N.T.I.C
Nouvelles technologies de l'information et de la communication

Mise à jour : Septembre 2014

Chambres de Métiers et de l'Artisanat
Région Rhône-Alpes

Utilisation par le salarié

L'utilisation des moyens informatiques professionnels à des fins personnelles est tolérée sous réserve qu'elle ne dégénère pas en abus. L'abus résulte généralement de :

1. La fréquence de l'utilisation à des fins personnelles (ex : durée excessive des connexions Internet à des fins personnelles).

2. La nature de cette utilisation personnelle

Ex : utilisation de l'accès Internet de l'entreprise pour visiter des sites prohibés ou à des fins illicites (téléchargement illicite…), mails contenants des propos injurieux ou diffamatoires...

Ces faits sont constitutifs de fautes professionnelles et donc susceptibles de sanctions pouvant aller le cas échéant jusqu'au licenciement.

Utilisation par l'employeur

Il faut distinguer deux situations :

1. Les informations contenues par l'ordinateur du salarié

- L'outil informatique mis à disposition par l'employeur (ordinateur, accès Internet…) demeure la propriété de l'entreprise ce qui autorise l'employeur à en vérifier le contenu (mails, dossiers sur le disque dur…) même en l'absence du salarié.

- Une exception demeure toutefois s'agissant des **éléments identifiés comme personnel :**

L'employeur ne peut accéder à ces fichiers **qu'en présence de l'intéressé ou après l'avoir dûment appelé**. Hors cette présence ou cet appel, il ne peut le faire que si un risque ou un événement particulier le justifie pour les mails personnels : l'employeur ne peut pas en revanche consulter les mails identifiés comme personnels. Ces messages sont en effet protégés par le secret des correspondances. En revanche l'employeur peut, s'il justifie d'un motif légitime, **demander au juge la désignation d'un huissier de justice**, dont les constatations, actées par procès verbal, pourront être utilisées notamment dans le cadre d'une procédure disciplinaire.

NB : *l'interdiction d'utiliser la messagerie professionnelle à des fins personnelles ne dispense pas l'employeur* de cette obligation de recourir au préalable au juge.

Le caractère personnel peut être établi notamment par l'utilisation des mentions « privé » ou « personnel » dans l'objet d'un message, ou pour dénommer un dossier ou un répertoire. En revanche la **simple mention d'un prénom ou des initiales du salarié, ne permet pas d'identifier un fichier comme personnel**.

2. Les moyens informatiques de contrôle et surveillance

Dans les entreprises sans institution représentative du personnel les dispositifs spécifiques de contrôle (badge, pointeuse, vidéosurveillance…) doivent tout de même :

2.1 être **justifié et proportionné** au but recherché :

- s'agissant de la nature et des conditions de *recueil des informations* :

- La justification doit s'appuyer sur des éléments déterminés et légitimes en lien avec l'activité (ex : poste dangereux ou sensible, pointeuse pour assurer un contrôle des heures,…).
- La proportionnalité s'étend tant aux moyens mis en œuvre qu'aux informations recherchées. Elle s'apprécie au regard du but recherché (ex : s'agissant d'un système de vidéosurveillance, le nombre, l'emplacement et les périodes de fonctionnement de caméras doivent être strictement nécessaires. Tel n'est pas le cas d'une caméra installée dans les vestiaires).

- s'agissant des conditions d'*accès aux informations* recueillies (ex : accès limité à un personnel qualifié comme le responsable de la sécurité…).

- s'agissant des conditions de *conservation des données recueillies* (ex: durée de conservation, nécessairement limitée dans le temps, ne peut excéder 1 mois en matière de vidéosurveillance, jusqu'à 6 mois est possible s'agissant des dispositifs de contrôle de l'utilisation d'Internet, et un an pour la téléphonie professionnelle.

2.2. donner lieu à une **information préalable des salariés** (sur la nature et l'objet du dispositif)

A contrario si le dispositif (ex : vidéosurveillance) est mis en place dans un local professionnel où aucun salarié ne travaille en principe (ex : une réserve) aucune information n'est nécessaire.

2.3 être **déclarés auprès de la CNIL pour tout** fichier ou traitement automatisé de données personnelles : cette formalité peut prendre plusieurs formes selon le fichier concerné. Généralement une déclaration dite « normale » est suffisante (ex : vidéosurveillance). Le recueil d'informations sensibles (ex : dispositif biométrique) doit en revanche faire l'objet d'une autorisation de la CNIL.

Pour savoir quelles formalités réaliser en fonction de chaque fichier et procéder aux déclarations en questions : cf. lien suivant