L’accès non biométrique aux locaux professionnels avec ou sans contrôle des horaires

Dans un environnement toujours plus sécuritaire, et face aux risques croissants d’espionnage industriel, l’heure est à la multiplication des systèmes de contrôle d’accès sur le lieu de travail.

Ces dispositifs utilisent des moyens plus ou moins complexes, nécessitant le recours à des outils numériques et/ou informatiques, voire à des systèmes de communications électroniques. Il peut s’agir de cartes magnétiques, avec ou sans contact, combinées à un dispositif de lecture desdites cartes, qui enregistre ou non les informations qu’elles contiennent. D’autres types de dispositifs sont également utilisés, tels que des codes secrets délivrés aux seules personnes habilitées.

Ainsi, l’essence même de tels systèmes repose dans la **nécessaire identification** des personnes aux fins de surveiller ceux qui pénètrent sur le lieu de travail ou dans certaines zones à accès restreint. Cette surveillance s’étend donc aussi bien à leur identité, qu’à la date, l’heure et la porte par laquelle ils ont pu accéder aux locaux.

Dans quels buts un employeur peut-il mettre en place un dispositif de contrôle d’accès ?

Les données personnelles peuvent être collectées pour **plusieurs finalités**, à condition que ces finalités soient :

- **déterminées** ;
- **explicites** ;
- **légitimes** ; et
- **non traitées ultérieurement de manière incompatible** avec ces finalités.

En vertu de ce principe de **limitation des finalités**, l’APDP considère que la mise en œuvre de tels dispositifs n'est admissible que dans le cadre des impératifs sécuritaires suivants :

- contrôler l’accès aux entrées et sorties d’une entreprise, d’un organisme ou d’un immeuble d’habitation ;
- contrôler l’accès à certains locaux limitativement identifiés comme faisant l’objet d’une restriction de circulation, justifiée par la sécurité des biens et des personnes qui y travaillent ;
- gérer les horaires et les temps de présence des employés ;
- contrôler l'accès des visiteurs ;
- permettre, le cas échéant, la constitution de preuves en cas d’infraction.

Quelle justification pour la mise en place un dispositif de contrôle d'accès ?

Pour être licite, un traitement automatisé de données personnelles doit répondre à au moins une des exigences prévues à l'article 5 de la Loi n° 1.565 du 3 décembre 2024.

L'APDP estime ainsi que la mise en place d'un dispositif de contrôle d'accès peut être justifiée par :

- le respect d'une **obligation légale** à laquelle est soumis le responsable du traitement ou son représentant ;
- l'exécution d'un **contrat** ou de **mesures précontractuelles** avec la personne concernée ;
- la réalisation d'un **intérêt légitime** poursuivi par le responsable du traitement ou un tiers, **à la condition de ne pas méconnaître l'intérêt ou les droits et libertés fondamentaux de la personne concernée**.

L'installation d'un dispositif de contrôle d'accès peut dans certains cas être justifiée par le consentement des personnes concernées. Cette justification est toutefois appréciée de manière **très stricte** par l'APDP, notamment dans le cadre d'un contrat de travail établissant un **lien de subordination** entre l'employeur et l'employé.

Quelles garanties mettre en place pour respecter la vie privée des salariés ?

Il appartient à l'employeur de démontrer que les droits et libertés des personnes concernées seront protégés.

Ces dispositifs ne sauraient ainsi être détournés de leur finalité. Ainsi, ils ne peuvent en aucun cas :

- conduire à un **contrôle permanent et inopportun** des personnes concernées ;
- permettre le **contrôle des quotas d'heures** que la loi confère aux **délégués du personnel** et aux **délégués syndicaux pour l'exercice de leurs fonctions** ;
- permettre le **contrôle des déplacements à l'intérieur de l'entité**, exception faite des zones limitativement identifiées comme faisant l'objet d'une restriction de circulation.

Quelles informations peuvent être collectées ?

Conformément aux dispositions de l'article 4 de la Loi n° 1.565 du 3 décembre 2024, les données à caractère personnel collectées doivent être « *adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles sont traitées* ».

L'APDP considère donc que les informations suivantes peuvent être collectées et traitées :

- identité : nom, prénoms, numéro de matricule interne, photographie ;
- informations relatives à la vie professionnelle : service, fonction, plages horaires habituellement autorisées, zones d'accès autorisées, congés, numéro de poste téléphonique ;
- informations temporelles ou horodatage : date et heure d'entrée, date et heure de sortie, date et heure de passage à une zone à accès restreint ;
- accès aux locaux : nom et/ou numéro de la porte d'entrée ou de sortie, ou du point de passage ;
- parking : numéro d'immatriculation du véhicule, numéro de la place de stationnement ;
- visiteurs : nom, prénoms, dates et heures de visite, société d'appartenance, identité de l'employé accueillant le visiteur ;
- badge ou carte : numéro de badge ou de la carte d'accès, date de délivrance, date de validité.

Combien de temps peuvent être conservées les données issues d'un système de contrôle d'accès ?

Conformément à l'article 4 de la Loi n° 1.565 du 3 décembre 2024, les données à caractère personnel objets du traitement ne peuvent être conservées sous une forme permettant l'identification des personnes concernées que pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités pour lesquelles elles sont traitées.

Aussi, l'APDP demande que :

- le badge soit immédiatement désactivé dès que le salarié n'est plus habilité à avoir accès aux locaux ;

- la photo soit supprimée dès la remise du badge ;

- les données relatives aux accès soient supprimées 3 mois après leur enregistrement ;

- les données utilisées pour le suivi du temps de travail soient conservées 5 ans.

Qui peut avoir accès aux données issues du dispositif de contrôle d'accès ?

L'accès aux données d'un dispositif de contrôle d'accès doit être limité aux **seules personnes** qui, dans le cadre de leur(s) fonction(s), peuvent **légitimement en avoir connaissance au regard des objectifs du dispositif**.

Il peut ainsi s'agir en interne du responsable informatique pour la création/désactivation des badges, du Service des Ressources Humaines pour la consultation des horaires ou encore du prestataire qui a accès au traitement dans le cadre de la maintenance du dispositif.

Concernant ce dernier, l'APDP rappelle que ses droits d'accès doivent alors être limités à ce qui est **strictement nécessaire à l'exécution de son contrat de prestation de service**. De plus, ledit prestataire est soumis aux mêmes obligations de sécurité et de confidentialité que celles imposées au responsable du traitement.

Lorsque le dispositif n'est mis en place qu'à des fins d'accès aux locaux **sans contrôle des horaires**, l'APDP rappelle qu'un accès en consultation par le Service des Ressources Humaines ne peut s'effectuer que dans le cadre d'une procédure disciplinaire **en lien** avec les objectifs du traitement.

L'APDP estime par ailleurs que la communication des données à la Direction de la Sûreté Publique peut être justifiée pour les besoins d'une enquête judiciaire.

A cet égard, elle rappelle qu'en cas de transmission, ladite Direction ne pourra avoir communication des informations que dans le strict cadre de ses missions légalement conférées.

Comment informer les personnes concernées ?

Conformément à l'article 10 de la Loi n° 1.565 du 3 décembre 2024 tout système de contrôle d'accès doit être porté à la connaissance des personnes concernées, que ce soit les employés, les visiteurs ou les prestataires.

Ces personnes **doivent** ainsi *a minima* recevoir les informations suivantes :

- **l'identité et les coordonnées professionnelles du responsable du traitement**, et le cas échéant de son **représentant** à Monaco, ou, à défaut, au sein d'un Etat membre de l'Union européenne ;
- les **finalités** du traitement et son **fondement juridique** ;
- les **intérêts légitimes** poursuivis par le responsable du traitement ou le tiers lorsque le traitement est réalisé sur ce fondement ;
- les **catégories de données** personnelles concernées ;
- la **durée de conservation** des données ou, lorsque cela n'est pas possible, **les critères utilisés** pour déterminer cette durée ;
- lorsque le traitement est fondé sur le **consentement** de la personne, le droit de celle-ci de retirer ce consentement **à tout moment** ;
- les **destinataires** ou **catégories** de destinataires ;
- les moyens d'exercer ses **droits d'accès, d'opposition, de rectification, d'effacement, de limitation** ou **de portabilité** ;
- le droit **d'introduire une réclamation auprès de l'Autorité de Protection des Données Personnelles (APDP)** ;
- le cas échéant, les **coordonnées du Délégué à la protection des données**.

La communication de cette information est laissée au **libre choix** de l'employeur. Pour les employés, cette communication peut par exemple s'effectuer par voie d'affichage ou par la communication d'une note interne à l'entreprise.

Concernant les visiteurs, cette information pourrait par exemple prendre la forme d'une mention portée sur le formulaire de collecte des informations personnelles qu'ils remplissent, le cas échéant.

Quelle sécurité mettre en place ?

L'APDP considère que le responsable du traitement doit prendre **toutes précautions utiles pour préserver la sécurité des données** objet du traitement et empêcher, notamment en mettant en place des mesures de contrôle et d'identification, que des employés non autorisés y aient accès.

De manière générale, elle estime que tout responsable du traitement devrait se poser les questions suivantes avant d'installer un dispositif de contrôle d'accès non biométrique :

- Y a-t-il des zones d'accès autorisées/non autorisées suivant le type de personnes concernées (salariés, prestataires, etc.) ?

- Comment s'effectue :
  - la demande d'affectation d'un badge ?
  - l'enrôlement /la création de badge ?
  - la remise de badge ?

- Comment la ou les personne(s) habilitée(s) se connecte(nt)- elle(s) au système de contrôle d'accès ?

- Chaque personne habilitée dispose-t-elle d'un identifiant et mot de passe individuels ?

- Y a-t-il une journalisation automatisée (traçabilité) des accès au système ?

- Quelle est la sécurité (ouverture session avec identifiant/mot de passe individuels, anti-virus, etc.) :
  - du serveur de contrôle d'accès ?
  - du ou des poste(s) de travail ?

- En cas d'accès distant (depuis l'extérieur) :
  - qui dispose de cet accès ?
  - par quel moyen (VPN, liaison point à point, etc.) ?
  - quelle est la sécurité de l'équipement utilisé ?

- En cas de panne du système, comment les « *ouvertures* » des portes s'effectuent elles ?