Le règlement intérieur peut-il prévoir la journalisation des accès informatiques ?

Réponse courte

Le **règlement intérieur** peut prévoir la **journalisation des accès informatiques** (logs de connexion, traçabilité des actions), à condition de respecter les principes de **finalité**, de **proportionnalité** et de **transparence** prévus par l'article L.261-1 du Code du travail et le **RGPD**. Les salariés doivent être **informés** de l'existence, des finalités et de la durée de conservation de ces journaux.

La journalisation doit être justifiée par des **motifs légitimes** (sécurité informatique, protection des données, traçabilité réglementaire) et ne peut servir de base à une **surveillance permanente et systématique** des salariés.

Définition

La **journalisation des accès informatiques** désigne l'**enregistrement automatique** des connexions, actions et événements réalisés par les utilisateurs sur les **systèmes d'information** de l'entreprise. Ces **logs** peuvent inclure les heures de connexion, les applications utilisées, les fichiers consultés ou modifiés, et les accès aux ressources réseau.

Cette **traçabilité** constitue un **traitement de données personnelles** soumis aux exigences du RGPD et du droit du travail luxembourgeois.

Conditions d’exercice

La journalisation des accès informatiques prévue dans le règlement intérieur doit respecter les conditions suivantes :

- Finalité légitime et déterminée (sécurité, conformité réglementaire, protection des données)
- Proportionnalité entre les données collectées et les objectifs poursuivis
- Information préalable et claire des salariés
- Durée de conservation limitée et justifiée
- Accès restreint aux personnes habilitées
- Respect des droits des salariés (accès, rectification, opposition)

La consultation de la délégation du personnel est obligatoire conformément à l'article L.414-3.

Modalités pratiques

L'intégration de dispositions relatives à la journalisation informatique dans le règlement intérieur nécessite :

- La définition précise des données collectées (types de logs, informations enregistrées)
- L'indication des finalités poursuivies
- La durée de conservation des logs (généralement 6 mois à 1 an pour la sécurité)
- Les personnes habilitées à accéder aux journaux
- Les conditions d'utilisation des logs à des fins disciplinaires
- Les modalités d'exercice des droits des salariés

Une analyse d'impact sur la protection des données (AIPD) peut être nécessaire selon la nature des données collectées.

Pratiques et recommandations

Il est recommandé de :

- Limiter la collecte aux données strictement nécessaires à la sécurité informatique
- Prévoir des durées de conservation différenciées selon les types de logs
- Encadrer strictement l'accès aux journaux (service informatique, direction)
- Ne pas utiliser les logs pour une surveillance comportementale des salariés
- Informer les salariés des conditions d'utilisation à des fins disciplinaires
- Documenter les procédures d'accès et d'analyse des logs

L'utilisation des logs à des fins disciplinaires doit être prévue dans le règlement intérieur pour être opposable aux salariés.

Cadre juridique

Référence	Objet
Article L.261-1	Protection des données et surveillance au travail
Article L.414-3	Consultation de la délégation du personnel
Article L.121-6	Respect de la vie privée du salarié
Règlement (UE) 2016/679 (RGPD)	Principes de traitement des données personnelles
Loi du 1er août 2018	Protection des données à caractère personnel
Recommandations CNPD	Traitement des données dans le cadre professionnel

La journalisation des accès informatiques ne peut servir de base à une sanction disciplinaire que si le salarié a été préalablement informé de l'existence et des modalités d'utilisation des logs. L'absence d'information rend les preuves obtenues inopposables.