


Surveillance vidéo sur le territoire communal : Quelles sont les règles ?


Règles applicables	Caméras de surveillance sur le territoire communal	
<p>Personne responsable : représentant légal de la collectivité (Maire, Président.e, Directeur.rice établissement public)</p> <p>Nature de la responsabilité : responsable d'un traitement automatisé de données à caractère personnel (séquences vidéo, images)</p> <p>Afin de mettre leur système de surveillance en conformité avec la réglementation en vigueur il est recommandé aux représentants légaux des collectivités et établissements d'associer au projet le responsable sécurité des systèmes d'information (RSSI), le délégué à la protection des données (DPD) et le relai RGPD qu'il aura désigné.</p> <p>Il est rappelé que HGI-ATD mutualise à titre gratuit une prestation de DPD sur désignation expresse des collectivités adhérentes (renseignements auprès de : accueil@atd31.fr).</p> <p>Les agents de la collectivité sont informés de la procédure de gestion du dispositif et de leur rôle (liste intervenants dans le traitement des images, habilitation d'accès aux images, exercice des droits des personnes).</p>		
	Projet Vidéoprotection	Projet vidéosurveillance
Identifier le type de dispositif	<u>Réservé aux seules autorités publiques</u> dont les mairies, à certaines conditions régies par le code de la sécurité intérieure : L. 251-2.	
Déterminer le motif d'installation des caméras	<p style="text-align: center;">Surveiller Voie publique / Lieu ouvert au public</p> <p>Pour assurer :</p> <ul style="list-style-type: none"> - <u>la protection des bâtiments et installations publics et de leurs abords</u> ; - 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 <u>sécurité des personnes et des biens</u> dans des <u>lieux particulièrement exposés à des risques d'agression, de vol ou de trafic de stupéfiants (...)</u> ; - la prévention d'actes de <u>terrorisme</u> ; - la prévention 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. <p><i>Par extension</i></p> <ul style="list-style-type: none"> - la prévention de l'abandon d'ordures, de déchets, de matériaux ou d'autres objets. 	<p style="text-align: center;">Surveiller Lieu privé, lieu non ouvert au public</p> <p>Pour assurer :</p> <p>Sécurité des biens et des personnes, à titre dissuasif et préventif ou pour identifier les auteurs de vols, de dégradations ou d'agression.</p>
Déterminer le fondement légal sur lequel repose le dispositif de surveillance	<p style="text-align: center;">Intérêt légitime de la personne responsable</p> <p>De façon générale, pour pouvoir être mis en œuvre, un traitement de surveillance vidéo doit être nécessaire à la poursuite d'intérêts légitimes de la collectivité qui traite les données, dans le strict respect des droits et intérêts des personnes soumises à la surveillance (RGPD, art. 6.1, f).</p> <p>L'autorité publique qui souhaite mettre en œuvre un dispositif de surveillance doit opérer une pondération entre son intérêt et les « intérêts ou libertés et droits fondamentaux des personnes » et doit également intégrer les « attentes raisonnables » de ces personnes.</p> <p>La sécurisation des biens et des personnes peut être obtenue par la mise en œuvre de moyens moins intrusifs que l'installation de caméras. L'utilisation de caméras doit rester limitée et constituer un moyen complémentaire à d'autres mesures de sécurité. Seules des circonstances exceptionnelles (établissements scolaires victimes d'actes de malveillance fréquents et répétés) justifient de filmer les élèves et les enseignants en continu.</p> <p>La CNIL recommande aux chefs d'établissements scolaires concernés d'adopter une « charte d'utilisation de la vidéosurveillance » en impliquant l'ensemble des acteurs (administration, personnel, représentants des parents d'élèves).</p> <p>Dans une école maternelle ou élémentaire, <u>c'est le maire qui décide</u>, ou non, d'installer des caméras.</p>	
Formalités		
<input checked="" type="checkbox"/> Demander une autorisation d'installation des caméras à la préfecture du lieu d'implantation du système En pratique :	Oui	Non
	<p>Définir les conditions de mise en œuvre du dispositif.</p> <p>Validité : 5 ans.</p> <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Déclarer la mise en service après autorisation <input checked="" type="checkbox"/> Assurer la traçabilité des informations obligatoires concernant les enregistrements réalisés, la date de 	

Surveillance vidéo sur le territoire communal : Quelles sont les règles ?

<p>Retirer le formulaire sur place : préfecture du département</p> <p>ou télécharger / remplir en ligne sur le site web du ministère de l'Intérieur :</p> <p>https://www.televideoprotection.interieur.gouv.fr</p>	<p>destruction des images, la date de leur extraction, du visionnage et le cas échéant de la transmission au parquet (art. R.252-11 CSI).</p> <p>NB : L'autorisation préfectorale n'est pas requise pour la mise en œuvre de dispositifs ne permettant pas d'identifier des personnes physiques directement ou indirectement, tels que : faible qualité de l'image, limitation du champ de vision des caméras ; utilisation d'une technique de masquage / floutage des images figurant des personnes ou des véhicules immatriculés.</p>	
<p><input checked="" type="checkbox"/> Demander une autorisation CNIL¹</p>	<p>Non</p>	<p>Si mise en place d'un système biométrique (reconnaissance faciale)</p>
<p><input checked="" type="checkbox"/> Documenter la conformité légale du projet</p>  <p style="text-align: center;">REGISTRE</p>	<p>Inscrire et documenter le dispositif de surveillance au registre des opérations de traitement de données de la collectivité dans les conditions de l'article 30 du RGPD.</p> <p>> Démontrer que le dispositif est mis en œuvre dans le respect de la réglementation applicable.</p>	
<ul style="list-style-type: none"> ▪ Délimiter zones de surveillance, définir emplacement et orientation caméras en fonction du but assigné au dispositif 	<p>Analyser la situation au cas par cas afin de vérifier la <u>nécessité</u> et la <u>proportionnalité</u> d'installer un dispositif de surveillance vidéo, notamment au regard de critères tels que la nature du lieu à placer sous surveillance, sa situation, sa configuration ou sa fréquentation.</p> <p>Le principe de minimisation des données en matière de surveillance vidéo implique qu'il ne doit être filmé que ce qui apparaît strictement nécessaire pour atteindre le but poursuivi.</p> <p>cf. dossier autorisation préfectorale</p> <p>Permet de vérifier la pertinence de l'installation du système dans la zone géographique ciblée.</p> <div style="border: 1px solid blue; padding: 5px; margin: 10px 0;"> <p style="text-align: center; color: blue;">BONNE PRATIQUE 👍</p> <p style="font-size: small;">Les caméras installées sur la voie publique ne doivent pas permettre de visualiser l'intérieur des immeubles d'habitation ni, de façon spécifique, leurs entrées. Des procédés de masquage irréversible de ces zones doivent être mis en œuvre et il est nécessaire de régulièrement contrôler leur bon fonctionnement.</p> <p style="text-align: right; font-size: x-small;">CNIL</p> </div>	<p><u>Précautions à prendre :</u></p> <p>Les établissements publics, les entreprises ne peuvent filmer que les abords immédiats de leurs bâtiments et installations (entrée, sortie, issues de secours, voies de circulation, façade extérieure par exemples <u>mais pas la rue</u>) dans les lieux susceptibles d'être exposés à des actes de terrorisme.</p> <p>Un particulier ne peut filmer que l'intérieur de sa propriété. Il n'est jamais autorisé à filmer la voie publique (même pour assurer la sécurité de son véhicule garé devant son domicile par exemple).</p> <p><u>Lieu de travail / Interdiction de surveiller</u> Espace travail agents ; zones de pause (vue générale) ; toilettes ; locaux syndicaux.</p> <p><u>Établissement scolaire :</u> interdiction de surveiller les élèves, de filmer les lieux de vie pendant les heures d'ouverture : cour de récréation, préau, salle de classe, cantine, foyer, etc.</p>
<ul style="list-style-type: none"> ▪ Informer les personnes filmées <i>ou susceptibles de l'être</i>, des conditions dans lesquelles leur image est traitée 	<p>Sur le lieu de travail / Obligation d'information préalable des instances représentatives du personnel</p> <p>Par voie d'affichage : format, nombre et localisation, adaptés à la situation des lieux et établissements (article R.253-3).</p> <p>Garantir une information claire et permanente (cf. modèles ci-dessous)</p> <div style="display: flex; justify-content: space-around; align-items: flex-start;"> <div style="border: 1px solid green; border-radius: 15px; padding: 10px; width: 45%;"> <p style="text-align: center; font-size: x-small;">VILLE PLACÉE SOUS VIDÉOPROTECTION pour la sécurité des personnes et des biens</p> <p style="font-size: x-small;">Pour toute information sur ce dispositif et/ou l'exercice de vos droits notamment accéder aux images qui vous concernent, contacter la mairie :</p> <p style="font-size: x-small;">- Délégué à la protection des données : dpd@nom-mairie.fr (en précisant le contexte et la nature de la demande) ;</p> <p style="font-size: x-small;">- Secrétariat : accueil@nom-mairie.fr / Tél. : 05 XX XX XX XX</p> <p style="font-size: x-small;">Les images sont conservées un mois et sont accessibles uniquement aux personnes strictement habilitées par le maire. En savoir plus : Consulter le site internet de la commune, rubrique « Politique de protection des données ».</p> <p style="font-size: x-small;">En cas de litige persistant, vous avez la faculté de saisir l'autorité de contrôle CNIL sur le site www.cnil.fr/plaintes.</p> </div> <div style="border: 1px solid green; border-radius: 15px; padding: 10px; width: 45%;"> <p style="text-align: center; font-size: x-small;">ETABLISSEMENT PLACÉ SOUS SURVEILLANCE VIDÉO pour la sécurité des personnes et des biens</p> <p style="font-size: x-small;">Pour toute information sur ce dispositif et/ou l'exercice de vos droits notamment accéder aux images qui vous concernent, contacter (indiquer le nom de l'établissement) :</p> <p style="font-size: x-small;">- Délégué à la protection des données : dpd@nom-etablissement.fr (en précisant le contexte et la nature de la demande) ;</p> <p style="font-size: x-small;">- Secrétariat : accueil@nom-etablissement.fr / Tél. : 05 XX XX XX XX</p> <p style="font-size: x-small;">Les images sont conservées un mois et sont accessibles uniquement aux personnes strictement habilitées par le maire. En savoir plus : Consulter le site internet de l'établissement, rubrique « Politique de protection des données ».</p> <p style="font-size: x-small;">En cas de litige persistant, vous avez la faculté de saisir l'autorité de contrôle CNIL sur le site www.cnil.fr/plaintes.</p> </div> </div>	


¹ CNIL : Commission nationale de l'informatique et des libertés.

Surveillance vidéo sur le territoire communal : Quelles sont les règles ?

	 <p>L'information sur le dispositif de surveillance peut être complétée sur un site internet et/ou intranet selon le public visé ; le contrat de travail.</p>	
<ul style="list-style-type: none"> ▪ Respecter les droits des personnes filmées 	<ul style="list-style-type: none"> <input checked="" type="checkbox"/> Permettre l'exercice des droits / Mettre en place une procédure Droit de visionner les enregistrements sous réserve du respect des droits des tiers qui peut nécessiter le masquage, floutage d'une partie des images. <input checked="" type="checkbox"/> Répondre dans le délai d'un mois / Tracer la demande au registre / Consulter le DPD 	
<ul style="list-style-type: none"> ▪ Conserver les images pour une durée limitée 	<p>La durée de conservation des images ne peut excéder un mois (art. L.252-3 du CSI). La collectivité veillera au respect de cette <u>durée limitée de conservation des images</u> précisée dans l'arrêté préfectoral d'autorisation.</p>	<p>En règle générale, conserver les images quelques jours suffisent pour effectuer des vérifications nécessaires en cas d'incident, et enclencher d'éventuelles procédures. Si une procédure est engagée, les images sont extraites du dispositif (après consignation de cette opération dans un cahier spécifique) et conservées pour la durée de la procédure.</p>
<ul style="list-style-type: none"> ▪ Sécuriser le dispositif / Risque atteinte vie privée 	<p>Garantir un niveau de <u>sécurité</u> adapté aux risques évalués d'atteinte à la vie privée des personnes surveillées.</p> <p>Le visionnage des images ne peut être opéré que par les personnes spécifiquement et individuellement habilitées (par exemple : les agents du centre de supervision urbain d'une commune). Ces personnes doivent être particulièrement formées et sensibilisées aux règles de mise en œuvre du dispositif envisagé.</p> <p>Paramétrage des fonctionnalités techniques telles que : politique d'habilitation, limitation des extractions, purge des images dans le délai légal, transmission chiffrée, <i>floutage</i> des images...</p> <p>Sécuriser l'accès aux images à distance (via internet depuis son mobile par exemple)</p>	
<ul style="list-style-type: none"> <input checked="" type="checkbox"/> Formaliser une analyse d'impact relative à la protection des données (AIPD)² afin de vérifier la conformité légale 	<p>La mise en œuvre d'un dispositif de vidéoprotection conduit à « la surveillance systématique à grande échelle d'une zone accessible au public », type de traitements expressément mentionné à l'article 35.1 du RGPD comme susceptible de présenter « un risque élevé pour les droits et libertés des personnes physiques », une AIPD doit être effectuée (cf. site CNIL, Ce qu'il faut savoir sur l'analyse d'impact relative à la protection des données (AIPD)).</p> <p>Par ce biais, une évaluation de la nécessité et de la proportionnalité du dispositif envisagé, au regard des finalités poursuivies, est opérée avant son implantation.</p> <p>Pour en savoir plus : L'analyse d'impact relative à la protection des données (AIPD)</p>	<p>Vérifier avec RSSI et DPD si nécessaire.</p> <p>L'AIPD doit être réalisée si :</p> <ul style="list-style-type: none"> <input checked="" type="checkbox"/> Surveillance systématique à grande échelle <input checked="" type="checkbox"/> Surveillance personnes vulnérables (salariés, enfants)
<ul style="list-style-type: none"> <input checked="" type="checkbox"/> Contractualiser la sous-traitance <p>Un prestataire doit toujours garantir la mise en œuvre de mesures techniques et organisationnelles</p>	<p><u>Risques du recours à un prestataire externe pour déployer et administrer un parc de caméras</u></p> <p>Cette pratique est notamment susceptible d'entraîner la duplication de l'ensemble des flux des caméras en dehors du système d'information de la collectivité, voire en dehors du territoire national. La couverture de ces risques, lorsque le recours à une externalisation du service s'avère nécessaire, passe par le respect de bonnes pratiques organisationnelles et contractuelles, selon la démarche décrite dans le guide ANSSI/ « Maîtriser les risques de l'infogérance - externalisation</p>	

² L'AIPD est un outil qui permet de construire un traitement conforme au RGPD et respectueux de la vie privée, lorsqu'un traitement de données personnelles est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées.

Surveillance vidéo sur le territoire communal : Quelles sont les règles ?

<p>appropriées pour respecter les règles applicables.</p>	<p>des systèmes d'information ».</p> <p>Si la collectivité recourt aux services d'un prestataire (société de gardiennage par exemple) pour traiter les l'information résultant de la vidéosurveillance, un contrat de sous-traitance répondant aux critères de l'article 28 du RGPD doit être mis en place (cf. Guide du sous-traitant CNIL).</p>
<p>Non respect des règles / Risques encourus</p> 	<p>Installer ou maintenir un système de vidéoprotection sans autorisation, procéder à des enregistrements non conformes aux règles applicables (ne pas les détruire dans le délai prévu, les falsifier, entraver l'action de la commission départementale de vidéoprotection ou de la CNIL, faire accéder des personnes non habilitées aux images ou utiliser ces images à d'autres fins que celles pour lesquelles elles sont autorisées est puni de trois ans d'emprisonnement et de 45 000 euros d'amende, sans préjudice des dispositions de l'article 226-1 du Code pénal et du Code du travail.</p> <p>Les investigations de la CNIL peuvent porter sur l'existence et la validité de l'autorisation préfectorale ou le respect des règles de protection des données lors de la mise en œuvre dispositif de surveillance (finalité, caractère proportionné, modalités d'information et respect des droits des personnes filmées, qualité des personnels autorisés à visionner les images, mesures permettant d'assurer la sécurité du traitement, durée de conservation des images).</p> <p>Si manquements constatés : La CNIL peut adresser à la collectivité concernée une mise en demeure de mettre en conformité le dispositif avec les règles applicables.</p> <p>Si manquement grave ou persistant, la CNIL peut appliquer les sanctions prévues par les textes (rappel à l'ordre, limitation temporaire ou définitive du traitement, sanction pécuniaire, etc.).</p>
<p>Mises en demeure CNIL <u>Vidéosurveillance excessive en milieu scolaire</u> 2018 : 25 plaintes déposées auprès de la CNIL</p>	<p>En l'absence de circonstance particulière propre aux établissements concernés par les plaintes, la CNIL les a mis en demeure de modifier leur dispositif : Réorienter, retirer ou déplacer les caméras pour ne filmer que les accès et les espaces de circulation ou de les paramétrer pour qu'elles ne fonctionnent qu'en dehors des heures d'ouverture de l'établissement et non en continu.</p>

En savoir plus : site CNIL [videosurveillance-vidéoprotection](#)