L'employeur peut-il utiliser un logiciel de traçage des frappes clavier ?

Réponse courte

L'utilisation d'un **keylogger** est en principe **interdite** au Luxembourg car elle constitue une surveillance permanente, intrusive et excessive du salarié, contraire aux principes de **nécessité** et de **proportionnalité**. Aucune finalité ordinaire de gestion RH ou de contrôle de productivité ne justifie un tel dispositif.

Une exception très étroite existe pour la **sécurité informatique** ou la prévention d'actes illicites graves, à condition que le keylogger soit ciblé, temporaire, proportionné, et qu'aucun moyen moins intrusif ne soit envisageable. L'employeur doit alors réaliser une AIPD, consulter la délégation du personnel, informer les salariés et documenter rigoureusement la nécessité. Tout usage non conforme expose à des amendes RGPD jusqu'à **20 millions d'euros** ou **4 %** du chiffre d'affaires mondial.

Définition

Le **keylogger** (logiciel de traçage des frappes clavier) capte l'intégralité des touches activées sur un poste informatique, y compris les identifiants, mots de passe, communications privées et messages personnels. Il s'agit d'un dispositif de surveillance particulièrement intrusif au sens du RGPD et de l'article L.261-1 du Code du travail.

Sa mise en œuvre constitue un traitement de **données à caractère personnel** soumis aux principes de licéité, de proportionnalité et de transparence.

Questions fréquentes

Existe-t-il des exceptions à l'interdiction du keylogger en entreprise ?

Oui, exception très étroite pour la sécurité informatique ou la prévention d'actes illicites graves, à condition que le keylogger soit ciblé, temporaire, proportionné, et qu'aucun moyen moins intrusif ne soit envisageable. AIPD obligatoire et consultation de la délégation requises.

L'employeur peut-il utiliser un keylogger au Luxembourg ?

Non, en principe interdit. Le keylogger constitue une surveillance permanente, intrusive et excessive contraire aux principes de nécessité et de proportionnalité. Aucune finalité ordinaire de gestion RH ou de contrôle de productivité ne justifie un tel dispositif selon la CNPD.

Quelle alternative au keylogger pour la sécurité informatique ?

Privilégier systématiquement les outils moins intrusifs : SIEM, journaux d'accès applicatifs, audits ponctuels. La démonstration de subsidiarité (aucun moyen moins intrusif ne suffit) conditionne la légalité de tout recours exceptionnel à un keylogger.

Quelles données un keylogger capte-t-il ?

L'intégralité des touches activées sur un poste informatique : identifiants, mots de passe, communications privées, messages personnels. Cette collecte exhaustive est jugée par nature disproportionnée par la CNPD, sauf incident de sécurité documenté affectant un poste précis.

Quelles obligations documentaires pour un keylogger exceptionnel ?

AIPD documentée (article 35 RGPD) analysant nécessité et proportionnalité, procès-verbal de consultation de la délégation (L.414-9), notice individuelle écrite aux salariés visés, périmètre restreint (postes ciblés, durée limitée à l'enquête), habilitation stricte d'accès.

Quelles sanctions pour un usage non justifié d'un keylogger ?

Amendes RGPD jusqu'à 20 millions d'euros ou 4 % du chiffre d'affaires mondial, sanctions pénales L.261-2 (8 jours à 1 an et 251 € à 125 000 €), irrecevabilité des preuves recueillies. La CNPD peut ordonner la cessation immédiate du dispositif.

Conditions d’exercice

Le keylogger ne se justifie quasiment jamais : la CNPD considère que la collecte exhaustive des frappes est par nature disproportionnée, sauf incident de sécurité documenté affectant un poste précis.

Condition	Exigence
Motif légitime restrictif	Sécurité du SI ou prévention d'infractions graves uniquement — exclu : contrôle de productivité ou présence
Subsidiarité	Démonstration qu'aucun moyen moins intrusif (logs réseau, audit ciblé) ne suffit
Ciblage	Postes nominativement désignés et durée limitée dans le temps
AIPD préalable	Obligatoire (article 35 RGPD) — risque élevé caractérisé
Information	Notice individuelle aux salariés concernés et consultation de la délégation (L.414-9)

Modalités pratiques

La CNPD n'autorise plus aucun dispositif sur déclaration préalable depuis le RGPD ; l'accountability impose à l'employeur de démontrer lui-même la conformité par sa documentation.

Démarche	Précision
AIPD documentée	Analyse de nécessité, proportionnalité, mesures de mitigation, consultation DPO
Procès-verbal délégation	Consultation préalable et débat motivé (L.414-9)
Notice individuelle	Information écrite des salariés visés avant activation
Périmètre restreint	Postes ciblés, durée limitée à l'enquête, finalité unique
Habilitation stricte	Accès aux données réservé au DPO et à la sécurité informatique
Conservation limitée	Suppression dès la finalité atteinte, généralement quelques semaines
Traçabilité des accès	Journalisation de chaque consultation des données captées

Pratiques et recommandations

Privilégier systématiquement les outils moins intrusifs : SIEM, journaux d'accès applicatifs, audits ponctuels.

Documenter par écrit les indices sérieux justifiant le recours au keylogger et l'absence d'alternative.

Limiter strictement le dispositif à la durée de l'enquête de sécurité.

Consulter un avis juridique spécialisé et le DPO avant toute mise en œuvre.

Sécuriser les données captées par chiffrement et accès restreint au DPO et à un référent sécurité.

Supprimer immédiatement les données dès la finalité de sécurité atteinte.

Cadre juridique

Référence	Objet
Art. L.261-1 du Code du travail	Surveillance des salariés — finalités limitatives
Art. L.261-2 du Code du travail	Sanctions pénales (8 jours à 1 an + 251 € à 125 000 €)
Art. L.414-9 du Code du travail	Co-décision de la délégation du personnel (? 150 salariés)
Loi modifiée du 1er août 2018	Protection des données personnelles
Règlement (UE) 2016/679 (RGPD)	Articles 5, 6, 9, 32, 35
Lignes directrices CNPD	Cybersurveillance sur le lieu de travail

L'usage non justifié d'un keylogger expose à des amendes administratives RGPD jusqu'à 20 millions d'euros ou 4 % du chiffre d'affaires mondial, à des sanctions pénales (L.261-2 : 8 jours à 1 an et amende de 251 € à 125 000 €) et à l'irrecevabilité des preuves recueillies. La CNPD peut ordonner la cessation immédiate du dispositif.