La reconnaissance faciale peut-elle être utilisée par un employeur au Luxembourg ?

Réponse courte

L'utilisation de la reconnaissance faciale par un employeur au Luxembourg est **très strictement encadrée** et dans la plupart des cas **interdite**. Le obligations RGPD classe les données biométriques parmi les **catégories spéciales** dont le traitement est en principe interdit (article 9). L'AI Act classe les systèmes d'identification biométrique en temps réel comme des **pratiques à risque inacceptable** (article 5) et les systèmes d'identification biométrique à distance comme des **systèmes à systèmes à haut risque**.

En milieu professionnel, la reconnaissance faciale pour le contrôle des accès ou le pointage peut être envisagée uniquement si elle est **strictement nécessaire**, **proportionnée** et qu'aucune alternative moins intrusive n'existe. La CNPD exige une **AIPD** préalable et le consentement du salarié ne constitue pas une base juridique valable en raison du déséquilibre de pouvoir dans la relation de travail.

Définition

La **reconnaissance faciale** est une technologie biométrique qui identifie ou vérifie l'identité d'une personne en analysant les caractéristiques géométriques de son visage. Elle utilise des algorithmes d'IA pour comparer une image faciale captée en temps réel avec une base de données de référence. On distingue la **vérification** (1:1, confirmation d'identité) de l'**identification** (1:N, recherche dans une base).

Au Luxembourg, les données biométriques sont des **données sensibles** au sens du RGPD. Leur traitement est soumis à des conditions renforcées et contrôlé par la CNPD. L'AI Act ajoute une couche réglementaire supplémentaire en classant les systèmes biométriques selon leur niveau de risque.

Questions fréquentes

Comment stocker les gabarits biométriques en cas d'utilisation ?

Stockage local sur le dispositif de lecture exclusivement, jamais en cloud ni sur serveur centralisé. Chiffrement obligatoire des données. Accès strictement limité aux personnes habilitées. Suppression automatique en cas de départ du salarié ou de fin de la finalité justifiant le traitement.

L'identification biométrique en temps réel est-elle interdite par l'AI Act ?

Oui, dans les espaces accessibles au public, depuis le 2 février 2025. L'article 5 de l'AI Act prohibe cette pratique parmi les risques inacceptables. L'identification biométrique à distance reste autorisée mais classée à haut risque, exigeant documentation, AIPD et supervision humaine.

La reconnaissance faciale peut-elle être utilisée par un employeur au Luxembourg ?

Très restrictivement. Les données biométriques sont des catégories spéciales RGPD (article 9), interdites de traitement sauf exceptions. L'AI Act interdit l'identification biométrique en temps réel et classe les systèmes d'identification à distance comme à haut risque. Une AIPD préalable est obligatoire.

Le consentement du salarié suffit-il pour la reconnaissance faciale ?

Non. Le consentement n'est pas une base juridique valable en raison du déséquilibre de pouvoir dans la relation de travail. La CNPD considère qu'un consentement libre est impossible. Une autre base juridique (obligation légale, sécurité impérative sans alternative) doit être démontrée.

Quelle position adopte la CNPD sur la reconnaissance faciale en entreprise ?

La CNPD adopte une position restrictive et exige une démonstration rigoureuse de la nécessité et de la proportionnalité. Dans la pratique, les alternatives non biométriques sont presque toujours suffisantes. Le déploiement sans AIPD préalable expose à des sanctions et à des recours des salariés.

Quelles alternatives à la reconnaissance faciale en entreprise ?

Privilégier des alternatives non biométriques : badges RFID, codes PIN, cartes magnétiques, applications mobiles. La reconnaissance faciale ne doit être envisagée qu'en dernier recours pour des raisons de sécurité impératives, après démonstration documentée de l'absence d'alternative proportionnée.

Conditions d’exercice

L'utilisation de la reconnaissance faciale en entreprise est soumise à des conditions cumulatives strictes.

Critère	Détail
RGPD - Données biométriques	Catégorie spéciale (art. 9) ; traitement interdit sauf exceptions ; le consentement du salarié n'est pas valable (déséquilibre de pouvoir) ; intérêt légitime insuffisant seul
Base juridique possible	Obligation légale ou réglementaire imposant la biométrie ; raisons d'intérêt public important ; sécurité impérative sans alternative proportionnée
AI Act - Interdiction	Identification biométrique en temps réel dans les espaces accessibles au public : interdite (art. 5) ; application depuis le 2 février 2025
AI Act - Haut risque	Identification biométrique à distance : système à haut risque (Annexe III) ; documentation technique, AIPD, supervision humaine obligatoires
Proportionnalité	Nécessité absolue démontrée ; absence d'alternative moins intrusive (badge, code, carte) ; limitation à des zones et finalités précises
AIPD obligatoire	Analyse d'impact CNPD avant tout déploiement ; évaluation des risques pour les droits et libertés ; mesures d'atténuation documentées

Modalités pratiques

Le déploiement de la reconnaissance faciale en entreprise exige un processus de conformité très strict.

Étape	Détail
Évaluation de la nécessité	Démontrer l'impossibilité d'utiliser des alternatives moins intrusives (badge RFID, code PIN, carte magnétique) ; documenter les raisons de sécurité impératives
AIPD préalable	Réaliser une analyse d'impact complète ; consulter le DPO ; soumettre à la CNPD si risque résiduel élevé ; documenter les mesures d'atténuation
Consultation obligatoire	Informer et consulter la délégation du personnel (art. L.414-1) ; obtenir l'avis du CSSEP si applicable ; documenter le processus de consultation
Garanties techniques	Stockage local des gabarits biométriques (pas de cloud) ; chiffrement des données ; suppression automatique en cas de départ du salarié ; accès restreint aux données
Information des salariés	Notice d'information RGPD complète ; explication de la finalité et des données traitées ; information sur les droits (accès, effacement, opposition)

Pratiques et recommandations

Privilégier systématiquement des alternatives non biométriques pour le contrôle d'accès et le pointage (badges, codes, applications mobiles), la reconnaissance faciale ne devant être envisagée qu'en dernier recours pour des raisons de sécurité impératives.

Réaliser une AIPD rigoureuse avant tout projet de reconnaissance faciale, en documentant précisément pourquoi aucune alternative moins intrusive ne permet d'atteindre le même niveau de sécurité.

Limiter strictement le périmètre d'utilisation aux zones et finalités identifiées dans l'AIPD, en interdisant toute extension non autorisée (surveillance, suivi des déplacements, reconnaissance des émotions).

Stocker les gabarits biométriques exclusivement en local sur le dispositif de lecture, en évitant tout stockage centralisé ou cloud qui augmente considérablement le risque de fuite de données.

Prévoir une procédure de suppression immédiate des données biométriques en cas de départ du salarié, de retrait du consentement (si applicable) ou de fin de la finalité justifiant le traitement.

Cadre juridique

Référence	Objet
RGPD - Article 9	Traitement des données biométriques : catégorie spéciale, interdiction de principe
RGPD - Article 35	AIPD obligatoire pour les traitements de données biométriques
AI Act (UE 2024/1689) - Article 5	Interdiction de l'identification biométrique en temps réel dans les espaces publics
AI Act - Annexe III	Classification à haut risque des systèmes d'identification biométrique à distance
Art. L.261-1	Encadrement du traitement des données personnelles des salariés
Art. L.414-1	Consultation de la délégation du personnel
Loi du 1er août 2018	Loi nationale de mise en oeuvre du RGPD au Luxembourg

La reconnaissance faciale en entreprise reste une mesure exceptionnelle au Luxembourg. La CNPD adopte une position restrictive et exige une démonstration rigoureuse de la nécessité et de la proportionnalité. Dans la pratique, les alternatives non biométriques (badges, codes) sont presque toujours suffisantes. L'employeur qui déploie un système de reconnaissance faciale sans AIPD préalable s'expose à des sanctions CNPD et à des recours des salariés.