Peut-on imposer un contrôle d’accès par empreinte digitale ?

Réponse courte

Un contrôle d’accès par empreinte digitale ne peut être imposé que si l’employeur démontre qu’il est strictement nécessaire et proportionné à la finalité poursuivie, notamment pour protéger des zones sensibles ou des données confidentielles, et qu’aucun autre moyen moins intrusif n’est suffisant. Il ne peut pas être utilisé pour le simple contrôle horaire ou la gestion des présences.

La mise en place d’un tel dispositif requiert la réalisation d’une analyse d’impact relative à la protection des données, l’information transparente des salariés, la consultation préalable de la délégation du personnel, ainsi que l’obtention d’une autorisation préalable de la CNPD. Une solution alternative doit être proposée aux salariés refusant légitimement le traitement de leurs données biométriques, afin d’éviter toute discrimination.

En l’absence de justification sérieuse ou d’autorisation de la CNPD, l’employeur s’expose à des sanctions et à la nullité des preuves issues du dispositif.

Définition

Le contrôle d’accès par empreinte digitale désigne l’utilisation de la reconnaissance biométrique des empreintes digitales des salariés pour autoriser ou refuser l’accès à certains locaux, équipements ou systèmes informatiques de l’entreprise. Ce procédé implique la collecte, le traitement et la conservation de données biométriques, qui sont considérées comme des données à caractère personnel sensibles au sens du droit luxembourgeois.

Les données biométriques sont définies comme des données à caractère personnel résultant d’un traitement technique spécifique, relatives aux caractéristiques physiques, physiologiques ou comportementales d’une personne physique, permettant ou confirmant son identification unique.

Conditions d’exercice

L’employeur ne peut recourir à un contrôle d’accès par empreinte digitale que si ce traitement est strictement nécessaire et proportionné à la finalité poursuivie. Il doit démontrer que d’autres moyens moins intrusifs (badges, codes, etc.) sont insuffisants pour garantir la sécurité requise.

La mise en place d’un tel dispositif n’est justifiée que pour la protection de zones sensibles, de données confidentielles ou de valeurs importantes, et non pour le simple contrôle horaire ou la gestion des présences. L’existence d’un risque avéré et élevé pour la sécurité des biens ou des personnes doit être établie.

L’égalité de traitement entre les salariés doit être respectée, et toute discrimination fondée sur le refus légitime de fournir des données biométriques est prohibée.

Modalités pratiques

Avant toute mise en œuvre, l'employeur doit réaliser une analyse d'impact relative à la protection des données (AIPD) conformément à l'article 39 de la loi du 1er août 2018. Cette analyse doit démontrer la nécessité, la proportionnalité et les mesures prises pour limiter les risques pour les droits et libertés des salariés.

L'information individuelle et transparente de chaque salarié concerné est obligatoire. Elle doit porter sur la finalité, la base légale, la durée de conservation des données, les destinataires, les droits d'accès, de rectification, d'opposition et d'effacement, ainsi que sur la possibilité d'introduire une réclamation auprès de la CNPD.

La consultation préalable de la délégation du personnel est imposée par l'article L.414-9 du Code du travail pour toute introduction ou modification d'un système de surveillance. L'employeur doit également solliciter une autorisation préalable auprès de la CNPD avant toute mise en œuvre du dispositif.

La traçabilité des accès, la documentation des traitements et l'encadrement humain du dispositif doivent être assurés.

Pratiques et recommandations

Il est recommandé de privilégier des dispositifs biométriques utilisant le stockage local des gabarits biométriques sur un support individuel détenu par le salarié, afin de limiter les risques d'atteinte à la vie privée.

Des mesures de sécurité renforcées doivent être prévues pour la conservation, l'accès et la suppression des données biométriques. Il convient de prévoir une solution alternative pour les salariés refusant légitimement le traitement de leurs données biométriques, afin d'éviter toute discrimination.

La durée de conservation des données doit être strictement limitée à la période nécessaire à la finalité poursuivie. Toute violation de données doit être notifiée à la CNPD et, le cas échéant, aux personnes concernées, conformément à l'article 41 de la loi du 1er août 2018.

Cadre juridique

- Loi modifiée du 1er août 2018 relative à la protection des personnes à l'égard du traitement des données à caractère personnel :
  - Article 9 (traitement des catégories particulières de données)
  - Article 39 (analyse d'impact relative à la protection des données)
  - Article 41 (notification des violations de données)
- Code du travail luxembourgeois :
  - Article L.414-9 (consultation de la délégation du personnel)
- Lignes directrices de la CNPD sur l'utilisation de la biométrie en milieu professionnel
- Principes généraux d'égalité de traitement et de non-discrimination (Code du travail, articles L.241-1 et suivants)
- Jurisprudence luxembourgeoise relative à la proportionnalité et à la justification des traitements biométriques

L'absence d'autorisation préalable de la CNPD ou la mise en œuvre d'un contrôle d'accès biométrique sans justification sérieuse expose l'employeur à des sanctions administratives et pénales, ainsi qu'à la nullité des preuves recueillies par ce dispositif. Il est essentiel de documenter chaque étape du processus et de garantir l'encadrement humain du système.