La CNPD doit-elle être notifiée lors de la mise en place d'un contrôle de l'activité informatique des salariés ?

Réponse courte

La notification systématique à la CNPD n'est plus requise lors de la mise en place d'un contrôle de l'activité informatique des salariés. Cependant, l'employeur doit réaliser une analyse d'impact relative à la protection des données (AIPD) si le dispositif est susceptible d'engendrer un risque élevé pour les droits et libertés des salariés.

Si l'AIPD révèle des risques élevés qui ne peuvent pas être atténués par les mesures prévues, l'employeur doit consulter préalablement la CNPD avant la mise en œuvre du dispositif. L'AIPD doit être documentée et tenue à disposition de la CNPD en cas de contrôle.

Définition

Le contrôle de l'activité informatique correspond à toute opération par laquelle un employeur surveille, collecte, analyse ou exploite des données relatives à l'utilisation des outils informatiques mis à disposition des salariés dans le cadre professionnel. Cela inclut notamment la surveillance des courriels, de la navigation Internet, des accès aux applications, des transferts de fichiers ou de l'utilisation des périphériques de stockage.

Ce type de contrôle constitue un traitement de données à caractère personnel, dès lors qu'il porte sur des informations identifiables relatives aux salariés. Il s'inscrit dans le cadre des obligations de sécurité, de conformité ou de gestion des ressources informatiques de l'entreprise.

Conditions d'exercice

La mise en place d'un dispositif de contrôle de l'activité informatique des salariés est strictement encadrée par le Code du travail luxembourgeois et la législation sur la protection des données. L'employeur doit démontrer un intérêt légitime, respecter le principe de proportionnalité et limiter le contrôle à ce qui est strictement nécessaire à la finalité poursuivie.

Le contrôle ne peut porter atteinte à la vie privée des salariés que dans la mesure où cette atteinte est justifiée, proportionnée et encadrée. L'égalité de traitement entre salariés doit être garantie, et toute discrimination est prohibée. L'employeur doit également assurer la traçabilité des opérations et garantir l'intervention d'un encadrement humain dans l'analyse des données collectées.

Modalités pratiques

Depuis l'entrée en vigueur du Règlement (UE) 2016/679 (RGPD) et de la loi modifiée du 1er août 2018, la notification systématique à la Commission nationale pour la protection des données (CNPD) n'est plus requise pour chaque dispositif de contrôle. Toutefois, l'employeur doit réaliser une analyse d'impact relative à la protection des données (AIPD) lorsque le traitement est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées, ce qui est généralement le cas pour les dispositifs de surveillance généralisée ou systématique.

L'AIPD doit être documentée, actualisée et conservée à disposition de la CNPD en cas de contrôle. Si l'AIPD révèle des risques élevés non atténués par les mesures envisagées, l'employeur a l'obligation de consulter préalablement la CNPD avant la mise en œuvre du dispositif. L'information individuelle et collective des salariés est obligatoire, précisant la nature, la finalité, la durée de conservation des données et les droits des personnes concernées.

Pratiques et recommandations

Avant toute mise en œuvre d'un contrôle de l'activité informatique, il est recommandé d'associer la délégation du personnel à la procédure d'information et de consulter le règlement interne ou la charte informatique de l'entreprise. L'employeur doit limiter l'accès aux données collectées aux seules personnes habilitées et mettre en place des mesures techniques et organisationnelles appropriées pour garantir la sécurité des données.

Toute modification substantielle du dispositif doit faire l'objet d'une nouvelle analyse d'impact. Il est conseillé de documenter l'ensemble des démarches (information, consultation, analyses, mesures de sécurité) afin d'assurer la traçabilité et la conformité en cas de contrôle par la CNPD.

Cadre juridique

- **Code du travail luxembourgeois**
  - Article L.261-1 et suivants (protection des données à caractère personnel dans les relations de travail)
  - Article L.121-6 (surveillance sur le lieu de travail, information et consultation du personnel)
- **Loi modifiée du 1er août 2018** relative à la protection des personnes à l'égard du traitement des données à caractère personnel
- **Loi du 2 août 2002** relative à la protection des personnes à l'égard du traitement des données à caractère personnel dans les relations de travail, telle que modifiée
- **Règlement (UE) 2016/679 (RGPD)**
- **Recommandations et lignes directrices de la CNPD**
- **Jurisprudence de la Cour supérieure de justice du Luxembourg** en matière de surveillance sur le lieu de travail

L’absence de notification systématique à la CNPD ne dispense pas l’employeur de ses obligations en matière d’analyse d’impact, d’information des salariés et de consultation préalable en cas de risques élevés non maîtrisés. En cas de doute, il est recommandé de solliciter un avis formel ou une consultation informelle auprès de la CNPD avant la mise en œuvre du dispositif de contrôle.