

Les dix commandements en matière de vidéosurveillance

Vous exploitez un restaurant, une boutique, vous dirigez une entreprise ou un Service Public, vous êtes copropriétaire et vous souhaitez utiliser un dispositif de vidéosurveillance

Voici ce que vous devez savoir !!!

Préalable

En vertu de l'article 83 de la Loi n° 1.565 du 3 décembre 2024, un système de vidéosurveillance est « *toute opération consistant en la captation, la transmission, l'enregistrement et l'exploitation d'images prises en tout lieu, qu'il soit public, ouvert au public ou privé, par une personne physique ou morale de droit privé ou une personne morale de droit public agissant en dehors de l'exercice de ses prérogatives de puissance publique* ».

1 – Des formalités tu effectueras

Si la Loi n° 1.565 du 3 décembre 2024 ne soumet plus les dispositifs de vidéosurveillance à l'autorisation préalable de l'APDP, elle demande néanmoins que certaines formalités soient effectuées par les responsables du traitement.

Ainsi, en vertu de l'article 85 de la Loi n° 1.565 du 3 décembre 2024, « *Les systèmes de vidéosurveillance installés dans des **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 systèmes installés dans les lieux **non ouverts au public** sont quant à eux portés, sans délai, à la connaissance de l'APDP.

Dans certains cas le responsable du traitement devra également effectuer une analyse d'impact notamment lorsque la surveillance s'exerce à grande échelle (centre commercial, ...).

Qu'entend-on par lieux ouverts au public et lieux non ouverts au public?

Conformément à l'exposé des motifs, il faut entendre par « *lieux ouverts au public* » les établissements tels qu'un restaurant, une galerie commerciale ou un guichet d'administration.

Les « *lieux non ouverts au public* » quant à eux sont par exemple un lieu privé (domicile, garage...) ou des locaux à usage professionnel tels que les bureaux ou les entrepôts.

S'agissant plus particulièrement des **domiciles**, ou tout autre lieu affecté à un usage personnel ou domestique, la déclaration auprès de l'APDP doit être effectuée **uniquement si des personnes extérieures au cercle familial ou amical interviennent au domicile** ex : gens de maison, aides à domicile.

2 – Une raison légitime tu trouveras

Conformément à l'article 4 de la Loi n° 1.565 du 3 décembre 2024, tout responsable du traitement doit s'assurer que les données à caractère personnel sont « *traitées de manière licite* ».

A cet effet, l'article 5 de la Loi prévoit que pour être licite, un traitement doit répondre à au moins une des 6 des exigences prévues par la Loi.

Le plus souvent, la mise en place d'un dispositif de vidéosurveillance sera justifiée par la réalisation d'un **intérêt légitime** poursuivi par le responsable du traitement.

Exemple : protéger sa boutique et les biens de valeur qu'elle contient contre les risques de vol ainsi que son personnel contre les risques d'agression

Le système de vidéosurveillance peut également être justifié par une **obligation légale** à laquelle est soumis le responsable du traitement ou par la **réalisation d'un but d'intérêt public** poursuivi par les organismes privés concessionnaires d'un service public ou investis d'une mission d'intérêt général.

Exemple : obligation dans le cahier des charges de mettre des caméras pour surveiller des installations sensibles



Le **consentement de la personne** concernée peut également être invoqué mais cette justification sera appréciée de manière très stricte par l'APDP, notamment en raison du lien de subordination découlant d'un contrat de travail conclu entre l'employeur et son employé, et devra être étayée et expliquée.

3 – Tes voisins tu n'espionneras pas

Compte tenu du caractère intrusif des dispositifs de vidéosurveillance, ceux-ci ne peuvent être mis en place que dans le cadre des fonctionnalités suivantes :

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

Toute autre fonctionnalité sera examinée de manière très attentive par l'Autorité.



L'APDP interdit que les systèmes de vidéosurveillance soient utilisés pour **contrôler le travail ou le temps de travail** du personnel et/ou conduisent à un **contrôle permanent et inopportun** des personnes concernées.

C'est ainsi qu'elle demande par exemples qu'aucune caméra ne soit installée :

- dans les vestiaires, les cabinets d'aisance, les bains-douches, les cabines d'essayage;
- dans les bureaux ainsi que les lieux privatifs mis à la disposition des salariés à des fins de détente ou de pause déjeuner ;
- dans les salles d'attentes ou salles de réunion ;
- dans les couloirs d'accès aux appartements ;
- en direction des tables des clients dans les salles de restauration.

4 – Les conversations d'autrui tu n'écouteras pas

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 elles 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.

En revanche, concernant la collecte de la voix dans le cas de l'exploitation d'un système de vidéosurveillance, l'APDP considère le plus souvent qu'une telle collecte est manifestement excessive au regard des fonctionnalités du traitement. En effet, la collecte de la voix en vue, par exemple, d'assurer la sécurité des biens et des personnes, peut conduire à une surveillance inopportune à l'égard des personnes concernées. L'Autorité sera donc particulièrement vigilante à la justification apportée par le responsable de traitement.

5 – Les personnes concernées tu informeras

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 coordonnées du délégué à la protection aux données personnelles s'il a été désigné ;
- un renvoi vers une information plus complète.



6 – Un droit d'accès tu donneras

Le droit d'accès est le droit pour toute personne concernée d'obtenir de l'entité ayant mis en place le système de vidéosurveillance la confirmation que des informations la concernant ont été collectées et la communication de ces informations sous une forme écrite, non codée et conforme au contenu des enregistrements.

L'entité est libre de choisir les modalités selon lesquelles les personnes concernées peuvent la contacter pour exercer leur droit d'accès (par voie postale, par courrier électronique, par téléphone, sur place...).

Lorsqu'une copie de l'enregistrement des caméras est fournie, les droits des tiers doivent être préservés (floutage...).

7 – Les accès internes tu délimiteras

Les images enregistrées **ne doivent pas être librement accessibles** à l'ensemble des employés ou des clients.

Le responsable du traitement doit ainsi s'assurer que n'ont accès aux images que les seules personnes autorisées, pour les **stricts besoins de l'accomplissement** de leurs missions.

Par ailleurs, pour chacune des catégories de personnes habilitées à avoir accès aux informations (direction, vendeurs, prestataire informatique...), l'entité doit déterminer avec précision les droits dont ces catégories disposent (consultation au fil de l'eau, consultation en différé, suppression des images, maintenance, tous droits...).

L'APDP apporte en effet une attention particulière aux catégories de personnes ayant accès aux informations.

Elle demande par ailleurs qu'une journalisation des accès aux enregistrements soit implémentée.

8 – Des mesures de sécurité tu prendras

Conformément à l'article 31 de la Loi n° 1.565 du 3 décembre 2024, les responsables du traitement doivent prendre des **mesures techniques et organisationnelles appropriées** afin de garantir un **niveau de sécurité adapté aux risques** pour les droits et libertés des personnes physiques.

Ces risques sont notamment :

- la destruction de données ;
- la perte de données ;
- l'altération de données ,
- la divulgation non autorisée de données ;
- l'accès non autorisé à des données personnelles.

Ces risques peuvent se produire de manière **accidentelle** ou **illicite**.

Par ailleurs, les différentes architectures de vidéosurveillance doivent reposer sur des serveurs, périphériques, équipements de raccordements (switchs, routeurs, pare-feux) qui doivent être protégés par un login et un mot de passe réputé fort, régulièrement renouvelé, et les ports non utilisés doivent être désactivés.

9 – Les communications et les accès distants tu protégeras

Les images issues des caméras sont susceptibles d'être communiquées à la Direction de la Sûreté Publique et aux Tribunaux monégasques pour les besoins d'une enquête judiciaire ou encore aux assureurs dans le cadre de l'instruction de dossiers d'indemnisation.

Il est donc important que la copie ou l'extraction d'informations issues de ce traitement soit chiffrée sur son support de réception (CD, clé USB...).

En outre, les accès distants, lorsque ceux-ci sont prévus, doivent être protégés. L'APDP demande ainsi que les équipements permettant de tels accès soient impérativement protégés par un **mot de passe réputé fort** ainsi que par des protocoles de type SSL (https, VPN, etc...).

Par ailleurs, elle demande qu'ils soient également paramétrés afin de se verrouiller automatiquement au-delà d'une courte période d'inactivité.

Enfin, en ce qui concerne plus particulièrement les « *smartphones* », tablettes et ordinateurs portables, l'APDP demande que l'accès à l'application permettant de visionner les images se fasse lui-aussi par le biais d'un **mot de passe réputé fort**.

10 – La durée de conservation tu limiteras

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'article 84 de la Loi prévoit que les images issues des systèmes de vidéosurveillance ne doit pas excéder **30 jours**.

En règle générale, conserver les images juste quelques jours suffit à effectuer les vérifications nécessaires en cas d'incident et permet d'enclencher d'éventuelles procédures pénales.