Présente :

Surveillance des travailleurs : Nouveaux procédés, multiples contraintes

Par

Olivier Rijckaert
Avocat, Bird & Bird
Bruxelles

Date de mise en ligne : 26 avril 2005

SURVEILLANCE DES TRAVAILLEURS :

NOUVEAUX PROCEDES, MULTIPLES CONTRAINTES

Olivier Rijckaert,
Avocat, Bird & Bird (Bruxelles)

L'on a peine à affirmer que la question de l'usage des « nouvelles » technologies sur le lieu de travail défraye encore la chronique (sociale). Une fois envolé l'inévitable effet de mode qui a suivi l'irrésistible ascension du courrier électronique et de l'Internet sur le lieu de travail, la doctrine s'est progressivement désintéressée de la matière. Le législateur est resté désespérément muet ; hormis quelques discrètes – mais pertinentes – interventions, la commission pour la protection de la vie privée s'est montrée bien silencieuse… Seuls les juridictions du travail, saisies de quelques litiges et les partenaires sociaux, signataires de la convention collective de travail n°81, ont fait montre d'une certaine activité dans ce domaine.

La matière aurait-elle perdu de son intérêt ou de son actualité ? Nous ne le pensons pas. Au fur et à mesure que les technologies de l'information et de la communication (« TIC ») s'imposent comme vecteur essentiel des échanges entre individus dans nos sociétés post-industrielles, elles poursuivent, en parallèle, leur marche inexorable sur le lieu de travail. Sur le devant de la scène, en tant qu'indispensables outils de travail et d'interaction entre les personnes. En coulisses, comme moyen aisé – parfois sournois - de contrôle des travailleurs, de leurs prestations et de leur comportement. C'est cette thématique que nous avons choisi d'aborder, au sens large.

I. INTRODUCTION

Nous nous attacherons tout d'abord à l'étude de la surveillance que l'employeur est en droit d'exercer sur l'usage que fait le travailleur du courrier électronique et de l'Internet. Un grand classique, certes, mais aussi une question qui a connu d'intéréssants développements au cours des trois dernières années, tant sur le plan réglementaire (la C.C.T. n°81) que jurisprudentiel.

Nous analyserons distinctement la question du contrôle des données stockées sur un support « fixe », tel le disque dur de l'ordinateur mis à disposition du travailleur. Ces données ne constituent en effet pas des « télécommunications » ni des « données de communication électronique en réseau ». Elles échappent donc au champ d'application de la C.C.T. n°81, de la loi du 21 mars 1991 et de l'article 314bis du Code pénal.

C'est ensuite la problématique de la géolocalisation des travailleurs qui retiendra notre attention. Cette technique, d'apparition récente, permet à l'employeur de localiser très précisément un travailleur, que ce soit par le biais de la technologie GSM ou grâce à la combinaison des technologies du GPS et du GSM.

La vidéosurveillance des travailleurs mérite que l'on s'y attarde quelque peu. Même si la convention collective de travail n°68 a déjà fait l'objet de multiples études de doctrine, il nous a paru utile d'en rappeler les principes, à la lumière de quelques récentes décisions de jurisprudence.

Notre attention se portera enfin sur un dernier mode de surveillance fréquemment utilisé, mais qui n'a pas encore véritablement attiré l'attention sous l'angle de la protection de la vie privée : le contrôle électronique des accès aux locaux de l'entreprise et du temps de travail, par le biais de cartes magnétiques.

II. LE CONTRÔLE DE L'UTILISATION D'INTERNET ET DE L'E-MAIL : CONSIDERATIONS CRITIQUES SUR LA C.C.T. n°81

(1) Introduction

À mesure que l'utilisation d'Internet et du courrier électronique s'est répandue dans les entreprises, un certain malaise a peu à peu envahi les acteurs du droit social dès qu'il s'agissait d'aborder la question de la surveillance de l'utilisation de ces moyens de communication par les travailleurs.

La doctrine s'est - parfois timidement - emparée de la question[1]. Les juridictions du travail ont rapidement été saisies d'un nombre croissant de litiges, la plupart portant sur le licenciement pour motifs graves d'un travailleur supposé avoir abusé du système de télécommunications mis à sa disposition par l'employeur[2]. Des décisions, parfois en sens radicalement opposés, ont été rendues, certaines ne contribuant pas véritablement à éclaircir les questions délicates que soulève la matière. Consciente du malaise naissant et confrontée à un nombre croissant de plaintes émanant de travailleurs, la Commission de la Protection de la Vie Privée a émis, d'initiative, deux avis circonstanciés[3]. Enfin, les partenaires sociaux ont conclu, le 26 avril 2002 au sein du Conseil National du Travail, la convention collective de travail n°81 «relative à la protection de la vie privée des travailleurs à l'égard du contrôle des données de communication électroniques en réseau » (ci-après «la C.C.T. n°81»).

Il nous faut d'emblée rappeler que la C.C.T. n°81 s'inscrit dans un ensemble législatif, réglementaire et jurisprudentiel vaste et complexe. Elle n'a pas d'existence autonome et ne saurait se substituer aux autres normes régissant la question du contrôle de l'utilisation que

[1] Voy. notamment O. Rijckaert, « Le contrat de travail face aux nouvelles technologies », Orientations, 2000, 204 et ss.; T. Claeys, "L'utilisation des nouvelles technologies et de l'e-mail durant le contrat de travail, la notion de faute et son évolution dans l'exécution du contrat de travail", in Le contrat de travail et la nouvelle économie, éd. du Jeune Barreau de Bruxelles, 2002, 255 et ss.; H. Barth, « 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 », J.T.T., 2002, 169; J. Vanthournout, "Internet @ Work : Sociaal-juridische aspecten", SD Uitgeverij, 2001 ; D. Dejonghe, « Werkgeverscontrole op e-mail en internetgebruik : C.A.O. nr.81 schetst de krijtlijnen, Oriëntatie, 2002, 225 ; P. De Hert et A.-C. Lacoste, « Persoonsgegevens en de contrôle van on-linecommunicatiemiddelen, C.A.O. 81 en advies 10/2000 », in Privacy en persoonsgegevens, Politeia, 2004, 155.

[2] Voyez notamment T.T. Bruxelles (24è ch.), 2 mai 2000, R.G. n° 93.534/99, inédit; T.T. Bruxelles (12è ch.), 22 juin 2000, R.G. n° 1.471/99, inédit; Arbeidshof Gent (2e k.), 22 octobre 2001, J.T.T., 2002, 41; Arbeidshof Gent (afd. Brugge, 7e k.), 4 avril 2001, J.T.T., 2002, 49 ; Arbeidshof Brussel (3e kamer), 10 februari 2004, www.juridat.be

[3] Avis d'initiative relatif à la surveillance par l'employeur de l'utilisation du système informatique sur le lieu de travail, n°10/2000 du 3 avril 2000; Avis d'initiative concernant la proposition de loi 2-891/1 du 29 août 2001 visant à réglementer l'utilisation des moyens de télécommunication sur le lieu de travail, n°39/2001 du 8 octobre 2001. Ces deux avis de la Commission de la protection de la vie privée peuvent être consultés en ligne : http://www.privacy.fgov.be.

font les travailleurs de l'e-mail et de l'Internet. Tout au plus y apporte-t-elle un éclairage supposé pragmatique, reflet d'un consensus entre les représentants des travailleurs et des employeurs.

Contrairement à certains auteurs, qui semblent considérer que la C.C.T. n°81 est l'alpha et l'oméga de la problématique qui nous occupe[4], nous pensons donc que l'analyse de ce que permet cette C.C.T. en termes de surveillance des travailleurs, doit nécessairement s'accomplir en tenant compte du cadre réglementaire et jurisprudentiel, plus large, qui balise la matière depuis quelques années.

Nous situerons tout d'abord la C.C.T. n°81 dans l'ordre juridique belge, en rappelant brièvement les principales dispositions légales garantissant la protection de la vie privée des individus et définissant les conditions d'une éventuelle ingérence dans celle-ci (2). Après avoir ensuite défini le champ d'application matériel de la C.C.T. n°81 (3), nous verrons qu'elle confirme le droit dont dispose l'employeur de réglementer l'usage des techniques de communication électroniques en réseau au sein de l'entreprise (4). Enfin, la majeure partie de cette première partie sera consacrée à l'examen des conditions dans lesquelles la C.C.T. n°81et les autres normes applicables autorisent le contrôle des échanges effectués par les travailleurs au moyen des techniques de communication électroniques en réseau mises à disposition par l'employeur (5).

(2) Situation de la C.C.T. n°81 dans l'ordre juridique

La C.C.T. n°81 s'intègre dans un cadre réglementaire qu'il est impossible de passer sous silence. Ce cadre assure, d'une part, le droit de l'employeur de réglementer et de contrôler les prestations du travailleur et l'usage qu'il fait des outils de travail mis à sa disposition et, d'autre part, le droit irréductible du travailleur au respect de sa vie privée au travail.

Parmi ces normes, essentielles à l'examen de la question qui nous occupe, citons notamment :

- les articles 2, 3, 16 et 17 de la loi du 3 juillet 1978 relative aux contrats de travail, imposant au travailleur d'exécuter le travail en se conformant aux instructions de l'employeur, sous le contrôle de ce dernier;

- l'article 8 de la Convention européenne des Droits de l'Homme qui pose le principe du droit des individus au respect de leur vie privée, tout en définissant les conditions d'une éventuelle ingérence dans l'exercice de ce droit[5];

- l'article 22 de la Constitution qui garantit le droit de chacun au respect de sa vie privée et familiale, sauf dans les cas et conditions fixées par la loi;

- la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques, dont l'article 109 ter D assure la protection du secret des télécommunications. Cet article

[4] M Goldfays et L. Van Moorsel, « Motif grave et consultation de sites pornographiques », Ors., 2003, 8.

[5] L'article 8 de la C.E.D.H. dispose : « *1.Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance ; 2. Il ne peut y avoir ingérence d'une autorité dans l'exercice de ce droit que pour autant que cette ingérence est prévue par la loi et qu'elle constitue une mesure qui, dans une société démocratique, est nécessaire à la sécurité nationale, à la sûreté publique, au bien être économique d pays, à la défense de l'ordre et à la prévention des infractions pénales (...)* ».

interdit aux tiers de prendre connaissance et d'utiliser des données transmises par voie de télécommunication, sauf exceptions;

- l'article 314 bis du Code pénal, qui interdit de prendre connaissance du contenu de toute télécommunication privée durant sa transmission. Est considérée comme privée, toute télé communication qui n'est pas destinée à être entendue par d'autres personnes que celles qui y participent;

- la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, qui prévoit notamment que ces données doivent être traitées loyalement et licitement, collectées pour des finalités déterminées, explicites et légitimes et rester adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont obtenues.

A l'exception de l'article 314bis du code pénal, dont il n'est curieusement pas fait mention dans le texte de la C.C.T. n°81, cette dernière se réfère explicitement à ces diverses sources, tout en spécifiant « qu'elle n'entend pas y déroger ». Précision superflue dans la mesure où elle ne pourrait bien entendu le faire, en application des principes régissant la hiérarchie des sources des obligations dans les relations de travail[6]. Précision quelque peu hypocrite, aussi : sur certains points, la C.C.T. n°81 déroge bel et bien aux normes supérioeures ayant le même objet…

L'ensemble de ces dispositions, de rang supérieur à la C.C.T. n°81, est guidé par une volonté identique : celle de garantir la protection de la vie privée des personnes tout en définissant strictement les conditions d'une éventuelle ingérence par un tiers dans celle-ci. Leur autre point commun, source de nombreuses difficultés, est qu'elles ne prévoient aucun régime particulier lorsque l'ingérence s'opère à l'initiative de l'employeur, dans le cadre de l'exécution du contrat de travail. Avec pour conséquence qu'en principe, une telle ingérence, même légitime, reste soumise au droit commun et ne pourrait s'accomplir que dans des circonstances exceptionnelles, d'une gravité particulière.

L'article 3 de la C.C.T. porte d'ailleurs une reconnaissance réciproque, par les partenaires sociaux, des intérêts contradictoires de chacune des parties et la difficulté de les concilier. Les travailleurs admettent ainsi que «*l'employeur dispose d'un droit de contrôle sur l'outil de travail et sur l'utilisation de cet outil par le travailleur dans le cadre de l'exécution de ses obligations contractuelles, y compris lorsque cette utilisation relève de la sphère privée* ». Quant aux employeurs, ils déclarent respecter «*le droit des travailleurs à la protection de leur vie privée dans le cadre de la relation de travail* »[7].

Les partenaires sociaux se sont ainsi clairement inscrits dans la mouvance doctrinale et jurisprudentielle récente, relative à la question. Tout en admettant la nécessité d'une protection de la vie privée du travailleur lors de l'exécution du contrat, tous semblent en effet s'accorder sur la légitimité d'une certaine ingérence de l'employeur dans la vie privée des travailleurs, en vue d'assurer une correcte exécution du contrat de travail ou de protéger les

[6] Loi du 5 décembre 1968 sur les conventions collectives de travail et les commissions paritaires, art. 51 : « La hiérarchie des sources des obligations dans les relations de travail entre employeurs et travailleurs, s'établit comme suit : 1° la loi dans ses dispositions impératives ; 2° les conventions collectives de travail rendues obligatoires (…) ».
[7] Article 3 de la C.C.T. n°81.

intérêts de l'entreprise qui seraient supérieurs à celui qu'a le travailleur au respect de sa vie privée[8]. Demeure la difficulté de concilier, en cette matière, les droits contradictoires de l'employeur et du travailleur, comme l'a fort justement relevé le Tribunal du travail de Bruxelles dans l'un des premiers jugements rendus en la matière : « *le fait que les échanges privés se (produisent) sur le lieu et pendant les heures de travail n'affecte pas leur protection. La circonstance qu'ils ont eu lieu à l'aide du matériel de l'employeur n'exclut pas la protection. Des actes de la vie privée sur le lieu et pendant les heures de travail se font presque toujours de cette manière, et ils sont pourtant protégés selon la (Cour européenne des Droits de l'Homme). Il pourrait être soutenu que l'employé a utilisé le matériel dans un but qui n'était pas celui pour lequel il lui a été confié, ce qui pourrait constituer une atteinte au droit de l'employeur. Cette atteinte n'a pas pour effet de supprimer la protection de la vie privée, il s'agit de concilier deux droits contradictoires (...)* »[9].

La frontière qui se dresse entre le contrôle légitime et l'ingérence illicite dans la vie privée du travailleur est ténue et a fait l'objet d'innombrables débats. Sans entrer dans le détail de ceux-ci, on constate que l'ingérence est généralement admise «*pour autant qu'on puisse relever une exigence de finalité (la nécessité de protéger une autre valeur fondamentale) et une exigence de proportionnalité (la protection de cette valeur fondamentale n'autorise que des atteintes à la vie privée strictement nécessaires)* »[10].

Nous verrons que, au-delà du prescrit de la C.C.T. n°81, qui présente de nombreuses carences et imprécisions, c'est cette double exigence de finalité et de proportionnalité qu'il convient de garder à l'esprit lors de l'analyse de la légitimité du contrôle, par l'employeur, de l'usage de l'email et de l'Internet.

(3) Le champ d'application matériel de la C.C.T. n° 81

La C.C.T. n° 81 réglemente le contrôle des communications « privées » du travailleur, à l'exclusion des échanges « professionnels » effectués à l'aide des techniques de communication électroniques en réseau (a). Elle n'autorise par ailleurs que la prise de connaissance des « données » de communication, à l'exclusion de leur « contenu » (b). Ces notions méritent d'être précisées.

(a) Communications « professionnelles » ou « privées » ?

Les procédures de contrôle et d'identification et les garanties offertes par la C.C.T. n°81 ne semblent s'appliquer qu'aux communications électroniques à caractère strictement privé. La C.C.T. exclut en effet de son champ d'application les communications dont le caractère professionnel « n'est pas contesté par le travailleur ». Qui plus est, elle autorise leur contrôle de manière inconditionnelle.

Probablement confrontés à des difficultés lors de la négociation du texte de la C.C.T., les partenaires sociaux se sont toutefois abstenus de définir ce qu'il y a lieu d'entendre par communication "privée" ou "professionnelle". La seule précision apportée à cet égard figure dans le rapport précédant le texte de la C.C.T. : c'est en principe au travailleur lui-même qu'il

[8] Voy. Hans Clauwaert, « Le droit fondamental à la vie privée », Rev. Trav., avril 1997, p. 11.
[9] T.T. Bruxelles (24è ch.), 2 mai 2000, R.G. 93.534/99, inédit.
[10] Laura Ballarin, « Le respect de la vie privée et la relation de travail », Rev. Trav ., avril 1997, p.21.

appartient de déterminer si la communication à laquelle il participe est, ou non, privée, en apportant une mention spécifique en ce sens dans l'objet du message[11].

Il faut toutefois rappeler, à ce propos, que pour l'application des articles 109terD de la loi du 21 mars 1991 et 314bis du code pénal, «*les communications ou télécommunications sont privées lorsqu'elles ne sont pas destinées à être entendues par tout un chacun* »[12]. C'est ainsi qu'une « *communication professionnelle, mais non destinée à être entendue par d'autres personnes que les partenaires à la conversation, est une communication privée au sens de la loi* »[13]. Le Ministre de la Justice a confirmé ce principe, en réponse à une question parlementaire portant sur le sujet qui nous occupe[14].

S'inscrivant donc en marge de ces dispositions légales – pourtant relevant de l'ordre public - les partenaires sociaux ont donc assoupli, en faveur de l'employeur, la protection légale offerte aux télécommunications à caractère professionnel. Ainsi, c'est sans la moindre équivoque que le rapport précédant le texte de la C.C.T. précise que, lorsque l'objet et le contenu des données de communication ont « un caractère professionnel non contesté par le travailleur », l'employeur est autorisé à en prendre connaissance, sans autre procédure ni avertissement[15].

En l'état actuel de la législation et, en particulier, eu égard à la portée des articles 314 bis du code pénal et 109ter D de la loi du 21 mars 1991, nous pouvons difficilement approuver le choix opéré par les partenaires sociaux. Aujourd'hui, la prise de connaissance des données ou du contenu des communications électroniques, qu'elles revêtent un caractère professionnel ou privé, suppose le consentement préalable des participants à ces communications ou l'existence d'une condition (légale ou cause de justification, voy. ci-dessous) permettant cette prise de connaissance. Prétendre que celle-ci puisse se faire « sans procédure ni avertissement » méconnaît manifestement le prescrit de normes hiérarchiquement supérieures à une C.C.T., même si celle-ci a été rendue obligatoire par arrêté royal. C'est au législateur, et à lui seul, qu'il appartient d'intervenir par le biais d'une modification des articles susvisés, en vue d'autoriser la prise de connaissance de données ou du contenu des télécommunications professionnelles échangées sur le lieu de travail.

Rappelons d'ailleurs que, dès l'arrêt Niemietz, la Cour européenne des droits de l'homme stigmatisait toute différenciation stricte entre communications « professionnelles » ou « privées », tant cette distinction est aujourd'hui difficile à établir[16].

En conclusion, bien que les partenaires sociaux aient, fût-ce indirectement, affirmé le principe de l'autorisation du contrôle du contenu des communications en réseau à caractère

[11] Rapport précédant le texte de la C.C.T. n°81, p. 9.
[12] Travaux préparatoires de la loi du 30 juin 1994, Doc. Parl., Sénat, sess. 1992-1993, n°843/1, p.7
[13] Doc. Parl. , Sénat, sess. 1992-1992, n°843/2, p.36
[14] Question n°93 de M. Geert Bourgeois du 28 avril 2000, Bull. Questions et réponses, Chambre, 2è session de la 50ème législature, p. 3816 : « (…) *la loi ne fait pas de distinction entre les communications professionnelles et non-professionnelles, de sorte que l'employeur ne peut également faire aucune distinction en la matière* ».
[15] Rapport précédant le texte de la C.C.T. n°81, p. 9.
[16] « La Cour ne juge ni possible ni nécessaire de chercher à définir de manière exhaustive la notion de « vie privée ». Il serait toutefois trop restrictif de la limiter à un « cercle intime » où chacun peut mener sa vie professionnelle à sa guise et d'en écarter entièrement le monde extérieur à ce cercle (…) 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 (…) ».

professionnel des travailleurs, nous pensons qu'un tel contrôle reste en principe interdit, compte tenu du prescrit des articles 314 bis du code pénal et 109ter D de la loi du 21 mars 1991. Pareil contrôle ne saurait être mis en place que moyennant l'autorisation expresse et préalable des intéressés ou si l'une des conditions légales préalable au contrôle est rencontrée.

(b) « Données » ou « contenu » des communications ?

Les dispositions de la C.C.T. n°81 sont applicables aux **données** de communication électroniques en réseau. Il s'agit des données «*relatives aux communications électroniques transitant par réseau, entendues au sens large et indépendamment du support par lequel elles sont transmises ou reçues par un travailleur dans le cadre de la relation de travail* »[17]. La C.C.T. faisant ici explicitement mention de l'article 109ter D la Loi du 21 mars 1991, on peut également se référer à la notion de "télécommunication" telle que définie par cette loi, à savoir « *toute transmission, émission ou réception de signes, de signaux, d'écrits, d'images, de sons ou de données de toute nature, par fil, radio-électricité, signalisation optique ou un autre système électromagnétique*»[18].

Sont ainsi visées les données relatives aux courriers électroniques (identité des participants, taille du message et de ses annexes), aux sites Internet visités, aux communications de messagerie («chat ») mais également les données transmises à l'aide de téléphones mobiles, par le biais des techniques dites «SMS», «WAP», «GPRS», etc.

Qu'en est-il en revanche du **contenu** de ces communications, tel par exemple le contenu des courriers électroniques échangés par le travailleur depuis le lieu de travail ? Bien que le texte même de la C.C.T. soit muet sur ce point, le rapport qui le précède précise clairement que seules les données de communication électroniques sont visées par la C.C.T. et pourront être contrôlées et individualisées selon les modalités qu'elle détermine. En revanche, leur contenu ne saurait l'être, «*sauf aux parties et certainement au travailleur à donner son accord conformément au prescrit des lois du 21 mars 1991 et 8 décembre 1992 précitée*». Ce point de vue est conforme à celui défendu par la Commission de la protection de la vie privée : "*la Commission considère que la prise de connaissance du contenu des courriers électroniques est excessive et contraire aux dispositions légales (...), de la même façon que le serait l'écoute et / ou l'enregistrement des communications téléphoniques de l'employé*"[19].

Si la C.C.T. n°81 a préféré exclure de son champ d'application (et donc, de la surveillance autorisée) le contenu des communications électroniques en réseau, nous verrons ci-dessous que l'employeur est malgré tout autorisé à en prendre connaissance, dans certaines circonstances exceptionnelles.

(4) Le droit de l'employeur de réglementer l'usage des technologies de communication électroniques en réseau

En se liant par un contrat de travail à son employeur, le travailleur s'engage à exécuter son travail avec soin, probité et conscience, au temps, au lieu et dans les conditions convenus. Il s'oblige en outre à agir conformément aux ordres et aux instructions donnés par l'employeur

[17] Article 2 de la C.C.T. n°81.
[18] Article 68, 4° de la loi du 21 mars 1991.
[19] Avis n°10/2000 du 3 avril 2000, p. 6.

en vue de l'exécution du travail[20]. La relation de travail se caractérise ainsi par l'existence d'un lien de subordination et par le pouvoir d'autorité de l'employeur, dont le contrôle peut s'avérer l'instrument naturel et légitime.

Pour peu qu'il respecte les dispositions légales, réglementaires et contractuelles applicables, l'employeur est libre de déterminer les conditions d'exécution du contrat de travail, tandis que le travailleur est tenu de s'y soumettre. Parmi ces conditions figurent les modalités d'utilisation des outils de travail mis à la disposition du travailleur, sous la responsabilité et aux frais de l'employeur. Nul ne conteste en effet que l'employeur dispose d'une maîtrise totale de sa propriété, des biens et des matières premières nécessaires à l'exécution du contrat de travail. Parmi ces biens figurent, dans le cadre de la question qui nous occupe, le réseau informatique, les ordinateurs qui y sont connectés et leurs accessoires.

La C.C.T. n°81 confirme le droit de l'employeur de réglementer l'usage de ces technologies. Elle n'entend nullement définir les conditions d'accès ni l'utilisation par le travailleur des moyens de communication électroniques en réseau au sein de l'entreprise : la détermination de ces conditions fait intégralement partie des prérogatives de l'employeur[21]. C'est d'ailleurs ce qu'avait relevé la Commission de la protection de la vie privée dans son avis du 8 octobre 2001[22].

Deux réflexions s'imposent à propos de cette reconnaissance du droit, pour l'employeur, d'interdire ou de réglementer l'usage, professionnel ou privé, de l'infrastructure informatique.

Tout d'abord, même si l'employeur dispose probablement de cette faculté, il ne nous semble pas opportun d'interdire radicalement tout usage de l'Internet et de l'e-mail par les travailleurs à des fins privées. Cette utilisation doit, certes, être réglementée par l'employeur, qui définira par exemple les sites dont la visite est interdite, les moments d'accès ou la fréquence moyenne d'utilisation privée autorisés, la taille des pièces jointes pouvant circuler sur le réseau, etc. En revanche, une interdiction absolue d'effectuer des communications privées au moyen de l'infrastructure informatique paraît irréaliste, comme l'a fort justement relevé M. l'avocat général Kehrig dans ses conclusions en marge de l'affaire « Nikon »[23].

Ensuite, l'employeur qui déciderait d'interdire purement et simplement toute utilisation de l'infrastructure informatique à des fins privées, ne dispose pas pour autant d'une marge

[20] Article 2, 3, 16 et 17 de la loi du 3 juillet 1978 relative aux contrats de travail.
[21] Rapport précédant le texte de la C.C.T. n°81, p. 5.
[22] "L'employeur a compétence pour fixer, d'une part, les conditions d'utilisation des moyens de communication, et d'autre part les modalités de contrôle du respect, par les employés, de ces conditions d'utilisation (…) En ce qui concerne les possibilités d'accès aux moyens de communication au sein de l'entreprise, l'employeur peut légitimement imposer des limites, tout en tenant compte des dispositions réglementaires assurant le bien être au travail, réglementant l'usage des nouvelles technologies sur le lieu de travail, et interdisant le harcèlement ou le mobbing" (Avis n°39/2001 du 8 octobre 2001, p.5).
[23] « Dans ce contexte, s'il est sans doute techniquement possible à un employeur, « pour éviter tout problème », d'interdire à un salarié subordonné toute communication non professionnelle pendant le temps de travail, sur intranet ou intranet, à partir, sur et vers un matériel appartenant à l'entreprise, une telle prohibition totale paraît, comme l'observe un spécialiste, tout-à-fait irréaliste au 21ème siècle. Comment, en effet, en l'absence d'abus manifeste ou d'actes illicites, empêcher un salarié d'appeler de son poste de travail, par téléphone ou par mail, pendant ses heures de pause ou de déjeuner, pour régler ses affaires personnelles urgentes ? Ne serait-ce pas d'ailleurs contre-productif ? », Concl. Avocat général Kehrig, sous Cass. (fr.), arrêt n° 4164 du 2 octobre 2001, et note O. RIJCKAERT, http://www.droit-technologie.org

de manœuvre plus large s'agissant du contrôle exercé sur les travailleurs. Certains auteurs[24] persistent à soutenir que, dès l'instant où l'employeur interdit tout usage privé des moyens de communication de l'entreprise, il serait autorisé à exercer un contrôle sans aucune limite, dès lors qu'il ne peut dans ce cas être question de « vie privée » du travailleur. Cette thèse, très contestable, fait fi de l'interprétation large donnée par la Cour européenne des droits de l'homme à l'article 8 de la Convention européenne des droits de l'homme et méconnaît manifestement les dispositions du droit belge réglementant le secret des communications. Celles-ci protègent en effet les communications effectuées dans la « sphère professionnelle », comme nous l'avons vu ci-dessus.

(5) Le contrôle et ses modalités

L'objet principal de la C.C.T. n°81 est de préciser les conditions dans lesquelles l'employeur serait autorisé à procéder au contrôle des échanges « privés » effectués par le travailleur au moyen du réseau de communication électronique de l'entreprise. Aux termes de la C.C.T., ce contrôle ne peut s'exercer qu'en vue de la poursuite de certaines finalités déterminées, dans le respect du principe de proportionnalité. Quand bien même la finalité poursuivie par l'employeur serait acceptable, le contrôle devra s'effectuer moyennant le respect d'une procédure déterminée et après que les travailleurs et leurs représentants en aient été dûment informés, dans le respect du principe de transparence.

Nous distinguerons ci-dessous le régime applicable au contrôle des *données* de communications électroniques en réseau (1), de celui applicable au *contenu* de ces communications, bien que la question de la surveillance de ce dernier ait été éludée par la C.C.T. n°81 (2).

(a) Le contrôle des données de communications électroniques en réseau

S'inspirant de la logique qui sous-tend la loi du 8 décembre 1992, la C.C.T. n°81 n'autorise le contrôle des données de communication électroniques en réseau qu'en vue de la poursuite de certaines finalités, dans le respect du principe de proportionnalité et moyennant une information préalable des travailleurs et de leurs représentants.

(i) Les circonstances dans lesquelles le contrôle est admis (principe de finalité)

La nécessité d'une correcte définition des finalités du contrôle est le fil conducteur des deux avis rendus d'initiative par la Commission de la protection de la vie privée en la matière[25].

S'inscrivant en droite ligne de ce principe et de ceux gouvernant la loi du 8 décembre 1992, la C.C.T. n°81 énumère quatre catégories de finalités pour lesquelles le contrôle est admis. Aux termes de l'article 5, §1er de la C.C.T., le contrôle des données de communication électroniques en réseau est autorisé en vue :

[24] Selon T. CLAEYS : « En pareil cas, l'outil informatique (et donc l'utilisation de l'e-mail et la consultation des sites Internet) reste en principe exclusivement dans la « sphère professionnelle », de sorte que le travailleur n'a, par définition, aucun droit au respect de la vie privée à faire valoir en lien avec ce matériel informatique », *op.cit.*, p.284

[25] Avis n°10/2000 du 3 avril 2000 et Avis n°39/2001 du 8 octobre 2001, *op. cit.*

> 1° de prévenir des faits illicites ou diffamatoires, des faits contraires aux bonnes mœurs ou susceptibles de porter atteinte à la dignité d'autrui ;
>
> 2° de protéger les intérêts économiques, commerciaux et financiers de l'entreprise auxquels est attaché un caractère de confidentialité et en vue de lutter contre les pratiques contraires ;
>
> 3° d'assurer la sécurité ou le bon fonctionnement technique des systèmes informatiques en réseau de l'entreprise, en ce compris le contrôle des coûts y afférents, ainsi que la protection physique des installations de l'entreprise ;
>
> 4° de garantir le respect de bonne foi des principes et règles d'utilisation des technologies en réseau fixés dans l'entreprise.

L'employeur est donc tout d'abord autorisé à procéder à un contrôle en vue de **prévenir la commission de faits illicites, diffamatoires, contraires aux bonnes mœurs** ou susceptibles de porter atteinte à la dignité d'autrui. Le commentaire de la C.C.T. n°81 précise que ces faits peuvent notamment consister en des actes de piratage informatique, tels la prise de connaissance non autorisée de données relatives à la gestion du personnel. Il peut également s'agir de la consultation de sites à caractère pornographique, ainsi que de sites incitant à la haine, la ségrégation ou la discrimination.

Curieusement, la C.C.T. n°81 ne semble viser que la *prévention*, et non la répression, des faits qu'elle énumère. Qu'en est-il lorsque le travailleur s'en est déjà rendu coupable, notamment lorsque la communication a déjà eu lieu ? A notre sens, le contrôle est également autorisé, ne fût-ce qu'en vue de prévenir la commission d'une nouvelle infraction par le travailleur qui en est l'auteur.

Confrontées à des faits antérieurs à l'entrée en vigueur de la C.C.T. n°81, les juridictions du travail ont admis l'exercice d'un contrôle par l'employeur dans de telles hypothèses. Ainsi, dans son jugement du 22 juin 2000, le tribunal du travail de Bruxelles a estimé légitime le contrôle et le dépôt du contenu d'un courrier électronique auquel était joint une image pornographique, non sollicitée par son destinataire. S'agissant manifestement d'un acte contraire aux bonnes moeurs et portant atteinte à la dignité d'autrui, l'employeur était autorisé - voire tenu – à y mettre fin, fût ce au prix d'une ingérence dans la vie privée du travailleur qui s'en était rendu coupable[26]. La Cour du travail de Gand a, quant à elle, reconnu la

[26] « *Overwegende dat artikel 109ter E van de wet van 21 maart 1991 bepaalt dat het verbod tot kennisname van telecommunicatie vervat in de bepalingen van artikel 109ter D van deze wet en van artikel 314bis van het strafwetboek niet van toepassing zijn wanneer de wet het stellen van de bedoelde handelingen toestaat of oplegt. Verder is de noodsituatie een algemeen aanvaarde uitzondering in het strafrecht, die zou toelaten om zonder medeweten of toestemming van de gesprekspartners een gesprek af te luisteren of van een E-mail bericht kennis te nemen op voorwaarde dat de overtreding van het verbod de enige middel is om hogere rechtsbelangen te beschermen zoals een fysische of psysiche integriteit (...).*

Men kan dit strafrechtelijk principe samen lezen met het beginsel dat men geen misbruik kan maken van zijn recht op privacy om een ander burger schade te berokkenen (...) zodat men zijn rechtmatige aanspraak op bescherming verliest (...)Overwegende dat op de werkgever de wettelijke verplichting rust overeenkomstig artikel 126 (lire « *artikel 16* ») *van de wet van 3 juli 1978 de goede zeden in acht te nemen en te doen nemen gedurende de uitvoering van de arbeidsovereenkomst (...)Dat de rechtbank meent dat het in deze omstandigheden gerechtvaardigd is dat de werkgever met het oog op het doen in acht nemen van de goede*

légitimité du contrôle, par l'employeur, des données de télécommunication relatives à un travailleur qui s'était rendu coupable d'actes de piratage informatique. Ces actes consistaient en l'envoi d'un e-mail au nom d'un tiers, sans autorisation, et en l'intrusion dans la messagerie électronique personnelle de l'administrateur du réseau informatique[27].

Le contrôle est ensuite autorisé par la C.C.T. n°81 en vue de **la protection des intérêts économiques, commerciaux et financiers de l'entreprise**, auxquels est attaché un caractère de confidentialité. Cette finalité vise la protection des secrets de fabrique et d'affaires, du know how et des informations confidentielles de l'entreprise. L'employeur est ainsi notamment autorisé à exercer un contrôle en vue de prévenir ou de réprimer toute infraction du travailleur aux dispositions de l'article 17, 3° de la loi du 3 juillet 1978 relative aux contrats de travail[28].

Nous avons vu que l'article 109ter E de la Loi du 21 mars 1991 autorise les tiers à prendre connaissance des données de télécommunication sil la finalité poursuivie est le bon fonctionnement du réseau (public) de télécommunication. La troisième finalité envisagée par la C.C.T. est l'application de ce principe au sein des entreprises. Est ainsi autorisé le contrôle effectué **en vue d'assurer la sécurité et / ou le bon fonctionnement technique des systèmes en réseau de l'entreprise**, ainsi que la protection physique des installations de l'entreprise. Le texte précise par ailleurs que le contrôle peut également avoir pour objet le contrôle des coûts afférents à l'utilisation du réseau.

Enfin, la dernière finalité reconnue par la C.C.T. n°81 est le **respect de bonne foi des principes et règles d'utilisation des technologies en réseau, fixés dans l'entreprise**. Est ici visé le contrôle effectué en vue de vérifier si les travailleurs se conforment aux directives d'utilisation de l'Internet et de l'e-mail fixées par l'employeur. Ces directives porteront notamment sur les catégories de sites dont la visite est autorisée (ou non), les périodes durant lesquelles l'utilisation privée des technologies de communication sont autorisées (ou interdites), etc. Comme nous le verrons ci-dessous, elles doivent faire l'objet d'une communication, spécifique et préalable, aux travailleurs de l'entreprise.

(ii) Les modalités d'individualisation des données relatives aux communications des travailleurs (principe de proportionnalité)

Il ne suffit pas de rencontrer l'une des finalités autorisées pour légitimer tout contrôle. Encore faut-il que celui-ci soit effectué dans le respect du principe de proportionnalité. C'est ce que rappelle l'article 6 de la C.C.T. n°81 : par principe, le contrôle des données de communication électroniques en réseau ne peut entraîner une ingérence dans la vie privée du travailleur. En cas d'ingérence, celle-ci doit être réduite au minimum.

---

zeden en welvoeglijkheid op zijn redactiedienst, d.w.z. ter bescherming van de goede zeden op het werk van het E-mail bericht een afdruk heeft genomen met het doel niet op het vervolgen van zijn werknemer maar van zijn afdanking om dringende redenen».

[27] Arbeidshof Gent (afd. Brugge, 7e k.), 4 avril 2001, *op. cit.*

[28] « *Le travailleur a l'obligation (...) de s'abstenir, tant au cours du contrat qu'après la cessation de celui-ci : a) de divulguer les secrets de fabrication, ou d'affaires, ainsi que le secret de toute affaire à caractère personnel ou confidentiel dont il aurait eu connaissance dans l'exercice de son activité professionnelle ; b) de se livrer ou de coopérer à tout acte de concurrence déloyale* ».

La mise en œuvre du principe de proportionnalité se traduit par une interdiction d'individualisation systématique et préalable des données de communication électroniques en réseau. Ainsi, l'identification des données relatives à la consultation de sites Internet ou à l'échange de courriers électroniques ne pourra, dans un premier temps, donner lieu à l'identification du travailleur effectuant ces consultations ou échangeant les courriers.

Sur ce point, la C.C.T. n°81 s'inscrit en droite ligne des recommandations formulées par la Commission de la protection de la vie privée, qui s'était clairement exprimée en faveur d'un contrôle préalable général, sans individualisation du travailleur : « *tout contrôle devrait être ponctuel et justifié par des indices laissant suspecter une utilisation abusive des outils de travail. Un contrôle général et a priori de l'ensemble des données de télécommunications de même qu'un enregistrement systématique de l'ensemble de ces données apparaît disproportionné par rapport à l'objectif poursuivi* »[29].

Tant la Commission que les partenaires sociaux tolèrent ainsi l'établissement périodique de listes générales portant sur les données relatives aux sites Internet visités, sans identification *a priori* des ordinateurs au départ desquels ces visites sont opérées. Si, sur cette base, des abus sont constatés, l'employeur est autorisé à identifier le travailleur fautif et à accomplir des devoirs d'enquête complémentaires à son égard, moyennant le respect de la procédure d'individualisation prévue par la C.C.T. (voy. ci-dessous). Les mêmes principes sont d'application en ce qui concerne le courrier électronique, à cette nuance près que la prise de connaissance du contenu du courrier n'est tolérée ni par la Commission de la protection de la vie privée, ni par la C.C.T. n°81.

(iii) L'information préalable des travailleurs et de leurs représentants (principe de transparence)

Préalablement à la mise en oeuvre du contrôle, la C.C.T. n°81 impose à l'employeur une double obligation d'information, au niveau collectif et individuel. La Commission de la protection de la vie privée avait déjà précisé, dans son avis du 3 avril 2000, la portée de l'obligation d'information des travailleurs. Selon elle, cette information doit au moins porter sur[30] :

- les modalités d'utilisation du courrier électronique et de l'Internet qui sont permises, tolérées ou interdites ;
- les finalités et les modalités du contrôle;
- l'existence d'un stockage des données de télécommunication et la durée de ce stockage ;
- les décisions pouvant être prises par l'employeur à l'endroit de l'employé sur la base du traitement des données collectées à l'occasion d'un contrôle ;
- le droit d'accès du travailleur aux données personnelles le concernant.

[29] Avis n°10 / 2000 du 3 avril 2000, p.6.

La C.C.T. rencontre en grande partie les attentes de la Commission de la protection de la vie privée sur ce point, en organisant et en définissant le contenu de l'information collective et individuelle à fournir préalablement à la mise en place du contrôle.

Aux termes de l'article 7 de la C.C.T. n°81, l'employeur qui souhaite instaurer un système de contrôle des données de communication électroniques en réseau est tenu d'informer le conseil d'entreprise sur tous les aspects du contrôle. A défaut de conseil d'entreprise, l'information est donnée au sein du comité pour la prévention et la protection au travail. A défaut de comité, c'est la délégation syndicale qui reçoit l'information. En l'absence de délégation syndicale, les travailleurs sont directement informés.

L'information collective doit au moins porter sur :

- la politique de contrôle ainsi que les prérogatives de l'employeur et du personnel de surveillance ;
- la (ou les) finalité(s) poursuivie(s) ;
- le fait que les données personnelles sont ou non conservées, le lieu et la durée de conservation ;
- le caractère permanent du contrôle[31].

La forme que doit revêtir l'information n'est pas précisée par la C.C.T.. Elle pourrait donc être fournie oralement par le chef d'entreprise, au cours d'une réunion ordinaire ou extraordinaire du Conseil d'entreprise. On recommandera toutefois à l'employeur de remettre un document écrit à chaque représentant des travailleurs et de l'annexer au procès verbal de la réunion au cours de laquelle la question a été examinée. Ceci facilitera l'administration de la preuve en cas de litige éventuel.

Cette obligation d'informer les représentants des travailleurs est conforme au prescrit de la recommandation n° R(89) du Comité des Ministres du Conseil de l'Europe, adoptée le 18 janvier 1989, qui dispose : « *Conformément aux législations et pratiques nationales et, le cas échéant, aux conventions collectives, les employeurs devraient informer ou consulter leurs employés ou les représentants de ceux-ci préalablement à l'introduction ou à la modification des systèmes automatisés pour la collecte et l'utilisation de données à caractère personnel concernant les employés. Ce principe s'applique également à l'introduction ou à la modification de procédés techniques destinés à contrôler les mouvements ou la productivité des employés*». A titre comparatif, le Code français du travail confie également aux organes

[30] Avis n°10/2000 du 3 avril 2000.

[31] Notons, à ce propos, que la Commission de la protection de la vie privée ne semble pas admettre l'idée d'un contrôle permanent : "*Tout contrôle devrait être ponctuel et justifié par des indices laissant suspecter une utilisation abusive des outils de travail. Un contrôle général et a priori de l'ensemble des données de télécommunications de même qu'un enregistrement systématique de l'ensemble de ces données apparaît disproportionné par rapport à l'objectif poursuivi*", Avis n° 10/2000 du 3 avril 2000, p. 6.

représentatifs la compétence d'examiner toute question relative au contrôle des activités des salariés[32].

Précisons que, aux termes de la C.C.T. n°81, les représentants des travailleurs doivent uniquement être *informés* sur ces aspects de la surveillance. La C.C.T. ne leur accorde en revanche aucune compétence d'avis ni, a fortiori, de décision. Est-ce à dire que les organes sociaux sont privés de tout pouvoir décisionnel en la matière ? Ce serait perdre de vue l'article 6 de la loi du 8 avril 1965 instituant les règlements de travail impose la mention, dans le règlement, des « *droits et obligations du personnel de surveillance* ». Il en va de même en ce qui concerne les sanctions qui seraient éventuellement applicables en cas d'usage fautif de l'outil informatique : celles-ci doivent nécessairement figurer dans le règlement de travail. Or, comme on le sait, toute modification du règlement de travail suppose l'accord du conseil d'entreprise. En outre, à défaut de dispositions spécifiques dans le règlement d'ordre intérieur du conseil, la modification ne sera adoptée que moyennant l'accord unanime des représentants des travailleurs. Par ailleurs, l'article 2, §1er de la C.C.T. n° 39 du 13 décembre 1983 impose à l'employeur qui a « *décidé d'un investissement dans une nouvelle technologie et lorsque celui-ci a des conséquences collectives importantes en ce qui concerne l'emploi, l'organisation du travail et les conditions de travail* » de procéder à une concertation avec les représentants des travailleurs sur les conséquences sociales de l'introduction de cette nouvelle technologie. Nous pensons donc, au vu de ces dispositions, que malgré le silence embarrassant de la C.C.T. n° 81 à cet égard, certaines questions particulières directement liées au contrôle des données de communication électroniques en réseau devraient faire l'objet d'un véritable échange de vues, voire même d'un accord, au sein du conseil d'entreprise.

On notera également que l'article 10 de la C.C.T. n°81 prévoit que le conseil d'entreprise (ou, à défaut, le comité ou, à défaut, la délégation syndicale) doit être consulté sur l'évaluation des systèmes de contrôle installés, en fonction des développements technologiques. Tel sera par exemple le cas lors de l'introduction d'une nouvelle technologie de surveillance, différant fondamentalement de la technologie originelle utilisée au moment de l'introduction du contrôle au sein de l'entreprise.

Outre l'information collective visée ci-dessus, l'employeur est tenu d'informer chaque travailleur individuellement de l'existence d'un contrôle et de ses modalités. Cette information a trait aux mêmes éléments que l'information collective. Elle doit en outre être complétée par une information sur :

- l'utilisation de l'outil mis à disposition des travailleurs pour l'exécution de leur travail, en ce compris les limites à l'utilisation fonctionnelle;
- les droits, devoirs et obligations des travailleurs et les interdictions éventuelles prévues dans l'utilisation des moyens de communication électronique en réseau de l'entreprise ;
- les sanctions prévues au règlement de travail en cas de manquement.

[32] Article 432-2-1 du Code du Travail : « *Le comité d'entreprise est informé et consulté, préalablement à la décision de mise en oeuvre dans l'entreprise, sur les moyens ou les techniques permettant un contrôle des salariés* ».

L'information à fournir individuellement à chaque travailleur est donc plus étendue que celle communiquée au conseil d'entreprise. Alors que ce dernier n'est informé que sur les modalités du contrôle, les travailleurs sont également informés sur les conditions et limites d'utilisation des outils de communication électronique en réseau, ainsi que sur les sanctions susceptibles de frapper tout usage irrégulier. L'information fournie devra être aussi complète que possible. Rappelons en effet que l'une des quatre finalités dont la poursuite autorise le contrôle est précisément « le respect de bonne foi des principes et règles d'utilisation des technologies en réseau » fixés au sein de l'entreprise. A défaut d'une définition précise et exhaustive de ces règles et principes par l'employeur, le contrôle de leur respect risquerait de perdre la légitimité que lui accorde la C.C.T. n°81.

Alors que l'article 7 de la C.C.T. ne définit pas les formes selon lesquelles l'information collective doit être communiquée, le commentaire de l'article 8 propose à l'employeur différents canaux de communication de l'information individuelle. Celle-ci pourra ainsi être transmise :

- dans le cadre d'instructions générales (circulaires, affichage, etc.) ;
- par mention dans le règlement de travail ;
- par mention dans le contrat de travail individuel ;
- par des consignes d'utilisation fournies à chaque utilisation de l'outil informatique.

(b) Le contrôle du contenu des télécommunications électroniques en réseau

Au cours de l'examen du champ d'application matériel de la C.C.T. n°81, nous avons vu que les partenaires sociaux semblent s'être entendus sur une interdiction de principe du contrôle du *contenu* des télécommunications à caractère privé échangées par le travailleur depuis le lieu de travail (par exemple, le texte d'un courrier électronique).

Comme nous l'avons vu, et contrairement à ce que laisse entendre le texte de la C.C.T. n°81, cette interdiction porte également sur la prise de connaissance du contenu des télécommunications professionnelles, qui tombent dans le champ d'application de l'article 314bis du Code pénal.

Est-ce à dire que *tout* contrôle du contenu soit interdit ? Nous ne le pensons pas. Rappelons en effet une nouvelle fois que la C.C.T. n°81 s'inscrit dans un cadre réglementaire et jurisprudentiel large. Elle ne peut se substituer à aucune des normes existantes, notamment l'article 314bis du code pénal. Cette disposition, qui interdit la prise de connaissance du contenu des télécommunications, connaît certaines exceptions qui légitimeraient dans certaines circonstances le contrôle, par l'employeur, du contenu de certains courriers électroniques à caractère privé ou professionnel échangés par le travailleur au moyen de l'infrastructure informatique de l'entreprise.

(i) L'interdiction de prise de connaissance du contenu des télécommunications

L'article 314bis du Code pénal[33] sanctionne «*celui qui, intentionnellement, à l'aide d'un appareil quelconque, écoute (...) prend connaissance (...) enregistre (...) pendant leur transmission, des communications ou télécommunications privées, auxquelles il ne prend pas part, sans le consentement de tous les participants à ces communications ou télécommunications* ».

Cette disposition protège le *contenu* (et non uniquement les données) des télécommunications. Le contenu de tout courrier électronique échangé depuis le lieu de travail bénéficie donc, quel qu'en soit l'objet, de la protection instaurée par l'article 314bis du Code pénal, au même titre que n'importe quelle autre télécommunication. Sa prise de connaissance par l'employeur durant sa transmission[34] est donc interdite, sauf à pouvoir invoquer l'une des exceptions légales.

(ii) Exceptions à l'interdiction

- **L'autorisation préalable de tous les participants à la communication**

Aux termes de l'article 314bis du Code pénal, l'interception ou l'enregistrement de télécommunications privées en vue de prendre connaissance de leur contenu est autorisée moyennant le consentement de *tous* les participants à cette communication.

Se pose la question de la forme que devrait revêtir cette autorisation. Selon certains, elle ne devrait être ni expresse, ni écrite : « *De toestemming hoeft niet noodzakelijk uitdrukkelijk of schriftelijk gegeven te worden, hoewel dat voor het bewijs van de rechtvaardigheidsgrond wel aan te raden valt* »[35]. Pour d'autres en revanche, le consentement du travailleur doit être exprimé de manière expresse et spécifique, préalablement à chaque contrôle. Ainsi, le consentement exprimé par le biais d'une clause insérée dans le règlement de travail ou même le contrat de travail, ne constituerait pas une «autorisation» permettant la prise de connaissance au sens l'article 314bis du code pénal. Pour certains auteurs, seule serait valable l'autorisation *ad hoc*, c'est-à-dire exprimée au moment même de l'examen des données de trafic[36].

La Commission pour la protection de la vie privée s'écarte de cette dernière approche pour le moins sévère et difficilement réalisable en pratique. Ainsi, selon la Commission, « *lorsqu'une police d'usage de l'internet fait l'objet d'une négociation avec les représentants des employés et du consentement explicite de chacun de ces employés, certains types de*

[33] Pour un commentaire détaillé de cette disposition et, plus généralement, de la loi du 30 Juin 1994, voy. L. Arnou, « Het respecteren van telefoongeheim in Belgïe na de afluisterwet van 30 Juni 1994 », computerrecht, 1995/4, pp. 156 et ss ; H. Bosly et D. Vandermeersch, « La loi belge du 30 juin 1994 relative à la protection de la vie privée contre les écoutes, la prise de connaissance et l'enregistrement de communications et de télécommunications privées », R.D.P., 1995, pp. 301 et ss.

[34] Selon nous, la transmission a lieu entre le moment où l'expéditeur envoie le message et celui où le destinataire en prend effectivement et entièrement connaissance. La prise de connaissance d'une copie d'un message stockée sur un serveur lors de sa transmission, doit être assimilée à une prise de connaissance durant cette transmission.

[35] Jos Dumortier, « Internet op het werk : controlerechten van de werkgever », Oriëntatie, 2000, pp. 35 et ss.

[36] Frank Hendrickx, « Privacy en arbeidsrecht – Een analyse van een grondrecht in arbeidsverhoudingen », proefschrift tot het behalen van de graad van doctor in de rechten, KUL, 1999, p. 239 ; Pascal Leduc, « Le contrôle des communications données ou reçues par le travailleur », Revue Ubiquité, 2000/5, p. 47.

contrôles, dont la nécessité apparaît tout à fait légitime, peuvent être opérés en toute légalité »[37]. La Commission a confirmé ce point de vue dans sa Recommandation n°1/2002 du 22 août 2002[38], en ces termes :

« En ce qui concerne les employés, une note de service ou le règlement de travail seul ne sont pas suffisants pour garantir le consentement libre de l'employé. Il s'agit de combiner le consentement individuel de l'employé avec la négociation d'un texte général à laquelle seront associés les représentants des employés (…) Le consentement obtenu par la mention des conditions d'enregistrements dans le règlement de travail ou le code de conduite, qui font l'objet d'une discussion au sein du conseil d'entreprise et contribuent ainsi au caractère libre du consentement, pourra par exemple être complété via un avenant au contrat de travail ou la signature d'un formulaire ad hoc par l'employé, garantissant ainsi le caractère individuel du consentement ».

La Commission admet ainsi que le travailleur puisse, par le biais d'un accord individuel de portée générale, valablement consentir à un contrôle – restreint et soumis à certaines conditions – du contenu des communications échangées depuis le lieu de travail. On notera en revanche, avec la Commission, que l'accord des représentants des travailleurs (au sein du conseil d'entreprise) ne saurait en revanche suffire : seul l'individu concerné dispose de la faculté d'autoriser une ingérence de l'employeur dans ses communications et, partant, sa vie privée.

Notons enfin que le courrier électronique suppose par nature la participation d'autres personnes que le travailleur à l'échange… L'article 314bis précisant que l'accord de *tous* les participants est requis, l'employeur devrait également recueillir le consentement de ces tiers avant de prendre connaissance du contenu de la communication. L'opération nous semble en pratique difficilement réalisable, sauf à supposer que ce consentement puisse être déduit des circonstances de l'espèce[39].

- **Autres exceptions**

Les exceptions à l'interdiction de prise de connaissance des *données* des télécommunications prévues par l'article 109terE, §1 de la loi du 21 mars 1991, sont également applicables en ce qui concerne l'interdiction de prise de connaissance de leur *contenu*, posée par l'article 314bis du Code pénal.

L'interdiction est ainsi levée lorsque la loi permet ou impose l'accomplissement des actes visés ou lorsque ces actes sont accomplis dans le but exclusif d'assurer le bon fonctionnement du réseau[40]. Par ailleurs, l'état de nécessité, cause générale de justification en droit pénal, pourrait également légitimer une violation, par l'employeur, de l'interdiction posée par l'article 314bis du code pénal.

[37] Commission de la protection de la vie privée, avis n° 13/2003 du 27 février 2003.
[38] Recommandation n°1/2002 du 22 août 2002 portant sur l'enregistrement des télécommunications effectuées dans le cadre des services bancaires, http://www.privacy.fgov.be.
[39] P. Leduc, *op.cit.*, p.48.
[40] L'article 109ter E, §1 prévoit également que l'interdiction ne s'applique pas lorque l'acte est posé en vue de permettre une intervention des services de secours ou d'urgence en réponse à une demande d'aide.

Nous tenterons de circonscrire ci-dessous la portée de ces trois exceptions dans le cadre particulier de la relation de travail.

- *L'autorisation légale*

L'autorisation légale, première des trois exceptions permet elle à l'employeur d'exercer un contrôle du contenu des télécommunications des travailleurs ? L'on pourrait tenter de défendre que l'article 17, 2° de la loi du 3 juillet 1978, consacrant l'autorité de l'employeur, constitue une « disposition légale » permettant l'exécution d'un contrôle au sens de l'article 109terE, §1, 1° de la loi. La plupart des auteurs ne sont toutefois pas de cet avis, en raison du caractère trop général de cette disposition[41]. Selon eux, l'article 109ter E, §1, 1° ayant pour objet de restreindre l'exercice d'un droit garanti par la Convention européenne des droits de l'homme, il doit être interprété de manière restrictive. Seule une loi autorisant expressément l'interception ou la prise de connaissance de la télécommunication répondrait au prescrit de l'article 109ter E, §1, 1°.

S'inscrivant en marge de cette appréciation, le Tribunal du travail de Bruxelles a estimé que l'application de l'article 16 de la loi du 3 juillet 1978, imposant à l'employeur d'assurer le respect des convenances et des bonnes moeurs sur le lieu de travail, constituerait une « autorisation légale » d'exercer un contrôle au sens de l'article 109terE, §1, 1° de la loi[42]. L'employeur serait ainsi autorisé à prendre connaissance du contenu de la télécommunication et à en faire usage, même sans le consentement préalable du travailleur concerné, dès l'instant où la sauvegarde des bonnes moeurs et le respect de la dignité des autres travailleurs le requièrent. Nous souscrivons à ce point de vue. Ne pas admettre que, dans des circonstances d'une gravité exceptionnelle, l'employeur puisse intervenir en prenant connaissance du contenu d'un e-mail, reviendrait à lui dénier la possibilité de respecter, entre autres, son obligation légale de garantir le respect des bonnes mœurs sur le lieu de travail.

- *Les impératifs techniques*

L'article 109ter E, §1 autorise la prise de connaissance des données (et, par ricochet, du contenu) lorsque les actes visés sont accomplis dans le but exclusif d'assurer le bon fonctionnement du réseau. On sait aujourd'hui que la visite intensive de sites Internet par un nombre élevé d'utilisateurs est de nature à engorger, voire sérieusement perturber, le réseau de télécommunication de l'entreprise. Certains fichiers sont très volumineux (images, fichiers musicaux MP3), tandis que la « bande passante » est coûteuse et limitée. Par ailleurs, le téléchargement de certains fichiers dits "exécutables" peut présenter des risques sérieux pour

[41] Selon P. Leduc, *op. cit.*, p. 47 (note 42) : « Il est bien évident que la faculté prévue par l'article 109ter E, §1, 1° ne peut résulter que d'une autorisation expresse (elle doit être expressément prévue par la loi) et ne peut se déduire de la seule existence d'un lien de subordination entre l'employeur et l'employé. De manière générale, toute disposition qui viendrait à restreindre l'exercice d'un droit garanti par la Convention européenne des droits de l'homme ne peut faire l'objet que d'une interprétation restrictive, en application du principe de proportionalité ».

[42] T.T. Bruxelles, 12è ch., 22 juin 2000, R.G. 88.187/98, inédit : « *Overwegende dat artikel 109ter E van de wet van 21 maart 1991 bepaalt dat het verbod tot kennisname van telecommunicatie vervat in de bepalingen van artikel 109ter D van deze wet en artikel 314bis van het strafwetboek niet van toepassing zijn wanneer de wet het stellen van de bedoelde handelingen toestaat of oplegt (...) Overwegende dat op de werkgever de wettelijke verplichting rust overeenkomstig artikel 126 (lire "16") van de wet van 3 juli 1978 de goede zeden in acht te nemen en te doen nemen gedurende de uitvoering van de arbeidsovereenkomst* ».

le réseau de l'entreprise, dans la mesure où ces ils sont souvent porteurs de virus. Même si la loi du 21 mars 1991 vise vraisemblablement le bon fonctionnement du réseau *public de télécommunications,* nous sommes d'avis que les impératifs liés au fonctionnement du réseau de l'entreprise pourraient justifier un certain contrôle de l'utilisation qui en est faite par les travailleurs. Il est clair toutefois que le contrôle éventuel ne pourrait s'inscrire que dans ce seul objectif (finalité), être indispensable (proportionnalité) et préalablement annoncé aux travailleurs (transparence).

- *L'état de nécessité*

Certains auteurs[43] soutiennent que l'état de nécessité, cause générale de justification en droit pénal, pourrait légitimer certaines « entorses » à l'interdiction posée par l'article 109ter D de la loi du 21 mars 1991. Sans entrer dans le détail, rappelons que l'état de nécessité permet, si certaines conditions strictes sont rencontrées, d'enfreindre la règle pénale. Il « *vise essentiellement une situation de crise, exceptionnelle, caractérisée par un dilemme, ou mieux : un conflit de valeurs. Si la loi pénale (faite pour une situation plus normale) était observée, cette obéissance entraînerait des conséquences néfastes, dépassant à ce point l'inconvénient de la transgression que le législateur se prononcerait certainement lui-même en faveur de la désobéissance* »[44]. Ainsi, la commission par le travailleur d'une infraction d'une gravité extrême (telle la réception ou la distribution d'images pédophiles ou la divulgation de secrets de fabrique) pourrait justifier que l'employeur enfreigne l'article 314bis du code pénal en vue d'empêcher la réalisation de l'infraction du travailleur. Il est bien entendu que l'employeur ne pourra procéder de la sorte que s'il a épuisé tous les autres moyens de prévenir ou d'interrompre la réalisation de l'infraction.

(6) L'individualisation des données

Nous avons vu que le contrôle instauré par l'employeur, dans le respect des règles exposées ci-dessus, ne peut en principe mener à une individualisation systématique et a priori, des données contrôlées. En d'autres termes, à ce stade de la procédure, l'employeur a connaissance des données échangées (adresses des sites visités, moment et durée des visites, …) mais il ignore encore l'identité du travailleur auquel ces données peuvent être attachées. L'objet de la procédure d'individualisation est précisément d'identifier le travailleur qui est à l'origine du transfert de données en cause.

Les modalités d'individualisation des données de communication électroniques en réseau font l'objet de la section II du chapitre IV de la C.C.T. n°81 (articles 11 à 17). Selon la finalité poursuivie par l'employeur, la C.C.T. distingue deux procédures d'individualisation. La commission d'actes illicites, nuisant aux intérêts de l'entreprise ou compromettant la sécurité du réseau peut donner lieu à une individualisation dite « directe ». Quant à violation des directives édictées par l'employeur relatives à l'usage de l'outil informatique, elle mènera à une individualisation «indirecte».

[43] F. Hendrickx, *op.cit.*, pp. 242 et 243.
[44] Chr. Henneau et J. Verhaegen, « Droit pénal général », Bruylant, Bruxelles, 1991, pp. 161 et 162.

(a) La procédure d'individualisation directe

La procédure d'individualisation directe est régie par l'article 15 de la C.C.T.. Elle peut être mise en branle par l'employeur lorsqu'il poursuit l'une des trois premières finalités décrites à l'article 5, §1er de la C.C.T., à savoir la prévention d'actes illicites, la sauvegarde des intérêts économiques et financiers de l'entreprise ou le maintien du bon fonctionnement et de la sécurité du réseau informatique.

L'employeur qui a exercé un contrôle – au départ anonyme – en vue de l'une de ces finalités et a constaté un manquement de la part d'un travailleur, est autorisé à identifier directement ce dernier, sans qu'une procédure d'information ou d'audition préalable ne doive être suivie. Il appartiendra ensuite à l'employeur de décider des suites à réserver à cette individualisation. Il pourra s'agir d'une audition du travailleur, le cas échéant en présence d'un membre de la délégation syndicale, ou de l'application immédiate d'une sanction, en fonction de la gravité du manquement commis.

(b) La procédure d'individualisation indirecte

Si la finalité poursuivie par l'employeur est le contrôle du respect des directives relatives à l'usage de l'outil informatique au sein de l'entreprise, l'identification du travailleur suspecté d'un éventuel manquement ne peut s'opérer que de manière indirecte.

Aux termes de l'article 16 de la C.C.T., l'employeur qui constate une irrégularité est tout d'abord tenu de respecter une phase préalable d'information de tous les travailleurs. Cette information, d'ordre général, a pour objet de porter à la connaissance de l'ensemble du personnel de l'entreprise, l'existence d'une « anomalie » et d'avertir les travailleurs du fait qu'il sera procédé, sans autre avertissement, à une individualisation des données si un nouveau manquement est constaté.

En cas d'irrégularité postérieure à cette information générale, l'employeur est autorisé à identifier le travailleur qui en est suspecté. Il doit ensuite entendre le travailleur à ce propos, avant de prendre une éventuelle mesure de sanction. Cet entretien a pour but de « *permettre au travailleur de faire part à l'employeur de ses objections vis-à-vis de sa décision ou de l'évaluation envisagée et de s'expliquer sur l'utilisation faite par lui des moyens de communication électroniques en réseau mis à sa disposition* »[45].

(c) Appréciation critique

Nous nous permettons de nous interroger sur la pertinence et la faisabilité de ces procédures d'individualisation. Premièrement, il est manifeste que l'employeur aura déjà identifié – secrètement, certes – le travailleur à l'origine de la communication litigieuse, compte tenu de ce que permet la technique et du fait que chaque ordinateur connecté au réseau est systématiquement identifié par une « adresse I.P. », véritable carte d'identité électronique.

Ensuite, la procédure d'individualisation indirecte et les garanties qu'elle est censée offrir, prêtent à sourire. Il suffirait à l'employeur, constatant un manquement, d'adresser un avertissement général à l'ensemble des travailleurs pour pouvoir, par la suite, procéder à toute individualisation sans plus aucun avertissement…

[45] Article 17, §1er, al. 3 de la C.C.T. n°81.

(7) Conclusions et recommandations pratiques

La C.C.T. n°81 du 26 avril 2002 entendait venir en aide aux employeurs et aux travailleurs en apportant un éclairage spécifique à la législation applicable et en organisant les modalités d'un contrôle par l'employeur, de l'usage des techniques de télécommunication. Il ne s'agit toutefois que d'un "éclairage". Les principes régissant la hiérarchie des sources des obligations en droit du travail empêchent en effet les partenaires sociaux de déroger, par le biais d'une convention collective de travail – même rendue obligatoire par arrêté royal – aux dispositions de la loi, a fortiori si elles sont d'ordre public. Or, tel est le cas de l'article 314bis du code pénal et de l'article 109ter D de la loi du 21 mars 1991, interdisant la prise de connaissance par un tiers des données et du contenu des télécommunications, y compris lorsqu'elles sont échangées sur le lieu de travail, qu'elles aient un caractère professionnel ou privé.

En pratique, on retiendra donc ce qui suit.

En l'état actuel de la législation, les données de télécommunications (adresses des sites internet visités, données relatives à un échange d'emails, etc.) et leur contenu ne peuvent faire l'objet d'une prise de connaissance par l'employeur, considéré comme tiers à ces communications. Ce principe vaut quelque soit leur objet : professionnel ou privé.

Cette prise de connaissance est toutefois autorisée dans deux circonstances principales :

- Si le travailleur a indubitablement marqué son consentement à la prise de connaissance des données ou du contenu des communications. Ce consentement doit être exprimé individuellement. Selon la Commission de la protection de la vie privée, il peut l'être par le biais d'une clause générale insérée dans le contrat de travail ou un avenant spécifique. Idéalement, le principe de la surveillance devra également faire l'objet d'une mention spécifique dans le règlement de travail. Précisons que, s'agissant du contenu du courrier électronique, le consentement des autres personnes intéressées est en principe également requis ;

- Si les conditions de l'état de nécessité sont rencontrées, notamment dans l'hypothèse où le travailleur se rend coupable d'actes manifestement illégaux ou d'une gravité particulière, l'employeur est autorisé à enfreindre la règle pénale en vue d'assurer la protection d'intérêts supérieurs à celui qu'à le travailleur au respect de sa vie privée. L'appréciation de l'état de nécessité sera laissé à l'appréciation de la juridiction éventuellement saisie d'un litige à ce sujet.

2. LE CONTROLE DES DONNÉES ELECTRONIQUES STOCKEES SUR UN SUPPORT FIXE

(1) Situation du problème

Nous avons examiné ci-dessus le régime de la surveillance qu'exerce l'employeur sur l'utilisation de l'email et de l'Internet par ses travailleurs. Celle-ci est soumise aux conditions qui régissent toute intrusion de tiers dans les télécommunications auxquelles ils ne prennent pas part.

Qu'en est-il, en revanche, du contrôle des données que le travailleur conserverait sur un support « fixe », ne faisant donc pas l'objet d'une télécommunication ou examinées après que leur transmission ait pris fin ? Il en va ainsi, par exemple, de copies d'emails, de documents, d'images, de sons, etc., stockés par le travailleur sur le disque dur de l'ordinateur mis à sa disposition.

Ces données ne bénéficient pas de la protection accordée aux données de communication électronique durant leur transmission. Il convient donc de leur consacrer une analyse distincte.

(2) Qualification juridique : secret des lettres ?

Les données stockées par un travailleur sur un support magnétique, tel un disque dur, ne constituent pas des données de télécommunications. Leur contrôle éventuel par l'employeur échappe donc à la sanction pénale des articles 109terD de la loi du 21 mars 1991 et 314bis du Code pénal.

Ces données constituent-elles en revanche des « lettres » ou de la « correspondance », bénéficiant de la protection que leur accorde les articles 29 de la Constitution[46] et 460 du Code pénal[47] ?

Nous ne le pensons pas : il est manifeste que ces deux dispositions protègent les lettres missives *confiées à la poste*. Tel n'est pas le cas des documents conservés par le travailleur sur le disque dur d'un ordinateur ou tout autre support magnétique.

C'est en ce sens que la Cour du travail de Liège a récemment confirmé la portée restrictive des articles 29 de la Constitution et 460 du Code pénal. Ainsi, pour la Cour, les envois d'e-mails n'entrent pas dans la notion de « correspondance », entendue comme échange épistolaire confié à la poste ou à un organisme chargé de la distribution du courrier. Selon la Cour, « *Il en va de même d'un journal intime, qui ne fait pas l'objet d'un envoi mais constitue un écrit qui, en principe, n'est consulté que par son auteur qui le conserve précieusement en un endroit connu de lui seul (...) il ne faut pas plus reconnaître à un courrier remis en mains propres de son destinatraire ou déposé à son attention la même valeur de correspondance*

[46] L'article 29 de la Constitution dispose : « Le secret des lettres est inviolable. La loi détermine quels sont les agents responsables de la violation du secret des lettres confiées à la poste ».

[47] L'article 490 du Code pénal dispose : « Quiconque sera convaincu d'avoir supprimé une lettre confiée à un opérateur postal, ou de l'avoir ouverte pour en violer le secret, sera puni d'un emprisonnement de huit jours à un mois (…) ».

protégée par l'inviolabilité de la correspondance ; il convient de le qualifier de lettre missive, courrier également protégé mais sur la base non du principe de l'inviolabilité des lettres mais des principes de droit privé liés au respect de la vie privée »[48].

Le raisonnement suivi par la Cour peut selon nous être intégralement transposé s'agissant de documents et de données entreposées sur le disque dur de l'ordinateur mis à disposition du travailleur. Est-ce à dire que ces données, ne bénéficiant pas des régimes applicables aux « télécommunications » et aux « lettres », échappent à toute protection et qu'elles pourraient par conséquent être sujettes, sans conditions, à l'inspection de l'employeur ? Il n'en est rien.

(3) Conditions du contrôle

Les données stockées par un travailleur sur un support magnétique, tel un disque dur, bénéficient de la protection accordée par l'article 22 de la Constitution et par l'article 8 de la Convention européenne des droits de l'homme.

Il est opportun à ce titre d'opérer une distinction entre les documents et données à caractère professionnel et ceux qui revêtent un caractère strictement privé : le degré de protection dont ils bénéficient est, naturellement, différent.

(a) Données et documents à caractère professionnel

Il semble à première vue légitime que l'employeur puisse librement accèder aux données et documents à caractère professionnel rassemblés par le travailleur sur le disque dur de l'ordinateur mis à sa disposition. Ces données et documents ne se distinguent en réalité pas fondamentalement de documents « traditionnels », sur papier, et l'on imagine mal que l'employeur ne puisse en prendre connaissance dans le cadre de l'exécution du contrat de travail.

Toutefois, dès l'instant où ces documents sont stockés sur un ordinateur individuel, traditionnellement protégé par un nom d'utilisateur et un mot de passe, support qui n'est en principe accessible qu'au travailleur, leur prise de connaissance ne peut, selon nous, être effectuée que dans le respect de l'article 8 de la Convention européenne des droits de l'homme et des principes de finalité, proportionnalité et transparence.

Faut-il tout d'abord rappeler que, dans ses arrêts Huvig, Niemietz et Halford[49], la Cour européenne des droits de l'homme a, sans la moindre ambiguïté, considéré que des échanges professionnels peuvent se trouver dans les notions de « vie privée » et de « correspondance » visées à l'article 8 de la Convention ?

[48] C. Trav. Liège (13è ch., section de Namur), 25 avril 2002, www.juridat.be; Voy également, dans le même sens, C. Trav. Liège (13è ch. Section Namur), 23 mars 2004, www.juridat.be.

[49] Cour E.D.H., arrêt du 24 avril 1990, Huvig c. France ; Cour E.D.H., arrêt du 16 décembre 1992, Niemitz c. Allemagne ; Cour E.D.H., arrêt du 25 juin 1997, Halford c. Royaume-Uni, dans lequel la cour précise : « Pour la Cour, il ressort clairement de sa jurisprudence que 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 » visées à l'article 8, par. 1 ».

Ensuite et par analogie, s'agissant des enregistrements de conversations téléphoniques professionnelles de travailleurs, effectués dans le cadre de contrôles de qualité ou en vue de conserver une preuve de transactions (dans le secteur bancaire ou boursier, par exemple), la Commission de la protection de la vie privée a confirmé à plusieurs reprises que, même si ces échanges téléphoniques ont un caractère strictement professionnel, leur contrôle par l'employeur constitue une ingérence et doit répondre aux conditions essentielles de finalité, proportionnalité et transparence.

Nous pensons qu'il en va de même s'agissant du contrôle par l'employeur des données à caractère professionnel stockées par le travailleur sur le disque dur auquel ce dernier est en principe le seul à avoir accès. Préalablement à tout contrôle effectué sans l'autorisation du travailleur, l'employeur devra s'interroger sur la finalité qui'il poursuit, la nécessité d'exercer le contrôle sous cette forme (proportionnalité) et, enfin, l'information préalable ou les attentes raisonnables du travailleur concerné (transparence)[50]. Ces principes devront bien entendu être appréciés plus souplement que s'il s'agit de contrôler des documents ou données que le travailleur a spécifiquement identifiés comme privés ou personnels (voy. ci-dessous).

(b) Données et documents à caractère privé ou personnel

Les documents ou données à caractère privé, identifiés comme tels et conservés par le travailleur sur le disque dur mis à sa disposition, bénéficient selon nous d'une protection encore plus étendue.

Ainsi, dans son – désormais célèbre – arrêt « Nikon » du 2 octobre 2001[51], la Cour de cassation française a décidé que "*le salarié a droit, même au temps et lieu de travail, au respect de l'intimité de sa vie privée; celle-ci implique en particulier le secret des correspondances; 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*".

En l'espèce, les messages dont l'employeur avait pris connaissance étaient stockés sur le disque dur de l'ordinateur mis à disposition du travailleur, dans un dossier intitulé « personnel ». Il ne s'agissait donc pas de données de télécommunication ni de données à caractère professionnel: la mention portée par le travailleur sur le dossier contrôlé ne prêtait pas à confusion.

Dans ses conclusions précédant l'arrêt, M. L'avocat général Kehrig rappelle que, en vertu de son pouvoir de direction, l'employeur a le droit de contrôler et de surveiller l'activité de ses salariés pendant le temps de travail. Cette prérogative est toutefois en concurrence avec d'autres droits, dont celui du travailleur au respect de sa vie privée. Ainsi, la surveillance et le contrôle ne peuvent en principe s'exercer que dans le respect des principes de loyauté et de transparence. Pour l'avocat général, le travailleur doit être informé sur les dispositifs mis en place en vue de collecter des renseignements le concernant, l'utilisation de moyens secrets n'étant pas admise.

[50] On pourrait ainsi admettre que l'employeur accède aux documents professionnels du travailleur en cas d'absence prolongée de ce dernier ou d'urgence particulière.
[51] Cass. (fr.), 2 octobre 2001, http://www.droit-technologie.org

Un éventuel contrôle par l'employeur des documents ou données à caractère privé, clairement identifiés comme tels et entreposés sur le disque dur mis à disposition du travailleur, ne peut donc être effectué que dans des circonstances tout-à-fait exceptionnelles. La finalité poursuivie devra être licite: il pourra par exemple s'agir d'une situation se rapprochant de "l'état de nécessité" (voy. ci-dessus). Ainsi, l'employeur qui soupçonne un travailleur de se prêter, au moyen de l'ordinateur mis à sa disposition, à des activités illégales, des actes de concurrence déloyale ou mettant gravement en péril la relation de travail, poursuivrait selon nous une finalité légitime en exerçant le contrôle. En application du principe de proportionnalité, ce contrôle devrait être l'ultime moyen, le "dernier recours", à disposition de l'employeur pour constater l'infraction. Enfin, idéalement, le travailleur devrait être informé de la possibilité pour l'employeur d'exercer le contrôle en question. Un éventuel défaut d'information préalable du travailleur ne nous semble toutefois pas constituer un obstacle à la surveillance, si le manquement recherché est d'une gravité particulière.

3. LE CONTROLE DES DEPLACEMENTS DU TRAVAILLEUR : LES DONNEES DE GEOLOCALISATION

(1) Situation du problème

La technologie du « Global Positioning System » (ou « GPS ») s'est considérablement perfectionnée au cours des dernières années. Elle s'est également largement diffusée, au point que nombre de véhicules en sont aujourd'hui équipés. Sa fonction première est d'aider le conducteur à établir aisément son itinéraire et à trouver son chemin sans avoir recours à des cartes sur papier.

Par ailleurs, nul n'est besoin de mentionner l'essor du GSM. A ce jour, la plupart des travailleurs en sont équipés. Nombre d'employeurs mettent, à leurs frais, à disposition de leur personnel un appareil GSM muni d'une carte SIM.

Les possibilités offertes par la combinaison de ces deux technologies n'ont pas échappé à l'industrie. Ainsi, un nombre croissant de sociétés se spécialisent aujourd'hui dans l'offre de services de localisation des personnes, par le biais d'une technologie qui marie celle du GPS et celle du GSM. Le principe en est relativement simple : il est possible d'adresser à un GSM déterminé un signal précis. Ce GSM, s'il est embarqué dans un véhicule muni de la technologie GPS, interroge alors le terminal GPS qui lui indique très précisément la position du véhicule. Au tour du GSM de retourner cette information vers la personne qui a sollicité l'information. L'opération se déroule en l'espace de quelques secondes et peut s'effectuer au départ de n'importe quel ordinateur personnel, pourvu qu'il soit muni du logiciel nécessaire et, bien entendu, d'un abonnement au service auprès du prestataire. Miracle technologique…

Les mêmes possibilités sont aujourd'hui offertes moyennant la simple possession d'un terminal GSM : celui-ci émet constamment des signaux le reliant à l'une des milliers de stations de base, émetteurs qui jalonnent le territoire. L'identification de la station de base connectée au GSM en question permet de déterminer assez précisément la position du travailleur.

On perçoit immédiatement l'usage que peuvent faire les employeurs de cette technologie : il devient aisé, pour un coût relativement modique, de suivre en temps réel et avec une précision stupéfiante, les déplacements de ses travailleurs.

Cette nouvelle technologie peut être utilisée à des fins diverses : que l'on songe par exemple aux représentants de commerce visitant une clientèle ou aux techniciens appelés à effectuer de fréquents déplacements sur des chantiers mobiles. Il est possible de déterminer précisément leur position et de dresser en conséquence leur itinéraire ou leur planning de visites. Sortie de ce contexte d'organisation du travail, la technologie permet également d'exercer une surveillance quasi permanente sur les déplacements d'un travailleur.

Il n'existe évidemment à l'heure actuelle aucune législation réglementant spécifiquement la problématique. Cette forme de surveillance tombe toutefois indiscutablement dans le champ d'application de la loi du 8 décembre 1992.

(2) Conditions de traitement des données de localisation d'un travailleur

Les données de localisation d'un travailleur constituent des données à caractère personnel, tombant dans le champ d'application de la loi du 8 décembre 1992.

Le traitement de ces données par l'employeur doit donc nécessairement répondre aux conditions générales de licéité des traitements de données à caractère personnel, énoncées par la loi. Nous verrons également que le traitement devrait faire l'objet d'un accord préalable du travailleur et, en principe, d'une déclaration préalable auprès de la Commission de la protection de la vie privée.

(a) Finalité : déterminée, explicite et légitime ?

Aux termes de l'article 4, §1, 2° de la loi, les données à caractère personnel ne peuvent être collectées que pour des finalités déterminées, explicites et légitimes. Le traitement de données de localisation des travailleurs répond-il à cette condition ? Rien n'est moins sûr et la question devra faire l'objet d'une appréciation au cas par cas.

Si l'employeur collecte ces données exclusivement en vue d'optimiser l'organisation du travail et les déplacements de travailleurs dont la fonction est itinérante, la finalité nous semble conforme au prescrit légal. Encore faut-il que la « filature » électronique ne soit pas permanente : si tel était le cas, elle ne répondrait pas selon nous à l'exigence de proportionnalité qui doit régir toute intrusion dans la vie privée des individus.

On pourrait ainsi concevoir que, confronté à une demande d'intervention urgente auprès d'un client ou sur un chantier particulier, l'employeur interroge ponctuellement le système de géolocalisation afin d'identifier rapidement le technicien le plus proche du site en question, pour lui demander d'adapter son planning et assurer ainsi une intervention plus rapide. En revanche, ne répondrait pas à l'exigence de légitimité une surveillance constante des mouvements des travailleurs durant la journée pour, par exemple, mesurer la rapidité ou l'efficacité de leurs déplacements. Par rapport à la finalité poursuivie - l'optimisation de la rentabilité de la force de travail - l'ingérence serait clairement disproportionnée.

On rappellera par ailleurs que, même si la finalité de la collecte des données de localisation est, d'apparence, légitime, encore faut-il que les données en question ne soient pas ultérieurement utilisées à des fins incompatibles avec ces finalités, compte tenu des prévisions raisonnables des intéressés. Ainsi, des données de localisation originellement collectées en vue de faire face à une situation particulière, telle la demande urgente d'un client, ne pourraient par la suite être utilisées à des fins d'évaluation ou de sanction du travailleur.

(b) Consentement du travailleur

Aux termes de l'article 5 de la loi, le traitement de données à caractère personnel ne peut, entre autres, être effectué que lorsque la personne concernée y a indubitablement donné son consentement, ou lorsqu'il est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie.

Le traitement de données de localisation est-il « nécessaire à l'exécution » du contrat de travail ? Nous avons peine à le croire. Si tel était le cas, il faudrait en déduire que, préalablement à cette innovation technologique que constitue la géolocalisation, les contrats de travail des travailleurs itinérants ne pouvaient être exécutés correctement…. Des données telles l'identité et l'adresse du domicile du travailleur sont incontestablement nécessaires à l'exécution du contrat de travail. Tel n'est pas le cas, en revanche, des données de géolocalisation : elles permettent, certes, une meilleure organisation du travail, voire une meilleure exécution du contrat liant l'employeur à ses clients, mais ne sont en rien indispensables à l'exécution du travail en tant que tel.

Il en résulte que, pour être licite, le traitement de ces données devra faire l'objet d'un accord non équivoque de la part des travailleurs concernés, recueilli par le biais d'un écrit individuel. Cet écrit contiendra toutes les informations pertinentes quant au traitement, notamment une description précise de ses finalités et des catégories de destinataires.

Ce consentement peut-il être recueilli par le biais d'une information collective des travailleurs, au sein du conseil d'entreprise par exemple, ou par le biais d'une modification du règlement de travail ? Nous ne le pensons pas. D'une part, la loi du 8 décembre 1992 ne prévoit pas que le consentement puisse être recueilli « collectivement » ou à l'intervention de tiers. D'autre part, la lettre de la loi nous semble particulièrement claire : c'est bien *la personne concernée* qui doit *indubitablement* exprimer son consentement (Loi, article 5).

(c) Déclaration du traitement à la Commission de la protection de la vie privée

Préalablement à la mise en oeuvre d'un traitement entièrement ou partiellement automatisé, le responsable du traitement est tenu d'en faire la déclaration auprès de la Commission de la protection de la vie privée (Loi, article 17, § 1er).

L'arrêté royal du 13 février 2001, portant exécution de la loi du 8 décembre 1992, énonce toutefois es catégories de traitements exemptées de cette obligation de déclaration auprès de la Commission.

Dans le cadre de la relation de travail, on relèvera que seules deux catégories de traitements sont ainsi exemptées de l'obligation de déclaration:

1. Les traitements de données qui se rapportent exclusivement à des données à caractère personnel nécessaires à l'administration des salaires du personnel. La dispense de déclaration ne vaut par ailleurs que pour autant que ces données soient utilisées exclusivement pour l'administration des salaires, qu'elles soient uniquement communiquées aux destinataires qui en ont le droit et qu'elles ne soient pas conservées au delà du temps nécessaire aux finalités du traitement (A.R., article 51).

2. Les traitements de données à caractère personnel qui visent exclusivement l'administration du personnel au service du ou travaillant pour le responsable du traitement. Ce traitement ne peut toutefois se rapporter ni a des données relatives à la santé de la personne concernée, ni à des données sensibles ou judiciaires au sens des articles 6 et 8 de la loi, ni à des données destinées à une évaluation de la personne concernée (A.R., article 52).

Les données de localisation ne peuvent être considérées comme des données nécessaires à l'administration des salaires. Ces données comprennent des données telles les nom et prénom, l'adresse et la composition familiale du travailleur. Certainement pas des données relatives aux déplacements du travailleur durant l'exécution du contrat.

Pourraient-elles alors être considérées comme des données «visant « exclusivement l'administration du personnel » ? La question prête à discussion. Nous pensons toutefois que, par « administration du personnel », l'on a entendu viser des données nécessaires au respect, par l'employeur, de ses obligations légales, ou encore des données indispensables pour une correcte exécution du contrat de travail, au sens strict. En tout état de cause, les données collectées ne peuvent en aucun cas être destinées à une évaluation du travailleur.

Nous pensons donc qu'une déclaration spécifique du traitement des données de localisation auprès de la Commission de la protection de la vie privée, s'impose.

4. LA VIDÉOSURVEILLANCE

La Convention collective de travail n°68 relative à la protection de la vie privée des travailleurs à l'égard de la surveillance par caméras sur le lieu de travail[52] s'inscrit dans le cadre de la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel. Elle a pour but de définir les objectifs et les conditions de l'introduction d'une surveillance par caméras sur le lieu de travail, en tenant compte à la fois du respect de la vie privée des travailleurs et des nécessités du bon fonctionnement de l'entreprise.

Par « surveillance par caméras », on entend tout système de surveillance comportant une ou plusieurs caméras et visant à surveiller certains endroits ou certaines activités sur le lieu de

[52] Convention collective de travail n°68 conclue le 16 juin 1998 au sein de Conseil National du travail, relative à la protection de la vie privée des travailleurs à l'égard de la surveillance par caméras sur le lieu du travail, rendue obligatoire par l'A.R. du 20 septembre 1998, M.B. du 2 octobre 1998, p. 32486. Pour une étude détaillée du texte de cette convention, voy. R. Delarue et M. Weyns, « De CAO nr 68 beschermt de persoonlijke levenssfeer ten opzichte van camerabewaking op de arbeidsplaats », Oriëntatie, 1999, pp. 25 et ss.

travail, à partir d'un point qui s'en trouve géographiquement éloigné. La convention collective s'applique même si les images ne sont pas conservées par l'employeur.

La surveillance par caméras sur le lieu de travail est donc explicitement autorisée. Elle ne peut toutefois s'exercer que moyennant le respect de conditions strictes, issues des principes de finalité, de proportionnalité et de transparence, conditions nécessaires à toute ingérence dans la vie privée des individus. Le principe de transparence se traduit par une obligation d'information et de consultation des organes de concertation et des travailleurs, préalablement et lors de la mise en œuvre du contrôle.

(1) Rappel des conditions générales d'utilisation des caméras sur le lieu de travail

La Convention collective de travail n°68 admet une ingérence dans la vie privée du travailleur, par le biais de la vidéosurveillance, moyennant le respect des principes de finalité, de proportionnalité et de transparence.

Le principe de finalité est défini par l'article 4 § 1er de la C.C.T. : la surveillance n'est autorisée que lorsque *certaines finalités précises* sont poursuivies. Ces finalités sont au nombre de quatre :

1° la sécurité et la santé des travailleurs ;
2° la protection des biens de l'entreprise ;
3° le contrôle du processus de production. Ce contrôle peut viser tant les machines que les travailleurs. Dans ce dernier cas, le contrôle ne peut avoir pour but que l'évaluation et l'amélioration de l'organisation du travail ;
4° le contrôle du travail des travailleurs. S'il sert au mesurage du travail en vue de déterminer la rémunération ou s'il a des implications sur les droits et les obligations du personnel de surveillance, le contrôle supposera une modification du règlement de travail en ce sens, portant la mention expresse de la possibilité et des modalités du contrôle par caméras. Enfin, le contrôle par caméras ne peut constituer l'unique élément d'évaluation du travailleur ou de certains aspects de son travail.

La surveillance peut être permanente ou temporaire si les finalités poursuivies sont la sécurité et la santé, la protection des biens de l'entreprise ou le contrôle du processus de production portant exclusivement sur des machines. En revanche, si elle a pour objet le contrôle du processus de production portant sur les travailleurs ou le contrôle du travail du travailleur, la surveillance ne peut être que temporaire.

Il importe de relever que, quelle que soit la finalité poursuivie, le contrôle par caméras ne peut en principe être secret, sauf à respecter les conditions strictes posées par le code d'instruction criminelle à ce sujet.

Le respect du principe de proportionnalité suppose quant à lui que la surveillance soit *adéquate, pertinente et non excessive* au regard des finalités poursuivies. Dans l'hypothèse où, nonobstant le respect de ce principe, le contrôle par caméras entraîne une ingérence dans la vie privée du travailleur, celle-ci doit, selon les termes de la C.C.T., « *être réduite au minimum* ».

(2) Information des travailleurs et de leurs représentants

Le respect du principe de transparence se traduit par une obligation d'information des travailleurs et de leurs représentants. Ainsi, préalablement à l'instauration du contrôle par caméras et lors de la mise en œuvre de celui-ci, l'employeur est tenu d'informer le conseil d'entreprise ou, à défaut, le comité pour la prévention et la protection au travail ou, à défaut, la délégation syndicale ou, à défaut, les travailleurs.

L'information doit au moins porter sur les aspects suivants :

- la ou les finalité(s) poursuivie(s) ;
- le fait que les images soient ou non conservées ;
- le nombre de caméras et leur emplacement ;
- les périodes durant lesquelles les caméras fonctionnent.

L'information fournie doit être précise. Ainsi, si l'une des finalités poursuivies est le contrôle du travail des travailleurs, l'employeur est tenu de communiquer un motif précis permettant de justifier raisonnablement le contrôle.

L'information doit en outre être préalable à la décision d'instaurer le contrôle, sous peine de rendre celui-ci irrégulier. Les renseignements fournis par l'employeur doivent être suffisamment précis pour permettre aux représentants des travailleurs de procéder à des échanges de vue, de formuler des avis, suggestions et objections. Enfin, l'employeur est tenu de préciser les suites qu'il entend donner aux observations formulées par les représentants des travailleurs.

Même si la convention collective de travail n°68 est muette à cet égard, il est recommandé de fournir l'information préalable par écrit aux représentants des travailleurs. Il importe en outre qu'il soit véritablement procédé à un échange de vues avec ceux-ci. Les procès-verbaux du conseil ou du comité devront par ailleurs permettre d'établir l'effectivité des échanges en reprenant les objections formulées par les représentants des travailleurs et les réponses apportées par l'employeur.

La jurisprudence considère que « *les informations doivent être données avec une précision suffisante, l'objectif de la communication étant, non seulement, de contribuer à la transparence du système et ainsi de rendre possible son installation dans un climat de confiance, mais encore de permettre au travailleur de vivre dans l'entreprise sans qu'il soit procédé à une surveillance permanente de ses comportements* »[53].

Depuis l'entrée en vigueur de la C.C.T. n°68, la jurisprudence condamne systématiquement l'installation et l'utilisation de caméras de surveillance opérées en violation du respect de la procédure d'information préconisée par la convention collective de travail n°68. Ainsi, ont récemment été jugées irrecevables par un Tribunal du travail, les images vidéo produites par l'employeur à titre de preuve d'un vol commis par un travailleur dans l'entreprise, au motif que l'employeur n'était pas en mesure d'établir de manière certaine qu'il avait préalablement procédé à l'information du conseil d'entreprise et des travailleurs sur les aspects de la

[53] T.T. Mons, 17 novembre 2003, R.G. 2016/00/M, inédit.

surveillance par caméras sur le lieu de travail[54]. La Cour de cassation a, quant à elle, récemment cassé un arrêt de la cour d'appel de Bruxelles qui avait considéré que l'absence d'information préalable des travailleurs n'entraînait pas l'irrecevabilité du mode de preuve utilisé, à savoir un enregistrement vidéo[55].

Outre l'information préalable, visée ci-dessus, l'employeur est tenu de consulter le conseil ou le comité s'il apparaît que la surveillance par caméras a des implications sur la vie privée d'un ou de plusieurs travailleurs. Dans ce cas, le conseil examine les mesures qui doivent être prises en vue de réduire cette ingérence au minimum.

Enfin, les organes de concertation doivent régulièrement évaluer les systèmes de surveillance mis en œuvre et, si nécessaire, proposer des améliorations en fonction des évolutions technologiques. Ces améliorations devraient aboutir à une ingérence moindre dans la vie privée des travailleurs, en application du principe de proportionnalité.

5. LE CONTRÔLE DES ACCÈS ET DU TEMPS DE TRAVAIL

(1) Situation du problème

L'accès aux locaux de la plupart des entreprises s'effectue aujourd'hui au moyen d'un système de « badges » : une carte magnétique individualisée est remise à chaque travailleur, portant un code individuel qui permet d'identifier avec certitude le travailleur qui en fait usage.

La fonction première du système est de sécuriser l'accès aux locaux professionnels, à l'instar d'une clef « traditionnelle ». L'une de ses fonctions accessoires est de contrôler les présences des travailleurs, le moment de leur arrivée et de départ, voire même leurs déplacements au sein de l'entreprise. Certains employeurs ont par ailleurs remplacé la traditionnelle « pointeuse » par un contrôle électronique du temps de travail, qui enregistre les heures auxquelles les travailleurs font usage de leur badge pour accéder à l'entreprise ou la quitter.

(2) Conditions de traitement des données relatives aux accès à l'entreprise et du temps de travail

Le contrôle des accès à l'entreprise et du temps de travail constitue un traitement de données à caractère personnel, au sens de la loi du 8 décembre 1992. Le traitement de ces données par l'employeur doit donc répondre aux conditions générales de licéité des traitements, énoncées par la loi.

---

[54] T.T. Charleroi (2è ch., Section de Charleroi) 4 novembre 2002, R.G.149.512A, inédit.

[55] Cass. (2è ch.), 9 juin 2004, www.juridat.be : « Attendu qu'en vertu de l'article 9, §1er, de la convention collective de travail n°68 du 16 juin 1988 relative à la protection de la vie privée des travailleurs à l'égard de la surveillance par caméras sur le lieu du travail, rendue obligatoire par arrêté royal du 20 septembre 1998, l'employeur doit, préalablement et lors de la mise en œuvre de la surveillance par caméras, informer les travailleurs de tous les aspects de cette surveillance visés au paragraphe 4 de cette disposition ; Attendu qu'en se bornant à considérer que « l'information préalable de la mise en œuvre de la surveillance par caméra aurait en l'espèce privé de tout effet pratique la surveillance projetée » et « que l'absence d'information préalable, à la supposer contraire au prescrit de l'article 9 de la convention collective de travail n°68 du 16 juin 1998, n'entraîne pas l'illégalité du mode de preuve utilisé », la chambre des mises en accusation n'a pas légalement justifié sa décision ».

(a) Finalité : déterminée, explicite et légitime ?

Nous avons vu que, aux termes de l'article 4, §1, 2° de la loi, les données à caractère personnel ne peuvent être collectées que pour des finalités déterminées, explicites et légitimes.

La finalité première du traitement de données d'accès est la protection des locaux de l'entreprise. En soi, cette finalité nous paraît déterminée, explicite et légitime. Toutefois, dès l'instant où l'employeur utilise également le système en vue de déterminer les temps de présence ou de travail du personnel, il s'écarte de cette finalité originelle. Même si cette seconde finalité nous paraît, en soi, légitime, elle doit faire l'objet d'une information claire et spécifique des travailleurs, sous peine de n'être ni déterminée, ni explicite.

Enfin, une troisième finalité envisageable est celle du contrôle des déplacements au sein même de l'entreprise. A moins qu'il s'agisse de protéger certains locaux sécurisés (local informatique, coffre, …), cette finalité nous paraît excessive au regard du droit du travailleur au respect de sa vie privée et de sa liberté de déplacement.

(b) Consentement et information des travailleurs

Aux termes de l'article 5 de la loi, le traitement de données à caractère personnel ne peut, entre autres, être effectué que lorsque la personne concernée y a indubitablement donné son consentement, ou lorsqu'il est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie.

Dès l'instant où le traitement des données a pour objet le contrôle des accès aux locaux de l'entreprise, il peut être considéré comme étant nécessaire à l'exécution du contrat de travail. Il en va selon nous de même si la finalité du traitement est le contrôle des prestations du travailleur.

Il ne serait donc pas nécessaire de recueillir le consentement exprès des travailleurs.

Toutefois, leur information s'impose, en application des dispositions de la loi du 8 décembre 1992 régissant l'information des personnes concernées quant au traitement de leurs données à caractère personnel.

Par ailleurs, le traitement des données d'accès en vue du contrôle des présences et du temps de travail devrait faire l'objet d'une mention spéficique dans le règlement de travail de l'entreprise. En effet, aux termes de l'article 6, §1er, 2° de la loi du 8 avril 1965 instituant les règlements de travail, le règlement de travail doit mentionner « les modes de mesurage et de contrôle du travail en vue de déterminer la rémunération ». L'utilisation du système des contrôles d'accès en vue du contrôle des moments de début et de fin du travail constitue bien un mesurage du travail au sens de cette disposition.

(c) Déclaration du traitement à la Commission de la protection de la vie privée

Préalablement à la mise en oeuvre d'un traitement entièrement ou partiellement automatisé, le responsable du traitement est tenu d'en faire la déclaration auprès de la Commission de la

protection de la vie privée (Loi, article 17, § 1er).

L'arrêté royal du 13 février 2001, portant exécution de la loi du 8 décembre 1992, énonce toutefois les catégories de traitements exemptées de cette obligation de déclaration auprès de la Commission. Comme on l'a vu ci-dessus, sont ainsi exemptées de l'obligation de déclaration les traitements de données nécessaires à l'administration des salaires du personnel et des données visant exclusivement l'administration du personnel.

L'on peut considérer que le traitement de données relatives aux accès à l'entreprise soit nécessaire à l'administration des salaires, pour peu qu'il ait pour seules finalités les accès à l'entreprise, le contrôle du temps de présence des travailleurs et, partant, la détermination de leur rémunération. La poursuite de toute autre finalité supposera en revanche la déclaration du traitement auprès de la Commission.

6. CONCLUSIONS

Le droit dont dispose le travailleur au respect de sa vie privée sur le lieu de travail est aujourd'hui reconnu par l'écrasante majorité des auteurs et par la jurisprudence. La frontière entre la vie « privée » et la vie « professionnelle » est d'ailleurs difficile à établir. A tel point que la Cour européenne des droits de l'homme considère que la distinction est, dans certains cas, sans pertinence…

Quant aux « nouvelles » technologies, tout en facilitant considérablement l'exécution du contrat de travail, elles permettent une surveillance plus serrée, plus aisée et quasi automatique des travailleurs qui les utilisent.

La matière fait l'objet d'un arsenal législatif et réglementaire complexe et disparate, finalement peu adapté au contexte spécifique des relations de travail. Le silence du législateur devient d'ailleurs embarrassant…

Dans ce cadre, ce sont les principes fondateurs en matière de protection de la vie privée et de conditions d'une éventuelle ingérence qui devraient guider l'employeur lorsqu'il exerce un contrôle sur ses travailleurs par le biais des « nouvelles » technologies : finalité, proportionnalité et transparence. L'appréciation du respect de ces principes reviendra, au cas par cas, aux juridictions du travail saisies de litiges.

Bien des difficultés seront toutefois écartées dès l'instant où l'employeur aura consulté les représentants des travailleurs sur la question et recueilli le consentement libre, éclairé et individuel de chaque travailleur quant aux modalités de la surveillance mise en œuvre.

Olivier Rijckaert
Avocat – Bird & Bird
Avenue d'Auderghem 22-28
B-1040 Bruxelles
Belgique

olivier.rijckaert@twobirds.com
Matière à jour au 5 avril 2005