Une entreprise peut-elle utiliser des outils de screen monitoring ?

Réponse courte

Le **screen monitoring** est admissible uniquement si la surveillance n'est ni systématique ni permanente, qu'elle poursuit une **finalité légitime** précise (sécurité informatique, prévention d'actes illicites) et qu'elle est strictement **proportionnée**, dans la même logique restrictive que celle imposée au keylogger. Il ne peut jamais servir au contrôle continu de la productivité ou de la présence des salariés.

Avant la mise en place, l'employeur doit consulter la délégation du personnel (article L.414-9), informer individuellement chaque salarié, mener un test de proportionnalité documenté, réaliser une **AIPD** si le risque est élevé (article 35 RGPD) et tenir le registre des traitements. Toute utilisation doit être ponctuelle, justifiée par un **risque avéré**, documentée et encadrée par une politique interne claire ; à défaut, les preuves sont irrecevables.

Définition

Le **screen monitoring** désigne les dispositifs permettant à l'employeur de visualiser, capturer ou enregistrer, en temps réel ou a posteriori, l'activité affichée sur l'écran de l'ordinateur d'un salarié : captures d'écran périodiques, vidéo, journalisation des applications et sites web consultés.

Ces outils impliquent un **traitement de données à caractère personnel**, parfois sensibles (correspondances privées, données médicales, opinions), qui engage la responsabilité de l'employeur au regard du RGPD et de la loi modifiée du 1er août 2018.

Questions fréquentes

Le screen monitoring peut-il servir à contrôler la productivité des salariés ?

Non, le screen monitoring ne peut jamais servir au contrôle continu de la productivité ou de la présence des salariés. Il doit être ponctuel, justifié par un risque avéré et limité à la sécurité informatique ou à la prévention d'actes illicites.

Quelles alternatives moins intrusives au screen monitoring sont recommandées ?

La CNPD recommande de privilégier les dispositifs moins intrusifs : journalisation des connexions, alertes de sécurité ciblées, DLP. Le principe de subsidiarité impose de retenir l'alternative la moins attentatoire avant tout screen monitoring.

Quelles formalités doit accomplir l'employeur avant de déployer un outil de surveillance d'écran ?

L'employeur doit consulter la délégation du personnel (article L.414-9), informer individuellement chaque salarié, réaliser une AIPD si le risque est élevé (article 35 RGPD) et tenir le registre des traitements. Une charte informatique doit encadrer le dispositif.

Quelles preuves issues du screen monitoring sont irrecevables ?

Toute preuve issue d'un dispositif sans information préalable, sans AIPD ou sans consultation de la délégation est irrecevable devant le tribunal du travail. Les sanctions disciplinaires fondées sur ces preuves sont nulles.

Quelles sanctions encourt une entreprise qui surveille les écrans sans autorisation ?

L'employeur s'expose à des sanctions administratives jusqu'à 4 % du chiffre d'affaires mondial. Les preuves sont irrecevables et toute sanction disciplinaire fondée dessus est nulle devant le tribunal du travail.

Une entreprise peut-elle utiliser des outils de screen monitoring au Luxembourg ?

Oui, mais uniquement de manière non systématique ni permanente, pour une finalité légitime précise (sécurité informatique, prévention d'actes illicites) et de façon strictement proportionnée. La surveillance permanente d'écran est présumée disproportionnée par la CNPD.

Conditions d’exercice

La surveillance permanente d'écran est présumée disproportionnée par la CNPD : l'usage doit être ciblé sur un risque précis et limité dans le temps, jamais déployé comme outil RH ordinaire.

Condition	Exigence
Surveillance permanente interdite	Captures continues présumées disproportionnées
Finalité légitime	Sécurité informatique, prévention d'actes illicites
Proportionnalité	Périmètre, durée et données strictement limités
Subsidiarité	Alternatives moins intrusives privilégiées (logs, alertes)
Information préalable	Notice individuelle remise avant activation
Consultation	Délégation du personnel (article L.414-9)

Modalités pratiques

L'AIPD est requise dès qu'un dispositif de screen monitoring est susceptible d'engendrer un risque élevé pour les salariés ; sa documentation conditionne la recevabilité des preuves issues du dispositif.

Démarche	Précision
Analyse d'impact (AIPD)	Article 35 du RGPD, obligatoire si risque élevé
Consultation de la délégation	Procès-verbal préalable (article L.414-9)
Information individuelle	Finalité, durée, données collectées, droits
Politique interne	Charte informatique précisant les modalités de contrôle
Registre des traitements	Article 30 du RGPD, fiche dédiée
Habilitation des accès	Liste nominative et traçabilité des consultations
Conservation limitée	Durée justifiée, suppression irréversible à l'issue

Pratiques et recommandations

Réserver le screen monitoring aux situations exceptionnelles fondées sur une suspicion documentée.

Privilégier les dispositifs moins intrusifs : journalisation des connexions, alertes de sécurité, DLP ciblé.

Documenter chaque activation du dispositif, son périmètre et sa durée.

Encadrer l'analyse des données par une procédure humaine excluant toute décision purement automatisée.

Communiquer une politique interne claire sur l'usage des outils numériques et les modalités de contrôle.

Cadre juridique

Référence	Objet
Art. L.261-1 du Code du travail	Traitement de données pour surveillance des salariés
Art. L.414-9 du Code du travail	Consultation/co-décision de la délégation du personnel
Loi modifiée du 1er août 2018	Protection des données à caractère personnel
Règlement (UE) 2016/679 (RGPD)	Articles 5, 6, 12-14, 32, 35
Lignes directrices CNPD	Cybersurveillance sur le lieu de travail

Tout usage de screen monitoring sans information préalable, sans AIPD ou sans consultation de la délégation rend les preuves irrecevables et expose l'employeur à des sanctions jusqu'à 4 % du chiffre d'affaires mondial. Les sanctions disciplinaires fondées sur ces preuves sont nulles devant le tribunal du travail.