Portail du droit Belge
DroitBelge.Net

http://www.droitbelge.net

infos@droitbelge.net

Date	Juillet 2002
Catégorie	Dossier

La convention collective de travail relative à la protection de la vie privée des travailleurs a l'égard du contrôle des données des communications électroniques en réseau du 26 avril 2002

Auteur: Bertrand Geradin (Avocat au barreau de Bruxelles)

bertrand.geradin@ceha-law.be

La convention collective de travail relative à la protection de la vie privée des travailleurs a l'égard du contrôle des données des communications électroniques en réseau du 26 avril 2002

I - INTRODUCTION

L'informatique a envahi progressivement les entreprises et a rapidement laissé apparaître certaines conséquences au niveau de la relation existant entre le travailleur et l'employeur.

Pour l'entreprise, ces nouvelles technologies posent des nouveaux problèmes en matière de sécurité puisque des informations sur toute la vie de l'entreprise, la gestion des commandes, ses secrets de fabrique, etc. sont disponibles en dehors de l'entreprise.

Pour les employés, la difficulté réside au niveau de la capacité qu'a la société de conserver toutes les traces laissées par la personne connectée et, ainsi, à porter atteinte au respect de sa vie privée.

L'équilibre entre les exigences de rentabilité et de sécurité des entreprises, d'une part, et la préservation d'un espace de liberté individuelle sur le lieu de travail, d'autre part, est particulièrement délicat à trouver.

Techniquement, le contrôle des e-mails et de l'accès à Internet est facilité par la nature même des nouvelles technologies. Le courrier électronique peut être automatiquement sauvegardé sur le serveur informatique de l'entreprise. Le connexion à Internet fait l'objet de données d'identification comparables aux données d'une communication téléphonique (adresse du site consulté, moment et durée de la visite). Ces données font, dans la plupart des cas, également l'objet d'un enregistrement automatique sur le serveur de l'entreprise

C'est dans ce contexte que le Conseil national du travail a décidé d'adopter une convention collective de travail en vue d'assurer l'application effective des normes fondamentales qui garantissent le droit de toute personne au respect de sa vie privée et de donner un cadre légal au contrôle qu'exercent les employeurs sur l'utilisation des moyens de télécommunications mis à la disposition des travailleurs dans le respect des règles de proportionnalité et de transparence qui découlent notamment de la Convention européenne des droits de l'homme.

Les nouvelles technologies n'étant pas utilisées uniformément dans les entreprises, cette convention se veut souple pour coller véritablement à la réalité de la vie chaque société.

II - BREVE RECENSION DES NORMES JURIDIQUES EN PRESENCE

L'organisation conventionnelle du contrôle de l'employeur doit s'effectuer en respectant un ensemble d'exigences légales qui constituent autant de balises que les entreprises doivent soigneusement coordonner[1].

1. Du point de vue de l'employé

1. La convention de sauvegarde des droits de l'homme et des libertés fondamentales [2]

L'article 8 de la convention consacre le droit de chacun au respect de sa vie privée et familiale.

Ce texte contient les limites mêmes de sa portée en ce qu'il organise un système dérogatoire fondé sur l'existence d'une loi et sur la nécessité qu'il y a de rendre compatible le respect de la vie privée et la vie en société. Tout est question de proportion et de nécessité[3].

2. La recommandation n° R (89) 2 du Comité des Ministres du Conseil de l'Europe aux Etats Membres sur la protection des données à caractère personnel utilisées à des fins d'emploi[4]

L'article 3 de cette recommandation prévoit que :

« *3.1 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 de 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.

3.2 L'accord des employés ou de leurs représentants devrait être recherché avant l'introduction ou la modification de tels systèmes ou procédés, lorsque la procédure de consultation mentionnée au paragraphe 3.1 révèle une possibilité d'atteinte au droit au respect de la vie privée et de la dignité humaine des employés, à moins que d'autres garanties appropriées ne soient prévues par la législation ou la pratique nationale »

---

[1] Un tableau récapitulatif est disponible sur le site de l'Agence Wallonne des Télécommunications , www.awt.be

[2] Convention Européenne de sauvegarde des droits de l'homme et des libertés fondamentales, Rome, 4 novembre 1950

[3] R. DE BAERDEMAEKER, « Utilisation d'Internet : quelle clause prévoir ? » in *Contrat de travail*, actes du séminaire IFE du 14 et 15 février 20 01, Bruxelles, p. 3.

[4] Adoptée par le Comité des Ministres le 18 janvier 1989.

3. La Constitution belge

« *Chacun a droit au respect de sa vie privée et familiale, sauf dans les conditions fixées par la loi* » (Constitution, art. 22)

Ce droit est susceptible de dérogation.

« *Le secret des lettres est inviolable* » (Constitution, art. 29)

4. La loi relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel

Le traitement des données à caractère personnel n'est autorisé que dans certaines hypothèses.

Préalablement, la loi définit le « traitement » comme étant : « *toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données à caractère personnel, …*». (art1, § 2)

Les données à caractère personnel sont quant à elles : « *toute information concernant une personne physique identifiée ou identifiable* » (art1, §1).

L'article 5 prévoit de manière exhaustive, les cas dans lesquels le traitement de données à caractère personnel peut être effectué et notamment l'accord indubitable de la personne concernée et que le traitement soit nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures pré-contractuelles prises à la demande de celle-ci.

L'article 4 fixe pour sa part les conditions auxquelles est soumis ce traitement en disposant que les données à caractères personnel doivent être :

« *1° traitées loyalement et licitement;*

2° collectées pour des finalités déterminées, explicites et légitimes, et ne pas être traitées ultérieurement de manière incompatible avec ces finalités, … ;

3° adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont obtenues et pour lesquelles elles sont traitées ultérieurement;

4° exactes et, si nécessaire, mises à jour…;

5° conservées sous une forme permettant l'identification des personnes concernées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont obtenues ou pour lesquelles elles sont traitées ultérieurement… ».

5. La législation pénale

L'article 314bis du Code pénal organise la répression d'un certain nombre de faits liés à l'écoute intentionnelle et la prise de connaissance éventuellement par enregistrement des communications ou des télécommunications privées[5].

Il est toutefois prévu que cette disposition ne s'appliquera pas en cas de consentement de tous les intervenants.

6. Loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques (dite loi « belgacom »)

L'article 109 ter D de cette loi énonce l'interdiction pour les tiers de prendre connaissance et d'utiliser des données transmises par voie de télécommunication, assortie toutefois d'une exception dans le cas où le tiers obtient l'autorisation de toutes les personnes qui participent aux communications[6].

« *Sous réserve de l'autorisation de toutes les autres personnes directement ou indirectement concernées par l'information, l'identification ou les données visées ci-après, il est interdit à quiconque, qu'il agisse personnellement ou par l'entremise d'un tiers :*

1° de prendre frauduleusement connaissance de l'existence de signes, de signaux, d'écrits, d'images, de sons ou de données de toute nature transmis par voie de télécommunications, en provenance d'autres personnes et destinées à celles-ci (modifié par l'article 13, § 2, 1° de la loi du 30 juin 1994) ;

2° de transformer ou de supprimer frauduleusement par n'importe quel procédé technique l'information visée au 1° ou d'identifier les autres personnes ;

3° de prendre connaissance intentionnellement de données en matière de télécommunications, relatives à une autre personne ;

4° de révéler ou de faire usage quelconque de l'information, de l'identification et des données obtenues intentionnellement ou non, et visées aux 1°, 2°, 3°, de les modifier ou de les annuler »

7. Loi du 8 avril 1965 instituant les règlements de travail

« Le règlement de travail doit indiquer …

5° les droits et obligations du personnel de surveillance » (art. 6).

---

[5] R. DE BAERDEMAEKER, *op.cit*, p. 3.

[6] Convention collective de travail relative à la protection de la vie privée des travailleurs a l'égard du contrôle des données des communications électroniques, Rapport du Conseil national du Travail, 26 avril 2002, p. 3.

8. Proposition de loi du 29 août 2001 visant à réglementer l'utilis ation des moyens de télécommunications sur le lieu de travail[7]

« *L'employeur qui entend exercer un contrôle sur l'utilisation des moyens de communication mis à disposition des travailleurs sur le lieu de travail, doit, préalablement à la mise en oeuvre de la mesure de contrôle envisagée, informer les travailleurs directement ou indirectement visés par cette mesure, sur la nature, les finalités et les modalités du contrôle envisagé ainsi que sur les sanctions susceptibles d'être prises par l'employeur à l'encontre des travailleurs convaincus d'avoir enfreint les règles fixées par ce dernier.*

Peuvent justifier un contrôle des communications, les finalités suivantes :

a) protéger les droits et libertés d'autrui,

b) protéger les biens et les secrets de fabrication de l'entreprise contre la destruction ou le vol,

c) satisfaire aux exigences de sécurité au travail,

d) contrôler les prestations du travailleur et la manière dont celui-ci s'acquitte de sa mission,

e) garantir le respect des bonnes mœurs sur le lieu de travail,

f) assurer la prévention, la recherche et la détection d'actes susceptibles d'engager la responsabilité de l'employeur,

g) empêcher la divulgation d'informations confidentielles ou préjudiciables pour l'entreprise, ses contractants, les tiers ou les autres travailleurs,

h) garantir la sécurité et le bon fonctionnement du réseau,

i) Prévenir et détecter toute utilisation du service concerné qui serait abusive ou incompatible avec les règles fixées par l'employeur.

La surveillance exercée par l'employeur dans le cadre de la présente loi doit être adéquate, pertinente et non excessive au regard de la finalité de contrôle poursuivie. Les données recueillies à l'occasion du contrôle ne peuvent être utilisées par l'employeur de manière incompatible avec la finalité précisée »

Cette proposition de loi est pour l'instant à l'examen auprès de la commission des affaires sociales du Sénat[8].

[7] *Doc. parl*, Sénat, sess. ord. 2001-2002, n° 2-891/1.
[8] Elle l'est toujours en date du 18 mai 2002.

9. La convention collective n° 39 du 13 décembre 1983 concernant l'information et la concertation sur les conséquences sociales de l'introduction des nouvelles technologies

Cette convention prévoit, en son article 2, § 1, que :

« *Lorsque l'employeur 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 ou les conditions de travail, il est tenu, au plus tard trois mois avant le début de l'implantation de la nouvelle technologie, d'une part de fournir une information écrite sur la nature de la nouvelle technologie, sur les facteurs qui justifient son introduction ainsi que sur la nature des conséquences sociales qu'elle entraîne et d'autre part, de procéder à une concertation avec les représentants des travailleurs sur les conséquences sociales de l'introduction de la nouvelle technologie* ».

2. Du point de vue de l'employeur

1. L'article 544 du Code civil

« *La propriété est le droit de jouir et disposer des choses de la manière la plus absolue, pourvu qu'on en fasse pas un usage prohibé par les lois et les règlements* ».

Les moyens de communication appartiennent à l'employeur et sont mis à la disposition du travailleur dans le cadre normal de l'exercice du contrat de travail.

2. La Loi relative au contrat de travail[9]

Les principes affirmés dans les articles 16, 17 et 18 de la loi sur le contrat de travail, restent, par excellence, l'expression des obligations qu'ont, dans la relation de travail qui les lies, le travailleur et l'employeur. C'est dans le respect de ces règles fondamentales que se situe naturellement la convention collective de travail[10].

En vertu de l'article 16 « *l'employeur et le travailleur se doivent le respect et des égards mutuels…* ».

[9] Loi du 3 juillet 1978

[10] Convention collective de travail relative à la protection de la vie privée des travailleurs a l'égard du contrôle des données des communications électroniques en réseau, 26 avril 2002, Rapport, p. 5.

L’article 17 prévoit que le travailleur a l'obligation, notamment « *d'agir conformément aux ordres et aux instructions qui lui sont données par l’employeur, ses mandataires ou ses préposés, en vue de l'exécution du contrat* », de s'abstenir, tant au cours du contrat qu'après la cessation de celui-ci « *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* » et « *de se livrer ou de coopérer à tout acte de concurrence déloya*le ».

La responsabilité de l’employé est limitée par l’article 18 :

« *En cas de dommages causés par le travailleur à l’employeur ou à des tiers dans l'exécution de son contrat, le travailleur ne répond que de son dol et de sa faute lourde. Il ne répond de sa faute légère que si celle-ci présente dans son chef un caractère habituel plutôt qu’accidentel…* »

3. L’article 1384 du Code civil

Responsabilité du fait d'autrui : « *on est responsable non seulement du dommage que l’on cause, mais également de celui qui est causé par le fait des personnes dont on doit répondre ou des choses que l’on a sous sa garde* ».

III - LES INCERTITUDES DE LA JURISPRUDENCE

1. Jalons pour une protection de la vie privée des travailleurs sur le lieu de travail : l'arrêt NIEMIETZ c. ALLEMAGNE[11]

Dans cette affaire, la Cour Européenne des Droits de l'Homme a estimé qu'il serait trop restrictif de limiter le respect de la vie privée à un « *cercle intime* » et d'en écarter le monde du travail.

Elle consacrait ainsi le fait que la notion de vie privée englobe également la vie professionnelle de chacun.

« *Le respect de la vie privée doit aussi englober, dans une certaine mesure, le droit pour l'individu de nouer et développer des relations avec ses semblables.*

Il paraît, en outre, n'y avoir aucune raison de principe de considérer cette manière de comprendre la notion de "vie privée" comme excluant les activités professionnelles ou commerciales: après tout, c'est dans leur travail que la majorité des gens ont beaucoup, voire le maximum d'occasions de resserrer leurs liens avec le monde extérieur.

Un fait, souligné par la Commission, le confirme: dans les occupations de quelqu'un, on ne peut pas toujours démêler ce qui relève du domaine professionnel de ce qui en sort. Spécialement, les tâches d'un membre d'une profession libérale peuvent constituer un élément de sa vie à un si haut degré que l'on ne saurait dire en quelle qualité il agit à un moment donné ».

Ce principe est cependant d'une application plus délicate à l'heure des nouvelles technologies. En effet, le phénomène de convergence ne permet plus de distinguer nettement ce qui relèverait de la vie professionnelle et ce qui ressortirait à l'intimité de la vie privée : le disque dur de l'ordinateur est également "bavard" dans un domaine que dans l'autre[12].

Le message électronique envoyé ou reçu dans les mêmes conditions techniques qu'il soit d'ordre professionnel ou personnel, la consultation de sites internet s'opère à l'identique quelle que soit la nature du site et le motif de la connexion[13].

2. Les premières décisions de la jurisprudence belge

Dès 1990, la Cour de cassation de Belgique décidait que les conversations téléphoniques sont comprises dans la notion de vie privée et de correspondance, et de ce fait, protégées par l'article 8 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales[14].

---

[11] Cour.eur.D.H., 16 décembre 1992, *J.T.T.*, 1994, p. 65 et sur www.echr.coe.int
[12] Rapport relatif à la cybersurveillance sur les lieux de travail, CNIL, 5 février 2002, p. 8 , www.cnil.fr,
[13] *Ibidem*, p. 8
[14] Cass., 10 avril 1990, *Pas*., p. 932.

La plupart des employés se voient aujourd'hui octroyer une adresse de messagerie et un accès à Internet par leur employeur. Cet outil est destiné à leur permettre d'accéder à différentes informations nécessaires pour leur travail et à correspondre de manière rapide avec leurs collègues ou avec des clients. Ce faisant, l'employeur offre à ses employés un outil de travail performant.

En vue de maintenir un environnement de travail professionnel et de protéger les informations confidentielles, les entreprises ont établi des chartes ou directives d'utilisations d'Internet, visant à limiter l'utilisation du courrier électronique et l'accès à Internet.

Les entreprises ont également instauré des règles relatives à la surveillance des courriers électroniques et de l'accès à l'Internet.

La doctrine belge a tranché en faveur des employés en estimant que « *toutes les communications passées par un travailleur, depuis l'entreprise, sont des communications privées au sens de la loi du 30 juin 1994 relative à la protection de la vie privée contre les écoutes, la prise de connaissance et l'enregistrement de communication et de télécommunications, et à ce titre, il est donc interdit à l'employeur d'écouter ces communications ou de les enregistrer, sauf si le travailleur l'y autorise*[15] »

Les tribunaux ont également été contraint de prendre position face au licenciement d'employés suite à l'usage abusif des courriers électroniques. Ces affaires sont particulièrement délicates à aborder parce qu'elles sont en rapport étroit avec la protection de la vie privée.

2.1. Tribunal du Travail de Bruxelles, 10 avril 1999[16]

Dans cette première affaire, un salarié d'une entreprise exerce, en dehors de ses heures de travail, une activité de travailleur indépendant de revendeur de matériel informatique.

Dans le cadre de son activité professionnelle étrangère à celle de son employeur, il utilise, durant ses heures de travail rémunérées par son employeur, l'infrastructure de l'entreprise ainsi que sa messagerie professionnelle, et ce, sans aucune autorisation.

Suite à ces découvertes, l'entreprise licencie cet employé pour faute grave.

Le tribunal de travail de Bruxelles a estimé que l'attitude indélicate et fautive du salarié pouvait justifier une mise en garde, voire un licenciement moyennant un préavis, mais non un licenciement pour faute lourde.

[15] L. BALLARIN, « le respect de la vie privée et la relation de travail », *Rev. Trav.*, 1997, p. 27.
[16] Trib. trav. Bruxelles, 10 avril 1999, www.droit -technologie.org

2.2. Tribunal du Travail de Bruxelles, 2 mai 2000[17]

Dans cette deuxième affaire, il est reproché à l'employé d'une étude d'huissier de justice d'avoir entretenu une abondante correspondance électronique de nature privée avec une de ses collègues.

S'inquiétant de l'absence de productivité de son travailleur, l'employeur a pris la décision d'effectuer un contrôle général de l'activité de celui-ci. Le contrôle a montré que l'employé avait échangé avec l'une des ses collègues plusieurs centaines de mails privés en onze jours, depuis son ordinateur de bureau. A la lumière de ces faits, l'employé indélicat avait donc été licencié pour motif grave sans préavis et sans indemnité.

Hormis, le fait de savoir si ce licenciement était ou non abusif, le tribunal a dû préciser si l'employeur avait effectivement le droit de produire en justice la copie du contenu des courriers électroniques du travailleur licencié.

Pour le Tribunal, ces messages relevaient de la sphère privée et étaient donc protégés par l'article 8 de la Convention européenne des droits de l'homme. Le fait que ces messages aient été échangés pendant les heures de travail, sur le lieu de travail et avec le matériel de bureau n'était pas, selon les juges, de nature à affecter la protection du contenu de ces correspondances.

Ainsi, après avoir précisé que le droit à la protection à la vie privée n'était pas absolu « notamment lorsque cette protection se heurte à des droits opposés tel le droit de contrôle de l'employeur », le tribunal a souligné que cet outil ne saurait conduire à substituer au contrôle normal de productivité, la surveillance électronique.

Dès lors, en vue de respecter la vie privée des employés, les contrôles éventuellement mis en oeuvre ne peuvent porter que sur le volume des messages échangés, la taille des messages échangés et le format des pièces jointes.

2.3. Tribunal du Travail de Bruxelles, 22 juin 2000[18]

Dans cette affaire, un employé avait envoyé à l'une de ses collègues un courrier électronique contenant une photo pornographique. Qui plus est, il avait tenu des propos dénigrants à l'égard de son employeur et s'était offert un abonnement « X » sur le compte de la société.

Licencié pour motif grave suite à ces faits, le travailleur postule le rejet de ces pièces conformément aux articles 109ter D de la loi dite « Belgacom » et à l'article 314bis du code pénal.

[17] Trib. trav. Bruxelles, 2 mai 2000, www.droit -technologie.org
[18] Trib. trav. Bruxelles, 22 juin 2000, www.droit -technologie.org

Le tribunal a donné tort à l'employé en relevant que, conformément à l'enseignement de la Cour de cassation[19], le droit au respect de la vie privée n'est pas absolu et ne peut empêcher, en vertu de ses obligations personnelles découlant de l'article 17 de la loi sur le contrat de travail, que l'employeur veille au respect des convenances et des bonnes mœurs au sein de l'entreprise.

En fin de compte, le tribunal estima que la seule tenue de propos dénigrant suffisait à établir le motif grave, la circonstance étant aggravée par le fait que le message fut envoyé en copie à d'autres travailleurs.

2.4. Tribunal du travail de Verviers, 20 mars 2002[20]

Tout comme dans la première affaire, un employé utilise le matériel de la société informatique de la société qui l'emploie, pour exercer une activité parallèle.

Après avoir contrôlé l'ordinateur de son employé et découvert son activité parallèle, la société le licencie pour motif grave.

L'entreprise se défend d'avoir violé l'article 29 de la constitution (secret de la correspondance) et l'article 8 de la Convention européenne des droits de l'homme, au motif que l'employeur a un droit de contrôle des activités déployées par son travailleur.

Le tribunal, s'appuyant sur le déjà célèbre arrêt « *Nikon*[21] » de la Cour de cassation française, a donné tort à l'employeur.

Dans cet arrêt, rendu le 2 octobre 2001, un employeur avait licencié un salarié après avoir constaté, en ouvrant le disque dur du collaborateur et ouvert un fichier « personnel », que celui-ci menait une activité extra-professionnelle durant son temps de travail.

La cour a estimé que : « *le salarié a droit, même au temps et au 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* »[22].

Le tribunal du travail de Verviers, après avoir décidé que « *ce principe peut être transposé sans problème en droit belge* », a jugé que le comportement de l'employeur violait le secret de l'article 29 de la constitution (secret de la correspondance) et l'article 8 de la Convention européenne des droits de l'homme et que « *la preuve obtenue de la sorte de l'exercice d'une activité concurrente est une preuve illicite et ne peut être prise en considération dans l'appréciation du motif grave* ».

[19] Cass., 7 octobre 1981, *Pas.*, 1982, p. 194 et s.
[20] Trib. trav. Verviers, 20 mars 2002, *J.T.T*, 2002, p. 183.
[21] Cass. fr. (soc.), 2 octobre 2001, arrêt n° 4164, disponible sur www.courdecassation.fr
[22] Cass. fr. (soc.), 2 octobre 2001, arrêt n° 4164, disponible sur www.courdecassation.fr

VI - CONVENTION COLLECTIVE DE TRAVAIL RELATIVE A LA PROTECTION DE LA VIE PRIVEE DES TRAVAILLEURS A L'EGARD DU CONTROLE DES DONNEES DE COMMUNICATION ELECTRONIQUES EN RESEAU

En date du 26 avril 2002, le Conseil national du travail a adopté la convention collective du 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.

1. Portée de la convention

« *§ 1. La présente convention collective de travail a pour but de garantir le respect du droit fondamental des travailleurs au respect de leur vie privée dans la relation de travail, en définissant, compte tenu des nécessités d'un bon fonctionnement de l'entreprise, pour quelles finalités et à quelles conditions de proportionnalité et de transparence un contrôle des données de communication électroniques en réseau peut être installé et les modalités dans lesquelles l'individualisation de ces données est autorisée.*

Elle ne porte pas préjudice aux dispositions plus favorables prévues au niveau de la commission paritaire ou de l'entreprise.

§ 2. La présente convention collective de travail ne vise pas les modalités d'accès et/ou d'utilisation des moyens de communication électroniques en réseau de l'entreprise qui sont de la prérogative de l'employeur. Cette convention laisse donc en l'état les règles et pratiques d'information voire de consultation éventuellement en vigueur dans les entreprises.

Elle ne porte pas non plus préjudice aux règles et pratiques existant dans les entreprises en ce qui concerne l'exercice des activités syndicales.» (art. 1)

Elle s'attache ainsi à établir un strict équilibre entre d'une part, la protection de la vie privée du travailleur sur le lieu de travail, et d'autre part, les prérogatives de l'employeur lui permettant d'assurer le bon fonctionnement de l'entreprise[23].

Le champ d'application de la convention est clairement défini et exclut de manière exprès les modalités d'accès et d'utilisation des ressources informatiques de l'entreprise, et ce, conformément, à l'obligation qu'a le travailleur d'exécuter son contrat conformément aux instructions qui lui sont données par son employeur.

De la sorte, l'employeur peut, librement déterminer les modalités d'utilisation du courrier électronique et de l'Internet qui sont permises, tolérées ou interdites.

[23] Commission de la protection de la vie privée, Avis d'initiative relatif à la surveillance par l'employeur de l'utilisation du système informatique sur le lieu de travai l, avis n° 10/2000 du 3 avril 2000, p. 13.

Cependant, il ne peut établir les finalités et les modalités de contrôle de l'utilisation des moyens de télécommunication mis à la disposition du personnel que moyennant le respect des conditions prescrites dans cette convention.

La fixation de ces conditions assure tant à l'employeur qu'au travailleur une sécurité juridique[24].

2. Notion de données de communication électroniques en réseau

« O*n entend par données de communication électroniques en réseau les 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* » (art. 2).

Par cet article, on a entendu souligner que cette convention s'inscrit dans un principe de neutralité technologique.

En effet, la Commission nationale du travail a défini un cadre suffisamment large pour englober l'ensemble des technologies en réseau, tout en ne perdant pas de vue l'imbrication croissante et l'évolution rapide de ces technologies et du support auquel elles recourent.

On peut cependant regretter que cette convention collective n'ait pas différencié le contrôle des e-mails de celui des sites Internet visités

3. Engagement réciproque des parties

« *Les organisations signataires affirment les principes suivants :*

- *Les travailleurs reconnaissent le principe selon lequel 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, compte tenu des modalités d'application prévues par la présente convention ;*

- *Les employeurs respectent le droit des travailleurs à la protection de leur vie privée dans le cadre de la relation de travail et des droits et obligations que celle-ci implique pour chacune des parties* » (art. 3)

Jusqu'à présent, l'employeur était privé de toute possibilité (légale) de contrôle sur les communications de ses employés, sauf consentement de tous les « intéressés ».

[24] Exposée des motifs, Proposition de loi visant à réglementer l'utilisation des moyens de télécommunication sur le lieu du travail, *op. cit.*

Le problème résidait dans le fait que les dispositions existantes (l'article 109*ter* D de la loi « belgacom » et l'article 314*bis* du Code pénal) ne sont pas adaptées à la spécificité des relations professionnelles. Ces dispositions ne font, en effet, aucune distinction entre les communications privées et les communications professionnelles.

Cette convention collective permet, aujourd'hui, moyennant une information préalable et le respect de certaines conditions, d'effectuer un contrôle des données des communications électroniques du travailleur (art 7 et s.).

Elle prévoit que les employés reconnaissent, à l'entreprise, un droit de contrôle sur l'outil de travail et sur l'utilisation de celui-ci.

4. Modalités d'application de la convention collective

4.1. CONTROLE DES DONNEES

Le désir de contrôle de l'employeur est légitime et nécessaire. Mais ce contrôle ne peut être sans limite, dès lors qu'il existe une utilisation personnelle d'Internet par le salarié sur le lieu de travail. En effet, le contrôle ne doit pas porter une atteinte excessive à la vie privée du salarié, [25]ou à ses libertés individuelles et collectives, et notamment au secret de sa correspondance. Un équilibre doit donc être trouvé entre un usage personnel raisonnable et un contrôle proportionné.

Le contrôle des données de communication électroniques en réseau n'est autorisé que pour autant qu'il soit satisfait aux principes de finalité, de proportionnalité et de transparence que les conditions de procédures définies dans cette convention, visent à garantir.

L'employeur se voit donc reconnaître la possibilité d'effectuer un contrôle sur les données de communication électronique en réseau à caractère personnel à la seule condition que ce contrôle soit effectué pour une ou plusieurs des finalités reconnues comme légitimes.

[25] « Rapport d'étape du groupe de travail "relations du travail et Inter net" », 28 février 2002, *Forum des droits sur l'Internet,* p. 10, www.foruminternet.org.

1. Principe de finalité

« *§ 1. Le contrôle de données de communication électroniques en réseau n'est autorisé que lorsque l'une ou plusieurs des finalités suivantes est ou sont poursuivies :*

1° la prévention de faits illicites ou diffamatoires, de faits contraires aux bonnes mœurs ou susceptibles de porter atteinte à la dignité d'autrui ;

2° la protection des intérêts économiques, commerciaux et financiers de l'entreprise auxquels est attaché un caractère de confidentialité ainsi que la lutte contre les pratiques contraires ;

3° la sécurité et/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° le respect de bonne foi des principes et règles d'utilisation des technologies en réseau fixés dans l'entreprise.

§ 2. L'employeur définit clairement et de manière explicite la ou les finalités du contrôle. » (art. 5)

Il s'agit d'une énumération exhaustive des finalités pour lesquelles le contrôle par l'employeur des données de communication électronique est autorisé. L'ingérence dans la vie d'autrui ne peut être un but en soit. Il faut que le contrôle poursuive un but précis [26]
Aucune dérogation ne peut ainsi être apportée à cette liste, sauf à la limiter en faveur du travailleur.

Les données récoltées ne peuvent donc être collectées que pour la finalité de contrôle précisée, et ne peuvent normalement être utilisées à des fins différentes[27].

Le traitement doit, en toute hypothèse, être compatible à l'objectif annoncé initialement.

Les faits illicites ou diffamatoires, faits contraires aux bonnes mœurs ou susceptibles de porter atteinte à la dignité d'autrui peuvent notamment consister en des actes de piratage informatique, dont la prise de connaissance non autorisée de données de communication électroniques en réseau relatives à la gestion du personnel ou de fichiers médicaux confidentiels, ou encore en la consultation de sites à caractère pornographique ou pédophile, de même qu'en celle de sites incitant à la discrimination, à la ségrégation, à la haine ou à la violence à l'égard d'un groupe, d'une communauté ou de leurs membres, en raison de la race, de la couleur, de l'ascendance, de la religion ou de l'origine nationale ou ethnique de ceux-ci ou de certains d'entre eux[28].

[26] 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 tra vail », *J.T.T.*, 2002, p. 169.
[27] voir toutefois les exceptions prévues à l'article 13.
[28] Convention collective de travail relative à la protection de la vie privée des travailleurs a l'égard du contrôle des données des communications électroniques, Rapport du Conseil national du Travail, 26 avril 2002, p.16

Les pratiques contraires aux intérêts financiers, économiques et commerciaux de l'entreprise peuvent notamment prendre la forme de publicité dénigrante au sens de l'article 23, 6° de la loi du 14 juillet 1991 sur les pratiques du commerce et sur l'information et la protection du consommateur, de divulgation de fichiers ainsi que de la violation des secrets d'affaires y compris la recherche et le développement, les processus de fabrication et toutes données confidentielles[29].

Il y a lieu en outre de souligner qu'en cas de surveillance secrète des données de communication électroniques en réseau, les dispositions du Code pénal s'appliquent et que cette forme de surveillance ne peut être introduite qu'en conformité avec les prescriptions du Code de procédure pénale.

2. Principe de proportionnalité

« *Par principe, le contrôle des données de communication électroniques en réseau ne peut entraîner une ingérence dans la vie privée du travailleur.*

Si toutefois ce contrôle entraîne une ingérence dans la vie privée du travailleur, cette ingérence doit être réduite à un minimum. » (art. 6)

En vertu de ce principe, le contrôle doit revêtir, dans toutes les hypothèses, un caractère adéquat, pertinent et non excessif au regard des finalités poursuivies.

L'entreprise ne peut, dans l'exercice de son contrôle, faire plus que ce qui est nécessaire pour atteindre ses objectifs.

La Commission de la protection de la vie privée a déduit de ce principe, que le contrôle ne peut nécessairement être que temporaire et concerner les personnes à l'égard desquelles il existe des soupçons d'abus[30].

On peut noter que cette convention ne précise à aucun moment si le contrôle effectué peut être ou non permanent.

Selon le rapport accompagnant cette convention collective, la fonction de contrôle est quasi indissociable des systèmes de réseau véhiculant des données de communication électroniques, « *de sorte qu'il est apparu que cette distinction risquait d'être artificielle et la préférence s'est portée sur le traitement lui-même dont la convention fixe clairement les limites par rapport au contenu des données*[31] ».

[29] Convention collective de travail relative à la protection de la vie privée des travailleurs a l'égard du contrôle des données des communications électroniques, Rapport du Conseil national du Travail, 26 avril 2002 p. 16

[30] Commission de la protection de la vie privée, Avis d'initiative relatif à la surveillance par l'employeur de l'utilisation du système informatique sur le lieu de travail, avis n° 10/2000 du 3 avril 2000

[31] *Ibidem.*, p. 7.

Cette abstention est particulièrement regrettable et risque de conduire à un contrôle permanent des données des communications électroniques en réseau au motif que la finalité poursuivie nécessite un contrôle permanent (par exemple, la protection des intérêts économiques de la société).

Ce contrôle permanent semble de plus déjà été accepté par la jurisprudence dans certains cas spécifiques[32] (en l'espèce pour surveiller l'accès à des informations confidentielles).

Néanmoins, le principe de proportionnalité développé dans cette loi, combiné au principe de nécessité, laisse à penser que cette dérive est difficilement envisageable.

De plus, dans son avis d'initiative du 3 avril 2000[33], la Commission de la protection de la vie privée a estimé que :

« *Tout contrôle devra 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.*

Il est en outre peu conforme à la dignité humaine - et pas nécessairement productif - de faire travailler des employés sous une surveillance constante ».

Ce principe a d'ailleurs été explicitement repris dans 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.

3. Principe de transparence

Ce principe de transparence est essentiel en ce qu'il implique qu'une mesure de surveillance n'est autorisée que lorsque les travailleurs ont été informés au préalable de la nature et de la finalité de la mesure envisagée ainsi que des limites du contrôle ainsi autorisé.

En effet, la norme autorisant la mesure de surveillance doit être suffisamment accessible et précise, de sorte que les personnes concernées soient à tout moment en mesure de prévoir dans quelles circonstances et à quelles conditions il peut être porté atteinte à leur vie privée

Le dialogue entre employeur et employé doit permettre d'établir de manière suffisamment détaillée les caractéristiques de la politique de contrôle de l'entreprise.

[32] Cour trav. Liège, 25 octobre 1990, *J.T.T.*,199, p. 158.
[33] Commission de la protection de la vie privée, Avis d'initiative relatif à la surveillance par l'employeur de l'utilisation du système informatique sur le lieu de travail, avis n° 10/2000 du 3 avril 2000.

Dans son avis d'initiative du 3 avril 2000[34], la Commission de la vie privée avait précisé les caractéristiques de la politique de contrôle de l'employeur dont les travailleurs devront être informés :

« - *les modalités d'utilisation du courrier électronique et de l'Internet qui sont permises, tolérées ou interdites ;*

- *les finalités et modalités du contrôle de cette utilisation (nature des données collectées, étendue et circonstances des contrôles, personnes ou catégories de personnes sujettes aux procédures de contrôle) ;*
- *l'existence d'un stockage des données de télécommunication et la durée de ce stockage, par exemple sur un serveur central, dans le cadre de la gestion technique du réseau, et les éventuels systèmes de cryptage existants ;*
- *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 de l'employé aux données à caractère personnel le concernant.* »

Toujours selon la commission, « *la transparence des méthodes de contrôle envisagées devra passer par une concertation avec les employés et leurs représentants au sein des organes de dialogue de l'entreprise ou des services concernés* »[35].

Le Conseil national du travail, n'a pas manqué d'examiner attentivement ces nécessités de transparence et de les intégrer dans cette convention collective.

Le Principe de transparence est intitulé, « *Conditions de procédure* » pour les besoins de la convention et est subdivisé en deux parties, la première relative à l'information et à son contenu, la deuxième relative aux consultations nécessaires entre les représentants des entreprises et ceux des travailleurs.

[34] Commission de la protection de la vie privée, Avis d'initiative relatif à la surveillance par l'employeur de l'utilisation du système informatique sur le lieu de travail, avis n° 10/2000 du 3 avril 2000.
[35] *Ibidem.*.

Information

Information collective (art. 7)

« *§1. L'employeur qui souhaite installer un système de contrôle des données de communication électroniques en réseau, informe le conseil d'entreprise sur tous les aspects du contrôle visés à l'article 9, § 1er de la présente convention, conformément aux dispositions de la convention collective de travail n° 9 du 9 mars 1972 coordonnant les accords nationaux et les conventions collectives de travail relatifs aux conseils d'entreprise.*

§2. A défaut de conseil d'entreprise, cette information est fournie au comité pour la prévention et la protection au travail ou, à défaut, à la délégation syndicale ou, à défaut, aux travailleurs. »

L'accent est ainsi mis sur les dispositions conventionnelles en vigueur en matière d'informations des représentants des travailleurs.

Information individuelle (art. 8)

« *§1. Lors de l'installation du système de contrôle des données de communication électroniques en réseau, l'employeur informe les travailleurs concernés sur tous les aspects du contrôle visés à l'article 9, §§ 1er et 2.*

§2. L'information fournie est effective, compréhensible et mise à jour. Le choix de son support est laissé à l'employeur.

§3. Cette information ne dispense pas les parties de respecter le principe d'exécution de bonne foi des conventions. »

Le choix du support est laissé à la discrétion de l'employeur, pour autant que l'information fournie soit effective, compréhensible et mise à jour.

Cette information pourra être réalisée, notamment, dans le cadre d'instructions générales (circulaires, affichage, etc.), par mention dans le règlement de travail, par mention dans le contrat de travail individuel ou encore par des consignes d'utilisation fournies à chaque utilisation de l'outil (mention sur écran de messages à l'allumage du poste de travail et/ou lors de l'activation de certains programmes)[36].

Il va de soi que le §2 ne dispense pas, par ailleurs, de l'application de la réglementation en la matière, prévoyant des mentions obligatoires au règlement de travail comme, par exemple, en matière de sanctions[37].

[36] Convention collective de travail relative à la protection de la vie privée des travailleurs a l'égard du contrôle des données des communications électroniques, Rapport du Conseil national du Travail, 26 avril 2002, p. 18.

[37] Convention collective de travail relative à la protection de la vie privée des travailleurs a l'égard du contrôle des données des communications électroniques, Rapport du Conseil national du Travail, 26 avril 2002, p. 18

Contenu de l'information (art. 9)

« *§1. L'information collective et individuelle visée respectivement aux articles 7 et 8, porte sur les aspects suivants du contrôle des données de communication électroniques en réseau :*

- *la politique de contrôle ainsi que les prérogatives de l'employeur et du personnel de surveillance ;*
- *la ou les finalités poursuivies ;*
- *le fait que des données personnelles soient ou non conservées, le lieu et la durée de conservation ;*
- *le caractère permanent ou non du contrôle.*

§2. En outre, l'information individuelle visée à l'article 8 porte sur :

- *l'utilisation de l'outil mis à la disposition des travailleurs pour l'exécution de leur travail, en ce compris les limites à l'utilisation fonctionnelle ;*
- *les droits, devoirs, 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.* »

Cet article a pour but de permettre un dialogue entre l'employeur et les travailleurs afin que l'introduction de cette surveillance puisse se faire dans un climat de confiance.

La situation juridique dans laquelle se trouve les intervenants et, en particulier, la sécurité juridique indispensable à la vie en société, s'en trouve grandement améliorée en ce qu'il sera dorénavant possible de fixer les limites de ce qui est autorisé et de ce qui est interdit.

Les juristes ne devront plus bricoler avec des bouts de chandelles et pourront enfin renseigner de manière claire et précise les entreprises sur les précautions et les mesures à prendre[38].

Consultation (art. 10)

« *Une évaluation des systèmes de contrôle installés est en outre réalisée régulièrement, selon le cas, au sein du conseil d'entreprise, du comité pour la prévention et la protection au travail ou avec la délégation syndicale de manière à faire des propositions en vue de les revoir en fonction des développements technologiques.* »

Cette procédure d'évaluation périodique a comme objectif de déterminer, si en raison des développements technologiques, il n'existe pas possible de mieux atteindre l'objectif de non-ingérence ou d'ingérence minimale dans la vie privée des travailleurs[39].

[38] En ce sens, H. BARTH, *op. cit*., p. 175.
[39] Convention collective de travail relative à la protection de la vie pr ivée des travailleurs a l'égard du contrôle des données des communications électroniques, Rapport du Conseil national du Travail, 26 avril 2002, p. 7

4.2. INDIVIDUALISATION DES DONNEES

1. Champ d'application

Au terme de la présente convention, il y a lieu d'entendre par individualisation des données de communication électroniques en réseau :

« *l'opération consistant à traiter des données de communication électroniques en réseau collectées lors d'un contrôle installé par l'employeur en vue de les attribuer à un travailleur identifié ou identifiable* » (art 12, §1).

La mise en œuvre des modalités d'individualisation des données de communications électroniques en réseau ne peut :

« *rendre inopérantes les garanties offertes aux employeurs et aux travailleurs par la présente convention collective de travail par l'attribution d'un caractère exclusivement professionnel ou privé à l'ensemble des données de communication électroniques en réseau* » (art. 11).

D'autre part, les règles que nous allons examiner ci-après ne s'applique pas l'objet et au contenu des données de communication électroniques en réseau dont le caractère professionnel n'est pas contesté par le travailleur.

Dans cette hypothèse, l'employeur pourra consulter ces données sans autre procédure.

L'individualisation des données de communication électroniques en réseau est, en fonction de la finalité que poursuit le contrôle, opérée, soit dans le cadre d'une procédure directe (prévue à l'articles 15), soit dans le cadre d'une procédure indirecte (prévue aux articles 16 et 17).

La procédure est dite indirecte dans la mesure où elle comporte une phase préalable d'information.

2. Principe de finalité et de proportionnalité

Tout comme le contrôle des données, leur individualisation s'inscrit dans le respect des principes de finalité, de proportionnalité (et de nécessité).

2.1. Principe de finalité (art. 13)

« *§1. L'employeur individualise les données de communication électroniques en réseau de bonne foi et en conformité avec la ou les finalités que poursuit ce contrôle.*

§ 2. Si les données de communication électroniques en réseau collectées sont traitées en vue de finalités autres que celleS pour laquelle le contrôle a été installé, l'employeur doit s'assurer que ce traitement est compatible avec la finalité initialement poursuivie et prendre toutes les mesures nécessaires pour éviter les erreurs d'interprétation. »

Ainsi, lorsque le traitement des données est effectué pour une autre finalité que celle poursuivie initialement, il doit rester compatible avec la finalité initiale.

Il est utile de rappeler que, de même que pour toute autre collecte de données, les données de télécommunications visées ne peuvent être collectées que pour la finalité de contrôle précisée, et ne peuvent être traitées ultérieurement de manière incompatible avec ces finalités, compte tenu de tous les facteurs pertinents, notamment des prévisions raisonnables de l'intéressé et des dispositions légales et réglementaires applicables[40].

2.2. Principe de proportionnalité (art.14)

« *§1. L'employeur ne peut individualiser les données de communication électroniques en réseau collectées lors d'un contrôle, d'une manière incompatible avec le ou les finalités poursuivies et visées à l'article 5, § 1er.*

§2. Sont individualisées les données de communication électroniques en réseau nécessaires à la ou les finalités poursuivies pour le contrôle. Elles doivent être adéquates, pertinentes et non excessives au regard de cette ou ces finalités. »

Les données doivent bien entendu être traitées loyalement et licitement.

En tout état de cause, seules les données de communication électroniques pourront être individualisées.

Leur contenu ne pourra en aucune manière être attribué à un travailleur identifié ou identifiable (individualisé) à moins d'obtenir l'accord exprès et préalable de tous les participants à la communication.

[40] Loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel, *M.B.*, 18 mars 1993, art. 4.

3. Conditions de procédure

3.1. individualisation directe des données de communication électroniques en réseau

« *L'individualisation directe des données de communication électroniques en réseau est autorisée lorsque le contrôle poursuit l'une ou plusieurs des finalités visées à l'article 5, § 1er, 1°, 2° et 3°* » (art.15)

Cet article permet à l'employeur qui constate une anomalie, de procéder directement, à partir des données globales dont il dispose, à une individualisation des données de manière à retracer l'identité du responsable de l'anomalie.

Cette individualisation directe n'est autorisée que lorsque le contrôle est destiné à (1°) la prévention de faits illicites ou diffamatoires, de faits contraires aux bonnes mœurs ou susceptibles de porter atteinte à la dignité d'autrui, (2°) la protection des intérêts économiques, commerciaux et financiers de l'entreprise auxquels est attaché un caractère de confidentialité ainsi que la lutte contre les pratiques contraires et (3°) à la sécurité et/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 ;

En pratique, les éventuelles anomalies peuvent être constatées par la consultation périodique des données de communication électroniques en réseau (statistiques par exemple) collectées dans l'entreprise ou par toute autre source d'information[41].

3.2. Individualisation indirecte de données de communication électroniques en réseau, moyennant le respect d'une phase préalable d'information

Individualisation indirecte

« *§1. L'individualisation des données de communication électroniques en réseau n'est autorisée que moyennant le respect d'une phase préalable d'information lorsque le contrôle poursuit la finalité visée à l'article 5, § 1er, 4°.*

§2. L'information visée au § 1er a pour objet de porter à la connaissance du ou des travailleurs, de manière certaine et compréhensible, l'existence de l'anomalie et de les avertir d'une individualisation des données de communication électroniques en réseau lorsqu'une nouvelle anomalie de même nature sera constatée » (art. 16)

Cet article concerne donc les atteintes au respect, de bonne foi, des principes et règles d'utilisation des technologies en réseau, fixés dans l'entreprise.

[41] Convention collective de travail relative à la protection de la vie privée des travailleurs a l'égard du contrôle des données des communications électroniques en réseau, 26 avril 2002, Rapport, p. 22.

Cette information vise à éviter la survenance d'une nouvelle anomalie de même nature et a donc, un caractère principalement dissuasif. Il s'agit d'une véritable procédure de « *sonnette d'alarme* » qui informe les travailleurs d'une anomalie et d'une individualisation des données en cas de récurrence.

Il s'agit ici principalement des utilisations des ressources informatiques qui, bien que ne portant pas directement atteinte aux intérêts économiques de l'entreprise ou à sa sécurité, pénalisent la productivité de celle-ci. On pense notamment à un usage abusif des courriers électroniques à caractère privé, à la consultation excessive de sites Internet à caractère non professionnel (bourse, résultas sportifs, sites pornographiques, échange de blagues, …).

L'entreprise pourra donc individualiser ce type de données mais devra auparavant passer par une phase préalable d'information.

Phase préalable d'information

« *§1. Le travailleur auquel une anomalie d'utilisation des moyens de communication électroniques en réseau peut être attribuée par application de la procédure d'individualisation indirecte visée à l'article 16, sera invité à un entretien par l'employeur.*

Cet entretien est préalable à toute décision ou évaluation susceptible d'affecter individuellement le travailleur.

Il a pour but de permettre au travailleur de faire part à l'employeur de ses objections vis-à-vis de la 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.

§2. Le § 1er n'est pas d'application en cas de suspension de l'exécution du contrat de travail pour quelque cause que ce soit. » (art. 17)

Cette phase a pour objet de prévoir un entretien auquel l'employeur invite le travailleur afin de permettre d'éviter les éventuels malentendus et contribuer à ré-instaurer un climat de confiance entre l'employeur et le travailleur. « *Autrement dit, un employeur ne pourra plus licencier quelqu'un pour mauvais usage des technologies sans être passé par cette phase de dialogue*[42] ».

Cet entretien va permettre au travailleur de s'expliquer sur l'utilisation faite des moyens de communication électronique en réseau mis à sa disposition. Le travailleur pourra, s'il le souhaite, se faire assister d'un délégué syndical[43].

En pratique, cet entretien est instauré lorsque le travailleur responsable d'une anomalie est identifié et se déroule donc, parallèlement, à l'individualisation des données.

---

[42] V. GENOT et L. VAN RUYMBEKE, « votre patron sait tout sur vous », *le vif l'express*, 25 janvier 2002, p. 39.

[43] Convention collective de travail relative à la protection de la vie privée des travailleurs a l'égard du contrôle des données des communications él ectroniques en réseau, 26 avril 2002, p. 9

V - CONCLUSIONS

Espérons que cette nouvelle convention collective de travail apporte enfin la sécurité juridique indispensable en cette matière particulièrement sensible.

On a voulu combler l'absence de législation qui entoure l'utilisation des nouvelles technologies et construire un véritable squelette autour duquel chaque société va pouvoir exercer un contrôle sur les membres de son personnel.

Qu'on ne se trompe néanmoins pas, cette convention est née du souhait des employeurs d'avoir un cadre légal pour mettre en place un contrôle sans risquer de devoir affronter des procès à l'issue incertaine.

Certaines notions, comme « la protection des intérêts économiques, commerciaux et financiers de l'entreprise » ou « la sécurité et le bon fonctionnement des systèmes informatiques », sont très larges et laissent une grande marge de manœuvre aux entreprises.

Il appartiendra à la jurisprudence de consacrer cette convention et d'en préciser les contours un peu trop souples.

Soulignons quand même que cette convention tend à ce que le contrôle ne puisse donner lieu qu'à une ingérence, réduite au minimum, dans la vie privée du travailleur.

L'objectif n'est pas de tout contrôler mais de permettre à l'entreprise de fonctionner de manière performante.

Bibliographie

1. Législation

- Convention de sauvegarde des droits de l'homme et des libertés fondamentales, Rome, 4 novembre 1950, approuvée par la loi du 13 mai 1955, *M.B.*, 19 août 1955, art 8.
- Recommandation n° R (89) 2 du Comité des Ministres du Conseil de l'Europe aux Etats Membres sur la protection des données à caractère personnel utilisées à des fins d'emploi, adoptée par le Conseil des Ministres le 18 janvier 1989, art. 3.
- Constitution, art. 22 et 29
- Code pénal, art. 314 bis
- Code civil, art. 544 et 1384
- Loi du 8 avril 1965 instituant les règlements de travail, *M.B.*, 5 mai 1965, art. 6
- La Loi relative au contrat de travail du 3 juillet 1978, *M.B.*, 22 août 1978, art. 16, 17 et 18
- Loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques, *M.B.*, 27 mars 1991, art. 109 ter D
- Loi du 8 décembre 1992, relative à la vie privée à l'égard des traitements de données à caractère personnel, *M.B.*, 18 mars 1993, modifiée parla loi du 11 décembre 1998, art. 1 et s.
- Proposition de loi du 29 août 2001 visant à réglementer l'utilisation des moyens de télécommunications sur le lieu de travail, *Doc. parl*, Sénat, sess. ord. 2001-2002, n° 2-891/1.
- Convention collective n° 39 du 13 décembre 1983 concernant l'information et la concertation sur les conséquences sociales de l'introduction des nouvelles technologies, art. 2
- Convention collective du travail n° 81 du 26 avril 2002, relative à la protection de la vie privée des travailleurs à l'égard du contrôle des données de communication électroniques en réseau

2. Etudes doctrinales

- BALLARIN, L., « le respect de la vie privée et la relation de travail », *Rev. Trav.*, 1997, p. 3 et s.
- BARTH, H., « 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, p. 169 et s.
- CNIL, Rapport relatif à la cybersurveillance sur les lieux de travail, 5 février 2002, p. 8 , www.cnil.fr,

- DE BAERDEMAEKER, R., « Utilisation d'Internet : quelle clause prévoir ? » in *Contrat de travail*, actes du séminaire IFE du 14 et 15 février 2001, Bruxelles
- GENOT, V., et VAN RUYMBEKE, L., « votre patron sait tout sur vous », *le vif l'express*, 25 janvier 2002, p. 36 et s.
- LAGASSE, F., « La vie privée et le droit du travail », CDS, 1997, p. 417.
- LEDUC, P., « Le contrôle des communications données ou reçues par le travailleurs », *Revue Ubiquité*, 2000, n° 5.
- RIJCKERT, O., « Le contrat de travail face aux nouvelles technologies », *Orientations*, 2000, p. 201 et s.
- VERBIEST, T., « la surveillance de l'usage de l'Internet dans l'entreprise : quelle légalité ? », à consulter sur www.droit-technologie.org.
- Agence Wallonne des Télécommunications, tableau récapitulatif des normes applicables en matière de « cybersurveillance », à consulter sur www.awt.be
- « Rapport d'étape du groupe de travail "relations du travail et Internet" », 28 février 2002, *Forum des droits sur l'Internet*, p. 10, à consulter sur www.foruminternet.org.

3. Décisions de jurisprudence

- Cour.eur.D.H., arrêt *Niemietz c/ l'Allemagne*, 16 décembre 1992, *J.T.T.*, 1994, p. 65
- Cass., 7 octobre 1981, *Pas.*, 1982, p. 194 et s.
- Cass., 10 avril 1990, *Pas.*, p. 932.
- Cass. fr. (soc.), 2 octobre 2001, arrêt n° 4164, à consulter sur www.courdecassation.fr
- Cour trav. Liège, 25 octobre 1990, *J.T.T.*,199, p. 158.
- Trib. trav. Bruxelles, 10 avril 1999, R.G. n° 70520/98, à consulter sur www.droit-technologie.org
- Trib. trav. Bruxelles, 2 mai 2000, R.G. n° 93.534/99, à consulter sur www.droit-technologie.org
- Trib. trav. Bruxelles, 22 juin 2000, R.G. n° 1471/99, à consulter sur www.droit-technologie.org
- Trib. trav. Verviers, 20 mars 2002, *J.T.T*, 2002, p. 183.
- Commission de la protection de la vie privée, Avis d'initiative relatif à la surveillance par l'employeur de l'utilisation du système informatique sur le lieu de travail, avis n° 10/2000 du 3 avril 2000, à consulter sur www.privacy.fgov.be

Table des matières

I - INTRODUCTION p. 1

II - BREVE RECENSION DES NORMES EN PRESENCE p. 2

1. Du point de vue de l'employé p. 2

1. La convention de sauvegarde des droits de l'homme et des libertés fondamentales p. 2
2. La recommandation n° R (89) 2 du Comité des Ministres du Conseil de l'Europe aux Etats Membres sur la protection des données à caractère personnel utilisées à des fins d'emploi p. 2 p. 2
3. La constitution belge p. 3
4. La loi relative à la vie privée à l'égard des traitements de données à caractère personnel p. 3
5. La législation pénale p. 4
6. Loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques (ou loi « belgacom ») p. 4
7. Loi du 8 avril 1965 instituant les règlements de travail p. 4
8. Proposition de loi du 29 août 2001 visant à réglementer l'utilisation des moyens de télécommunications sur le lieu de travail p. 5
9. La convention collective n° 39 du 13 décembre 1983 concernant l'information et la concertation sur les conséquences sociales de l'introduction des nouvelles technologies p.6

2. Du point de vue de l'employeur p. 6

2.1. L'article 544 du Code civil p. 6
2.2. La Loi relative au contrat de travail p. 6
2.3. L'article 1384 du Code civil p. 7

III - LES INCERTITUDES DE LA JURISPRUDENCE p. 8

1. Jalons pour une protection de la vie privée des travailleurs sur le lieu de travail : l'arrêt NIEMIETZ c. ALLEMAGNE p. 8

2. Les premières décisions de la jurisprudence belge p. 8

2.1. Tribunal du Travail de Bruxelles, 10 avril 1999 p. 9
2.2. Tribunal du Travail de Bruxelles, 2 mai 2000 p. 10
2.3. Tribunal du Travail de Bruxelles, 22 juin 2000 p. 10
2.4. Tribunal du travail de Verviers, 20 mars 2002 p. 11

IV - LA CONVENTION COLLECTIVE RELATIVE A LA PROTECTION DE LA VIE PRIVEE DES TRAVAILLEURS A L'EGARD DU CONTROLE DES DONNEES DE COMMUNICATION ELECTRONIQUES EN RESEAU p. 12

1. Portée de la convention p. 12

2. Notion de données de communication électroniques en réseau p. 13

3. Engagement réciproque des parties p. 13

4. Modalités d'application de la convention collective p. 14

4.1. contrôle des données p. 14

1. Principe de finalité p. 15
2. Principe de proportionnalité p. 16
3. Principe de transparence p. 17

Information p. 19

Information collective p. 19
Information individuelle p. 19
Contenu de l'information p. 20

Consultation p. 20

4.2. individualisation des données p. 21

1. Champ d'application p. 21

2. Principe de finalité et de proportionnalité p. 21

2.1. Principe de finalité p. 22
2.2. Principe de proportionnalité p. 22

3. Conditions de procédure p. 23

3.1. Individualisation directe des données de communication électroniques en réseau p. 23

3.2. Individualisation indirecte de données de communication électroniques en réseau, moyennant le respect d'une phase préalable d'information p. 23

3.2.1. Individualisation indirecte p. 23
3.2.2. Phase préalable d'information p. 24

V - CONCLUSIONS p. 25

BIBLIOGRAPHIE p. 26