

FGTB

CCT N° 81

**un équilibre trouvé entre
le respect de la vie privée des travailleur(se)s
et le contrôle légitime de l'employeur**



CCT N° 81

**un équilibre trouvé entre
le respect de la vie privée des travailleur(se)s
et le contrôle légitime de l'employeur**

Table de matière

AVANT-PROPOS	
La CCT n° 81: un équilibre trouvé entre le respect de la vie privée des travailleur(se)s et le contrôle légitime de l'employeur	7
I. LES CONSTATS	9
II. LES PRINCIPES GARANTIS PAR LA CCT N° 81	10
2.1. Le respect de la vie privée des travailleurs	10
2.2. Le droit de contrôle de l'employeur et les obligations respectives des parties	11
III. LA CCT N° 81 DANS LA PRATIQUE	12
3.1. Champ d'application	12
3.2. Lors de l'installation du système de contrôle	12
3.2.1. Obligation d'informer	12
3.2.1.1. Information collective	12
3.2.1.2. Information individuelle	12
3.2.2. Principes de contrôle	15
3.2.2.1. Par principe, le contrôle des données ne peut entraîner une ingérence dans la vie privée du travailleur	15
3.2.2.2. Seule la poursuite de certaines finalités permet un contrôle	16
3.3. Après l'installation du système de contrôle	17
3.3.1. Individualisation	17
3.3.1.1. Principes	17
3.3.1.2. L'individualisation peut être synthétisée comme suit	18
3.3.2. Evaluation dans l'entreprise	21
3.3.2.1. Une évaluation des systèmes de contrôle installés est réalisée régulièrement	21
3.3.2.2. Intervenir en cas de risque d'immixtion dans la vie privée afin de négocier la réduction de ce risque	21
3.3.2.3. L'évaluation peut être invoquée à chaque fois qu'un problème concret s'est posé au sein de l'entreprise. ...	21
IV. QUELQUES CONSEILS PRATIQUES	22

Avant-propos

La CCT n° 81: un équilibre trouvé entre respect de la vie privée des travailleur(se)s et contrôle légitime de l'employeur

Les nouvelles technologies de communication en réseau ont envahi le lieu de travail.

Pour nombre de travailleuses et de travailleurs, elles sont devenues un outil de travail incontournable qui leur offre une plus grande rapidité d'exécution de leurs tâches ainsi qu'une plus grande indépendance. C'est tout profit également pour les employeurs qui voient la productivité augmenter, au même titre que certaines formes de flexibilité...

Ces nouvelles technologies de communication ne sont pas sans soulever des problèmes particuliers dans le cadre de la relation de travail en termes de contrôle que l'employeur peut exercer sur l'exécution du contrat de travail par ses travailleurs et, en termes de respect de la vie privée auquel les travailleurs peuvent prétendre.

La FGTB a saisi le Conseil National du Travail en juin 2000 afin de développer un instrument conventionnel qui donnerait une réponse adaptée à cette conciliation du droit à la vie privée sur le lieu de travail avec le droit de contrôle qui appartient à l'employeur.

Le 26 avril 2002, la CCT n° 81 relative à la protection de la vie privée des travailleurs à l'égard du contrôle des données de communication électroniques en réseau a été conclue entre partenaires sociaux au sein du Conseil National du Travail. Un arrêté royal du 12 juin 2002 l'a ensuite rendue obligatoire à l'égard de tous les employeurs et les travailleurs du secteur privé belge et ce, sous peine de sanction pénale en cas de non respect.

Cette CCT s'inscrit dans le cadre juridique existant en termes de respect de la vie privée et de contrôle sur le lieu de travail. Elle en précise la portée et le modalise dans le cadre de la relation employeur-travailleur. Elle offre surtout un champ d'intervention à nos délégué(e)s en précisant les modalités d'information et de consultation à respecter dans l'entreprise et en encadrant strictement les procédures de contrôle que l'employeur peut éventuellement mettre en œuvre.

Le respect de la vie privée est une valeur fondamentale que la FGTB défend et revendique, y compris sur le lieu de travail.

La CCT n° 81 s'inscrit dans cette approche et concrétise une revendication formulée lors de notre Congrès d'octobre 2001.

La présente brochure développe les principes contenus dans la CCT n° 81 en termes opérationnels pour nos délégué(e)s confronté(e)s aux nouvelles technologies de communication en réseau sur le lieu de travail.

Nous vous en souhaitons bonne lecture.

André MORDANT,
Secrétaire Général.

Mia DE VITS,
Présidente.

I. LES CONSTATS

- Au cours de ces dernières années, les moyens de communication électroniques en réseau ont connu une très large diffusion au sein des entreprises. De plus en plus de travailleurs ont accès à ces moyens de communication dans le cadre de leur activité professionnelle, et en particulier au courrier électronique (e-mail) et à l'internet.
- Parallèlement, des modes de contrôle se sont développés afin d'assurer le bon fonctionnement du réseau en évitant, entre autres, des phénomènes d'engorgement ou des problèmes de virus. Des règlements unilatéraux sont très souvent imposés par les employeurs, sans que les modalités de contrôle ne fassent l'objet, ni d'une information, ni d'une consultation des travailleurs.
- Cependant, la vie privée ne s'arrête pas aux portes de l'entreprise. Ainsi en a décidé la Cour Européenne des droits de l'homme:

«Aucune raison de principe ne permet d'exclure les activités professionnelles ou commerciales de la notion de vie privée»et «tout type d'appel est protégé par la Convention européenne des droits de l'homme qu'il émane du domicile ou des locaux professionnels (peu importe le contenu de la conversation)».

«Pour la Cour, il ressort clairement de sa jurisprudence que les appels téléphoniques émanant de locaux professionnels, (...) peuvent se trouver compris dans la notion de «vie privée»et de «correspondance»visées à l'art. 8, § 1».

=> Cette jurisprudence¹ peut être invoquée directement devant les tribunaux belges.

- En partant du constat que la majorité des problèmes rencontrés actuellement reposent sur des défauts d'information voire, de formation, la FGTB a insisté sur la nécessité de lier l'information et la responsabilisation des travailleur(se)s car, en cas d'erreur, le/la travailleur(se) pourra alors arguer qu'il n'a PAS bénéficié de l'information complète. La FGTB a dès lors saisi le CNT en juin 2000 afin de vérifier la faisabilité d'une solution conventionnelle en la matière.
- Le 26 avril 2002, après de longs travaux, les partenaires sociaux ont conclu la CCT n°81 afin 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 selon lesquelles l'individualisation de ces données est autorisée.

¹Affaire Niemietz contre Allemagne (72/1991/324/396) – arrêt du 16 décembre 1992.

II. LES PRINCIPES GARANTIS PAR LA CCT N°81

2.1. LE RESPECT DE LA VIE PRIVÉE DES TRAVAILLEURS

Le respect de la vie privée est un droit de l'Homme fondamental déjà garanti légalement par:

- **La Convention européenne des droits de l'homme:**

«Toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance».

> = directement applicable en droit belge.

- **la Constitution:**

«Chacun a droit au respect de sa vie privée et familiale, sauf dans les cas et conditions fixés par la loi».

- **la loi du 8 décembre 1992 relative à la protection de la vie privée:**

Autorisation du traitement informatisé des données personnelles à certaines conditions:

- respect des principes d'information, de finalité, de transparence et de proportionnalité des actions entreprises;
- réserver un droit d'accès aux travailleurs et;
- réserver un droit de rectification du travailleur par rapport aux données traitées.

- **la loi du 21 mars 1991 dite «loi Belgacom»:**

«Sous réserve de l'autorisation de toutes les 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:

- de prendre frauduleusement connaissance de l'existence de signes, signaux, d'écrits, d'images, de sons ou de données de toute autre nature transmis par voie de télécommunication, en provenance d'autres personnes et destinées à celles-ci;
- de prendre connaissance intentionnellement de données en matière de télécommunications, relatives à une autre personne».

- **l'article 314bis du Code Pénal:**

Des sanctions pénales sont prévues pour «quiconque, soit intentionnellement, soit à l'aide d'un appareillage quelconque écoute, fait écouter, prend connaissance ou fait prendre connaissance, enregistre ou fait enregistrer, pendant leur transmission, des communications ou des télécommunications privées auxquelles il ne prend pas part, sans le consentement de tous les participants à ces communications ou télécommunications».

L'ensemble de ces dispositions restent donc d'application et, la CCT n°81 ne fait que modaliser ces normes fondamentales de manière à en assurer l'applicabilité effective dans l'entreprise et, par conséquent dans la relation de travail.

2.2. LE DROIT DE CONTRÔLE DE L'EMPLOYEUR ET LES OBLIGATIONS RESPECTIVES DES PARTIES

La loi du 3 juillet 1978 sur les contrats de travail reste, par excellence, l'expression des obligations qu'ont, dans la relation de travail qui les lie, le travailleur et l'employeur.

- le travailleur et l'employeur se doivent le respect et des égards mutuels ainsi que le respect des convenances et des bonnes mœurs pendant l'exécution du contrat de travail;
- l'exécution du travail doit se faire par le travailleur avec soin, probité et conscience conformément aux instructions de l'employeur et sans commettre de concurrence déloyale, sans divulguer de secrets de fabrication, ou encore, nuire à sa santé ou à celle d'autrui;
- le travailleur, en cas de dommage causé à l'employeur ou à des tiers, ne peut répondre que de sa faute lourde ou intentionnelle. Sa responsabilité est donc limitée.

C'est dans le respect de ces règles fondamentales que se situe naturellement la CCT n°81.

III. LA CCT N°81 DANS LA PRATIQUE

3.1. CHAMP D'APPLICATION

- Toutes les technologies en réseau, indépendamment du support.
Donc: internet, e-mail, WAP, le cadre défini est cependant suffisamment large pour ne pas exclure l'évolution future de ces technologies.
- Toutes les communications électroniques en réseau tant internes qu'externes.
- L'employeur a la possibilité d'effectuer un contrôle sur les données de communication électroniques en réseau, mais uniquement dans le cadre des finalités prévues dans la CCT.
- Le contrôle ne peut concerner que les données, pas leur contenu, sauf accord du travailleur.
- La CCT n°81 ne vise NI les modalités d'accès et/ou d'utilisation des moyens de communication électroniques en réseau de l'entreprise qui sont des prérogatives de l'employeur, NI l'exercice des activités syndicales. Les partenaires sociaux n'ont PAS voulu intervenir dans les accords existants déjà dans les entreprises (ex: accord relatif à l'information syndicale aux travailleurs via e-mail etc.). Cependant, rappelons que, techniquement, tout est contrôlable et que les écrits restent... Il faut donc user à cet égard de prudence et ne jamais faire ou dire via le réseau ce que l'on n'oserait faire ou dire par courrier "classique".

3.2. LORS DE L'INSTALLATION DU SYSTÈME DE CONTRÔLE

3.2.1. Obligation d'informer

3.2.1.1. Information collective

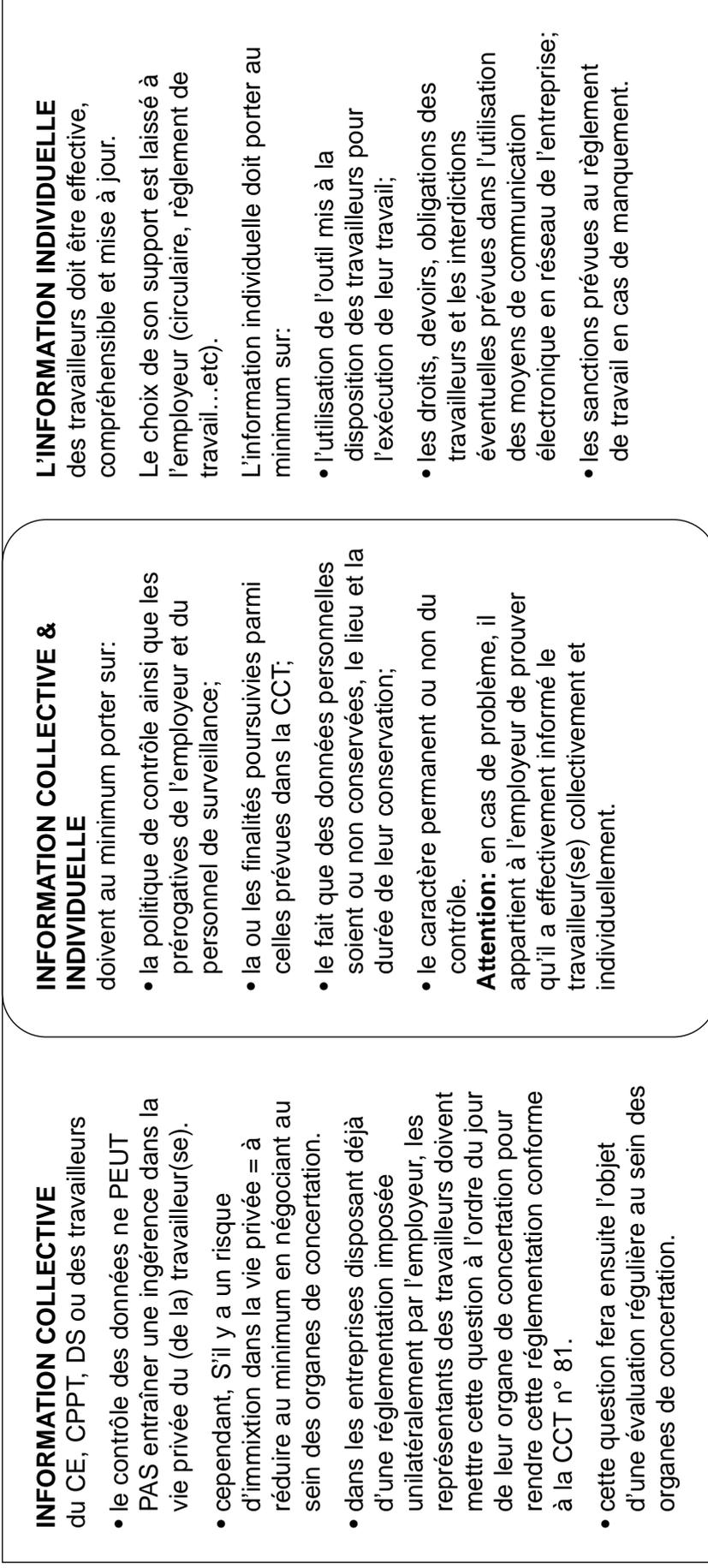
- L'employeur qui souhaite installer un système de contrôle informe le CE sur tous les aspects du contrôle et ce conformément aux dispositions de la CCT n°9 du 9 mars 1972 concernant le conseil d'entreprise.
- A défaut de CE, cette information est fournie au CPPT ou, à défaut, à la DS, ou à défaut, aux travailleurs.

3.2.1.2. Information individuelle

- Lors de l'installation du système de contrôle, l'employeur informe les travailleurs concernés sur tous les aspects du contrôle.
- L'information fournie doit être effective, compréhensible et mise à jour. Ceci signifie que l'information doit être portée à la connaissance des travailleurs, que les instructions doivent être claires et compréhensibles pour tous les travailleurs (aussi pour ceux qui n'ont pas de diplôme d'informaticien) et qu'il doit y avoir une mise à jour régulière (en fonction de l'évolution technologique et des circonstances spécifiques pour l'entreprise).

- Dans ce cadre, il est important de faire le lien entre information et formation aux travailleurs.
- L'information peut être fournie dans le cadre d'instructions générales, 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 (par ex. des messages à l'écran).

Le schéma ci-après esquisse le contenu de l'information



Dans la pratique, plusieurs situations peuvent se produire:

- L'employeur a déjà fixé des règles d'application dans l'entreprise:
Le rôle du CE/CPPT/DS peut consister à mettre ce point à l'ordre du jour dans le but de vérifier dans quelle mesure le document est conforme aux dispositions de la CCT n°81 et dans quelle mesure l'employeur a rempli son devoir d'information.

NB: tout règlement contenant des dispositions qui sont contraires à la CCT, est caduc et ce, parce qu'il constituera le plus souvent une infraction à la législation de base à laquelle la CCT donne exécution.

- Il n'existe pas de document mais tous les travailleurs sont au courant des pratiques de contrôle dans l'entreprise.
Dans ce cas également, cette question doit être mise à l'ordre du jour du CE/CPPT/DS pour que la situation soit conforme aux dispositions de la CCT.
- L'employeur souhaite installer un système de contrôle: il doit fournir les informations collectives et individuelles.
- Il n'y a ni règlement, ni pratiques de contrôle: il appartient aux représentants syndicaux de déterminer si une discussion dans les organes de concertation est opportune ou non.

3.2.2. Principes de contrôle

L'employeur souhaite installer un système de contrôle ou le système existant sera évalué: quels sont les points dont il faut tenir compte?

Hormis les principes mentionnés sous le point «champ d'application», voici les points dont il faut tenir compte.

3.2.2.1.

Par principe, le contrôle des données ne peut entraîner une ingérence dans la vie privée du travailleur ou à tout le moins cette ingérence doit être réduite au strict minimum et ce, dans le cadre d'une collecte des données globales de l'entreprise.

Il s'agit plus précisément de ne traiter et de ne collecter en vue du contrôle que les données qui sont nécessaires à un tel contrôle, c'est à dire les données qui, compte tenu de la finalité légitime poursuivie par le contrôle, entraînent l'ingérence la plus réduite possible dans la sphère privée du travailleur.

Exemples:

- en cas de contrôle des sites internet, est proportionnelle la collecte des données relatives à la durée de connexion par poste de travail et non l'individualisation par travailleur;
- en ce qui concerne l'usage du courrier électronique, est visée la collecte de données du nombre et du volume des courriers sortants par poste de travail et non l'identification du travailleur qui les transmet.

3.2.2.2.

Seule la poursuite des 4 finalités de contrôle suivantes est permise:

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

Quelques exemples

Les faits illicites ou diffamatoires, faits contraires aux bonnes mœurs ou susceptibles de forte atteinte à la dignité d'autrui peuvent notamment consister en des actes de piratage informatique, 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 bien 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.

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:

Quelques exemples

Ces pratiques peuvent prendre la forme d'une publicité dénigrante (au sens de la loi sur les pratiques du commerce), de divulgation de fichiers, de la violation des secrets d'affaires, du non respect de la confidentialité de certaines données.

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.

L'employeur est tenu de définir de manière claire et explicite les finalités poursuivies par le contrôle.

L'exercice d'un contrôle par l'employeur ne peut être accepté pour aucune autre finalité en dehors de cette liste.

- Dans tous les cas, le contrôle devra revêtir un caractère adéquat, pertinent et non excessif au regard de la (ou des) finalité(s) poursuivies.

A cette occasion le caractère permanent ou non du contrôle peut être discuté.

Dans ce contexte, il convient d'attirer l'attention sur un avis de la Commission de la Protection de la vie privée:

«Un contrôle général et à 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 surveillance constante».

- **Pour rappel: le contrôle du contenu des données n'est possible que si le travailleur et toutes les autres parties concernées par la communication ont donné leur accord!**

3.3. APRES L'INSTALLATION DU SYSTEME DE CONTROLE

3.3.1. Individualisation

Par individualisation, il convient de comprendre 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.

En principe, l'employeur fait d'abord un contrôle global sans pouvoir déterminer à quel travailleur l'anomalie peut être imputée. En deuxième lieu, il va déterminer le responsable de l'anomalie.

3.3.1.1. Principes:

- L'individualisation doit se faire de bonne foi et en conformité avec les finalités poursuivies.
- Si les données sont traitées en vue de finalités autres que celle pour laquelle le contrôle a été installé, l'employeur doit s'assurer que ce traitement est compatible avec la finalité initialement poursuivie et doit prendre toutes les mesures nécessaires pour éviter les erreurs d'interprétation.
- L'individualisation doit se faire de manière compatible avec la ou les finalités poursuivies. Seules les données nécessaires à la (aux) finalité(s) poursuivie(s) pourront être individualisées. Ces données doivent être adéquates, pertinentes et non excessives au regard de cette ou ces finalités.
- Il en va de même en matière de sanctions infligées aux travailleurs: elles devront être proportionnelles à l'éventuelle faute commise par ceux-ci.. Dans le cas où des sanctions spécifiques sont proposées, il convient d'adapter au préalable le règlement de travail.

En tout état de cause, seules les données de communication électroniques peuvent être individualisées. Leur contenu ne pourra l'être sauf aux parties, et certainement au travailleur, à donner son accord conformément au prescrit des lois du 21 mars 1991 et du 8 décembre 1992.

Rappelons que la CCT n°81 vise à trouver un juste équilibre entre vie privée et vie professionnelle.

- Les modalités d'individualisation sont différentes (procédure directe ou indirecte) exclusivement selon la finalité poursuivie (voir ci-après).
Dans le cadre de la procédure, dite de «sonnette d'alarme», une nouvelle information est adressée à l'ensemble des travailleurs afin d'expliquer les problèmes qui ont été rencontrés dans l'entreprise et, en cas de récurrence de la part d'un travailleur, un entretien, préalable à toute décision et/ou évaluation, est prévu en présence, s'il le souhaite, de son/sa délégué(e) syndical(e).

3.3.1.2. L'individualisation peut être synthétisée comme suit:

PROCEDURE DIRECTE	PROCEDURE INDIRECTE (PHASE PRÉALABLE D'INFORMATION)
<p>L'individualisation peut être opérée sans autre formalité lorsque la finalité du contrôle tient à :</p> <ul style="list-style-type: none"> • la prévention de faits illicites, diffamants ou contraires aux bonnes mœurs ou susceptibles de porter atteinte à la dignité d'autrui ; • 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 ; • la sécurité et/ou le bon fonctionnement technique de l'ensemble des systèmes informatiques en réseau de l'entreprise, en ce compris le contrôle des coûts y afférents ; 	<p>Par contre et lorsque l'objectif tient au respect de bonne foi des règles et principes d'utilisation des technologies fixées dans l'entreprise, il y a lieu de respecter une phase dite de sonnette d'alarme qui vise essentiellement à parer, préciser ou rappeler par une information au travailleur quelles sont ces règles et principes.</p> <p>Cette procédure indirecte de contrôle, l'individualisation des données ne s'applique pas à celles dont le caractère professionnel n'est pas contesté par le travailleur. De plus, la mise en œuvre de ce principe ne peut rendre inopérantes les garanties offertes aux employeurs et aux travailleurs par la présente CCT par l'attribution d'un caractère exclusivement professionnel aux données de communication électroniques en réseau.</p> <p>L'employeur ne pourra PAS invoquer le caractère professionnel de toutes les données de communication émanant de l'entreprise, ceci aboutirait à nier l'existence de la vie privée du travailleur sur son lieu de travail.</p> <p>De même, le travailleur ne pourra PAS invoquer le caractère privé de tous ses communications car, il est sur son lieu de travail pour exécuter son contrat de travail.</p>

	<p>L'individualisation s'inscrit dans une procédure en 3 étapes :</p> <ul style="list-style-type: none">a. Information préalable L'employeur, préalablement à l'individualisation des données, informe les travailleurs du non respect d'une des règles d'utilisation fixées dans l'entreprise. Cette information 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.b. Contrôle individualisé En cas de détection d'une nouvelle anomalie, l'employeur peut réaliser le contrôle individualisé lui permettant de retracer l'identité de la/des personnes(s) responsable(s) des anomalies.c. Entretien préalable L'employeur, dans le cadre d'une procédure contradictoire, laisse au travailleur ainsi identifié la possibilité de s'expliquer à l'occasion d'un entretien. 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.

Conformément à la convention collective n° 5 du 24 mai 1971 concernant le statut des délégations syndicales du personnel des entreprises, notamment en son article 13, le travailleur peut, lors de cet entretien, se faire assister par son délégué syndical.

3.3.2. EVALUATION DANS L'ENTREPRISE

3.3.2.1. Une évaluation des systèmes de contrôle installés est réalisée régulièrement selon le cas, au sein du CE, du CPPT ou avec la délégation syndicale dans le but de formuler des propositions visant à adapter ces systèmes aux développements technologiques.

> Cette évaluation devrait être effectuée régulièrement afin de vérifier si la procédure est toujours adaptée aux nouvelles technologies et à l'organisation du travail.

3.3.2.2. Intervenir en cas de risque d'immixtion dans la vie privée afin de négocier la réduction de ce risque.

Cette intervention peut se situer à tout moment

En effet, si l'on constate par exemple que d'autres finalités que celles figurant dans la CCT sont prévues par l'employeur, si aucune procédure de sonnette d'alarme n'est prévue dans le document adressé par l'employeur ou encore, si ce dernier prévoit que toutes les communications dans l'entreprise ont un caractère professionnel; **les représentants des travailleurs doivent intervenir pour rétablir la garantie du respect de la vie des travailleurs sur le lieu du travail.**

3.3.2.3. En outre, cette possibilité d'évaluation pourrait être invoquée afin d'adapter la procédure à chaque fois qu'un problème concret s'est posé au sein de l'entreprise.

IV. QUELQUES CONSEILS PRATIQUES

- Dans le cas où les données obtenues sont traitées en vue de finalités autres que celle prévue, la CCT stipule que l'employeur doit s'assurer que ce traitement est compatible avec la finalité initialement poursuivie et doit prendre toutes les mesures nécessaires pour éviter les erreurs d'interprétation.

Dans la pratique, il peut s'avérer utile de convenir avec l'employeur que ce dernier informe les représentants des travailleurs lorsque pareille situation se produit.

- Il est important de signaler que, pour que l'utilisation des technologies informatiques corresponde aux besoins de l'entreprise, des mesures de prévention s'imposent, comme par ex. un blocage des sites web dont le contenu n'est d'aucune utilité ou encore orienter vers un serveur spécial les e-mail dont le volume est important. En effet, pareilles mesures rencontrent les intérêts de l'employeur sans porter préjudice à ceux des travailleurs.

FGTB

**Fédération Générale
du Travail de Belgique**

Juillet 2002

•
Lay-out: FGTB
Impression: New Goff
Photo couverture: Reporters
•

Rue Haute 42 • 1000 Bruxelles
Tel: +32 (0)2 506 82 11
Fax: +32 (0)2 506 82 29
e-mail: infos@fgtb.be
www.fgtb.be

Editeur Responsable:
Mia DE VITS

**Cette brochure a été réalisée avec le soutien de
Fonds Social Européen
et du Ministère de l'emploi et du travail**

