L’installation de caméras sur le lieu de travail

De nombreux employeurs ont aujourd’hui recours à des systèmes de vidéosurveillance afin, par exemple, d’assurer la sécurité des personnes ou des biens au sein de leurs locaux ou de protéger les accès aux bâtiments.

Ces systèmes conduisent souvent à recueillir des informations permettant d’identifier une **personne physique déterminée ou déterminable**, même si, parfois, ce n’est pas l’objectif recherché, soulevant ainsi des problèmes particuliers en matière de protection des données à caractère personnel.

Dans quels buts un employeur peut-il mettre en place un dispositif de vidéosurveillance ?

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, compte tenu du caractère intrusif des dispositifs de vidéosurveillance, la mise en œuvre de tels dispositifs n'est admissible que dans le cadre des impératifs sécuritaires suivants :

- assurer la sécurité des personnes ;
- assurer la sécurité des biens ;
- permettre le contrôle d'accès ;
- permettre la constitution de preuve en cas d’infraction.

A ces impératifs peuvent s’ajouter des fonctionnalités propres à l’activité de l’employeur concerné comme, par exemple, l’évaluation du matériel et des effectifs sur le chantier lorsque ledit employeur est une société de travaux publics.

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

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 vidéosurveillance peut être justifiée par :

- le respect d'une **obligation légale** à laquelle est soumis le responsable du traitement ou son représentant ;
- un motif d'**intérêt public** poursuivi par les organismes privés concessionnaires d'un service public ou investis d'une mission d'intérêt général ;
- la réalisation d'un **intérêt légitime** poursuivi par le responsable du traitement ou par un tiers, **à la condition de ne pas méconnaître l'intérêt ou les droits et libertés fondamentaux de la personne concernée**.

Cette dernière justification est la plus utilisée par les responsables de traitement qui considèrent souvent l'installation de caméras comme nécessaire pour se prémunir contre les risques de vol et d'agression.

L'APDP est alors très vigilante au respect des droits et libertés des personnes concernées, en vérifiant notamment que l'implantation des caméras n'empiète pas sur leur sphère privée.

L'installation d'un dispositif de vidéosurveillance peut dans certains cas être justifiée par le consentement des personnes. 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.

En conséquence, l'APDP demande à l'employeur de s'assurer que le dispositif de vidéosurveillance mis en œuvre :

- ne permet pas de **contrôler le travail ou le temps de travail** du personnel ;
- ne conduit pas un **contrôle permanent et inopportun** des personnes concernées.

C'est ainsi qu'elle considère que les caméras peuvent filmer :

- les entrées et sorties des bâtiments, en faisant attention toutefois à ne filmer que la surface strictement nécessaire ;
- les issues de secours et les voies de circulation ;
- les couloirs ;
- les lieux de stockage de marchandise ;
- les machines de production (uniquement machines) ;
- les locaux techniques ;
- les archives ;
- les lieux pouvant être considérés comme sensibles (ex : salles serveurs),
- le parking intérieur, extérieur et/ou souterrain à condition de ne pas filmer la voie publique;
- les zones de livraison ou de chargement, les quais de livraison et de déchargement.

L'APDP estime toutefois que l'installation de dispositif de vidéosurveillance est **strictement interdite** dans :

- les ateliers (production, montage/démontage…) où travaillent des employés (sauf justification particulère) ;
- les vestiaires, les cabinets d'aisance, les bains-douches, les toilettes;
- les bureaux ainsi que tous lieux privatifs mis à la disposition des salariés à des fins de détente ou de pause déjeuner ;
- les locaux syndicaux et leurs accès lorsque ceux-ci ne mènent qu'à ces seuls locaux.

Par ailleurs, elle rappelle que les caméras ne doivent pas filmer les employés sur leur poste de travail, sauf circonstances particulières dûment justifiées. Ainsi, une caméra pourra par exemple filmer un employé manipulant de l'argent à condition toutefois d'être orientée de manière à filmer davantage la caisse que ledit employé.

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 : image, visage et silhouette des personnes ;
- données d'identification électronique : logs de connexion des personnes habilitées à avoir accès aux images ;
- informations temporelles et horodatage : lieu et identification de la caméra, date et heure de la prise de vue

L'APDP considère que la **collecte de la voix** dans le cas de l'exploitation d'un traitement de vidéosurveillance apparaît manifestement excessive au regard de objectifs poursuivis par ce traitement.

En effet, la collecte de la voix en vue d'assurer la sécurité des biens et des personnes peut conduire à une surveillance pouvant être **inopportune** à l'égard des personnes concernées.

L'APDP sera donc **particulièrement vigilante à la justification** apportée par l'employeur.

Exemple : une caméra peut être autorisée dans un « *local d'interpellation* » en cas de vol et/ou d'infraction lorsqu'elle a pour but de protéger aussi bien les personnes interpellées que le personnel du magasin.

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

Conformément à l'article 84 de la Loi n° 1.565 du 3 décembre 2024, la conservation des images issues des systèmes de vidéosurveillance ne doit pas excéder **30 jours.**

Qui peut avoir accès aux données issues du dispositif de vidéosurveillance ?

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

Il peut ainsi s'agir en interne du directeur d'une boutique qui peut avoir accès en consultation en différé aux images en cas d'infraction, du personnel de l'accueil qui peut avoir accès aux images en consultation au fil de l'eau ou encore du prestataire qui a accès au traitement dans le cadre de la maintenance du dispositif.

Concernant ce dernier, l'APPD rappelle que ses droits d'accès doivent 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 Service des Ressources Humaines a accès aux images, l'APDP rappelle qu'un tel accès en consultation ne peut s'effectuer que dans le cadre d'une procédure disciplinaire en lien avec les objectifs du traitement, c'est-à-dire en cas d'atteinte à la sécurité des biens ou des personnes.

L'APDP estime par ailleurs que la communication des images 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 vidéosurveillance doit être porté à la connaissance des personnes concernées.

A cet égard, l'article 84 de la Loi précise que l'information du public de la présence d'un système de vidéosurveillance dans les **lieux ouverts au public** est réalisée par le responsable du traitement de façon **visible et permanente** au moyen d'un **panneau placé à l'extérieur des lieux concernés**.

Dans les lieux **non ouverts au public**, ce même article prévoit que l'information de la personne concernée est réalisée par le responsable du traitement de façon **visible et permanente** au moyen d'un **panneau placé à l'intérieur des lieux concernés ou par une information appropriée des personnes concernées.**

Le **panneau d'affichage** mentionné à l'article 84 doit comporter *a minima* :

- les finalités du traitement ;
- l'identité du responsable du traitement ;
- les informations relatives à l'exercice des droits de la personne concernée :
- la durée de conservation ;
- les coordonnés du délégué à la protection aux données personnelles s'il a été désigné ;
- un renvoi vers une information plus complète.

Les dispositifs de vidéosurveillance installés dans les **lieux ouverts au public** ou **filmant les abords de voies publiques, d'espaces ouverts au public ou à la circulation du public**, sont soumis à l'**autorisation préalable du Ministre d'Etat**.

Les dispositifs de vidéosurveillance installés dans les **lieux non ouverts au public** sont portés, sans délai, à la **connaissance de l'APDP.**

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 des caméras :

- Le serveur se trouve-t-il dans un local fermé, accessible uniquement aux personnes habilitées à y avoir accès ?
- Y' a-t-il des moniteurs ou PC déportés ? Où se situent-ils et quelle est leur utilité ? Sont-ils (moniteurs) à l'abri des regards du public ? Comment les PC sont-ils sécurisés (ex : session sécurisée, anti-virus, etc.) ?
- Y'a-t-il des logs de connexion (traçabilité) des personnels habilités à avoir accès aux images et au traitement ?
- Le serveur est-il protégé par un identifiant de connexion et mot de passe propres à chaque personne habilitée à y avoir accès ?
- Existe-t-il des accès distants (PC, tablettes, smartphones….) ? Si oui, ces accès sont-ils protégés par un identifiant de connexion et mot de passe propres à chaque utilisateur ? La connexion est-elle sécurisée (HTTPS, VPN, autres…) ?
- Quel est le nombre de caméras déployées?
- Les caméras sont-elles mobiles ? Possèdent-elles la fonction zoom ? Une fonctionnalité d'enregistrement sonore ?
- En cas d'extraction des données :
  - qui est en charge de l'extraction (par exemple, le prestataire) et quelle est sa procédure?
  - sur quel support se fait l'extraction (clé USB, CD…) ?
  - ce support est-il chiffré ? L'information est-elle chiffrée ?