Quelles sont les règles à respecter pour contrôler l'usage d'Internet et des outils informatiques ?

Réponse courte

Le contrôle de l'usage d'Internet et des outils informatiques est une forme de **surveillance des salariés** au sens de l'**article L.261-1** du Code du travail. Il doit être **justifié** par une finalité légitime (sécurité, prévention des abus, protection des intérêts de l'entreprise), **proportionné** à cette finalité et **transparent** pour les salariés.

Toute mise en place implique une **charte informatique** communiquée individuellement, une **information ou un avis préalable de la délégation du personnel** et le respect du **RGPD**. Les dispositifs de surveillance **généralisée, permanente ou intrusive** sont interdits. Les contrôles doivent être ciblés, tracés et documentés. Les preuves obtenues en violation de ces règles sont inexploitables devant le tribunal du travail.

Définition

Le **contrôle de l'usage informatique** regroupe l'ensemble des dispositifs permettant à l'employeur de surveiller l'utilisation par les salariés de la messagerie, d'Internet, des outils collaboratifs et du matériel mis à disposition. Ces contrôles constituent des traitements de données personnelles soumis au RGPD et à l'article L.261-1 du Code du travail.

Questions fréquentes

Comment encadrer le contrôle de l'usage d'Internet au travail ?

Le contrôle doit être justifié par une finalité légitime (sécurité, prévention des abus), proportionné et transparent. Une charte informatique communiquée individuellement et l'avis préalable de la délégation du personnel sont obligatoires selon l'article L.261-1 du Code du travail.

Qu'est-ce qu'une charte informatique en entreprise ?

La charte informatique est un document écrit annexé au règlement intérieur, précisant les règles d'usage des outils informatiques et les modalités de contrôle. Elle doit être remise individuellement aux salariés contre signature à l'embauche, pour formaliser leur information.

Quand faut-il réaliser une AIPD pour un dispositif de contrôle ?

Une AIPD (analyse d'impact relative à la protection des données) est requise si le dispositif présente un risque élevé pour les droits des salariés, conformément à l'article 35 du RGPD. Elle doit précéder toute mise en place du contrôle.

Que se passe-t-il en cas de contrôle informatique illicite ?

Un contrôle mis en place sans information préalable ou sans respect de la procédure de consultation est illicite. La CNPD peut prononcer une amende administrative et les preuves obtenues sont inexploitables devant le tribunal du travail.

Quelle durée de conservation pour les logs informatiques ?

La conservation des logs et journaux de connexion doit être limitée à la durée strictement nécessaire à la finalité poursuivie, généralement six mois maximum. Le principe de limitation de la conservation découle de l'article 5.1.e du RGPD.

Une surveillance permanente d'Internet est-elle autorisée ?

Non, les dispositifs de surveillance généralisée, permanente ou intrusive sont interdits. Les contrôles doivent être ciblés, tracés et documentés. La proportionnalité exige une mesure adaptée et strictement nécessaire à l'objectif poursuivi.

Conditions d’exercice

Tout dispositif de contrôle de l'usage informatique exige une finalité légitime, un test de proportionnalité, une charte informatique transparente et l'avis préalable de la délégation du personnel (art. L.261-1).

Condition	Détail
Finalité légitime	Sécurité informatique, prévention des abus, conformité légale
Proportionnalité	Mesure adaptée et strictement nécessaire à l'objectif
Transparence	Charte informatique claire et accessible à tous les salariés
Information individuelle	Remise contre signature de la charte à chaque salarié
Délégation du personnel	Information ou avis préalable selon le type de dispositif
Limitation des accès	Seules les personnes habilitées consultent les données
Exclusion vie privée	Respect du secret des correspondances personnelles

Modalités pratiques

Le contrôle des outils informatiques impose une AIPD préalable, une charte informatique remise individuellement aux salariés, une consultation de la délégation du personnel et une traçabilité des contrôles ciblés.

Étape	Détail
Analyse d'impact	AIPD si risque élevé pour les droits des salariés
Charte informatique	Rédaction précisant les règles d'usage et de contrôle
Consultation délégation	Avis préalable de la délégation du personnel
Information salariés	Remise individuelle de la charte signée
Contrôles automatisés	Outils de filtrage, antivirus, détection d'intrusion
Contrôles ciblés	Procédure formalisée avec motif écrit et traçabilité
Conservation limitée	Durée proportionnée à la finalité du contrôle

Pratiques et recommandations

Rédiger une charte informatique complète et compréhensible, annexée au règlement intérieur et signée à l'embauche, précisant les règles d'usage et les modalités de contrôle.

Privilégier les contrôles automatisés, anonymisés et globaux (statistiques de navigation, filtrage de sécurité) aux contrôles individuels ciblés.

Documenter chaque contrôle ciblé par un motif écrit, une traçabilité technique et un compte rendu accessible au DPO.

Consulter systématiquement la délégation du personnel avant toute nouvelle mesure de surveillance ou modification du dispositif existant.

Limiter la conservation des logs et journaux de connexion à la durée strictement nécessaire à la finalité poursuivie, généralement six mois maximum.

Cadre juridique

Le cadre juridique combine droit du travail, RGPD et droits fondamentaux.

Référence	Objet
Art. L.261-1 Code du travail	Surveillance des salariés
Art. L.414-9 Code du travail	Information et avis de la délégation du personnel
Règlement (UE) 2016/679 (RGPD)	Protection des données personnelles
Loi du 1er août 2018	Régime général au Luxembourg
Art. 5 et 6 RGPD	Principes et bases légales du traitement
Art. 35 RGPD	Analyse d'impact (AIPD)
Art. 8 CEDH	Droit au respect de la vie privée

Un contrôle mis en place sans information préalable ou sans respect de la procédure de consultation est **illicite**. La CNPD peut prononcer une amende administrative et les preuves obtenues sont inexploitables devant le tribunal du travail.