Quelles sont les obligations de l’entreprise en matière de sécurité des données de surveillance ?

Réponse courte

L’entreprise doit mettre en place des **mesures techniques et organisationnelles appropriées** pour garantir la sécurité, l’intégrité et la confidentialité des données issues des dispositifs de surveillance. Cela inclut le contrôle des accès, le chiffrement ou la pseudonymisation, la traçabilité des opérations, la limitation des personnes autorisées à consulter les données, ainsi que la conservation des données uniquement pendant la durée strictement nécessaire à la finalité poursuivie.

L’employeur doit également tenir un registre des activités de traitement, documenter toute violation de données et, en cas de risque pour les droits des personnes concernées, notifier la CNPD dans les meilleurs délais. Il est recommandé de réaliser une analyse d’impact, de former les personnes habilitées, de prévoir des procédures pour l’exercice des droits des salariés et de procéder à des audits réguliers de sécurité et de conformité. Toute absence de mesures adaptées ou conservation excessive expose l’employeur à des sanctions.

Définition

Les données de surveillance correspondent aux informations collectées par l’employeur via des dispositifs de contrôle ou de surveillance des salariés, tels que la vidéosurveillance, la géolocalisation, le contrôle d’accès ou la surveillance informatique. Lorsqu’elles permettent d’identifier directement ou indirectement une personne physique, ces données sont qualifiées de données à caractère personnel au sens du Code du travail luxembourgeois et de la loi modifiée du 1er août 2018 relative à la protection des personnes à l’égard du traitement des données à caractère personnel.

La collecte et le traitement de ces données impliquent le respect de principes fondamentaux, notamment la licéité, la loyauté, la transparence, la limitation des finalités, la minimisation des données, l’exactitude, la limitation de la conservation, l’intégrité et la confidentialité.

Conditions d’exercice

L’employeur ne peut mettre en place un dispositif de surveillance que pour des finalités déterminées, légitimes et proportionnées, telles que la sécurité des biens et des personnes ou le contrôle du respect des obligations professionnelles. Toute collecte de données doit être précédée d’une information claire et complète des salariés concernés, précisant la nature, la finalité, la durée de conservation et les destinataires des données.

La consultation préalable de la délégation du personnel est obligatoire (article L.261-1 du Code du travail). Lorsque le dispositif est susceptible d’engendrer un risque élevé pour les droits et libertés des personnes concernées, l’avis préalable de la Commission nationale pour la protection des données (CNPD) est requis. L’employeur doit également

garantir l'égalité de traitement entre les salariés et veiller à ce que la surveillance ne porte pas atteinte à la dignité humaine.

Modalités pratiques

L'employeur doit mettre en œuvre des mesures techniques et organisationnelles appropriées pour garantir la sécurité, l'intégrité et la confidentialité des données de surveillance. Ces mesures incluent notamment :

- Le contrôle des accès physiques et logiques aux données
- Le chiffrement et la pseudonymisation lorsque cela est possible
- La traçabilité des accès et des opérations effectuées sur les données
- La limitation stricte des personnes autorisées à consulter ou traiter les données

Les données de surveillance doivent être conservées uniquement pendant la durée strictement nécessaire à la réalisation de la finalité poursuivie, puis supprimées ou anonymisées de manière sécurisée. Toute violation de données doit être documentée et, en cas de risque pour les droits des personnes concernées, notifiée à la CNPD dans les meilleurs délais.

L'employeur doit également assurer la traçabilité des accès et garantir l'encadrement humain des dispositifs automatisés, conformément aux principes de transparence et de contrôle effectif.

Pratiques et recommandations

Il est recommandé à l'employeur de réaliser une analyse d'impact relative à la protection des données (AIPD) avant la mise en place de tout dispositif de surveillance susceptible d'engendrer un risque élevé. Les personnes habilitées à accéder aux données de surveillance doivent être formées à la sécurité et à la confidentialité des données.

Un registre des activités de traitement doit être tenu à jour, incluant les dispositifs de surveillance. L'employeur doit prévoir des procédures pour permettre l'exercice effectif des droits des salariés (accès, rectification, effacement, limitation, opposition). Il est conseillé de procéder régulièrement à des audits de sécurité et de conformité, et de documenter toute action ou incident relatif à la sécurité des données.

Cadre juridique

Les obligations en matière de sécurité des données de surveillance sont fixées par :

- **Code du travail luxembourgeois** :
  - Article L.261-1 (consultation de la délégation du personnel)
  - Article L.121-6 (protection de la vie privée et des données personnelles)
- **Loi modifiée du 1er août 2018 relative à la protection des personnes à l'égard du traitement des données à caractère personnel** :
  - Article 24 (responsabilité du responsable du traitement)
  - Article 25 (protection des données dès la conception et par défaut)
  - Article 30 (registre des activités de traitement)
  - Article 32 (sécurité du traitement)
  - Article 33 (notification des violations de données à la CNPD)
  - Article 34 (communication des violations aux personnes concernées)
- **Lignes directrices de la CNPD** applicables aux dispositifs de surveillance en entreprise

Toute méconnaissance de ces obligations expose l'employeur à des sanctions administratives et pénales.

L'absence de mesures de sécurité adaptées ou la conservation excessive des données de surveillance constitue une violation susceptible d'entraîner des sanctions financières, une interdiction d'utilisation des dispositifs concernés et une atteinte aux droits fondamentaux des salariés.