Un logiciel de surveillance peut-il être installé à distance sans prévenir le salarié ?

Réponse courte

Non : l'installation à distance d'un logiciel de surveillance, comparable à un keylogger, sans information préalable du salarié est **strictement illicite** au Luxembourg. L'employeur doit informer individuellement chaque salarié concerné par écrit avant le déploiement (articles 12-13 RGPD, L.261-1) et consulter la **délégation du personnel** (article L.414-9). Une analyse d'impact sur la protection des données est obligatoire si le risque pour les salariés est élevé.

L'installation clandestine constitue une violation pénale (L.261-2 : 8 jours à 1 an d'emprisonnement et amende de 251 € à 125 000 €) et administrative (jusqu'à 20 millions € ou 4 % du chiffre d'affaires mondial). Les preuves recueillies sont **irrecevables** devant le tribunal du travail et toute sanction disciplinaire fondée sur ces données est annulable.

Définition

L'**installation à distance d'un logiciel de surveillance** désigne le déploiement, sans intervention physique sur le poste, d'un programme permettant de collecter des données sur l'activité du salarié : courriels, navigation, frappes clavier, captures d'écran, applications utilisées, géolocalisation.

Cette opération constitue un **traitement de données à caractère personnel** d'une intensité particulière, soumis aux articles 5, 6, 13, 32 et 35 du RGPD ainsi qu'à l'article L.261-1 du Code du travail. Elle relève systématiquement de la **cybersurveillance** au sens des lignes directrices CNPD.

Questions fréquentes

Faut-il consulter la délégation du personnel avant d'installer un logiciel de surveillance ?

Oui, la consultation préalable de la délégation est obligatoire au titre de l'article L.414-9 du Code du travail, avec procès-verbal conservé. Cette obligation est cumulative avec l'information individuelle exigée par l'article 13 du RGPD.

La régularisation a posteriori d'une surveillance clandestine est-elle possible ?

Non, la régularisation a posteriori ne purge pas la violation initiale. La bonne foi de l'employeur n'exonère pas en cas de défaut d'information préalable, et l'installation clandestine constitue une circonstance aggravante en contentieux.

Les preuves obtenues par un logiciel installé clandestinement sont-elles utilisables en justice ?

Non, les preuves recueillies par un dispositif illicite sont irrecevables devant le tribunal du travail. Toute sanction disciplinaire fondée sur ces données est annulable, même en cas de bonne foi de l'employeur.

Peut-on installer un logiciel de surveillance à distance sur le poste d'un salarié sans le prévenir au Luxembourg ?

Non, l'installation à distance d'un logiciel de surveillance sans information préalable est strictement illicite. L'employeur doit informer chaque salarié par écrit (articles 12-13 RGPD, L.261-1) et consulter la délégation du personnel (article L.414-9) avant tout déploiement.

Quelles données peut collecter un logiciel de surveillance à distance ?

Il peut collecter courriels, navigation web, frappes clavier, captures d'écran, applications utilisées et géolocalisation. Cette collecte constitue un traitement de données personnelles d'intensité particulière, soumis aux articles 5, 6, 13, 32 et 35 du RGPD.

© 2026 www.pixie.lu · IA/RH spécialisée en droit du travail luxembourgeois

Quelles sanctions pénales pour une surveillance clandestine d'un salarié ?

L'article L.261-2 du Code du travail prévoit 8 jours à 1 an d'emprisonnement et une amende de 251 € à 125 000 €. S'y ajoute la sanction administrative RGPD pouvant atteindre 20 millions € ou 4 % du chiffre d'affaires mondial.

Une AIPD est-elle obligatoire avant de déployer un logiciel de monitoring ?

Oui, une analyse d'impact (article 35 RGPD) est obligatoire pour un dispositif intrusif présentant un risque élevé pour les salariés. Elle doit être documentée et révisée à chaque modification du dispositif.

Conditions d’exercice

L'installation clandestine d'un logiciel de surveillance n'est jamais admise, même en cas de soupçon grave : la procédure régulière (information, consultation, AIPD) doit être respectée préalablement.

Condition	Exigence
Information préalable	Notice individuelle écrite avant le déploiement (article 13 RGPD)
Consultation délégation	Article L.414-9 préalable, procès-verbal conservé
AIPD	Obligatoire pour un dispositif intrusif (article 35 RGPD)
Finalité légitime	Sécurité des systèmes, lutte contre la fraude, protection des données
Proportionnalité	Aucun moyen moins intrusif disponible, périmètre justifié

Modalités pratiques

Toute décision automatisée fondée sur les données collectées (alerte de productivité, blocage d'accès) doit faire l'objet d'une intervention humaine au titre de l'article 22 du RGPD.

Démarche	Précision
Notice individuelle	Article 13 RGPD : finalité, données, durée, destinataires, droits
Consultation de la délégation	Article L.414-9, préalable au déploiement
AIPD	Documentée et révisée à chaque modification (article 35 RGPD)
Charte informatique	Précise les outils utilisés et leur finalité
Registre des traitements	Description complète du logiciel et de ses finalités
Habilitation des accès	Liste nominative restreinte des personnes pouvant consulter les données
Encadrement humain	Article 22 RGPD pour toute décision automatisée

© 2026 www.pixie.lu · IA/RH spécialisée en droit du travail luxembourgeois

Pratiques et recommandations

Documenter rigoureusement la procédure d'information, de consultation et d'AIPD avant tout déploiement.

Privilégier des outils ciblés et temporaires plutôt qu'un monitoring permanent et généralisé.

Restreindre les accès aux données collectées à un nombre minimal de personnes habilitées.

Définir une durée de conservation strictement limitée à la finalité (quelques mois maximum).

Désactiver la collecte sur les espaces marqués comme personnels par le salarié.

Auditer annuellement la pertinence et la proportionnalité du dispositif avec la délégation et le DPO.

Cadre juridique

Référence	Objet
Art. L.261-1 du Code du travail	Traitement de données pour surveillance des salariés (loi du 1er août 2018)
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 pour les installations de contrôle
Loi modifiée du 1er août 2018	Protection des personnes à l'égard du traitement des données à caractère personnel
Art. 5, 6, 13, 22, 32, 35 du RGPD	Principes, licéité, information, décision automatisée, sécurité, AIPD
Lignes directrices CNPD	Cybersurveillance sur le lieu de travail

L'installation clandestine est une circonstance aggravante en cas de contentieux : la sanction RGPD se cumule avec la sanction pénale (L.261-2) et l'inopposabilité des preuves. La bonne foi de l'employeur n'exonère pas en cas de défaut d'information. La régularisation a posteriori ne purge pas la violation initiale.

Les contenus sont rédigés et mis à jour régulièrement à partir de sources officielles. Leur usage ne remplace pas une consultation juridique et doit être validé par un professionnel du droit.