L'employeur peut-il surveiller l'activité des salariés sur leur ordinateur professionnel ?

Réponse courte

La **cybersurveillance** de l'activité informatique des salariés est possible au Luxembourg sous des **conditions strictes** : finalité légitime explicite (sécurité informatique, protection du secret des affaires, vérification du respect des obligations contractuelles), **proportionnalité** stricte, **surveillance graduée** (contrôle global anonymisé avant contrôle individualisé), interdiction de la surveillance permanente et systématique des frappes ou de la captation continue d'écran.

L'employeur doit informer **individuellement** chaque salarié concerné par écrit (charte informatique ou notice), **consulter la délégation du personnel** (article L.414-9), réaliser une AIPD si le risque est élevé (article 35 du RGPD), tenir un **registre des traitements** (article 30 du RGPD) et garantir la confidentialité des courriels et fichiers identifiés comme personnels. Aucune déclaration préalable à la CNPD n'est requise depuis le 25 mai 2018.

Définition

La **cybersurveillance** désigne l'ensemble des dispositifs techniques permettant à l'employeur de contrôler l'utilisation des outils numériques mis à disposition des salariés (courriels, navigation, fichiers, accès aux applications, transferts).

Elle constitue un **traitement de données à caractère personnel** soumis au RGPD et à l'article L.261-1 du Code du travail. La CNPD recommande une **surveillance graduée** : contrôle global anonymisé en première intention, contrôle individualisé seulement en cas d'indice détecté.

Questions fréquentes

Faut-il consulter la délégation du personnel avant une cybersurveillance ?

Oui, consultation obligatoire avec procès-verbal préalable conformément à l'article L.414-9 du Code du travail. Pour les entreprises d'au moins 150 salariés, la co-décision de la délégation est requise avant toute mise en place du dispositif.

Faut-il déclarer un dispositif de cybersurveillance à la CNPD au Luxembourg ?

Non, aucune déclaration préalable n'est requise depuis le 25 mai 2018. L'employeur doit toutefois réaliser une AIPD si le risque est élevé (article 35 RGPD), tenir un registre des traitements (article 30 RGPD) et démontrer la conformité en cas de contrôle.

L'employeur peut-il surveiller l'activité des salariés sur leur ordinateur professionnel ?

Oui, sous conditions strictes : finalité légitime explicite (sécurité informatique, protection du secret des affaires), proportionnalité stricte, surveillance graduée (contrôle global anonymisé avant individualisé). La surveillance permanente et systématique des frappes ou la captation continue d'écran est interdite.

Les courriels personnels du salarié sont-ils protégés sur l'ordinateur de travail ?

Oui, les courriels identifiés comme personnels par le salarié bénéficient d'une protection absolue, sauf en sa présence ou avec son accord. La distinction explicite entre contenus professionnels et personnels doit figurer dans la charte informatique.

Qu'est-ce que la surveillance graduée prônée par la CNPD ?

Méthode imposée par la CNPD : contrôle global anonymisé en première intention, contrôle individualisé seulement en cas d'indice détecté. Un dispositif qui permet d'identifier individuellement les salariés dès le premier niveau est considéré comme disproportionné par défaut.

Une charte informatique est-elle obligatoire pour la cybersurveillance ?

L'information écrite est obligatoire (charte informatique ou notice individuelle signée). La charte facilite la matérialisation de l'information préalable exigée par les articles 12-13 du RGPD et l'article L.261-1 du Code du travail. À défaut, une notice individuelle équivalente s'impose.

Conditions d'exercice

La surveillance graduée est l'une des règles cardinales de la CNPD : un dispositif qui permet d'identifier individuellement les salariés dès le premier niveau de contrôle est considéré comme disproportionné par défaut.

Condition	Exigence concrète
Finalité légitime	Sécurité informatique, secret des affaires, vérification contractuelle
Surveillance graduée	Contrôle global anonymisé puis individualisé en cas d'indice
Proportionnalité	Pas de surveillance permanente, pas de captation systématique
Information préalable	Notice individuelle écrite ou charte informatique signée
Consultation délégation	Article L.414-9 : co-décision pour ? 150 salariés

Modalités pratiques

L'AIPD doit être réalisée pour tout dispositif de cybersurveillance étendu ; elle est systématiquement demandée par la CNPD lors d'un contrôle et son absence caractérise un manquement autonome.

Démarche	Précision
Charte informatique	Document interne définissant usages autorisés et modalités de contrôle
Information individuelle	Notice écrite remise et signée par chaque salarié
Consultation délégation	Procès-verbal préalable conformément à L.414-9
AIPD	Article 35 du RGPD si risque élevé
Surveillance graduée	Étape 1 anonymisée, étape 2 individualisée justifiée par indices
Registre des traitements	Article 30 RGPD : finalités, durées, destinataires
Habilitation des accès	Liste nominative restreinte avec traçabilité

Pratiques et recommandations

Privilégier une charte informatique claire signée par chaque salarié.

Limiter la surveillance individualisée aux situations d'indices détectés au niveau global.

Documenter chaque passage de l'étape 1 à l'étape 2 par un motif écrit.

Sécuriser l'accès aux logs et aux données collectées par authentification forte.

Réviser annuellement la pertinence du dispositif avec la délégation et le DPO.

Distinguer explicitement les contenus identifiés comme personnels, qui bénéficient d'une protection renforcée.

Cadre juridique

Référence	Objet
Art. L.261-1 du Code du travail	Traitement de données pour surveillance des salariés
Art. L.261-2 du Code du travail	Sanctions pénales en cas de violation
Art. L.414-9 du Code du travail	Co-décision de la délégation du personnel
Art. 5, 6, 12-13, 30, 35 du RGPD	Principes, licéité, information, registre, AIPD
Loi modifiée du 1er août 2018	Régime général de protection des données
Lignes directrices CNPD cybersurveillance	Surveillance graduée et bonnes pratiques

Une cybersurveillance non conforme expose l'employeur à des sanctions RGPD jusqu'à 4 % du chiffre d'affaires mondial, à des sanctions pénales L.261-2 et à l'irrecevabilité des éléments collectés. Les courriels identifiés comme personnels par le salarié bénéficient d'une protection absolue, sauf en sa présence ou avec son accord.