Quelles sanctions encourt l'employeur pour une vidéosurveillance ou géolocalisation illicite des salariés au Luxembourg ?

Réponse courte

La vidéosurveillance et la géolocalisation des salariés sur le lieu de travail sont strictement encadrées par l'article L.261-1 du Code du travail, qui pose le principe d'un traitement licite uniquement pour des finalités précises (sécurité, contrôle de production, organisation du travail). L'employeur doit informer préalablement les salariés et la délégation du personnel, et respecter les obligations issues du règlement (UE) 2016/679 (RGPD) et de la loi modifiée du 1er août 2018.

Les sanctions pénales sont prévues à l'article L.261-2 du Code du travail et peuvent inclure des amendes, complétées par les sanctions administratives de la CNPD (jusqu'à 4 % du chiffre d'affaires annuel mondial pour les violations RGPD les plus graves). À cela s'ajoutent le risque de nullité des preuves issues du dispositif illicite et la possibilité d'une action civile en réparation engagée par les salariés concernés.

Définition

La surveillance des salariés sur le lieu de travail désigne tout dispositif permettant à l'employeur de collecter, stocker ou analyser des données relatives à l'activité des travailleurs : vidéosurveillance, géolocalisation des véhicules, badgeage biométrique, monitoring informatique, écoute téléphonique, journaux d'accès. Ces dispositifs constituent un traitement de données à caractère personnel au sens du RGPD.

L'article L.261-1 du Code du travail subordonne la légalité du traitement à des conditions cumulatives : finalité légitime et proportionnée, information préalable des salariés, consultation et information de la délégation du personnel, respect des principes de minimisation et de durée de conservation. L'absence d'une seule de ces conditions rend le dispositif illicite et expose l'employeur à des sanctions pénales et administratives.

Conditions d’exercice

L'article L.261-1 du Code du travail autorise la surveillance des salariés uniquement pour des finalités limitativement énumérées : nécessités de sécurité et de santé, protection des biens, contrôle du processus de production portant uniquement sur les machines, contrôle temporaire de la production ou des prestations du travailleur, et organisation du travail selon les horaires de travail. Toute autre finalité est par principe illicite.

L'information préalable des salariés est obligatoire et doit être individuelle, claire et complète (finalité, modalités, durée de conservation, droits d'accès et de rectification). La délégation du personnel doit être informée et co-décisionnaire pour les traitements affectant la santé et la sécurité (article L.414-9 du Code du travail). À défaut

d'accord, la décision peut être soumise à l'Office national de conciliation.

Le dispositif doit en outre faire l'objet d'une analyse d'impact relative à la protection des données (AIPD) lorsqu'il présente un risque élevé pour les droits et libertés des personnes. La CNPD peut intervenir en contrôle, sur plainte ou d'office, et infliger des amendes administratives.

Modalités pratiques

- Vérifier la finalité du traitement et son adéquation aux cas autorisés par l'article L.261-1.
- Informer individuellement chaque salarié par écrit (note interne, avenant, panneau d'information).
- Consulter la délégation du personnel et obtenir sa co-décision pour les traitements concernant la santé-sécurité (article L.414-9).
- Réaliser une analyse d'impact relative à la protection des données (AIPD) lorsque requise.
- Tenir un registre des traitements et désigner un délégué à la protection des données (DPO) si nécessaire.
- Limiter la durée de conservation des images et données aux besoins strictement nécessaires.
- Sécuriser l'accès aux enregistrements et tracer toute consultation.

Pratiques et recommandations

Le DRH doit cartographier l'ensemble des dispositifs de surveillance déployés dans l'entreprise (caméras, géolocalisation, monitoring) et vérifier leur conformité au regard de l'article L.261-1 et du RGPD. Une revue périodique permet d'identifier les dispositifs obsolètes ou disproportionnés et de procéder aux ajustements nécessaires.

Il est recommandé de formaliser une politique interne de surveillance, validée par la délégation du personnel et communiquée à l'ensemble des salariés, précisant les finalités, les modalités, les destinataires des données et les droits des personnes. Cette politique doit être mise à jour à chaque évolution technologique ou organisationnelle.

En cas de doute sur la légalité d'un dispositif, il est prudent de solliciter une consultation préalable de la CNPD. La preuve obtenue par un dispositif illicite est en principe écartée par les juridictions, ce qui peut compromettre une procédure disciplinaire ou un licenciement fondé sur des éléments tirés de la surveillance.

Cadre juridique

- **Article L.261-1 du Code du travail** (surveillance des salariés sur le lieu de travail)
- **Article L.261-2 du Code du travail** (sanctions pénales en cas de surveillance illicite)
- **Article L.414-9 du Code du travail** (co-décision de la délégation du personnel sur les traitements affectant santé-sécurité)
- **Règlement (UE) 2016/679 du 27 avril 2016** relatif à la protection des données (RGPD)
- **Loi modifiée du 1er août 2018** relative à la protection des personnes à l'égard du traitement des données à caractère personnel
- **Loi du 1er août 2018** portant organisation de la Commission nationale pour la protection des données

Le DRH doit s'assurer que tout dispositif de surveillance respecte le triple test : licéité de la finalité, proportionnalité de la collecte et information préalable. Toute défaillance expose à un cumul de sanctions pénales (Code du travail) et administratives (CNPD) particulièrement lourdes.