

N.T.I.C. (Nouvelles Technologies de l'Information et de la Communication)

L'utilisation de l'outil informatique par le salarié à des fins non professionnelles

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 la **fréquence de l'utilisation** à des fins personnelles
Ex : durée excessive des connexions Internet à des fins personnelles.
- Ou de 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 contenant 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.

L'utilisation de l'outil informatique par l'employeur en vue de prouver la faute du salarié

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 :

- pour les dossiers personnels : 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, **demandeur 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 ne peut reposer exclusivement sur une volonté de mettre sous surveillance un salarié ou un groupe particulier de salariés. Elle 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 (responsable de la sécurité...).

- s'agissant des conditions de *conservation des données* recueillies

Ex : la durée de conservation, nécessairement limitée dans le temps, ne peut excéder un mois en matière de vidéosurveillance. Une durée allant jusqu'à 6 mois est possible s'agissant des dispositifs de contrôle de l'utilisation d'Internet, voire un an pour la téléphonie professionnelle.

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

NB : 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**

Tout fichier ou traitement automatisé de données personnelles doit, en principe, faire l'objet d'une déclaration auprès de la CNIL.

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.

Le guide pratique édité par la CNIL (page 40) indique précisément quelles formalités réaliser en fonction de chaque fichier :

http://www.cnil.fr/fileadmin/documents/Guides_pratiques/Guide_employeurs_salaries.pdf

Ces déclarations peuvent être réalisées via le site de la CNIL :

<http://www.cnil.fr/vos-responsabilites/declarer-a-la-cnil/>