénales (afin d'éviter que la responsabilité pénale de l'employeur soit mise en cause pour diffamation, pornographie, pédophilie, vol, espionnage industriel...), la protection de la morale ou des droits et libertés d'autrui (le droit de propriété de l'employeur, sa bonne réputation, les droits des tiers...).

En outre, la surveillance exercée doit être adéquate, pertinente et non excessive au regard de la finalité assignée au contrôle.

D. Principe de proportionnalité

Enfin, il est requis que les moyens et mesures choisis pour exercer le contrôle représentent l'ingérence la plus petite possible dans la vie privée du travailleur. Autrement dit, le moyen utilisé perd sa légitimité si des moyens moins nuisibles permettent d'atteindre le même objectif de protection. Il s'agit d'opter pour la solution qui limite le plus possible l'atteinte à la vie privée.

Ainsi, on ne conçoit pas un contrôle général et *a priori* des communications, ni un enregistrement systématique et permanent de l'ensemble des données. On préférera un contrôle ponctuel et fondé sur des indices ou des soupçons d'une utilisation abusive ou malveillante. Par exemple, le contrôle se justifie aisément si un travailleur accuse des retards très importants dans l'accomplissement de ses prestations ou en cas d'engorgement anormal du réseau entravant les communications dans l'entreprise, etc. Cela étant, il existe aussi différentes solutions techniques permettant de cibler des courriers suspects. On songe à des logiciels qui identifient l'expédition de courriers électroniques en chaîne ou qui bloquent des courriers électroniques de nature à provoquer un ralentissement du réseau. Tel est le cas en particulier lorsque des images ou des fichiers de taille excessive sont attachés aux messages.

On estime généralement que la prise de connaissance du *contenu* des *e-mails* est excessive dans la plupart des cas ; d'ordinaire, un contrôle de la *liste* des courriers devrait suffire pour mettre à jour une transgression des règles fixées par l'employeur (tout comme une facture téléphonique suffit à faire apparaître des montants anormalement élevés). Pratiquement, il est souvent conseillé que l'employeur s'engage formellement à ne pas lire ou surveiller systématiquement les *e-mails*, se réservant la possibilité d'effectuer un contrôle uniquement à condition d'y être légalement obligé ou s'il a des motifs raisonnables de croire qu'un employé a commis une infraction pénale ou manque gravement aux directives claires et connues de tous dans l'usage du courrier électronique.

La norme de conduite de l'employeur devrait être celle d'un employeur prudent et raisonnable ne lisant pas le courrier de ses employés par curiosité mal placée.

S'agissant de la surveillance des sites consultés par un employé particulier, la prise de connaissance ne pourra être réalisée systématiquement, sous peine de violer le principe de proportionnalité. En revanche, on peut admettre qu'une liste *globale* des sites visités, sur une période *déterminée*, soit établie, *sans que soient identifiés dans un premier temps les auteurs des requêtes*. L'employeur pourra alors prendre des mesures appropriées s'il découvre une durée anormale de consultation de l'Internet ou la mention d'adresses de sites suspects. A cet égard, il est à remarquer que l'enjeu ne devrait pas être, en définitive, de surprendre ou de piéger les travailleurs, mais de parvenir à ce qu'ils adaptent leur comportement de manière à remplir correctement leurs engagements, au mieux des intérêts de l'entreprise. En bref, comme pour les *e-mails*, le contrôle n'est admissible que s'il est raisonnablement justifié.

Selon certains auteurs (Claeys et Dejonghe, 2001, 121 ; Barth, 2002, 174), un contrôle systématique des communications, y compris de leur contenu, est néanmoins concevable dans des circonstances exceptionnelles (protection contre l'espionnage industriel s'il existe des indices précis d'une révélation de secrets d'entreprise, protection des bonnes mœurs, faits de *hacking*, etc.).

L'admissibilité du contrôle s'apprécie aussi au regard des possibilités de solution alternative moins contraignante. Ainsi, la légitimité d'un contrôle pourrait s'avérer douteuse dans le cas où l'employeur pouvait aisément prévenir certains abus moyennant le placement d'un logiciel de filtrage bloquant l'accès à certains sites ou l'installation d'un système limitant l'envoi d'*e-mails* vers des adresses préétablies…

Conclusion

D'emblée, la question du contrôle par les employeurs de l'utilisation du courrier électronique et de l'Internet par les employés fait apparaître une nette opposition des intérêts en présence.

Toutefois, au-delà de cette divergence de vues, il apparaît qu'un terrain d'entente peut être trouvé. Les travailleurs peuvent et doivent comprendre qu'une utilisation honnête et raisonnable des technologies de l'information contribue au bon accomplissement de leur travail et, par voie de conséquence, à la bonne marche de l'entreprise. Il est évident qu'ils y trouvent directement leur compte. De leur côté, les employeurs doivent mesurer le risque de détérioration de l'ambiance de travail, et partant, de motivation et de productivité si leurs employés se savent constamment surveillés. Le bon sens leur commandera dès lors, non pas de s'interroger unilatéralement sur les moyens de surveiller et de piéger leurs subordonnés, mais de chercher des solutions équilibrées et respectueuses de cette part d'autonomie à laquelle ces derniers aspirent… et ont droit.

Compte tenu des incertitudes juridiques en la matière, on aperçoit l'intérêt d'adopter une réglementation spécifique, par exemple sous la forme d'une loi ou d'une Convention collective de travail, de manière à fixer le cadre juridique global dans lequel peut s'exercer le contrôle des *e-mails* et du *surf* sur l'Internet. Tandis que cette règle claire et publique énoncerait les principes minimum à respecter en matière de cybersurveillance (conditions à remplir, limites assignées au contrôle, régime des sanctions…), les entreprises conserveraient bien entendu une certaine latitude pour *préciser*, dans leur règlement intérieur ou dans leurs contrats de travail, les usages concrètement autorisés, tolérés ou interdits, ainsi que la politique de surveillance effectivement suivie.

Puissent les principes exposés dans la présente étude guider les décideurs, sinon dans l'élaboration d'un tel cadre juridique général et contraignant, du moins dans la conduite d'une politique de surveillance équitable au sein des entreprises.

Repères bibliographiques

BALLARIN, L. (1997), « Le respect de la vie privée et la relation de travail », *Rev. trav.*

BART, H. (2002), « Contrôle de l'employeur de l'utilisation privée que font ses travailleurs des nouvelles technologies de l'information et de communication au lieu de travail », *Journal des tribunaux du travail*, pp. 169-177.

BOURRIE-QUENILLET, M., et RODHAIN, F. (2002), « L'utilisation de la messagerie électronique dans l'entreprise. Aspects juridiques et managériaux en France et aux Etats-Unis », *J.C.P.*, G., I-102, pp. 63-69.

CLAEYS, Th. et DEJONGHE, D. (2001), « Gebruik van e-mail en internet op de werkplaats en controle door de werkgever", *Journal des tribunaux du travail*.

Commission de la protection de la vie privée (Belgique), Avis d'initiative n° 10 du 3 avril 2000 relatif à la surveillance par l'employeur de l'utilisation du système informatique sur le lieu de travail, disponible sur le site Internet la Commission (www.privacy.fgov.be).

Commission Nationale Informatique et Libertés (CNIL, France), Rapport relatif à la cybersurveillance sur les lieux de travail du 5 février 2002, disponible sur le site Internet de la Commission (adresse : www.cnil.fr).

GERADIN, B., « La convention collective de travail relative à la protection de la vie privée des travailleurs à l'égard du contrôle des données des communications électroniques en réseau du 26 avril 2002 », étude disponible sur le site www.droit-technologie.org

REVEILLON, A. (2002), « La e-surveillance des employés. Le contrôle des e-mails et des sites visités », *Revue Ubiquité – Droit des technologies de l'information*, n° 11, pp. 33-53.

VERBIEST, Th., « La surveillance de l'usage de l'Internet dans l'entreprise : quelle légalité ?, *L'Echo*, 20 janvier 2000, article disponible sur le site www.droit-technologie.org