Qui peut accéder aux données issues de la surveillance ?

Réponse courte

Seules les personnes expressément habilitées par l'employeur peuvent accéder aux données issues de la surveillance, dans le cadre de leurs fonctions et pour des finalités déterminées, légitimes et proportionnées. Il s'agit principalement des membres de la direction, des responsables des ressources humaines et, le cas échéant, du personnel chargé de la sécurité informatique ou physique, dans la stricte mesure de leurs attributions.

L'accès à ces données ne peut être accordé à des tiers extérieurs à l'entreprise que sur obligation légale, judiciaire ou réglementaire expresse. Les personnes autorisées doivent être désignées par écrit, et chaque accès doit être consigné dans un registre précisant l'identité, la date, l'heure et le motif de la consultation.

Définition

Les données issues de la surveillance désignent l'ensemble des informations collectées par l'employeur au moyen de dispositifs techniques destinés à surveiller l'activité des salariés ou à protéger les biens de l'entreprise. Ces dispositifs incluent notamment la vidéosurveillance, la géolocalisation, le contrôle des accès, la surveillance des communications électroniques et l'enregistrement des appels téléphoniques.

Ces données sont considérées comme des données à caractère personnel lorsqu'elles permettent d'identifier directement ou indirectement un salarié. Leur traitement est soumis à des règles strictes de protection des données et de respect de la vie privée, conformément au Code du travail luxembourgeois et à la législation spécifique sur la protection des données.

Conditions d'exercice

L'accès aux données issues de la surveillance est strictement limité aux personnes expressément habilitées par l'employeur, dans le cadre de leurs fonctions et pour des finalités déterminées, légitimes et proportionnées. Seuls les membres de la direction, les responsables des ressources humaines et, le cas échéant, le personnel chargé de la sécurité informatique ou physique peuvent accéder à ces données, dans la stricte mesure de leurs attributions.

Toute consultation doit répondre à un objectif légitime, tel que la sécurité des biens et des personnes, la prévention des infractions ou la vérification du respect des obligations professionnelles. L'accès ne peut être accordé à des tiers extérieurs à l'entreprise, sauf en cas d'obligation légale, judiciaire ou réglementaire expresse.

Modalités pratiques

L'employeur doit désigner, par écrit, les personnes autorisées à accéder aux données issues de la surveillance, en précisant la nature des données accessibles, les finalités poursuivies et les modalités d'accès. Un registre des accès doit être tenu, mentionnant l'identité de la personne ayant accédé aux données, la date, l'heure et le motif de la consultation.

Les salariés doivent être informés, individuellement et collectivement, de l'existence des dispositifs de surveillance, des catégories de données collectées, des finalités poursuivies, des personnes habilitées à y accéder et de leurs droits d'accès, de rectification et d'opposition. Toute transmission de données à des sous-traitants doit faire l'objet d'un encadrement contractuel strict, garantissant la confidentialité, la sécurité des informations et la traçabilité des accès.

Pratiques et recommandations

Il est recommandé de limiter l'accès aux données issues de la surveillance au strict nécessaire, en fonction des responsabilités de chaque personne habilitée. Les accès doivent être régulièrement réévalués et adaptés en cas de changement de fonction ou de départ d'un salarié.

Les procédures internes doivent prévoir des contrôles périodiques afin de vérifier le respect des règles d'accès, de traçabilité et d'égalité de traitement entre les salariés. Toute violation ou accès non autorisé doit être immédiatement signalé à la direction et, le cas échéant, à la Commission nationale pour la protection des données (CNPD). Il est conseillé de former les personnes habilitées aux obligations de confidentialité, à la protection des données à caractère personnel et à l'encadrement humain des dispositifs automatisés.

Cadre juridique

- **Code du travail luxembourgeois** :
  - Article L.261-1 à L.261-4 (protection des données à caractère personnel dans les relations de travail)
  - Article L.121-6 (égalité de traitement et non-discrimination)
  - Article L.414-9 (consultation du personnel sur l'introduction de dispositifs de surveillance)
- **Loi du 1er août 2018 portant organisation de la Commission nationale pour la protection des données et du régime général sur la protection des données**
- **Loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel**
- **Règlement (UE) 2016/679 (RGPD), applicable au Luxembourg**
- **Jurisprudence luxembourgeoise sur la proportionnalité et la justification de l'accès**
- **Obligation de déclaration ou d'autorisation préalable auprès de la CNPD selon la nature du dispositif**

L’accès non autorisé ou injustifié aux données issues de la surveillance constitue une violation grave susceptible d’engager la responsabilité de l’employeur et de la personne ayant accédé indûment aux données. Il est essentiel de documenter précisément les habilitations, d’assurer la traçabilité des accès et de sensibiliser les personnes concernées aux risques encourus, y compris en matière de sanctions administratives et pénales.