



ENSEIGNEMENT CATHOLIQUE
SECRETARIAT GENERAL
LEGISLATION ET GESTION SCOLAIRES

L.G.S./07 /23
Cl. *.*

**Aux Pouvoirs Organiseurs,
Aux Chefs d'Etablissements
de l'Enseignement Fondamental
de l'Enseignement Secondaire
de l'Enseignement de Promotion Sociale
de l'Enseignement Supérieur
Catholique
des Centres PMS et
des Internats libres subventionnés**

Madame, Monsieur,

Bruxelles, le 18 juin 2007

OBJET : TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION ET RESPECT DE LA VIE PRIVEE.

Les Commissions Paritaires

- Centrale de l'enseignement libre subventionné,
- Centrale de l'enseignement supérieur non universitaire libre subventionné
- Centrale des Centres PMS libres subventionnés

ont adopté, dans le courant des mois de mai et juin, chacune pour leur champ de compétence, une décision collective de travail, relative à *la protection de la vie privée des membres du personnel à l'égard du contrôle des données de communication électroniques.*

Cette décision, qui s'inscrit en droite ligne dans le sillage de la Convention collective de travail n°81 adoptée au sein du Conseil National de Travail ainsi que dans le cadre de l'article 109ter de la loi du 21 mars 1991 portant réforme de certaines entreprises publiques économiques et 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 poursuivait un double objectif :

- permettre à l'employeur de contrôler l'utilisation des moyens de communication électroniques mis à la disposition des membres du personnel (accès internet, email, ...), et le cas échéant, de prendre les sanctions nécessaires
- garantir le respect de la vie privée des membres du personnel.

Ce double objectif nous semble parfaitement atteint par l'équilibre instauré par le texte entre les articles 5,6, et 7 d'une part, rappelant les principes à respecter, les articles 9 et 10 relatifs à l'obligation de transparence lors de l'installation des contrôles, et les articles 13 et 14 qui prévoient une procédure strictes et garantissant les droits de chacun.

Vous trouverez en annexe la convention collective telle qu'adoptée par la commission paritaire dont vous dépendez. Nous attirons votre attention sur sa date d'entrée en vigueur, soit le 1^{er} septembre 2007.

Vous trouverez dans le texte, les commentaires précis se rapportant aux articles. Néanmoins, il nous paraissait utile d'attirer votre attention sur les grands principes qui sous-tendent cette décision :

- **Principe de finalité**

Les contrôles instaurés par l'employeur devront répondre à une ou plusieurs des finalités suivantes :

1. la prévention de faits illicites ou diffamatoires, de faits contraires aux bonnes mœurs ou susceptibles de porter atteinte à la dignité d'autrui ;
Exemple : visite à partir des outils informatiques mise à disposition sur le lieu de travail, de sites à caractère pornographiques ou pédophiles, visite sur des sites à caractère raciste, nazi, etc...
2. la protection des informations à caractère confidentiel ;
Exemple : la transmission de données concernant les membres du personnel, la transmission de données concernant les délibérations, la transmission de données issues du dossier des consultants (centres PMS), etc...
3. la sécurité et/ou le bon fonctionnement technique des systèmes informatiques en réseau de l'établissement (du centre), en ce compris le contrôle des coûts y afférents, ainsi que la protection physique des installations de l'établissement (du centre) ;
Exemple : introduction malveillante de virus dans le système, dépassement systématique des maximums autorisés pour les fichiers joints aux mails, manipulations volontaires ayant pour but de perturber le fonctionnement du réseau, etc.
4. le respect de bonne foi des principes et règles d'utilisation des technologies en réseau fixés dans le règlement de travail de l'établissement (du centre) et du PO.
Si les outils informatiques mis à la disposition des membres du personnel sont destinés par priorité à un usage professionnel, il faut constater que la jurisprudence unanime reconnaît « un certain droit » pour le membre du personnel à utiliser à des fins privées, les outils de communications mis à sa disposition par le pouvoir organisateur dans le cadre du contrat de travail. Ceci doit cependant se faire dans le respect du principe de bonne foi, et l'on ne pourrait pas admettre qu'un membre du personnel passe un temps considérable sur des sites de vente, de voyage, de discussion en ligne ou d'intérêt général ou particulier – sites tout à fait légaux par ailleurs - au détriment du travail qui lui est confié.

- **Principe de proportionnalité**

Par principe, le contrôle des données de communications électroniques en réseau ne peut entraîner une ingérence dans la vie privée du membre du personnel.

Si toutefois ce contrôle entraîne une telle ingérence, **celle-ci doit être réduite au minimum** c'est-à-dire ne viser qu'à collecter les données de communications électroniques en réseau nécessaires au contrôle en fonction de la ou des finalités légitimes poursuivies

Nous attirons votre attention sur le point suivant : les données de communications **ne concernent pas les contenus** mais visent par exemple le nombre, le volume, la durée, la fréquence des communications. Le contrôle éventuel sur ces données s'inscrit bien entendu dans le cadre des finalités visées ci-dessus.

- **Principe de transparence**

L'employeur qui met en place un système de contrôle en avertit préalablement le Conseil d'entreprise ou l'Instance de Concertation Locale ou, à défaut le Comité pour la prévention et la protection au travail ou, à défaut, la délégation syndicale, ou à défaut l'ensemble des membres du personnel.

A titre indicatif, cette information pourra être réalisée :

- dans le cadre d'instruction générale (circulaires, affiches, etc) ;
- par mention au règlement de travail ;
- par mention dans le contrat d'engagement ;
- par des consignes d'utilisation fournies à chaque utilisateur de l'outil (mention sur écran de messages à l'allumage de l'outil et/ou lors de l'activation de certains programmes).

Il va de soi que ce choix du support ne dispense pas de l'application de la réglementation en la matière prévoyant des mentions obligatoires au règlement de travail¹.

Les membres du personnel devront être clairement avertis de « qui peut faire quoi ».

- d'une part, la politique de contrôle mise en place par le pouvoir organisateur (contrôle permanent, par sondage, de semaine en semaine....) et quelles sont les finalités poursuivies par ce contrôle.
- d'autre part :
 - o **qui**, au point de vue technique, **est habilité à effectuer ce contrôle** : la personne ou le service mandaté par le pouvoir organisateur directeur pour autant qu'il dispose des capacités techniques pour le faire.
 - o **quelles seront les prérogatives de la personne ou du service** habilité au contrôle. Il semble important de rappeler que cette personne ou ce service sera tenu à la plus stricte confidentialité sur le résultat du contrôle, et que tout abus dans la divulgation et/ou l'utilisation des informations recueillies dans le cadre du contrôle pourra donner lieu à des sanctions disciplinaires

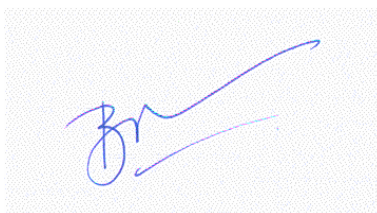
- **Procédure**

La procédure permettant d'individualiser les données recueillies lors d'un contrôle, et donc l'identification précise du membre du personnel en cause variera selon la finalité poursuivie :

- **directe dans le cas des finalités 1 à 3** visées ci-dessus : dès qu'une anomalie est détectée (visite d'un site à caractère pédophile ou raciste, transmission d'informations à caractère confidentiels, introduction volontaire d'un virus dans le système, ...), le membre du personnel responsable pourra, sans avertissement préalable, être identifié et, le cas échéant, sanctionné
- **indirecte dans le cas de la finalité n° 4** : si une anomalie de ce type devait être détectée, le membre du personnel sera informé qu'il fait désormais l'objet d'une surveillance particulière. Si de nouvelles anomalies devaient apparaître, le membre du personnel serait alors invité à venir s'expliquer devant l'employeur, le cas échéant dans le cadre d'une procédure disciplinaire, moyennant, bien entendu, le respect des procédures nécessaires.

Nous restons à votre disposition pour tout renseignement complémentaire que vous souhaiteriez obtenir, plus particulièrement S. Vanoirbeck, 02/256 70 42, stephane.vanoirbeck@segec.be.

Espérant que ces informations pourront vous être utiles, je vous prie d'agréer, Madame, Monsieur, mes salutations distinguées



Bénédicte BEAUDUIN
Directrice

¹ *Au sujet des procédures de modification du règlement de travail, voir notamment les communications LGS 04/29 du 26/11/2004 (Fond) et 05/06 du 4 février 2005 (Sec) disponibles sur le site du service LGS, rubrique « communications » ou sur le site des Fédérations (BI). Pour toute question sur ce sujet, n'hésitez pas à contacter N.Dasnoy, 02/256 70 43, nathalie.dasnoy@segec.be*