

Peut-on surveiller l'activité des salariés sur leur ordinateur professionnel ?

Réponse courte

La surveillance de l'activité des salariés sur leur ordinateur professionnel est possible au Luxembourg, mais elle est strictement encadrée. L'employeur doit poursuivre un objectif légitime, respecter le principe de proportionnalité et éviter toute surveillance systématique, permanente ou intrusive, sauf justification exceptionnelle.

Avant toute mise en place, l'employeur doit informer individuellement et collectivement les salariés, consulter la délégation du personnel et obtenir l'avis préalable de la CNPD. Toute surveillance doit être documentée, limitée à ce qui est strictement nécessaire et garantir la confidentialité des données.

Définition

La surveillance de l'activité des salariés sur leur ordinateur professionnel désigne l'ensemble des dispositifs techniques ou organisationnels permettant à l'employeur de contrôler, enregistrer, analyser ou accéder aux données relatives à l'utilisation des équipements informatiques mis à disposition dans le cadre du contrat de travail. Cette surveillance peut inclure la consultation des courriels professionnels, le suivi de la navigation internet, l'analyse des fichiers stockés ou l'utilisation de logiciels de monitoring.

Conditions d'exercice

Au Luxembourg, la surveillance des salariés sur leur poste informatique est strictement encadrée. L'employeur ne peut mettre en place un dispositif de surveillance que si celui-ci poursuit un objectif légitime, tel que la sécurité des systèmes informatiques, la prévention des comportements illicites, la protection des intérêts économiques de l'entreprise ou la vérification du respect des obligations contractuelles. La surveillance doit être proportionnée au but recherché et ne pas porter atteinte de manière excessive à la vie privée des salariés. Toute surveillance systématique, permanente ou intrusive est prohibée, sauf justification particulière et exceptionnelle.

Avant toute mise en œuvre, l'employeur doit informer individuellement et collectivement les salariés concernés, en précisant la nature, la finalité et les modalités du dispositif. L'avis préalable de la délégation du personnel, lorsqu'elle existe, est obligatoire. En outre, la Commission nationale pour la protection des données (CNPD) doit être consultée pour avis préalable sur tout dispositif de surveillance informatique, conformément à la loi modifiée du 1er août 2018 relative à la protection des personnes à l'égard du traitement des données à caractère personnel.

Modalités pratiques

La mise en place d'une surveillance informatique requiert une documentation précise : politique interne de sécurité informatique, charte d'utilisation des outils numériques, registre des traitements de données. L'information des salariés doit être réalisée par écrit, mentionnant les données collectées, la durée de conservation, les droits d'accès, de rectification et d'opposition, ainsi que les coordonnées du responsable du traitement.

L'accès aux données personnelles, telles que les courriels identifiés comme privés ou les fichiers personnels, n'est possible qu'en présence du salarié ou après l'avoir dûment informé et invité à être présent. L'employeur doit veiller à limiter l'accès aux seules personnes habilitées et à garantir la confidentialité des données traitées. Toute collecte de données doit être limitée à ce qui est strictement nécessaire à la finalité poursuivie.

Pratiques et recommandations

Il est recommandé de privilégier des mesures préventives telles que la sensibilisation des salariés à la sécurité informatique et l'adoption de chartes d'utilisation claires. Les dispositifs de surveillance doivent être ciblés, temporaires et proportionnés. L'employeur doit éviter toute surveillance généralisée ou permanente, notamment l'enregistrement continu des frappes clavier ou la captation d'images sans motif impérieux.

En cas de contrôle ponctuel, il convient de documenter la procédure, d'enregistrer les motifs précis et de respecter le principe de minimisation des données. La CNPD recommande de procéder à une analyse d'impact relative à la protection des données pour tout dispositif susceptible d'engendrer un risque élevé pour les droits et libertés des salariés.

Cadre juridique

La surveillance de l'activité informatique des salariés est encadrée principalement par la loi modifiée du 1^{er} août 2018 relative à la protection des personnes à l'égard du traitement des données à caractère personnel, les articles [L.261-1](#) et suivants du Code du travail relatifs à la protection de la vie privée au travail, ainsi que par la jurisprudence de la Cour supérieure de justice et les lignes directrices de la CNPD. Toute violation des règles relatives à la proportionnalité, à l'information préalable ou à la consultation des instances représentatives expose l'employeur à des sanctions administratives et pénales, ainsi qu'à la nullité des preuves obtenues par un dispositif illicite.

La mise en place d'une surveillance informatique sans information préalable des salariés ou sans consultation de la CNPD constitue une infraction susceptible d'entraîner l'invalidation des preuves recueillies et des sanctions à l'encontre de l'employeur.

Les contenus sont rédigés et mis à jour régulièrement à partir de sources officielles. Leur usage ne remplace pas une consultation juridique et doit être validé par un professionnel du droit.