



Travail &  
Données personnelles

# Les outils informatiques au travail



L'utilisation des outils informatiques s'est largement développée dans le monde du travail. Une utilisation personnelle de ces outils est tolérée si elle reste raisonnable et n'affecte pas la sécurité des réseaux ou la productivité. C'est à l'employeur de fixer les contours de cette tolérance et d'en informer ses employés.

## ► Le contrôle de l'utilisation d'Internet et de la messagerie : dans quel but ?

L'employeur peut contrôler et limiter l'utilisation d'internet (dispositifs de filtrage de sites, détection de virus...) et de la messagerie (outils de mesure de la fréquence des envois et/ou de la taille des messages, filtres « anti-spam »...)

Ce contrôle a pour objectif :

1. D'assurer la sécurité des réseaux qui pourraient subir des attaques (virus, cheval de troie...)
2. De limiter les risques d'abus d'une utilisation trop personnelle d'internet ou de la messagerie (consultation de sa messagerie personnelle, achats de produits, de voyages, discussions sur les réseaux sociaux...).

**Par défaut, les courriels ont un caractère professionnel.** L'employeur peut les lire, tout comme il peut prendre connaissance des sites consultés, y compris en dehors de la présence de l'employé.

### À noter

Les marque-pages, « favoris » ou « bookmark » du navigateur ne constituent pas un espace personnel ou privé. Ajouter un site internet à ses « favoris » ne limite donc pas le pouvoir de contrôle de l'employeur.

## ► Quelles garanties pour la vie privée ?

### Les limites au contrôle de l'employeur

- l'employeur ne peut pas recevoir en copie automatique tous les messages écrits ou reçus par ses employés, c'est excessif,
- les « keyloggers » permettent d'enregistrer à distance toutes les actions accomplies sur un ordinateur. Sauf circonstance exceptionnelle liée à un fort impératif de sécurité, ce mode de surveillance est illicite,
- les logs de connexion ne doivent pas être conservés plus de 6 mois.



### • La protection des courriels personnels :

Un employé a le droit, même au travail, au respect de sa vie privée et au secret de ses correspondances privées.

Un employeur ne peut pas librement consulter les courriels personnels de ses employés, même s'il a interdit d'utiliser les outils de l'entreprise à des fins personnelles.

Pour qu'ils soient protégés, les messages personnels doivent être identifiés comme tels, par exemple :

- en précisant dans leur objet « Personnel » ou « Privé »,
- en les stockant dans un répertoire intitulé « Personnel » ou « Privé ».

Les courriers ne seront pas considérés comme personnels du simple fait de leur classement dans le répertoire « mes documents » ou dans un dossier identifié par les initiales de l'employé.



Cette protection n'existe plus si une enquête judiciaire est en cours (par exemple, si l'employé est accusé de vol de secrets de l'entreprise) ou si l'employeur a obtenu une décision d'un juge l'autorisant à accéder à ces messages.

En cas de litige, il appartient aux tribunaux d'apprécier la régularité et la proportionnalité de l'accès par l'employeur à la messagerie. L'employeur peut ainsi demander au juge de faire appel à un huissier qui pourra prendre connaissance des messages de l'employé.

#### • Les fichiers

Par défaut, les fichiers ont un caractère professionnel et l'employeur peut y accéder librement.

Lorsque les fichiers sont identifiés comme personnels, l'employeur peut y accéder :

- en présence de l'employé ou après l'avoir appelé,
- en cas de risque ou événement particulier, qu'il appartient aux juridictions d'apprécier.

#### • La communication des mots de passe

Les identifiants et mots de passe (session Windows, messagerie...) sont confidentiels et ne doivent pas être transmis à l'employeur. Toutefois, si un employé absent détient sur son poste des informations indispensables à la poursuite de l'activité, son employeur peut exiger la communication de ses codes si l'administrateur réseau n'est pas en mesure de fournir l'accès au poste.

### ➤ L'information des employés

Les instances représentatives du personnel doivent être informées ou consultées avant la mise en œuvre d'un dispositif de contrôle de l'activité.

Chaque employé doit être notamment informé :

- des finalités poursuivies,
- de la base légale du dispositif (obligation issue du code du travail par exemple, ou intérêt légitime de l'employeur),
- des destinataires des données,
- de la durée de conservation des données,
- de son droit d'opposition pour motif légitime,
- de ses droits d'accès et de rectification,
- de la possibilité d'introduire une réclamation auprès de la CNIL.

Cette information peut se faire au moyen d'une charte, annexée ou non au règlement intérieur, d'une note individuelle ou d'une note de service...

### ➤ Quelle formalité

Si l'employeur a désigné un Délégué à la protection des données (DPO), il doit être associé à la mise en œuvre des dispositifs de contrôle.

Les différents systèmes de contrôle des outils informatiques doivent être inscrits au registre des activités de traitement tenu par l'employeur.

### ➤ Quels recours ?

En cas de difficulté, vous pouvez saisir :

- les services de l'inspection du Travail,
- le procureur de la République,
- le service des plaintes de la CNIL, sur les modalités de mise en œuvre d'un dispositif de contrôle de l'activité.

### ➤ Textes de référence

- **Le code civil :**  
Article 9 (protection de l'intimité de la vie privée)
- **Le code du travail :**  
Article L. 1121-1 (droits et libertés dans l'entreprise)  
Article L. 1222-3 et L. 1222-4 (information des employés)  
Article L. 2323-47 (information/consultation du comité d'entreprise)
- **Le code pénal :**  
Articles 226-1 et suivants (protection de la vie privée)
- [Le Règlement européen sur la protection des données personnelles \(RGPD\)](#)



Pour plus d'informations, consultez la rubrique « Besoin d'aide » sur [www.cnil.fr](http://www.cnil.fr). Vous pouvez également appeler la permanence juridique de la CNIL au **01 53 73 22 22**, les lundi, mardi, jeudi et vendredi de 10h à 12h et de 14h à 16h.