Quelles règles s'appliquent à la surveillance des connexions internet des salariés au Luxembourg ?

Réponse courte

La **surveillance des connexions Internet** est autorisée pour des **finalités précises** (sécurité du SI, prévention des abus, conformité légale) et doit rester **proportionnée**. La surveillance généralisée, permanente ou préventive sans motif est interdite, et l'accès au contenu des communications identifiées comme privées est prohibé sauf décision judiciaire.

L'employeur doit informer individuellement chaque salarié, consulter la délégation du personnel (article L.414-9 du Code du travail pour les entreprises d'au moins 150 salariés), réaliser une AIPD si le risque est élevé et tenir un registre des traitements. La conservation des logs se limite généralement à **6 à 12 mois** sauf justification documentée. Les preuves issues d'un dispositif non conforme sont **irrecevables** devant le tribunal du travail.

Définition

La **surveillance des connexions Internet** désigne tout dispositif technique permettant de contrôler l'usage par les salariés des ressources de navigation : sites consultés, durée des connexions, téléchargements, applications utilisées. Elle constitue un traitement de **données à caractère personnel** au sens du RGPD.

Elle vise à encadrer l'usage des outils numériques mis à disposition par l'employeur tout en respectant la vie privée et le secret des correspondances. L'accès au contenu des correspondances privées est interdit sauf exception légale.

Questions fréquentes

Combien de temps conserver les logs de navigation internet ?

Généralement 6 à 12 mois en principe, avec justification documentée au-delà. La durée doit être inscrite au registre des traitements (article 30 RGPD) et adaptée à la finalité poursuivie.

Faut-il privilégier une analyse statistique ou un contrôle nominatif des connexions internet ?

L'analyse globale et anonymisée est préférée. Un contrôle nominatif n'est admissible qu'en cas de soupçon caractérisé documenté, après procédure contradictoire. La CNPD recommande les statistiques globales en première intention.

L'employeur peut-il lire les courriels privés des salariés ?

Non, l'accès au contenu des correspondances et fichiers identifiés comme privés est interdit sauf décision judiciaire. Le secret des correspondances reste protégé même sur les outils professionnels mis à disposition par l'employeur.

L'employeur peut-il surveiller la navigation internet des salariés au Luxembourg ?

Oui, pour des finalités précises (sécurité du SI, prévention des abus, conformité légale) et de manière proportionnée. La surveillance généralisée, permanente ou préventive sans motif est interdite par l'article L.261-1 du Code du travail.

Quelles sanctions en cas de surveillance internet non conforme ?

Amendes administratives RGPD jusqu'à 4 % du chiffre d'affaires mondial, sanctions pénales L.261-2 (251 € à 125 000 €) et irrecevabilité des preuves devant le tribunal du travail si l'information préalable est absente.

Une charte informatique est-elle obligatoire pour la surveillance internet ?

Oui, la charte annexée au règlement intérieur ou au contrat fixe les règles d'usage et de surveillance, et conditionne la recevabilité de toute mesure disciplinaire fondée sur la consultation de sites par le salarié.

Conditions d’exercice

Le contrôle ne peut porter sur les contenus marqués comme privés ; les statistiques globales doivent être préférées aux analyses individualisées sauf soupçon caractérisé.

Condition	Exigence
Finalité limitative	Sécurité du SI, prévention des abus, respect des obligations légales — pas de surveillance comportementale
Statistiques préférées	Analyse globale et anonymisée plutôt qu'individuelle ; ciblage sur soupçon caractérisé
Pas d'accès aux contenus privés	Interdiction d'ouvrir les courriels et fichiers identifiés comme personnels
Information préalable	Notice individuelle écrite et charte informatique
Consultation	Délégation du personnel (L.414-9) ou ITM à défaut

Modalités pratiques

Les logs sont par principe consultés sous forme statistique anonymisée ; un contrôle nominatif n'est admissible qu'en cas de soupçon documenté, après procédure contradictoire.

Démarche	Précision
Notice individuelle	Finalité, données, durée, destinataires, droits, distinction professionnel/privé
Charte informatique	Annexée au règlement intérieur ou contrat ; règles d'usage et de surveillance
Procès-verbal délégation	Consultation préalable (L.414-9)
AIPD	Obligatoire si risque élevé (article 35 RGPD)
Registre des traitements	Article 30 RGPD
Conservation	6 à 12 mois en principe ; justification documentée au-delà
Procédure contradictoire	Pour tout contrôle nominatif aboutissant à une mesure disciplinaire

Pratiques et recommandations

Privilégier les analyses statistiques anonymisées avant tout contrôle individuel.

Documenter par écrit les indices justifiant un contrôle nominatif.

Sécuriser les accès aux logs par habilitation nominative et journalisation.

Exclure tout accès aux courriels et fichiers identifiés comme privés sauf décision judiciaire.

Sensibiliser les salariés à l'usage approprié d'Internet via la charte informatique.

Garantir le contradictoire avant toute mesure disciplinaire fondée sur les logs.

Cadre juridique

Référence	Objet
Art. L.261-1 du Code du travail	Surveillance des salariés (loi du 1er août 2018)
Art. L.261-2 du Code du travail	Sanctions pénales
Art. L.414-9 du Code du travail	Co-décision de la délégation du personnel
Loi modifiée du 1er août 2018	Protection des données personnelles
Règlement (UE) 2016/679 (RGPD)	Articles 5, 6, 12-13, 30, 32, 35
Lignes directrices CNPD	Cybersurveillance sur le lieu de travail

Une surveillance généralisée et permanente sans information préalable rend les preuves recueillies irrecevables devant le tribunal du travail. L'employeur s'expose à des amendes administratives RGPD jusqu'à 4 % du chiffre d'affaires mondial et à des sanctions pénales (L.261-2 : 251 € à 125 000 €).