MINISTÈRE
DE LA CULTURE
Liberté
Égalité
Fraternité

Direction générale des patrimoines et de l'architecture

Mise en ligne : juillet 2022

SÛRETÉ – VOL – MALVEILLANCE n°4

VIDÉOPROTECTION / VIDÉOSURVEILLANCE

Cette fiche a pour objet d'exposer les recommandations élémentaires à mettre en œuvre pour assurer la sécurisation des établissements culturels et cultuels, de leurs abords et des biens à protéger.

La **vidéoprotection** ou la **vidéosurveillance** est devenue un des **éléments, fondamentaux et incontournables, de la protection électronique d'un site**. Elle vient ainsi renforcer la protection mécanique et les moyens humains.

Un système vidéo permet de prévenir les atteintes à la sécurité des personnes et des biens (agression, vol, dégradation, actes de terrorisme, etc.) par la visualisation, en direct ou en différé, d'images de zones définies. Il peut constituer une aide à la surveillance, un moyen de contrôle d'accès, un moyen de détecter l'intrusion d'individus et le déplacement d'objets, un outil de levée de doute à distance en cas d'alarme, mais également une aide à l'enquête après la survenance d'un évènement.

La conception d'un système vidéo passe par une **étude préalable des risques et des besoins,** puis par l'établissement d'un cahier des charges fonctionnel. Le choix des matériels devra être adapté aux besoins et aux moyens mis à disposition pour les exploiter et traiter les informations qui en découlent (images, alarmes, etc.).

L'amélioration constante des techniques, de la qualité des images, fournies par les caméras, et des logiciels nécessite d'être particulièrement vigilant sur l'usage qui sera fait des images (atteinte aux libertés publiques, droit à la vie privée, confidentialité, etc.). Il est donc nécessaire de respecter le cadre légal de l'implantation des caméras et de l'utilisation des images vidéo, en suivant les principes contenus dans le tableau ci-dessous :

Vidéoprotection	Vidéosurveillance
Lieux ou établissements ouverts au public et espaces publics (voie publique, espaces d'expositions, boutiques, salles de lecture, espaces d'entrée et de sortie du public, etc.).	Lieux privatifs, locaux à usage exclusivement professionnel, et espaces non accessibles au public (réserves, magasins d'archives, bureaux, locaux de travail, ateliers, etc.).
Relève du code de la sécurité intérieure (CSI) (articles L251-1 à L255-1 et R251-1 à R253-4).	Relève du code du travail et du respect de la vie privée (article 9 du code civil).
Autorisation du préfet territorialement compétent (à Paris le Préfet de police) délivrée pour une durée de 5 ans renouvelable, après avis de la commission départementale de vidéoprotection (formulaire téléchargeable ou à remplir en ligne).	Avis des instances représentatives du personnel (information et consultation).

Vidéoprotection	Vidéosurveillance
Se conformer aux formalités liées au RGPD et à la loi « Informatique et Libertés » (soumis au contrôle de la CNIL). Une analyse d'impact sur la protection des données (AIPD) peut être demandée. Associer le Délégué à la protection des données (DPO).	
Information obligatoire, en permanence et de façon visible, des personnes (employés et visiteurs) de la présence d'un dispositif vidéo dans les lieux concernés (affiches ou panonceaux ; information du public sur le site internet). Pour la vidéoprotection, l'information doit a minima comporter un pictogramme représentant une caméra, les finalités du traitement installé, la durée de conservation des images, le nom ou la qualité et le numéro de téléphone du responsable du traitement et du délégué à la protection des données (DPO), l'existence de droits « Informatique et libertés » et le droit d'introduire une réclamation auprès de la Commission nationale de l'informatique et des libertés (CNIL), en précisant ses coordonnées.	
Maximum légal d'enregistrement des images = 1 mois	
Les caméras orientées sur la voie publique ne doivent pas visualiser l'intérieur des immeubles d'habitation ni, de façon spécifique, l'entrée des immeubles.	

DIAGNOSTIC

Le diagnostic doit répondre aux questions suivantes :

- quelles sont les spécificités de mon établissement et quelles sont les menaces auxquelles il est exposé ?
- quels sont les objectifs et finalités que je souhaite assigner au système vidéo : dissuader, détecter et empêcher les vols et la malveillance, contrôler les accès, etc. ?
- quelles sont les zones à surveiller (zones publiques, zones techniques, réserves, extérieurs) ?
- quels seront l'usage des caméras et des moyens associés (surveillance 24h/24 ou simple enregistrement, nombre et compétence des agents de surveillance nécessaires, etc.)
- quel sera le lieu d'implantation des matériels choisis (choix du matériel à adapter) ?

L'expertise des conseillers de la MISSA est fortement recommandée pour aider à l'analyse des besoins et évaluer la pertinence du dispositif mis en place.

LES MATÉRIELS

Le choix technique doit tenir compte du coût de la mise en œuvre technique, du coût organisationnel (affectation de tâches nouvelles, personnels professionnels), du coût de la maintenance et de la fiabilité du matériel du système sur le long terme.

Trois niveaux de définition et de résolution des images sont définis par le ministère de l'Intérieur : détection, reconnaissance et identification d'un visage (arrêté du 3 août 2007 portant définition des normes techniques des systèmes de vidéosurveillance).

Il est préconisé, dans les établissements culturels, d'être dotés de **caméras de haute résolution, en couleur et fonctionnant en mode jour/nuit, permettant d'assurer, *a minima*, la reconnaissance des individus** et des objets.

Le dispositif devra répondre aux caractéristiques et recommandations suivantes :

- le choix de l'implantation des caméras ainsi que le niveau d'éclairement et la nature de la végétation environnante (elle ne doit pas obstruer le champ de vision des caméras) sont déterminants pour une bonne acquisition des images ;
- les zones qui doivent être couvertes par les caméras sont, en général, les zones de passage obligé, les zones d'entrée et de sortie, l'accueil, les zones d'exposition et de conservation, les locaux sensibles, les caisses et les issues de secours ;
- en fonction des zones à protéger, le choix pourra porter sur des caméras fixes, mobiles ou orientables ; sur des caméras dômes, motorisés avec ou sans zoom, dites « PTZ » (180° ou 360°). Tous ces systèmes peuvent être également à infra-rouge, thermiques, etc. ;
- les caméras doivent être placées à une hauteur suffisante, de manière à ne pas pouvoir être manipulée ou masquée facilement. Elles devront disposer d'une détection de masquage, de désorientation et de coupure d'alimentation ;
- une durée de conservation des images d'au moins 15 jours est conseillée, avec un maximum légal de 30 jours ;
- une surveillance et un enregistrement 24h/24 et 7j/7 sont à privilégier. Pour un gain de stockage, il est conseillé d'enregistrer en continu le jour, et sur déclenchement la nuit en cas de survenance d'un évènement ;
- fonctionner en mode IP (Internet Protocol) permet une meilleure souplesse dans l'organisation du système par la suite (facilité de déplacement des caméras, du report des images sur différents PC, etc.) ;
- l'utilisation de caméras dites « *intelligentes* » est pertinent sur certains sites, principalement à l'extérieur de manière à signaler un comportement humain laissant supposer qu'une tentative d'effraction est possible (détection de mouvement, de personnes, de véhicules et d'animaux) ;
- les caméras, installées en extérieur, devront être protégées contre le vandalisme, les agressions climatiques et environnementales (IP 65 ou IP 66 ; répondant aux tolérances de température, de luminosité, etc.). La présence de luminaires ou de spots à détection de mouvement permet d'améliorer l'éclairage de nuit de la zone à surveiller ;
- il est utile de choisir des grands écrans pour éviter la fatigue des opérateurs qui pourront visualiser plusieurs images grâce à un multiplexeur. Il sera nécessaire d'optimiser les fonctions et de disposer d'équipements permettant d'exploiter les images vidéos : lecture en arrière, ralenti, définition de critères personnalisés pour le déclenchement des alertes ou des notifications, notifications et alertes en temps réel permettant un affichage automatique de la zone où l'événement s'est produit, extraction des enregistrements, journaux d'événements, consignation d'alarme et affichage des procédures, etc. ;
- la visualisation vidéo doit être utilisée comme un moyen de levée de doute. Couplée au dispositif de détection d'intrusion, les opérateurs de télésurveillance peuvent ainsi analyser, en cas d'alarme, la situation à distance puis alerter, directement et immédiatement, les forces de l'ordre si nécessaire. Il est important, en cas de transmission d'images vers un télésurveilleur, de choisir un prestataire spécialisé et qualifié (certification APSAD R31). Les images peuvent être transmises également à la police municipale lorsque la ville dispose d'un centre de supervision urbain (CSU) ;
- il est conseillé que le responsable de la sûreté/sécurité, le directeur et les cadres d'astreinte puissent se connecter à distance au système vidéo et recevoir les alarmes, *via* un ordinateur, une tablette ou un smartphone, afin de réaliser une levée de doute immédiate, en cas d'intrusion ou d'événement, puis alerter la police, la gendarmerie ou les pompiers ;

- avant la validation définitive du dispositif, faire des tests pour s'assurer de la qualité des images visionnées et enregistrées, selon différents moments de la journée et de la nuit (luminosité, éclairage, phare, etc.) et tenant compte de l'environnement climatique (pluie, brouillard, etc.). Tester et nettoyer régulièrement les caméras ;
- il est important que le matériel choisi puisse s'adapter à l'évolution des technologies, mais aussi à l'évolution de l'établissement et de ses espaces, en particulier dans les espaces d'expositions temporaires ;
- pour assurer la continuité de service, ces dispositifs doivent bénéficier d'une alimentation de secours, en cas de coupure de courant. Des tests doivent être régulièrement effectués (vérification de la visualisation sur alarme, enregistrements des évènements, nettoyage des caméras, etc.).

Même si les dispositifs d'analyse vidéo ou audio peuvent, grâce notamment à l'intelligence artificielle, venir efficacement compléter les capacités des systèmes vidéo (vidéo augmentée ou vidéo intelligente, détection de présence ou d'intrusion, reconnaissance faciale ou identification corporelle, lecture automatisée de plaques d'immatriculation, analyse comportementale, détection automatique d'anomalie, détection d'objet abandonné, détection d'incivilité, suivi de personnes, chutes, vérification du port des EPI, gestion de parking, comptage de personnes, détection et dynamique des foules détection de départ de feux/fumée, détection des inondations, prise de température automatique, détection du port de masque, respect des mesures de distanciation sociale, etc.), ils ne constitue pas un moyen de remplacement de la **présence et du contrôle humain**.

ASSURER LA SÉCURISATION DU SYSTÈME VIDEO

Les dispositifs vidéo présentent des niveaux d'exposition souvent élevés, compte tenu de leur emplacement et de leur accessibilité. Ils constituent ainsi, une **cible de choix pour des personnes mal-intentionnées** (sabotage, vandalisme, espionnage, etc.), mais également une porte d'entrée significative pour une **intrusion dans le système d'information de l'établissement**.

Les liaisons entre les différents équipements

Pour la qualité de transmission, il est recommandé de privilégier le réseau filaire de type IP. La fibre optique peut être utilisée pour obtenir un meilleur débit sur de grandes distances. Les liaisons sans fil (Wi-Fi, radio, 4G, 5G, etc.), plus rapides à déployer et moins coûteuses, présentent des risques de piratage plus élevées, et leur fiabilité peut être perfectible (sujettes aux interférences provenant d'autres signaux radio ou électriques, à un dysfonctionnement technique ou à une simple coupure temporaire du réseau).

Quelle que soit la solution choisie, il est nécessaire de se prémunir de la cybermalveillance et de **sécuriser l'ensemble des éléments constituant le système vidéo**. Pour cela, il est fortement recommandé d'appliquer strictement les règles d'hygiène informatique (charte d'utilisateur, guide de l'ANSSI, etc.), et de se référer aux « Recommandations sur la sécurisation des systèmes de contrôle d'accès physique et de vidéoprotection » de l'ANSSI, dont les points importants sont décrits ci-dessous :

- cloisonnement physique du câblage et des équipements réseau dédiés (éviter de laisser des ports apparents et accessibles, notamment la prise réseau murale pour le raccordement d'une caméra IP) ;
- les liaisons filaires associées aux caméras extérieures doivent être si possible non apparentes et protégées physiquement (encastrées, bien enterrées, etc.). Il est judicieux de dédier physiquement un réseau support pour les caméras extérieures différent de celui des caméras internes ;
- cloisonnement logique des systèmes vidéo des autres composantes du système d'information de l'établissement (désactiver les ports inutilisés sur les commutateurs réseau) ;

- filtrage et chiffrement, par des solutions de cryptage, ainsi qu'une authentification forte des flux, en provenance et à destination, des dispositifs vidéo (images, administration, etc.) ainsi que chiffrement des données vidéos sauvegardées sur disque dur ;
- activer un deuxième chiffrement dans le cas d'une connectivité sans-fil ;
- les mots de passe par défaut des caméras doivent être remplacés par des mots de passe spécifiques, robustes et, dans la mesure du possible, différents pour chaque équipement (désactiver les fonctions d'administration non utilisées) ;
- dans le cas où le serveur de gestion vidéo est externalisé sur un service d'informatique en nuage (cloud) ou chez un prestataire de services, il convient d'être très vigilant sur le niveau de sécurisation des services qui sont proposés. Il est recommandé de choisir un prestataire de services qualifié par l'ANSSI.

Les systèmes d'enregistrement et d'archivage

L'installation d'un système de vidéo doit satisfaire à l'obligation de sécurisation des données. Ainsi, les équipements, d'enregistrement et d'archivage, doivent être dans des locaux sécurisés, sous contrôle d'accès, tandis que le visionnage et l'extraction des images ne peut être opéré que par les personnes, spécifiquement et individuellement, habilitées.

Ces personnes doivent être particulièrement formées et sensibilisées aux règles de mise en œuvre d'un système vidéo. En outre, un registre mentionnant notamment les enregistrements réalisés, la date de destruction des images, le cas échéant, la date de leur transmission au parquet doit être tenu. Le responsable de traitement doit faire droit à toute demande de visionnage des enregistrements par une personne qui a été filmée, sous réserve du respect des droits des tiers (masquage ou « floutage » d'une partie des images).

La maintenance

L'établissement doit disposer d'un contrat de maintenance, ou d'une organisation de maintenance interne, effectuant des vérifications périodiques, assurant le remplacement du dispositif défaillant et des interventions en cas de panne (matériel, serveur, logiciel, etc.). Pendant la panne, il est fortement conseiller de faire contrôler physiquement la zone concernée par un agent de surveillance.

Il est important de pouvoir bénéficier de matériel de remplacement sur site (caméras, écrans, équipement de stockage, etc.) ou de pouvoir se les faire amener le plus rapidement possible. Cette situation critique doit être **anticipée**, notamment par la présence de procédures spécifiques détaillant les **mesures de sécurité à mettre en place** pour compenser l'absence, partielle ou totale, de visibilité sur les zones couvertes par les caméras.

Il convient d'être particulièrement vigilant aux risques inhérents au recours à un prestataire, qui intègre et maintient, en local ou à distance, un parc de caméras, ou à une externalisation du service avec le transfert ou la duplication de l'ensemble des flux des caméras en dehors du système d'information de l'établissement, voire en dehors du territoire national (Se référer aux guides « Maîtriser les risques de l'infogérance – externalisation des systèmes d'information » et « Recommandations relatives à l'administration sécurisée des systèmes d'information » publiés par l'ANSSI).

LES CONSEILLERS SÛRETÉ

Il existe au sein du ministère de la Culture des experts en sûreté pour les patrimoines.

Ces recommandations étant générales, il conviendra de demander l'assistance et l'expertise des conseillers sûreté afin d'adapter au cas par cas les mesures nécessaires pour renforcer la sécurisation de l'établissement.

Pour les musées :

André POPON, commandant de police – tél. 06 07 35 22 68 ; andre.popon@culture.gouv.fr

Guy TUBIANA, commandant de police – tél. 06 63 10 58 24 ; guy.tubiana@culture.gouv.fr

Pour les monuments historiques :

Eric BLOT, commandant de police – tél. 01 40 15 76 83 ; eric.blot@culture.gouv.fr

Pour l'archéologie et les archives :

Yann BRUN, conseiller– expert sûreté – tél. 06 58 90 40 72 ; yann.brun@culture.gouv.fr

Secrétariat :

Françoise ROUFFIGNAC, assistante – tél. 01 40 15 34 94 ; francoise.rouffignac@culture.gouv