

NTIC - Nouvelles technologies de l'information et communication

Les NTIC, nouvel outil surveillance dans l'entreprise ?

Un salarié peut-il utiliser le matériel informatique à d'autres fins que professionnelles ?

Quels sont les risques de la « cybersurveillance » pour le salarié ?

Comment le réseau peut-il devenir un outil d'expression syndicale pour les Organisations Syndicales ?

Quelles sont les nouvelles prérogatives de la CNIL ? La création des CIL

Focus : l'employeur a installé des caméras de surveillance dans le hall d'entrée de notre entreprise. Or il n'a pas informé les représentants du personnel ni les salariés. Ce mode de surveillance est-il licite ?

Les NTIC, nouvel outil surveillance dans l'entreprise ?

Le développement de l'outil informatique et l'apparition des NTIC ont bouleversé les relations du travail au niveau de l'entreprise. Ce développement des NTIC a renforcé le contrôle des salariés. La loi prévoit :

• article L.120-2 du code du travail

La surveillance des salariés doit être justifiée par une raison objective et suffisante : la sécurité, les risques de vol, le contrôle du temps de travail... : c'est ce que l'on appelle le principe de finalité.

Les moyens mis en œuvre ne doivent pas être démesurés par rapport au but recherché : il s'agit du principe de proportionnalité. Par exemple, la vidéo-surveillance est acceptable pour assurer la sécurité et éviter les vols dans un magasin, pas dans un bureau.

• articles L.121-8, L.432-2-1

La direction est tenue de consulter le CE et d'informer les salariés de toutes les méthodes de surveillance mises en œuvre.

En aucun cas, un salarié ne saurait être surveillé à son insu.

En cas de contrôles clandestins constatés, le DP est habilité à saisir les prud'hommes en référé si l'employeur refuse de cesser sa surveillance.

La direction doit aussi consulter le CHSCT.

Un salarié peut-il utiliser le matériel informatique à d'autres fins que professionnelles ?

Globalement, sauf autorisation spéciale de l'employeur, il est en effet interdit d'utiliser son ordinateur à d'autres fins que professionnelles. L'entreprise pourrait d'ailleurs poursuivre le salarié pour abus de confiance.

Or, si le Web et notamment, le courrier électronique se révèle un formidable outil de travail, il peut être également utilisé au bureau à des fins privées. En conséquence, face à certains abus, de plus en plus d'employeurs veulent « cybersurveiller » l'usage du web et du courrier électronique.

Quels sont les risques de la « cybersurveillance » pour le salarié ?

1. L'utilisation de l'informatique :

Usage de Internet et de l'Intranet dans l'entreprise

Les traitements automatisés d'informations nominatives doivent faire l'objet d'une déclaration préalable à la CNIL.

Outre l'information préalable des salariés et du CE sur la mise en place du système, les salariés devront donner leur consentement exprès et être informés de leurs droits d'accès, de rectification et d'opposition en cas de traitement automatisé de données personnelles (Loi n° 78-17).

Ces NTIC peuvent donc entraîner de nouveaux modes de contrôle des salariés. Il s'agit de concilier le droit de contrôle et de surveillance de l'employeur sur l'activité des salariés dans le cadre de son pouvoir disciplinaire et de direction avec les droits et libertés fondamentales des salariés, tels que la protection de la vie privée ou la liberté d'expression.

Le courrier électronique

Les messages envoyés par les salariés à une personne extérieure ou interne à l'entreprise transitent par le système informatique de l'entreprise. Dès lors l'employeur est susceptible de conserver, archiver ou contrôler les courriers électroniques.

Si l'employeur est en droit de surveiller et de contrôler l'activité des salariés, ce n'est pas sans limite. En raison de l'absence de législation spécifique sur le contrôle des courriers électroniques, l'employeur devra informer préalablement les salariés du contrôle exercé. En effet, non seulement le devoir de loyauté dans les relations contractuelles est une condition de leur bonne exécution, mais surtout le principe du droit au respect de la vie privée doit être respecté (Code civil, art.9).

De plus, de récentes jurisprudences et en particulier l'arrêt Nikon du 2 octobre 2001 (n° 99-42.942 SA Nikon c/Onof) ont souligné la confidentialité du mail personnel au même titre que la lettre précisée « Personnel ». Il existe le même secret de la correspondance écrite qu'électronique au titre du respect des libertés fondamentales.

Un employeur a le droit d'interdire l'usage de la messagerie à des fins personnelles, mais ne peut en aucune façon, prendre connaissance à l'insu du salarié du contenu, alors que le message serait classé « Personnel ».

Le contrôle des fichiers informatiques

De même, depuis l'arrêt du 17 mai 2005, l'employeur ne peut ouvrir les fichiers identifiés par le salarié comme "personnels" contenus sur le disque dur de l'ordinateur mis à sa disposition qu'en présence de ce dernier.

2. la badgeuse (la RTT et ses conséquences)

Avec la mise en place de la loi sur les 35 heures, est réapparue la badgeuse. Cette badgeuse peut contrôler de façon stricte les horaires de travail des salariés et ainsi leur permettre de faire véritablement leur temps de travail. Mais cet outil peut aussi devenir un « flicage » à l'intérieur de l'entreprise par des procédés plus subversifs.

La mise en place d'un système permettant le contrôle des accès ou de la circulation dans l'entreprise, tels que les badges électroniques ou les cartes à puces magnétiques, peut avoir pour objectifs :

- le contrôle de l'accès à l'entrée et dans certains locaux de l'entreprise ;
 - la gestion des horaires variables et des temps de présence (décompter le temps de travail est une obligation légale en cas d'horaires individualisés) ;
 - la gestion de l'accès au restaurant d'entreprise et la mise en place d'un système de paiement. Ces dispositifs doivent être déclarés à la CNIL puisqu'ils constituent des traitements automatisés d'informations nominatives au sens de la loi de 1978.
- Ainsi la jurisprudence du 6/4/04 a confirmé qu'un système de badgage non déclaré à la CNIL était inopposable aux salariés. Le refus d'un salarié de se soumettre à un système non déclarée à la CNIL ne peut donc causer un licenciement.

Ces pratiques présentent des risques d'abus et de dérives :

- surveillance exagérée du personnel : visites et allées et venues contrôlées, consommations au restaurant d'entreprise, établissement de profils de salariés, repérage d'absences... ;
- entrave à la libre circulation des délégués du personnel (C. trav., art. L. 424-3).

3. la vidéosurveillance

L'employeur peut recourir à la vidéo-surveillance dans l'entreprise, sous réserve d'en informer au préalable les salariés et le CE.

Cette information préalable n'est cependant pas requise pour les locaux où les salariés ne travaillent pas. L'employeur peut surveiller les salariés dans le cadre de son pouvoir de direction, à la condition toutefois de respecter leur vie privée et les libertés individuelles au sein de l'entreprise (C. civ., art.9 ; C. trav., art.

L. 120-2). La mise en place d'un système de surveillance est dès lors soumise à une condition : l'information préalable des salariés et représentants du personnel.

Pour nous syndicalistes, l'utilisation d'Internet et du WEB peut constituer un **formidable outil de communication**. Reste à savoir ce qui est légal, ce que l'on peut faire et ne pas faire pour améliorer la communication avec les salariés et le dialogue social. L'article L. 412-8 du Code du travail issu de la loi du 4 mai 2004 sur le dialogue social, énonce que "un accord d'entreprise peut autoriser la mise à disposition des publications et tracts de nature syndicale, soit sur un site syndical mise en place sur Internet de l'entreprise, soit par la diffusion sur la messagerie électronique de l'entreprise. Dans ce dernier cas, cette diffusion doit être compatible avec les exigences de bon fonctionnement du réseau informatique de l'entreprise et ne pas entraver l'accomplissement du travail. L'accord d'entreprise définit les modalités de cette mise à disposition, en précisant notamment les conditions d'accès des organisations syndicales et les règles techniques visant à présenter la liberté de choix des salariés, d'accepter ou de refuser un message". De nombreux accords sur l'exercice du droit syndical et l'utilisation des nouveaux supports informatiques ont déjà été signés. Dans les faits, il s'avère que la négociation de tels accords reste difficile pour les OS. Les employeurs sont réservés à l'idée de permettre l'usage d'Intranet aux institutions représentatives du personnel. C'est ainsi que désormais toutes les communications syndicales par le biais des nouvelles technologies doivent faire l'objet d'un accord d'entreprise ou d'une autorisation de l'employeur :

-**création de sites externes** ou utilisation à des fins syndicales de l'Intranet

-**tracts syndicaux** : la loi du 4/5/04 relative au dialogue social s'est emparée de la question des tracts syndicaux dématérialisés ajoutant un 7ème alinéa à l'article L.412-8 du code du travail. Ce nouveau texte permet aux syndicats d'envoyer aux salariés des tracts électroniques, soit par le biais de la messagerie électronique de l'entreprise, soit en créant un site sur l'intranet de l'entreprise, nécessitant toujours la signature d'un accord (confirmation par jurisprudence du 25/1/05).

-**affichage syndical**

-**Le cas du « télévote » ou vote électronique** : au regard de l'état actuel de la jurisprudence et des dispositions législatives concernant les principes généraux du droit électoral, le vote par téléphone est illégal. Il en a été décidé ainsi à propos d'un accord préélectoral qui prévoyait un « télévote », dont l'organisation et le fonctionnement étaient confiés à des prestataires de services. Les principes de vote secret sous enveloppe et de déroulement et de dépouillement soumis au contrôle des électeurs ne pouvaient être respectés (Cass. soc. 20/oct. 1999, n° 98-60.359). Par conséquent, un vote par internet ou intranet ne pourrait être organisé en toute légalité.

Quelles sont les nouvelles prérogatives de la CNIL ? La création des CIL

Avec la réforme de la loi informatique et libertés du 6 août 2004, la CNIL a bénéficié de nouvelles prérogatives : un système de déclaration allégée mais un contrôle plus strict a posteriori facultative.

C'est ainsi que, désormais, les entreprises peuvent décider en un

C'est ainsi que, désormais, les entreprises peuvent désigner un correspondant Informatiques et Libertés (CIL). Il s'agit d'une désignation facultative permettant de bénéficier d'un allègement de formalités déclaratives auprès de la CNIL. Précisons que ces CIL ne bénéficient pas du statut de "salarié protégé". (décret 20 octobre 2005).

Focus : l'employeur a installé des caméras de surveillance dans le hall d'entrée de notre entreprise. Or il n'a pas informé les représentants du personnel ni les salariés. Ce mode de surveillance est-il licite ?

Avant toute mise en place d'un système de vidéosurveillance, l'employeur doit informer individuellement tous les salariés de l'entreprise. En second lieu, il doit consulter le CE. Enfin il doit déposer une déclaration préalable à la CNIL. L'employeur doit justifier ce système de contrôle par un intérêt légitime et le dispositif doit être proportionnel au but recherché. La mise en place de la vidéosurveillance peut être reconnue légitime dans les seuls cas suivants : dans un lieu ouvert au public, dans un lieu particulièrement exposé au risque de vol et d'agression, dans un but unique de sécurité des personnes et des biens, à défaut ce système de surveillance est considéré illicite.