L'usage d'un keylogger est-il légal dans une entreprise luxembourgeoise ?

Réponse courte

L'usage d'un **keylogger** en entreprise est en principe **interdit** au Luxembourg : la CNPD le considère comme une mesure hautement intrusive, présumée disproportionnée car équivalente à une surveillance généralisée et permanente des salariés, dans la même catégorie que le screen monitoring. Il ne peut être envisagé que dans des **circonstances exceptionnelles** dûment justifiées (enquête sur faits délictueux graves, impossibilité absolue d'alternative).

Avant toute mise en œuvre, l'employeur doit conduire un test de proportionnalité approfondi, réaliser une **AIPD** (article 35 RGPD), consulter la CNPD si le risque résiduel reste élevé (article 36), informer individuellement les salariés et consulter la délégation du personnel (article L.414-9). L'usage clandestin d'un keylogger est constitutif d'une infraction pénale (L.261-2) et entraîne la nullité absolue des preuves recueillies.

Définition

Un **keylogger** est un dispositif matériel ou logiciel qui enregistre de façon systématique et continue toutes les frappes clavier d'un salarié, y compris des contenus très sensibles : identifiants, mots de passe, correspondances privées, données médicales ou syndicales.

Au sens du RGPD, son usage constitue un traitement à risque élevé, qualifié de **surveillance généralisée et permanente**, présumée illicite par la CNPD sauf à démontrer une nécessité absolue et l'absence de toute alternative.

Questions fréquentes

Combien de temps un keylogger peut-il rester actif ?

Sa durée doit être strictement limitée à l'enquête et son périmètre ciblé sur un poste précis. Les données collectées sont supprimées immédiatement dès que la finalité est atteinte ou l'enquête close.

Dans quels cas exceptionnels un keylogger peut-il être envisagé ?

Uniquement dans des circonstances exceptionnelles : enquête sur faits délictueux graves ou protection d'intérêts vitaux, avec démonstration documentée qu'aucune alternative moins intrusive (DLP, journalisation, gestion des accès) ne permet d'atteindre la finalité.

Faut-it consulter la CNPD avant d'installer un keylogger ?

Oui, la consultation préalable de la CNPD (article 36 RGPD) s'impose si le risque résiduel reste élevé après les mesures d'atténuation. Une AIPD approfondie est systématiquement requise (article 35 RGPD).

L'usage d'un keylogger est-il légal dans une entreprise luxembourgeoise ?

Le keylogger est en principe interdit. La CNPD le considère comme une mesure hautement intrusive, présumée disproportionnée car équivalente à une surveillance généralisée et permanente des salariés.

Quelles sanctions pour un keylogger installé clandestinement ?

Infraction pénale au titre de l'article L.261-2 du Code du travail (8 jours à 1 an d'emprisonnement, 251 à 125 000 € d'amende), sanctions administratives jusqu'à 4 % du CA mondial et nullité absolue des preuves.

Un keylogger peut-il capter des données sensibles au sens du RGPD ?

Oui, il enregistre des identifiants, mots de passe, correspondances privées, données médicales ou syndicales. Ces données sensibles relèvent de l'article 9 du RGPD et bénéficient d'une protection renforcée.

Conditions d’exercice

La CNPD a expressément qualifié le keylogger de mesure exceptionnelle : sa mise en œuvre est admissible uniquement face à un risque grave et avéré, jamais à titre préventif ou pour un contrôle ordinaire de productivité.

Condition	Exigence
Surveillance interdite par principe	Le keylogger constitue une surveillance généralisée et permanente présumée disproportionnée
Finalité exceptionnelle	Enquête ciblée sur faits délictueux graves ou protection d'intérêts vitaux
Absence d'alternative	Démonstration documentée qu'aucun moyen moins intrusif n'est suffisant
Limitation temporelle	Durée strictement limitée à l'enquête, périmètre ciblé sur un poste
Consultation	Délégation du personnel et CNPD si risque résiduel élevé
Information	Individuelle et préalable, sauf circonstances exceptionnelles documentées

Modalités pratiques

L'AIPD doit être systématiquement réalisée pour tout keylogger : la CNPD considère ce dispositif comme intrinsèquement à risque élevé et susceptible de capter des données sensibles relevant de l'article 9 du RGPD.

Démarche	Précision
Analyse d'impact (AIPD)	Article 35 du RGPD, obligatoire et approfondie
Consultation préalable CNPD	Article 36 du RGPD si risque résiduel élevé
Consultation de la délégation	Procès-verbal préalable à toute installation (article L.414-9)
Information individuelle	Notice détaillée sur la nature, la portée et la durée
Limitation du périmètre	Poste(s) ciblé(s), durée définie, suppression à l'issue
Sécurité du traitement	Chiffrement, authentification forte, journalisation des accès
Encadrement humain	Procédure documentée d'analyse des données collectées

Pratiques et recommandations

Privilégier systématiquement les alternatives moins intrusives : journalisation des connexions, gestion fine des accès, DLP ciblé.

Limiter le keylogger à une durée strictement minimale et au seul poste de travail concerné par l'enquête.

Supprimer immédiatement les données dès que la finalité est atteinte ou que l'enquête est close.

Documenter chaque étape de l'analyse de proportionnalité, de la consultation et des accès aux données.

Associer le DPO et un conseil juridique dès la phase d'évaluation préalable du dispositif.

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 (8 jours à 1 an, 251 € à 125 000 €)
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, 9, 35, 36
Lignes directrices CNPD	Cybersurveillance sur le lieu de travail

L'usage clandestin d'un keylogger est constitutif d'une infraction pénale (L.261-2) et expose l'employeur à des sanctions administratives jusqu'à 4 % du chiffre d'affaires mondial. Les données recueillies sont nulles comme moyen de preuve et toute sanction disciplinaire fondée sur celles-ci est inopposable.