Janvier 2025

La vidéosurveillance dans les immeubles d'habitation

Les immeubles d'habitation sont de plus en plus nombreux à se doter de systèmes de vidéosurveillance afin d'assurer la **sécurité** de leurs résidents.

Or, utilisés sans discernement, de tels systèmes peuvent conduire à une **surveillance abusive des habitudes de vie ou du comportement** des personnes concernées, portant ainsi atteinte à leur vie privée.

Dans quels buts un dispositif de vidéosurveillance peut-il être installé dans un immeuble d'habitation ?

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 la constitution de preuve en cas d'infraction.

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 **ne peut être justifiée que** par 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**.

L'installation de caméras doit être décidée par le propriétaire de l'immeuble ou doit faire l'objet d'un vote par l'assemblée générale des copropriétaires.

Les responsables du traitement mettent ainsi très souvent en avant la nécessité de se prémunir contre les risques de vol et d'agression.

L'APDP est toutefois 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.

Il arrive que les responsables du traitement mettent en place des caméras afin de lutter contre les risques de vandalisme ou de dégradation. A cet égard, l'APDP rappelle que les images issues des caméras ne peuvent être utilisées qu'en cas de **fait constitutif d'une infraction.**

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

Les personnes concernées par un dispositif de vidéosurveillance installé dans un immeuble d'habitation sont bien entendu les **résidents et leurs visiteurs** mais également le **personnel y travaillant** ainsi que **tout prestataire** pouvant intervenir dans ledit immeuble.

Compte tenu du caractère intrinsèquement intrusif des dispositifs de vidéosurveillance, l'APDP rappelle que ceux-ci :

- ne doivent pas conduire à une surveillance **permanente et inopportune** des résidents ou de leurs visiteurs ;
- ne doivent pas permettre de **contrôler le travail ou le temps de travail** du personnel ou des prestataires.

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

- les entrées et sorties de l'immeuble, en faisant attention toutefois à ne filmer que la surface strictement nécessaire ;
- les espaces communs (hall d'entrée, parking, local vélos ou poussettes, portes d'ascenseurs).

L'APDP estime en revanche que l'installation de dispositif de vidéosurveillance est **strictement interdite** :

- dans les couloirs d'accès aux appartements ;
- en direction des portes d'entrée des appartements ;
- à l'intérieur des ascenseurs ;
- au niveau des terrasses privatives ;
- au niveau d'une piscine ou d'une salle de sport ;
- dans les bureaux ou au niveau des postes de travail du personnel ;
- en direction des accès, fenêtres, cours et/ou terrasses d'un immeuble voisin.

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 des 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.

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.**

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 prévoit que dans les lieux **non ouverts au public**, 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 non ouverts au public** sont portés, sans délai, à la **connaissance de l'APDP.** Tel est le cas des immeubles d'habitation.

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**.

Pour les immeubles d'habitation, l'APDP considère que les images ne doivent pas être accessibles à l'ensemble des résidents et estime qu'en règle générale, seuls sont autorisés :

- le gestionnaire de l'immeuble ;
- le syndic ;
- le(s) gardien(s)/concierge(s).

Ces derniers sont souvent les seuls à avoir **une visualisation au fil de l'eau** ; les autres catégories de personnes n'ayant en général accès aux images qu'en différé en cas de problèmes.

Les écrans de visualisation au fil de l'eau doivent être situés **à l'abri des regards des personnes non habilitées** à avoir accès aux images. Par ailleurs, lorsque l'écran se situe dans la loge ou l'appartement du concierge, une **mise en veille des écrans** doit être effectuée de manière régulière et l'activation doit se faire par un **mot de passe réputé fort**.

L'APDP considère que le prestataire technique peut également avoir accès au dispositif dans le cadre de ses missions de maintenance. A cet égard, les 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.

Enfin, la communication des images à la Direction de la Sûreté Publique peut être justifiée pour les besoins d'une **enquête judiciaire**.

L'APDP rappelle toutefois qu'en cas de transmission, ladite Direction ne pourra avoir communication des informations que dans le strict cadre de ses missions légalement conférées.

Quelle sécurité mettre en place ?

L'APDP considère que le responsable de 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 personnes non autorisées 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 ? La fonctionnalité d'enregistrement sonore est-elle activée ?

- En cas d'extraction des données :

    - qui est en charge de l'extraction (par exemple, le prestataire) et quelle est la procédure?
    - sur quel support se fait l'extraction (clé USB, CD…) ?
    - ce support est-il chiffré ? L'information est-elle chiffrée ?