Mai 2026 — **www.courrierdesmaires.fr**

LE COURRIER DES MAIRES
et des élus locaux

La vidéoprotection

Principal actionnaire: Info Services Holding.
Société éditrice: Groupe Moniteur SAS au capital de 333900 euros.
Siège social: 20, rue des Aqueducs, 94250 Gentilly.
RCS: Nanterre 403080823.
Numéro de commission paritaire: 0425 T 86402.
ISSN: 1252-1574.
Président-directeur de la publication: Julien Elmaleh.

RÉFÉRENCES

- Loi n° 2023-380 du 19 mai 2023 relative aux Jeux olympiques et paralympiques de 2024 et portant diverses autres dispositions.
- Loi n° 2011-267 du 14 mars 2011 d'orientation et de programmation pour la performance de la sécurité intérieure (Loppsi 2).
- Loi n° 95-73 du 21 janvier 1995 d'orientation et de programmation relative à la sécurité (Loppsi).
- Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.
- Directive 95/46/CE du Parlement européen et du Conseil, du 24 octobre 1995, relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.
- Code de procédure pénale (CPP)
- Code de la sécurité intérieure (CSI)

RESSOURCES

- Vidéoverbaliser les infractions routières : oui, mais pas n'importe comment !, article du Courrier des maires, septembre 2025,
courrierdesmaires.fr/article.59155
- Intelligence artificielle et vidéosurveillance : entre controverses et défis juridiques, article du Courrier des maires, octobre 2024,
courrierdesmaires.fr/article.58206
- Vidéosurveillance « intelligente » sur domaine public cherche financements… et éthique, article du Courrier des maires, avril 2023,
courrierdesmaires.fr/article.54421
- Les ressources de la Cnil
cnil.fr/fr/la-videoprotection
- Vidéoprotection : qui peut consulter les images ?
cnil.fr/fr/cnil-direct/question/videoprotectionvideosurveillance-qui-peut-consulter-les-images
- Mettre en place des dispositifs vidéos conformes,
cnil.fr/sites/default/files/2024-11/guide_rgpd_video_collectivites_territoriales.pdf
- Logement social et vidéosurveillance,
cnil.fr/sites/default/files/2025-11/logement_social-fiche11.pdf
- Les « caméras augmentées » dans l'espace public,
cnil.fr/fr/cameras-augmentees-espaces-publics
- Décisions de la Cnil sur l'utilisation de BriefCam et autres logiciels d'analyse vidéo par l'État et des communes,
cnil.fr/fr/utilisation-briefcam-logiciels-analyse-video-par-etat-communes-la-cnil-prononce-plusieurs-mises-en-demeure

LEXIQUE

CDV
Commission départementale de vidéoprotection.

OPJ
Officier de police judiciaire.

RGPD
Règlement général sur la protection des données.

La vidéoprotection

La vidéoprotection consiste à installer des caméras sur la voie publique et dans des lieux et établissements ouverts au public. Elle se distingue de la vidéosurveillance, qui concerne les lieux non ouverts au public.
La vidéoprotection a connu et connaît encore un essor important, témoignant de la sensibilité des autorités publiques et des individus à la préservation de l'ordre public et à la prévention des infractions. En tant qu'outil susceptible d'attenter aux libertés individuelles, en particulier au respect de la vie privée, elle fait l'objet d'un encadrement juridique strict, tant du point de vue du droit administratif que du droit des données personnelles.
Par ailleurs, le coût de l'installation, de l'exploitation et de l'entretien d'un dispositif de vidéoprotection pouvant s'avérer conséquent, notamment à l'échelle communale, la question de sa mutualisation entre autorités publiques revêt un enjeu particulier. Le législateur a, ces dernières années, fait évoluer le cadre applicable et les outils juridiques à disposition de l'administration. 50 questions-réponses pour actualiser ses connaissances sur la vidéoprotection.

Par Agathe Delescluse et David Conerardy,
avocats, cabinet Seban & associés

1

A quelles fins des systèmes de vidéoprotection peuvent-ils être mis en œuvre sur la voie publique ?

L'article L.251-2 du code de la sécurité intérieure (CSI) liste onze finalités : la protection des bâtiments et installations publics et de leurs abords ; la sauvegarde des installations utiles à la défense nationale ; la régulation des flux de transport ; la constatation des infractions aux règles de la circulation ; la prévention des atteintes à la sécurité des personnes et des biens dans des lieux particulièrement exposés à des risques d'agression, de vol ou de trafic de stupéfiants ainsi que la prévention, dans des zones particulièrement exposées, de certaines infractions douanières ; la prévention d'actes de terrorisme ; des risques naturels ou technologiques ; le secours aux personnes et la défense contre l'incendie ; la sécurité des installations accueillant du public dans les parcs d'attraction ; le respect de l'obligation d'être couvert, pour faire circuler un véhicule terrestre à moteur, par une assurance garantissant la responsabilité civile ; et la prévention et la constatation des infractions relatives à l'abandon de déchets ou d'autres objets.

2

Comment est appréciée l'exposition particulière à des risques d'agression, de vol ou de trafic de stupéfiants ?

De simples craintes de vols ou d'effractions, ou la commission ponctuelle de tels actes, ne suffisent pas à justifier l'implantation de caméras (TA Lyon, 12 juillet 2007, n° 0503476). Il convient en effet de démontrer, au vu des circonstances locales, l'utilité du dispositif et, ce faisant, la proportionnalité de l'atteinte à la vie privée qu'il engendre. Les données statistiques relatives aux atteintes aux personnes et aux biens, ainsi qu'aux infractions liées au trafic de stupéfiants, jouent un rôle important en la matière (TA Grenoble, 29 novembre 2024, n° 2101042 ; TA Rennes, 11 avril 2024, n° 2106360). À l'inverse, l'inefficacité de principe alléguée d'un dispositif de vidéoprotection pour prévenir la commission d'actes de délinquance, puis pour identifier et réprimer les auteurs d'infractions n'est pas prise en compte pour considérer qu'il y a lieu ou non de mettre en œuvre un tel système (par exemple : TA Rennes, 23 mars 2023, n° 200241).

3

Qu'est-ce que la vidéoverbalisation ?

La vidéoverbalisation consiste non seulement à constater, à distance, à l'aide d'un dispositif de vidéoprotection non automatisé (ce qui la distingue des radars de feu rouge ou de vitesse par exemple), une infraction, mais aussi à la sanctionner par l'établissement d'un procès-verbal par un agent verbalisateur. Elle concerne seulement des infractions commises à bord ou au moyen d'un véhicule dont la responsabilité pécuniaire incombe au titulaire du certificat d'immatriculation, en application des articles L.121-2 et L.121-3 du code de la route, par exception au principe de la responsabilité pénale du conducteur au titre des infractions commises à bord d'un véhicule (art. L.121-1 du même code). La vidéoverbalisation permet en effet de capturer l'image du véhicule afin d'en identifier la marque et la plaque d'immatriculation, ce qui permet de remonter jusqu'au titulaire de la carte grise, mais non d'identifier le conducteur dudit véhicule, qui peut ne pas en être le propriétaire.

4

Quelles infractions peuvent être vidéoverbalisées ?

Ce sont celles qui entrent dans le champ des deux finalités prévues par le CSI permettant de constater des infractions via un dispositif de vidéoprotection, à savoir les infractions aux règles de la circulation routière et celles relatives à l'abandon d'ordures, de déchets, de matériaux ou d'autres objets. En outre, seules les contraventions sont vidéoverbalisables, de sorte qu'est exclue la vidéoverbalisation des délits et des crimes.
Sont plus précisément concernées par la vidéoverbalisation les contraventions en matière de stationnement et d'acquittement des péages, certaines contraventions en matière de circulation (par exemple, usage du téléphone au volant, dépassement des vitesses maximales autorisées, non-respect des distances de sécurité entre véhicules) et les contraventions relatives à l'abandon d'ordures, de déchets, de matériaux ou d'autres objets commises au moyen d'un véhicule.

5

Qu'est-ce qu'une voie publique ?

La notion de voie publique ne fait pas l'objet d'une définition juridique précise. Il apparaît que le critère déterminant est celui de l'affectation à l'usage du public, et donc à la circulation générale. A contrario, le juge administratif a pu considérer qu'étaient dépourvues du caractère de voies publiques des places publiques non affectées à la circulation générale (CE, 22 avril 1960, Sieur Berthier, Lebon p. 264 ; CE, 21 mars 1984, commune de Barben c/ consorts Chaumard). On relèvera que des voies piétonnes sont des voies publiques (CE, 11 décembre 1985, ville d'Annecy ; CE, 3 juin 1994, commune de Coulommiers). La question de savoir si les voies privées ouvertes à la circulation générale pourraient être regardées comme des voies publiques au sens de l'article L.521-2 du CSI se pose.

6

Qui peut installer ces systèmes de vidéoprotection ?

Aux termes de l'article L.251-2 du CSI, les systèmes de vidéoprotection peuvent être mis en œuvre par « les autorités publiques compétentes ». Aucun texte ne liste néanmoins lesdites autorités. Celles-ci peuvent revêtir des formes juridiques variées puisque la compétence s'apprécie au regard de la finalité poursuivie. En somme, l'autorisation ne peut être délivrée qu'à une autorité publique qui détient la capacité d'agir pour le but poursuivi par le système de vidéoprotection, et seules peuvent se trouver dans le champ de captation les voies publiques où l'autorité publique exerce la compétence permettant le recours à la vidéoprotection. Il est ainsi possible que plusieurs autorités publiques soient compétentes, sur des fondements différents, pour l'installation, sur une même voie publique de systèmes de vidéoprotection.

7

Quelles sont les autorités publiques compétentes en matière de surveillance des voies publiques ?

La surveillance générale de la voie publique a été qualifiée par la jurisprudence, tant administrative que constitutionnelle, d'activité de police administrative (CE, 29 décembre 1997, commune d'Ostricourt, n° 170606 ; Cons. const. décision n° 2011-625 DC du 10 mars 2011, Loppsi 2). Et le Conseil constitutionnel a assimilé l'exploitation d'un système de vidéoprotection, et en particulier le visionnage des images, à une modalité d'exercice de la mission de surveillance de la voie publique (même décision du Conseil constitutionnel). De sorte que, en la matière, sont seules compétentes les autorités de police administrative, à savoir le maire, le président du conseil départemental et le préfet, l'importance de la compétence de chacune de ces autorités étant d'inégale importance. En effet, c'est principalement le maire qui est compétent, au titre de ses pouvoirs de police (art. L.2212-2 du CGCT), pour l'exploitation d'un dispositif de vidéoprotection destiné à assurer la surveillance des voies publiques de la commune.

8

La surveillance des voies publiques par un dispositif de vidéoprotection peut-elle être transférée ou déléguée ?

Non. Le principe selon lequel les pouvoirs de police ne se délèguent pas, ni ne s'exercent par voie contractuelle est affirmé de longue date et confirmé de manière constante par la jurisprudence (CE, 17 juin 1932, ville de Castelnaudary ; CE, 29 décembre 1997, commune d'Ostricourt, n° 170606 ; Cons. const. décision n° 2011-625 DC du 10 mars 2011, Loppsi 2). Ces exemples jurisprudentiels concernent des cas où la délégation était accordée à des personnes privées. Néanmoins, en l'absence d'habilitation légale, le même principe d'interdiction des délégations, ou des transferts, de pouvoirs de police au bénéfice de personnes publiques doit s'appliquer. A cet égard, l'article L.5211-9-2 du CGCT, qui traite des transferts de pouvoirs de police spéciale du maire dans le cadre intercommunal précise systématiquement que le transfert est réalisé « sans préjudice de l'article L.2212-2 du CGCT », c'est-à-dire que le maire demeure compétent, en tout état de cause, au titre de la police municipale, laquelle n'est pas transférée.

9

Peut-il y avoir une obligation d'installer un système de vidéoprotection pour une commune ?

Lors des débats parlementaires qui ont donné lieu à l'adoption de la Loppsi du 21 janvier 1995, le gouvernement a fait voter un amendement par lequel le préfet peut imposer à une commune de mettre en place un système de vidéoprotection aux fins de prévention des actes de terrorisme. Ce dispositif a fait l'objet d'une opposition marquée du Sénat, qui le considérait contraire au principe de libre administration des collectivités territoriales. Finalement, si le préfet ne peut contraindre une commune à installer un dispositif de vidéoprotection, l'article L. 223-8 du CSI prévoit qu'il peut lui demander de mettre en œuvre un tel système pour prévenir des actes terroristes. Dès lors, le conseil municipal a seulement l'obligation d'en délibérer dans les trois mois. De plus, le financement de l'installation et de la maintenance du système est négocié dans une convention conclue entre la commune et le préfet. Ainsi, la suggestion est encouragée par une participation financière de l'État.

10

L'installation d'un système de vidéoprotection nécessite-t-elle une autorisation préalable ?

Oui, elle est autorisée pour une durée de cinq ans renouvelable par arrêté préfectoral après avis de la commission départementale de vidéoprotection (CDV) (art. L.251-1 et L.252-4 du CSI). Cette commission entend, sur chaque demande, un représentant de la police nationale ou de la gendarmerie territorialement compétent ou un agent des douanes ou des services départementaux d'incendie et de secours (Sdis) ou un représentant de la police municipale concernée. Elle peut également demander à entendre le pétitionnaire ou solliciter tout complément d'information, et demander l'avis de toute personne qualifiée qui lui paraîtrait indispensable pour l'examen d'un dossier particulier (art. R.252-14 du CSI). Elle rend son avis dans un délai de trois mois. Le préfet dispose, au total, d'un délai de quatre mois pour se prononcer sur la demande. Son silence vaut, le cas échéant, décision de rejet (art. R.252-14 du CSI).

11

Que contient le dossier de demande d'autorisation ?

Le dossier administratif et technique de demande (art. R.252-3 du CSI) comprend un rapport de présentation, un plan de masse des lieux, un plan de détail indiquant le nombre et l'implantation des caméras, ainsi que les zones couvertes par celles-ci, la description du dispositif prévu pour la transmission, l'enregistrement et le traitement des images, la description des mesures de sécurité qui seront prises pour la sauvegarde et la protection des images éventuellement enregistrées, les modalités de l'information du public, le délai de conservation des images avec les justificatifs nécessaires, la désignation du responsable de la maintenance, les modalités du droit d'accès des personnes, la justification de la conformité du système de vidéoprotection aux normes techniques et, en cas de mise en œuvre d'un traitement de données à caractère personnel, l'engagement de conformité destiné à la Cnil. Si une analyse d'impact relative à la protection des données personnelles a été rédigée, elle est jointe au dossier et remplace les pièces avec lesquelles son contenu est redondant.

12

Que contient l'autorisation préfectorale ?

Au-delà de l'autorisation, l'arrêté préfectoral prescrit toutes les précautions utiles, en particulier quant à la qualité des personnes chargées de l'exploitation du système de vidéoprotection ou visionnant les images et aux mesures à prendre pour assurer le respect de la législation. Elle peut prescrire que les agents individuellement désignés et dûment habilités des services de police et de gendarmerie nationales, des douanes, des Sdis, des services de police municipale sont destinataires des images et enregistrements. Elle précise alors les modalités de transmission des images et d'accès aux enregistrements ainsi que la durée de conservation des images, dans la limite d'un mois à compter de cette transmission ou de cet accès, sans préjudice des nécessités de leur conservation pour les besoins d'une procédure pénale (art. L.252-2 et L.252-3 du CSI).

13

Les autorisations délivrées en matière de vidéoprotection sont-elles accessibles au public ?

Oui, l'autorisation est publiée au recueil des actes administratifs de la préfecture, sauf dérogation motivée par un impératif de défense nationale. Le préfet met à la disposition du public la liste des autorisations des systèmes de vidéoprotection publiées. Celle-ci précise pour chacun d'eux la date de son autorisation et le service ou la personne responsable. Il communique également la liste des systèmes de vidéoprotection autorisés sur le territoire de chaque commune au maire, qui la met à la disposition du public en mairie (art. R.252-16 du CSI).

14

Une autorisation peut-elle être délivrée en urgence ?

Oui, une autorisation provisoire de quatre mois maximum peut être délivrée aux autorités publiques compétentes dans l'hypothèse de la tenue imminente d'une manifestation ou d'un rassemblement de grande ampleur présentant des risques particuliers d'atteinte à la sécurité des personnes et des biens. Le président de la CDV est immédiatement informé de cette décision. Il peut alors la réunir sans délai afin qu'elle donne un avis sur la mise en œuvre de la procédure d'autorisation provisoire. L'autorisation d'installation du dispositif cesse d'être valable dès que la manifestation ou le rassemblement a pris fin. Sauf dans les cas où les manifestations ou rassemblements de grande ampleur ont déjà pris fin, le préfet recueille l'avis de la CDV sur la mise en œuvre du système de vidéoprotection et se prononce sur son maintien. La commission doit rendre son avis avant l'expiration du délai de validité de l'autorisation provisoire (art. L.252-6 du CSI). Une procédure similaire existe, en cas d'urgence et d'exposition particulière à un risque d'actes de terrorisme (art. L.223-4).

15

Les modalités d'un système de vidéoprotection autorisé peuvent-elles être modifiées ?

Le CSI n'envisage que la demande d'autorisation initiale et la procédure correspondante. Il n'est pas précisé si les modifications d'un système autorisé doivent conduire à une nouvelle demande ou à une demande de modification, ou si une simple déclaration desdites modifications suffit. Et aucune procédure spécifique n'est prévue. L'instruction du 20 mars 2024, relative à la mise en conformité du régime de la vidéoprotection avec le droit européen relatif à la protection des données, indique que les modifications doivent être portées à la connaissance du préfet, lequel évalue la nécessité de délivrer une nouvelle autorisation. Elle différencie néanmoins les cas où une nouvelle autorisation est, en tout état de cause, nécessaire (par exemple en cas de modification des finalités du système) et ceux dans lesquels le préfet dispose d'un pouvoir d'appréciation.

16

Quels agents et élus peuvent visionner les images issues des dispositifs de vidéoprotection de leur commune ?

S'agissant des agents, ce sont tout d'abord les agents de police municipale qui sont habilités à visionner les images, dans les limites de leurs missions fixées à l'article L.511-1 du CSI. En outre, le CSI autorise le visionnage des images par des agents agréés par le préfet, dès lors que ce visionnage ne nécessite pas de leur part d'actes de police judiciaire (art. L.132-14-1), c'est-à-dire des actes tendant à constater les infractions, à en rassembler les preuves et à en rechercher les auteurs (c'est par exemple le cas en matière de vidéoverbalisation, laquelle consiste à constater une infraction). S'agissant des élus, le maire est une autorité de police administrative générale (art. L.2212-2 du CGCT) et un officier de police judiciaire (art. 16 du CPP). Il est donc habilité à visionner les images prises sur le territoire communal. Les adjoints au maire titulaires d'une délégation d'attribution en matière de police municipale le peuvent aussi, sans accomplir aucun acte de police judiciaire. Les autres conseillers municipaux ne peuvent y avoir accès.

17

Gendarmerie et police nationales peuvent-elles accéder aux images de vidéoprotection communales ?

Deux fondements législatifs le permettent. L'article 60-1 du code de procédure pénale permet au procureur de la République ou à un officier de police judiciaire (OPJ) de requérir de toute personne, de tout établissement ou organisme privé ou public ou de toute administration publique susceptibles de détenir des informations intéressant une enquête, de lui remettre ces informations. Celles-ci peuvent résulter d'un système de vidéoprotection. D'autre part, l'autorisation préfectorale d'installation d'un système de vidéoprotection peut prescrire que les agents individuellement désignés et dûment habilités des services de police et de gendarmerie nationales sont destinataires des images et enregistrements. Cette faculté prévue par l'article L.253-3 du CSI ne saurait priver un OPJ des pouvoirs qu'il tient de l'article 60-1 du CPP (Crim. 9 janvier 2018, n° 17-82.946). En revanche, elle permet aux agents identifiés dans l'autorisation d'accéder aux images sans réquisition (Crim., 21 novembre 2023, n° 23-81.591).

18

Le respect de l'autorisation préfectorale peut-il être contrôlé ?

Oui. La CDV peut à tout moment exercer, sauf en matière de défense nationale, un contrôle sur les conditions de fonctionnement des systèmes de vidéoprotection. Pour cela, les membres de la commission peuvent, après information du procureur de la République, accéder aux lieux, locaux, enceintes, installations ou établissements servant à la mise en œuvre du système de vidéoprotection. Ils peuvent également demander communication de tous documents nécessaires, accéder aux programmes informatiques et aux données ainsi qu'en demander la transcription, et recueillir, sur place ou sur convocation, tout renseignement et toute justification utiles. Des experts désignés par l'autorité dont ceux-ci dépendent peuvent les assister, à la demande du président de la commission. Un procès-verbal contradictoire est dressé à l'issue des vérifications et visites ainsi menées. Toute personne intéressée peut saisir la commission de toute difficulté tenant au fonctionnement d'un système de vidéoprotection (art. L.253-1 et suivants du CSI).

19

Qui constitue la commission départementale de vidéoprotection ?

La CDV comprend quatre membres : un magistrat honoraire ou, à défaut, une personnalité qualifiée à raison de sa compétence dans le domaine de la vidéoprotection ou des libertés individuelles désigné par le premier président de la cour d'appel, président de la commission ; un maire, désigné par la ou les associations départementales des maires ; un représentant désigné par la ou les chambres de commerce et d'industrie territorialement compétentes et une personnalité qualifiée choisie en raison de sa compétence par l'autorité préfectorale (article L.251-4 et R.525-8 du CSI).

20

Quelles sont les conséquences administratives en cas d'irrégularité ?

La CDV émet, le cas échéant, des recommandations et propose la suspension ou la suppression des dispositifs non autorisés, non conformes à leur autorisation ou dont il est fait un usage anormal. Elle peut également proposer au préfet la suspension ou le retrait de l'autorisation d'installation. Dans cette hypothèse, l'intéressé doit avoir été mis à même de présenter, au préalable, ses observations.
Par ailleurs, le fait pour une autorité publique compétente d'installer et d'exploiter un système de vidéoprotection dans des conditions irrégulières constitue une faute de nature à engager sa responsabilité à l'égard des personnes dont l'image et/ou le domicile ont été filmés, en raison de l'atteinte portée à leur vie privée (par exemple : CAA Lyon, 25 août 2020, n° 18LY02616).

21

Peut-il y avoir des conséquences pénales ?

Oui. Si la loi du 19 mai 2023 relative aux Jeux olympiques et paralympiques de 2024 a allégé l'arsenal des sanctions pénales prévues par le CSI en matière de systèmes de vidéoprotection, puisque seule l'entrave à l'action de la CDV a été maintenue à l'article L.254-1, les autres infractions, comme le fait d'installer ou de maintenir un système de vidéoprotection non autorisé, de procéder à des enregistrements de vidéoprotection sans autorisation, de ne pas les détruire dans le délai prévu, de les falsifier, de faire accéder des personnes non habilitées aux images ou d'utiliser ces images à d'autres fins que celles pour lesquelles elles sont autorisées, qui ont été supprimées du CSI, demeurent réprimées par les articles L.226-16 et suivants du code pénal. Sont ainsi incriminés le fait de mettre en œuvre un traitement sans respecter les formalités préalables (art. 226-16), de ne pas détruire les données dans les délais prévus (art. 226-20), de détourner ces informations de leur finalité (art. 226-21) et, sous certaines conditions, de permettre à des tiers d'y avoir accès (art.226-22).

22

Les agents qui ne respecteraient pas l'autorisation préfectorale encourent-ils un risque personnel ?

Oui. Ils peuvent être sanctionnés pénalement et disciplinairement. Ainsi, un agent de police municipale a été condamné pour divulgation d'images de vidéoprotection à une personne non habilitée, en l'espèce des proches souhaitant récupérer la vidéo d'un mariage (Cass. crim., 12 novembre 2014, n° 13-81.071). Un autre agent a déjà été sanctionné pour s'être introduit sans autorisation dans le centre de vidéoprotection urbain d'une commune aux fins d'y visualiser des images à partir desquelles il avait dressé des procès-verbaux d'infraction aux règles de stationnement, alors que le système de vidéoprotection n'avait été autorisé qu'aux seules fins d'assurer la sécurité des personnes, la prévention des atteintes aux biens, la protection des bâtiments et la régulation du trafic routier. La sanction d'exclusion de ses fonctions pour une durée de six mois dont deux avec sursis a été jugée comme proportionnée par le juge administratif (CAA Bordeaux, 7 mars 2019, n° 17BX00743).

23

Les images de vidéoprotection constituent-elles des données à caractère personnel ?

Oui. La Cour de justice de l'Union européenne a rendu une décision le 11 décembre 2014 soumettant l'ensemble des systèmes de vidéoprotection aux dispositions de la directive du 24 octobre 1995 (l'ancêtre du RGPD), puisque ce système de surveillance comprenait bien des données à caractère personnel, qu'elles étaient bien identifiantes et qu'il y avait bien une activité de traitement. Il est indifférent que le responsable du traitement cherche ou non à identifier la personne concernée. Il suffit que cette identification soit objectivement possible pour que la qualification de donnée à caractère personnel soit retenue. Cette conception extensive de l'identifiabilité est constante, tant en jurisprudence qu'en doctrine administrative, afin de garantir une protection effective des personnes filmées. En conséquence, les traitements de vidéoprotection relèvent du champ d'application du règlement général sur la protection des données et de la loi « informatique et libertés ».

24

Quel régime juridique s'applique à la vidéoprotection lorsque des données personnelles sont enregistrées ?

Lorsque des dispositifs de vidéoprotection enregistrent des images permettant l'identification de personnes physiques, le régime juridique applicable repose sur une articulation entre le code de la sécurité intérieure et le droit des données personnelles. Le CSI constitue le cadre juridique principal lorsque les caméras filment la voie publique ou des lieux ouverts au public assimilés. Il encadre strictement les finalités autorisées, les conditions d'implantation des dispositifs, les procédures d'autorisation préfectorale et les durées maximales de conservation des images. Toutefois, ce régime spécifique ne se substitue pas au RGPD ni à la loi « informatique et libertés ». Il en résulte un régime juridique combiné, dans lequel le CSI fixe les conditions matérielles et finalités du recours à la vidéoprotection, tandis que le RGPD impose un socle commun d'obligations protectrices des droits et libertés des personnes filmées.

25

Qui est responsable de traitement pour un dispositif communal ?

Pour un dispositif mis en œuvre à l'échelle communale, la qualité de responsable de traitement revient à la collectivité locale qui l'exploite. En effet, c'est la commune qui détermine, sous réserve de validation par le préfet, les finalités poursuivies par la vidéoprotection, les moyens techniques utilisés, les conditions d'accès aux images ainsi que les durées de conservation. À ce titre, elle assume l'ensemble des obligations résultant du droit des données personnelles. Toutefois, la mise en place et l'exploitation de la vidéoprotection communale aux fins de surveillance générale de la voie publique s'inscrivent dans l'exercice des pouvoirs de police administrative générale. Le maire intervient donc en cette qualité, en application de ses compétences propres en matière de police municipale. Cette distinction présente un intérêt pratique, notamment en matière de gouvernance des traitements et de contentieux. Les demandes d'exercice de droits, les obligations d'information, la tenue du registre des activités de traitement ou encore la mise en œuvre des mesures de sécurité relèvent bien de la collectivité, représentée par le maire.

26

La désignation d'un délégué à la protection des données est-elle obligatoire ?

Oui, dès lors que le traitement est mis en œuvre par une autorité ou un organisme publics. Cette obligation résulte de l'article 37 du RGPD, qui impose la désignation d'un DPO indépendamment de la nature ou du volume des traitements réalisés. Une commune mettant en œuvre un dispositif de vidéoprotection entre ainsi nécessairement dans le champ de cette exigence. La finalité sécuritaire du dispositif ou son encadrement spécifique par le CSI est, à cet égard, indifférente. Dès lors que des données à caractère personnel sont traitées par une collectivité territoriale dans l'exercice de ses missions, la désignation d'un DPO constitue une obligation légale impérative. Cette obligation vise à garantir un niveau élevé de protection des droits et libertés des personnes concernées, en assurant une expertise interne ou externalisée en matière de conformité. Elle est rappelée de manière constante par la Cnil, qui souligne que la vidéoprotection ne saurait justifier aucune dérogation à cette exigence structurelle du RGPD.

27

Quelles sont les obligations en matière d'information du public ?

Les dispositifs de vidéoprotection impliquant le traitement de données à caractère personnel sont soumis à une obligation renforcée d'information du public. Cette information doit être délivrée de manière claire, visible et préalable à l'entrée dans le champ de la caméra, afin de permettre aux personnes concernées d'anticiper la captation de leur image. Un affichage placé après la zone filmée ou insuffisamment apparent ne saurait satisfaire aux exigences légales. D'expérience, les panneaux se situent à proximité immédiate des caméras et à l'entrée des villes. L'information doit mentionner l'identité du responsable de traitement, les finalités poursuivies par le dispositif, l'existence des droits reconnus aux personnes concernées ainsi que les modalités d'exercice de ces droits, notamment un point de contact effectif. Ces mentions constituent le socle minimal permettant d'assurer la transparence du traitement, conformément aux articles 12 et 13 du RGPD. La Cnil fournit de nombreux exemples de panneaux sur lesquels se fonder (voir la rubrique « Ressources »).

28

Les personnes filmées disposent-elles d'un droit d'accès aux images ?

Oui, dès lors que ces images constituent des données à caractère personnel. Ce droit s'exerce dans la limite tenant à la protection des droits des tiers et aux impératifs de sécurité publique (voir la rubrique « Ressources »). Lorsque les images comportent d'autres personnes identifiables, l'accès ne peut être accordé que si des mesures de protection appropriées sont mises en œuvre, notamment par le floutage ou l'occultation des tiers. À défaut, la communication des images peut être légalement refusée afin d'éviter une atteinte disproportionnée aux droits et libertés d'autrui. L'exercice du droit d'accès s'effectue auprès de la collectivité responsable du traitement, généralement par l'intermédiaire des services municipaux compétents.

29

Quelle est la durée maximale de conservation des images ?

Conformément à l'article L.252-3 du CSI, les images ne peuvent être conservées au-delà d'un délai maximal d'un mois. Ce plafond constitue une durée maximale légale et non une durée de principe : le responsable du traitement doit retenir une durée plus courte chaque fois que cela est possible, au regard des finalités effectivement poursuivies. Ce principe de limitation de la conservation rejoint les exigences de l'article 5, paragraphe 1, e), du RGPD, selon lequel les données à caractère personnel doivent être conservées pendant une durée n'excédant pas celle nécessaire à la réalisation des finalités du traitement. La conservation systématique des images jusqu'au terme d'un mois, sans justification opérationnelle, est ainsi susceptible de caractériser un manquement. Des modalités distinctes s'appliquent lorsque les images sont extraites pour les besoins d'une procédure judiciaire, administrative ou disciplinaire. Dans ce cas, les images peuvent être conservées au-delà du délai d'un mois, mais uniquement pour la durée strictement nécessaire à la procédure concernée, dans un environnement sécurisé et avec des accès limités.

30

Ce délai est-il impératif ?

Oui. Toutefois, ce plafond légal ne constitue pas une durée de référence automatique. Dans ce cadre, la Cnil rappelle, notamment dans son pack relatif au logement social de novembre 2025, que quelques jours suffisent dans la majorité des situations pour effectuer les vérifications nécessaires en cas d'incident. La durée de conservation ne saurait être déterminée en fonction des seules capacités techniques de stockage, mais exclusivement au regard des objectifs poursuivis par le traitement. En l'absence de réquisition judiciaire, des aménagements sont toutefois possibles. La Cnil rappelle que lorsqu'un responsable de traitement est informé du dépôt d'une plainte, il peut inviter la personne concernée à exercer son droit à la limitation du traitement, afin d'empêcher l'effacement automatique des images dans le délai d'un mois. Cette conservation ciblée permet de préserver les données en vue d'une éventuelle réquisition ultérieure, sans remettre en cause le caractère impératif du plafond légal.

31

L'existence d'un dispositif de vidéoprotection doit-elle être inscrite au registre des traitements ?

Obligatoirement. Cette obligation résulte de l'article 30 du RGPD. Le registre doit retracer de manière précise les finalités poursuivies (définies à l'art. L.251-2 du CSI), la base juridique du traitement, les catégories de données traitées, les personnes habilitées à accéder aux images, les durées de conservation prévues à l'article L.252-3 du même code, ainsi que les mesures de sécurité mises en œuvre conformément à l'article 32 du RGPD. Il constitue un outil central de démonstration de la conformité et de la responsabilité du responsable de traitement, au sens de l'article 5, paragraphe 2, du RGPD. Ce registre doit en outre être tenu à jour, afin de refléter toute évolution du dispositif, notamment en cas de modification des finalités, du périmètre des caméras ou des modalités d'accès aux images. Cette exigence est régulièrement rappelée par la Cnil, qui considère l'inscription et l'actualisation du traitement comme un préalable indispensable à la licéité de la vidéoprotection.

32

Quand mener une analyse d'impact relative à la protection des données ?

La réalisation d'une analyse d'impact relative à la protection des données (AIPD) est requise lorsqu'un dispositif de vidéoprotection est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées. Tel est le cas, en application de l'article 35 du RGPD, lorsque le traitement repose sur une surveillance systématique d'une zone accessible au public, ce qui correspond, par nature, à de nombreux dispositifs installés sur la voie publique ou dans des espaces ouverts au public. Au-delà de ce cas typique, la Cnil rappelle qu'une AIPD est également requise lorsque le traitement remplit au moins deux des neuf critères issus des lignes directrices du G29/CEPD (la structure regroupant toutes les Cnil européennes). Parmi ces critères figurent notamment l'ampleur du traitement (dont le nombre de personnes concernées) et l'usage innovant d'une technologie. L'AIPD doit être conduite avant la mise en service, afin d'apprécier la nécessité et la proportionnalité du dispositif, d'identifier les risques et de définir les mesures permettant de les réduire à un niveau acceptable.

33

Quelles mesures de sécurité appliquer pour protéger les images ?

Les images issues d'un dispositif de vidéoprotection doivent faire l'objet de mesures de sécurité techniques et organisationnelles renforcées, conformément à l'article 32 du RGPD. Ces mesures visent à garantir la confidentialité, l'intégrité et la disponibilité des images, compte tenu de leur sensibilité et des risques particuliers d'atteinte à la vie privée. L'accès aux images doit être strictement limité aux seules personnes habilitées. Ces accès doivent être tracés par des journaux de connexion permettant d'identifier les consultations, extractions ou suppressions d'images. Un cloisonnement des accès est requis afin de distinguer les fonctions de visualisation, d'administration et d'exportation. Les images doivent être protégées contre toute copie libre ou extraction non autorisée. La sécurité repose également sur la protection physique des équipements, les serveurs et postes de consultation devant être installés dans des locaux sécurisés et à accès restreint. La Cnil insiste, dans son guide de sécurité des données personnelles de 2024, sur la nécessité d'une approche globale combinant mesures techniques, organisationnelles et humaines.

34

Quel est le régime applicable au recours à un sous-traitant technique ?

Conformément à l'article 28 du RGPD, tout prestataire intervenant pour le compte de la collectivité, notamment pour l'installation, la maintenance ou l'hébergement du système, doit être lié par un contrat ou un acte juridique définissant précisément l'objet, la durée, la nature et les finalités du traitement, ainsi que les obligations du sous-traitant en matière de sécurité et de confidentialité. Ce contrat doit garantir que le sous-traitant n'agit que sur instruction documentée du responsable de traitement et qu'il met en œuvre des mesures techniques et organisationnelles appropriées pour protéger les images. En particulier, aucun accès direct aux images ne peut être accordé au prestataire sans encadrement strict. Les interventions doivent être ponctuelles, tracées et réalisées sous supervision, afin d'éviter tout accès autonome ou détourné aux données. La collectivité demeure pleinement responsable du traitement et doit assurer une supervision effective des prestations réalisées, notamment par des mécanismes de traçabilité.

35

La reconnaissance faciale peut-elle être intégrée dans un dispositif de vidéoprotection ?

Non, pas à ce jour. Elle constitue un traitement de données biométriques au sens du RGPD, c'est-à-dire des données à caractère personnel issues de caractéristiques physiques, physiologiques ou comportementales permettant l'identification unique d'une personne. Or, ces traitements sont, par principe, interdits par le RGPD et la loi « informatique et libertés », sauf exceptions strictement encadrées, qui ne trouvent pas à s'appliquer en matière de vidéoprotection. Cette qualification emporte des conséquences juridiques déterminantes. Les dispositifs de reconnaissance faciale relèvent d'un régime d'interdiction de principe, régulièrement rappelé par la Cnil, et ils ne peuvent pas être déployés dans le cadre de la vidéoprotection communale.

36

Les caméras « augmentées » peuvent-elles être intégrées dans un dispositif de vidéoprotection ?

Les caméras dites « augmentées » peuvent, sous conditions strictes, être intégrées dans un dispositif de vidéoprotection. Ces dispositifs reposent sur des technologies de vision par ordinateur ajoutant une surcouche logicielle permettant l'analyse automatisée des images, notamment la reconnaissance d'objets, de silhouettes, de mouvements ou d'événements, sans procéder à l'identification des personnes filmées. Ces traitements algorithmiques peuvent être déployés à partir de caméras existantes ou au moyen d'équipements dédiés. Sur le plan juridique, les caméras « augmentées » ne relèvent pas, par principe, du régime des traitements biométriques interdits, dès lors qu'elles n'impliquent pas des données issues de l'article 9 du RGPD. Elles demeurent toutefois pleinement soumises au RGPD et au CSI lorsqu'elles s'inscrivent dans un dispositif de vidéoprotection, impliquant une analyse rigoureuse de leur nécessité et de leur proportionnalité, en plus de réaliser une AIPD.

37

Les caméras « augmentées » peuvent-elles permettre de réaliser des statistiques ?

Oui, sous certaines conditions strictes. Un usage consistant à mesurer la fréquentation d'une zone ou à différencier les usages de l'espace public, par exemple entre piétons, véhicules, vélos et trottinettes, est en principe autorisé dès lors qu'il ne conduit pas à l'identification des personnes filmées et qu'il repose sur des données agrégées (voir nos « Ressources »). Les algorithmes utilisés doivent être configurés de manière à exclure toute reconnaissance individuelle et à produire uniquement des résultats statistiques anonymes. Une obligation renforcée d'information du public s'impose dans ce contexte. Les usagers doivent être clairement informés de l'existence du dispositif, de ses finalités statistiques et des modalités générales du traitement.

38

Peuvent-elles permettre la détection automatisée d'infractions présumées sur le domaine public ?

Non, pas en l'état du droit positif. Les usages consistant à identifier automatiquement des comportements ou des situations qualifiées d'irrégulières, tels que le stationnement interdit, la circulation à contre-sens, les dépôts sauvages de déchets ou certains regroupements de personnes considérés comme « anormaux », soulèvent des risques élevés d'atteinte aux droits et libertés fondamentaux. De tels dispositifs reposent sur une analyse algorithmique en temps réel de l'espace public, susceptible d'entraîner une surveillance généralisée et continue des personnes. Cette logique excède les finalités légalement admises de la vidéoprotection, et se heurte aux principes de nécessité et de proportionnalité posés par le RGPD. Elle est également susceptible d'induire des biais, des erreurs d'interprétation ou des décisions automatisées indirectes affectant les personnes filmées. Ces usages sont donc, par principe, interdits en l'absence de base légale spécifique les autorisant expressément.

39

Peuvent-elles permettre l'utilisation des fonctionnalités de recherche automatique dans les images pour répondre à des réquisitions judiciaires ?

Oui, mais dans certains cas seulement. Cet usage est licite s'il est strictement nécessaire pour exécuter la réquisition, qu'il demeure limité au périmètre de celle-ci, et que le système présente un niveau de sécurité élevé, conformément à l'article 32 du RGPD. Il peut notamment s'agir de rechercher un élément objectif, tel qu'un numéro de plaque d'immatriculation, afin d'identifier des séquences pertinentes à transmettre à l'autorité requérante.
En revanche, la recherche automatisée ne peut pas être utilisée à l'initiative des agents de police municipale à des fins d'enquête. La Cnil rappelle que ceux-ci ne sont pas habilités à de telles recherches en dehors d'une réquisition. L'accès doit être nominatif, journalisé, cloisonné, et toute extraction doit rester strictement encadrée, sans constitution de bases parallèles ou de copies libres.

40

Quelles obligations s'imposent en cas de violation de données ?

En cas de violation de données à caractère personnel – fuite, divulgation non autorisée ou accès illégitime à des images de vidéoprotection –, le responsable du traitement est soumis à des obligations strictes prévues par le RGPD. Conformément à son article 33, toute violation susceptible d'engendrer un risque pour les droits et libertés des personnes concernées doit être notifiée à l'autorité de contrôle dans un délai maximal de 72 heures après en avoir pris connaissance. Lorsque la violation est susceptible d'entraîner un risque élevé pour les personnes concernées, notamment en cas de diffusion d'images permettant leur identification, l'article 34 du RGPD impose également une information directe des personnes concernées. Cette information peut toutefois être écartée si des mesures techniques appropriées, telles que le chiffrement, rendent les données inintelligibles pour tout tiers non autorisé. Par ailleurs, l'article 33, paragraphe 5, du RGPD, impose au responsable du traitement de documenter toute violation, y compris ses effets et les mesures correctrices prises. Cette documentation participe de l'obligation de responsabilité (art. 5, paragraphe 2).

41

L'extraction d'images dans le cadre d'une procédure judiciaire fait-elle l'objet d'un traitement distinct ?

Oui, dans le cadre d'une procédure judiciaire, l'extraction d'images constitue un traitement distinct du traitement initial de captation et de conservation puisqu'elle poursuit une finalité autonome, à savoir l'exploitation probatoire desdites images aux fins de constatation des infractions, de poursuite de leurs auteurs ou de défense des droits en justice. Ce traitement repose sur une base juridique propre, résultant d'une réquisition judiciaire ou d'une décision de l'autorité compétente, dans le cadre des pouvoirs conférés à la police judiciaire. Les images extraites sortent alors du circuit de conservation ordinaire et font l'objet d'une conservation spécifique, strictement limitée aux besoins de la procédure. Cette conservation probatoire est encadrée par les exigences de nécessité et de proportionnalité prévues à l'article 5 du RGPD. Le responsable du traitement doit assurer une traçabilité renforcée des extractions, limiter les accès aux seules personnes habilitées et garantir la sécurité des supports de conservation.

42

Comment sont encadrées les opérations de maintenance lorsque le prestataire accède aux images ?

Conformément aux principes de sécurité et de minimisation posés par l'article 32 du RGPD, l'accès aux images doit demeurer exceptionnel, limité aux seules interventions strictement nécessaires à la maintenance du système. Ces accès doivent être réalisés sous la supervision effective de la collectivité responsable du traitement, afin d'exclure toute consultation autonome ou injustifiée. Chaque intervention doit faire l'objet d'une journalisation précise, permettant d'identifier la date, la durée, la nature de l'opération réalisée et les images éventuellement consultées. Cette traçabilité constitue une garantie essentielle en cas de contrôle ou de contentieux. Le prestataire ne peut procéder à aucune copie, extraction ou conservation des images, que ce soit sur des supports internes ou externes. Toute opération de maintenance doit s'effectuer sans stockage des données et dans des conditions garantissant leur confidentialité.

43

La visualisation de zones privées est-elle admissible lorsqu'elle est incidente ou involontaire ?

Non. L'article L.251-3 du CSI prohibe expressément la captation d'images à l'intérieur des immeubles d'habitation et, plus largement, de tout lieu relevant de la vie privée. En conséquence, le responsable du traitement doit mettre en œuvre des mesures préventives effectives, au premier rang desquelles figure le masquage permanent et irréversible des zones privées susceptibles d'entrer dans le champ de la caméra. Un masquage a posteriori ou ponctuel ne saurait être regardé comme conforme, dès lors que la captation elle-même demeure possible. En cas de visualisation accidentelle constatée, une correction immédiate du dispositif s'impose, accompagnée, le cas échéant, d'une analyse des risques et de mesures correctrices appropriées. La persistance d'une captation incidente caractérise un manquement aux exigences de proportionnalité et de minimisation prévues par le RGPD.

44

Le dispositif doit-il faire l'objet de réévaluations régulières au regard du RGPD ?

Oui. Cette obligation découle du principe de responsabilité posé à l'article 5, paragraphe 2, du RGPD, lequel impose au responsable de traitement de démontrer, dans la durée, la conformité de ses traitements aux principes de licéité, de nécessité et de proportionnalité. La réévaluation doit porter sur la persistance des finalités poursuivies, la pertinence des emplacements des caméras, l'adéquation des durées de conservation, ainsi que le périmètre des habilitations accordées aux agents. Elle permet de vérifier que le dispositif demeure strictement nécessaire au regard des risques identifiés et qu'il n'emporte pas d'atteinte excessive aux droits des personnes filmées. Cette analyse peut s'appuyer sur les retours d'incidents, les évolutions du contexte local ou les conclusions d'une analyse d'impact. Lorsque les risques diminuent ou disparaissent, le responsable de traitement est tenu de réduire le périmètre de la vidéoprotection, en désactivant certaines caméras ou en raccourcissant les durées de conservation.

45

Quels sont les recours des personnes s'estimant surveillées de manière disproportionnée ?

Il existe plusieurs voies de recours. En premier lieu, elles peuvent saisir les services de la collectivité afin de solliciter des explications sur le dispositif, d'en contester la proportionnalité ou de demander sa modification. Cette démarche peut notamment porter sur l'emplacement des caméras, leur orientation ou l'étendue du périmètre filmé. En parallèle, les personnes concernées peuvent déposer une plainte auprès de la Cnil, qui dispose de pouvoirs d'enquête et de contrôle sur les traitements de données à caractère personnel. La Cnil peut, le cas échéant, mettre en demeure la collectivité, prononcer des mesures correctrices ou constater un manquement aux principes du RGPD. Enfin, un recours contentieux peut être introduit devant le tribunal administratif, notamment par voie de référé, lorsqu'une atteinte grave et manifestement illégale à la vie privée est alléguée. En situation d'urgence, le juge administratif peut ordonner la suspension ou la modification du dispositif litigieux.

46

Un centre de supervision urbain peut-il faire l'objet d'une mutualisation ?

Oui. Le dispositif général de l'équipement collectif, prévu par le CGCT (article L.1311-5), est tout d'abord mobilisable. Il suppose qu'une commune, propriétaire du centre de supervision urbain (CSU), donne accès à cet équipement à d'autres communes, moyennant une participation financière aux frais de fonctionnement de l'équipement. Un dispositif de mutualisation spécifique à la vidéoprotection est ensuite prévu par le CSI (art. L.132-14). Il permet à un EPCI compétent en matière de dispositifs locaux de prévention de la délinquance (DLPD), à un syndicat mixte fermé (SMF) composé exclusivement de communes et d'EPCI compétents en matière de DLPD, et à un syndicat mixte ouvert restreint (Smor) composé exclusivement de communes et d'EPCI compétents en matière de DLPD et d'un ou deux départements limitrophes, et présidé par le maire d'une des communes ou le président d'un des EPCI, de décider, sous réserve de l'accord de la commune d'implantation, d'acquérir, d'installer et d'entretenir des dispositifs de vidéoprotection, au premier rang desquels, un CSU.

47

Comment la mutualisation d'un CSU dans le cadre d'un équipement collectif est-elle organisée ?

La mutualisation est organisée au sein d'une convention. Le montant de la participation financière est calculé par référence aux frais de fonctionnement de l'équipement et les modalités de calcul de cette participation sont définies au sein de la convention passée entre le propriétaire et les entités publiques utilisatrices. Ce dispositif est néanmoins limité au seul CSU. Il ne peut concerner les autres éléments d'un système de vidéoprotection comme les caméras, qui ne font pas l'objet d'une utilisation collective puisqu'elles sont placées sur le territoire de chaque commune. Il ne peut davantage concerner les agents, dont la mutualisation n'est pas envisagée par le texte. Ainsi, chaque commune devra envoyer son propre agent pour visualiser les images issues des caméras placées sur son territoire, sauf à créer, en parallèle, une police pluricommunale, sur le fondement de l'article L.512-1 ou L.512-1-2 du CSI.

48

Sur quoi porte la mutualisation prévue par le code de la sécurité intérieure ?

La mutualisation sur le fondement du CSI porte sur la partie « technique » du dispositif de vidéoprotection, à savoir l'acquisition, l'installation et l'entretien du dispositif. Elle ne se réduit pas au seul CSU. Elle porte en effet, plus largement, sur des « dispositifs de vidéoprotection », lesquels incluent le CSU (à tout le moins un moniteur pour visualiser les images), mais aussi les caméras, le matériel de raccordement au CSU, etc. Elle peut également inclure la mise à disposition de personnel pour visionner les images, activité qui relève, elle, de la partie « exploitation » du dispositif de vidéoprotection. Il s'agira soit d'agents de police municipale, soit d'agents agréés par le préfet, ces derniers ne pouvant néanmoins visionner les images que dans la mesure où cela ne nécessite pas de leur part d'actes de police judiciaire (voir question 47). Dans ce cas, pendant le visionnage des images prises sur le territoire d'une commune, ces agents sont placés sous l'autorité exclusive du maire de cette commune. En effet, le visionnage est une modalité d'exercice du pouvoir de police administrative, seul détenu par le maire.

49

Comment est organisée cette mutualisation ?

La mutualisation est de nature conventionnelle. Ainsi, une convention conclue entre l'EPCI ou le syndicat mixte et chacun de ses membres concernés fixe les modalités d'acquisition, d'installation, d'entretien et de mise à disposition des dispositifs de vidéoprotection et les modalités de mise à disposition du personnel chargé du visionnage. Dans ce cadre, il conviendra de fixer les conditions financières de la mutualisation en tenant compte de l'ensemble des charges financières induites pour l'EPCI ou le syndicat mixte (investissement et fonctionnement, dont charges de personnels). L'intervention de l'EPCI ou du syndicat mixte ne suppose donc pas un transfert de compétence en la matière, lequel serait, en tout état de cause, impossible, s'agissant à tout le moins du volet exploitation du dispositif de vidéoprotection, en raison du caractère intransférable du pouvoir de police municipale du maire. Pour être complet, l'article L.132-14 du CSI prévoit enfin qu'une convention est conclue entre l'EPCI ou le syndicat mixte et l'Etat pour définir les modalités d'intervention des forces de sécurité de l'Etat.

50

Faut-il une autorisation préfectorale lorsqu'un équipement est mutualisé ?

Non. La personne publique propriétaire de l'équipement mutualisé n'a pas à obtenir d'autorisation préfectorale pour procéder à une mutualisation. Celle-ci est le fruit d'un accord des parties à la convention de mutualisation, quel qu'en soit le fondement juridique (équipement collectif du CGCT ou mutualisation spécifique en matière de vidéoprotection prévue par le CSI).
En revanche, chaque commune bénéficiaire de la mutualisation doit obtenir, à titre individuel, une autorisation préfectorale pour installer et exploiter un dispositif de vidéoprotection sur son territoire. Dans ce cadre, elle précisera, dans son dossier de demande, qu'elle a recours à une mutualisation plus ou moins étendue de son dispositif. A cet égard, rappelons que ledit dossier comprend la description du dispositif prévu pour la transmission, l'enregistrement et le traitement des images, ou encore la désignation du responsable de la maintenance s'il s'agit d'une personne ou d'un service différent de la personne ou du service responsable du système.

LE COURRIER DES MAIRES
et des élus locaux

Retrouvez tous les outils et contenus pour répondre inspirer et accompagner la mise en place des politiques publiques

Accès au logement, lutte contre les déserts médicaux, urbanisme commercial à réinventer, impérative transition énergétique, relance de l'industrie, accueil de la petite enfance, défis du maire employeur...
Le **magazine**, en version papier & numérique : Des dossiers de fonds et reportages pour aller au cœur des grandes problématiques d'actualité

ELECTIONS MUNICIPALES 2026 - Une couverture complète de la campagne électorale de l'avant-campagne, aux premiers mois de mandat
Un espace 100"% réservé aux municipales 2026 sur le site, une newsletter spéciale, des suppléments et numéros dédiés, des webinaires pour **une préparation optimale, une expertise juridique et réglementaire et une vision 360° des enjeux locaux :** couverture complète de l'écosystème électoral

Défis locaux décryptés, actualité du secteur public local scrutée par nos experts, quotidien des maires et projets innovants des élus...
Le site avec l'**accès direct** aux sujets majeurs et aux **indicateurs clés locaux** et **nationaux OpenData.** Un accès aux meilleures pratiques et **retours d'expériences** des élus pour inspirer votre réflexion autour de vos actions et identifier des **opportunités de financements** pour vos projets locaux.

Un accès aux indicateurs clés locaux et nationaux OpenData
Pour prendre des décisions éclairées, planifier efficacement et optimiser la gestion des ressources locales

Le statut de l'élu, la protection sociale des agents, la cybersécurité, la compétence eau et assainissement, les fonds européens, la prévention des risques naturels...
Le rendez-vous mensuel **50 questions/réponses** - 100% digital avec un mode de lecture dynamique.

Abonnez-vous au média de référence des élus locaux

LE COURRIER DES MAIRES et des élus locaux — BULLETIN D'ABONNEMENT **à renvoyer accompagné de votre règlement à :**
Le Courrier des maires et des élus locaux - Abonnement - 20, rue des Aqueducs - 94250 Gentilly

❍ **Oui, je souhaite m'abonner au Courrier des maires et des élus locaux.**

❍ **1 an au tarif professionnel** pour **329 €TTC***

❍ **1 an au tarif personnel** pour **229 €TTC***
(Servi à l'adresse personnelle et réglé par moyen personnel)

Je choisis mon mode de paiement :
❍ Virement à réception de facture
❍ Chèque bancaire à l'ordre du Courrier des Maires et des élus locaux

*TVA : 2,10% - offre réservée aux nouveaux abonnés en France métropolitaine, valable jusqu'au 31/12/2026. Tarifs DOM-TOM et étranger, nous consulter. Votre abonnement comprend durant cette période la réception de 6 n°. Conformément à la loi Informatique et liberté du 06/01/1978 et LCEN du 22/06/2004, vous disposez d'un droit d'accès et de rectification des données que vous avez transmises, en adressant un courrier au COURRIER DES MAIRES. GROUPE MONITEUR - S.A.S. au capital de 333 900 € - R.C.S. Créteil B 403.080.823 - N° TVA Intracommunautaire : FR 32 403 080 823. Toute commande implique l'acceptation des CGV consultables à : http://boutique.lagazette.fr/cgv. Pour consulter les règles RGPD du groupe : https://www.infopro-digital.com/rgpd-gdpr/

Mes coordonnées : Z60165PAG

❍ Mme ❍ M. Nom : .....

Prénom : .....

Établissement / Collectivité : .....

Service / Fonction : .....

Adresse : .....

Code Postal : |_|_|_|_|_| Ville : .....

E-mail : .....@.....

NOMINATIF ET EN MAJUSCULES – INDISPENSABLE pour ouvrir vos accès web

Tél. : |_|_|_|_|_|_|_|_|_|_| Fax : |_|_|_|_|_|_|_|_|_|_|

Siret : |_|_|_|_|_|_|_|_|_|_|_|_|_| Code Naf : |_|_|_|_|_|