



A²VMA-C

Fiche conseil « VIDEOSURVEILLANCE »
Recommandations pour l'utilisateur d'un système de vidéosurveillance

1. OBJECTIF

Etablir des conseils pour l'utilisateur d'un système de vidéosurveillance. Par utilisateur, il y a lieu de comprendre ici en première instance le secteur de la distribution ou le secteur bancaire ou le secteur commercial au sens large.

Il ne rentre **nullement** dans les intentions d'obliger les secteurs concernés d'installer systématiquement des caméras. Le but poursuivi est seulement de procurer un nombre de conseils et de recommandations auxdits secteurs de façon à pouvoir optimiser le système de vidéosurveillance dans lequel ils veulent investir.

2. OBJECTIFS DE L'UTILISATION D'UN SYSTEME DE VIDEOSURVEILLANCE

2.1 VIS-A-VIS DES AUTEURS

- Prévention de délits : Des caméras installées visiblement font partie de la prévention : elles ont un effet dissuasif.
- Contribution à l'optimisation de l'examen judiciaire :
De bonnes images filmées représentent un avantage pour les services policiers et les instances judiciaires pour pouvoir reconnaître et identifier les coupables.
Ces images pourraient être utilisées dans le cadre d'enquêtes (e. a. via Oproep 20/20 – Appel à témoins, Bulletin de Recherche et d'Information...) et sont également importantes comme charge de la preuve dans le cadre d'une affaire judiciaire.

2.2 VIS-A-VIS DU PERSONNEL DE L'ORGANISME VICTIME DU DELIT :

Fournir une contribution positive au sentiment de sécurité :

Concrètement, savoir que les images contribuent à améliorer l'enquête augmente la chance d'arrêter les auteurs.

2.3 VIS-A-VIS DES FORCES DE L'ORDRE :

Un système de vidéosurveillance installé dans un commerce et directement relié à la Police peut fournir de précieuses aux équipes d'intervention (nombre d'auteurs, type d'armement, etc...). Il permet une meilleure évaluation du dispositif à déployer et son adaptation en fonction de l'évolution de la situation, notamment une réduction de la mise en danger de la vie d'autrui.

3. RECOMMANDATIONS

3.1 EXIGENCES GENERALES FONCTIONNELLES

- Visage identifiable : indépendamment des conditions atmosphériques, de l'heure, de la luminosité, il faut obtenir une image identifiable et reconnaissable du visage de l'agresseur via l'enregistrement vidéo.
- Disponibilité rapide de l'image stockée : après un vol à main armée, les images doivent être rapidement disponibles pour les services de police afin de les analyser et de les exploiter.
- Fonctionnement sans intervention humaine : dans la mesure du possible, le système doit fonctionner sans intervention humaine et de préférence, filmer en permanence dans les périodes actives et sur base du principe du « motion détection » dans les périodes passives.
- Commande simple : l'installation doit être simple à manipuler et pouvoir être commandée par de simples manipulations. Un mode d'emploi dans la langue de l'utilisateur est indispensable.
- Contrôle simple : un test simple et régulier doit être effectué par l'utilisateur (minimum quotidiennement) pour vérifier le bon fonctionnement du système.
- Enregistrement de la date et de l'heure : lors de la recherche d'images, l'enregistrement de la date et de l'heure sur les images est important. Veuillez à ce que ces indications ne perturbent pas les objets intéressants dans les images

3.2 EXIGENCES PARTICULIERES FONCTIONNELLES

3.2.1 OÙ ?

- Aperçu global des situations à risques dans les bâtiments où les auteurs peuvent opérer : par ex. zone de caisses, guichets et self-service... Mise en place visible.
- Enregistrement détaillé : installation aux passages obligatoires pour entrer dans les lieux ; A hauteur des yeux (caméra orientée vers le visage des clients sans contre-jours).

3.2.2 COMMENT ?

- **Lumière et éclairage**
 - ✓ Lumière suffisante dans les zones d'enregistrement (jour et nuit).
 - ✓ Pas de contre-jour.
 - ✓ Pas d'influence d'un soleil changeant.
- **Emplacement de la caméra**
 - ✓ Position discrète des caméras.
 - ✓ Caméras à hauteur des yeux.
 - ✓ Une caméra placée juste à l'entrée.
- **Résolution de l'image**
 - ✓ Eviter tout élément pouvant nuire à la visibilité
 - ⇒ **Identification des personnes**
 - Correcte : la dimension d'un pixel fait moins que 1 mm
 - Possible : la dimension d'un pixel se trouve entre 1 et 2,5 mm
 - Peu possible : la dimension d'un pixel fait plus que 2,5 mm
 - ⇒ **Identification des plaques d'immatriculation**
 - Pour assurer la lisibilité, la hauteur des caractères doit correspondre à 15 pixels.
- **Qualité d'enregistrement**
 - ✓ Pas de compression ou une compression minimale
 - ✓ Vitesse d'enregistrement pas trop basse (min 15fr/s).
 - ✓ Enregistrements originaux disponibles pour l'analyse.

- **Entretien**

- ⇒ **Journalier**

- Toutes les caméras fonctionnent-elles ?
 - Les images sont-elles nettes ?
 - L'éclairage est-il bon ?
 - Les images sont-elles enregistrées ?
 - La date et l'heure sont-elles correctes ?
 - Le système est-il sécurisé ?

- ⇒ **Mensuel**

- Les objectifs sont-ils encore clairs ?
 - Les caméras ont-elles bougé ?
 - L'espace est-il encore sûr ?
 - La qualité des enregistrements est-elle suffisante ?

- ⇒ **Annuel**

- Le système fournit-il encore la qualité d'enregistrement requise ?
 - Un contrôle de la balance est-il réalisé ?
 - Un statut de Haute Définition est-il effectué ?
 - Un contrôle de la présence des documents et des manuels est-il effectué ?
 - Les opérateurs sont-ils recyclés ?
 - Le transfert des images sur un support fixe est-il fait correctement ?
 - Un entretien pour le système CCTV est-il prévu ?

3.3 ENREGISTREMENTS

- Appareillage : optez de préférence pour un enregistrement digital, sans ou avec un minimum de compression (compression = perte de qualité).
- Placement : placez l'appareillage d'enregistrement de préférence dans un endroit non accessible au public, hors de la vue ou dans une armoire fermée afin d'éviter que les enregistrements ne puissent être effacés par des personnes non qualifiées ou les auteurs.
- Formation/exercice : veillez à ce que les utilisateurs (aussi les nouveaux venus) puissent suivre une formation pour pouvoir actionner et manipuler l'appareil, remplacer les bandes et réparer de simples dérangements.
- Capacité : le disque doit offrir suffisamment de capacité pour couvrir les périodes d'enregistrements.

3.4 BACK-UP

Lors de stockage digital, il est conseillé de prévoir un back-up, par ex. stockage parallèle sur deux disques durs, stockage remote....

3.5 CHECK-LIST INCIDENTS

Indépendamment de l'application des prescriptions en vigueur qui sont imposées au responsable du traitement, il est utile que ce dernier puisse faire appel à une check-list en cas d'incident :

- 1) Contactez la police ;
- 2) Donnez une indication du lieu, du moment et une courte description des faits ;
- 3) Comparez l'heure effective avec l'heure enregistrée sur le support d'enregistrement et notez les constatations (correspondantes ou divergentes) ;
- 4) Mettez les enregistrements sur un support transportable sans porter atteinte à la qualité de l'information, faites si nécessaire 2 copies, une originale et une copie backup ;
- 5) Utilisez un support d'enregistrement de type READ-ONLY (CD-R, DVD-R) pour éviter une réécriture des données ;
- 6) Munissez le support d'enregistrement d'une étiquette avec mention du nom de l'organisme, la date et l'heure de l'incident, l'original, la copie, le nom et la signature du responsable ;
- 7) Sécurisez le support d'enregistrement en la plaçant dans une enveloppe scellée.

Dans l'attente de la transmission à la police, conservez les enveloppes scellées dans un lieu sécurisé (vol, température, matière, rayons directs du soleil, etc,...) ;

- 8) Vérifiez si les données disponibles peuvent être traitées par la police dans un contexte légal. Si ce n'est pas le cas, veuillez à ce que le logiciel ou hardware nécessaire soit disponible au moment où la police récolte l'information ;
- 9) Veuillez à ce que les documents utiles soient disponibles :
 - Personne de contact
 - Téléphone du responsable
 - Installateur
 - Téléphone de l'installateur
 - Type d'installation
 - Manuel technique
 - Plan de caméras
 - Document pour la remise du matériel sécurisé (date, détenteur, récepteur, service).

4. LEGISLATION

4.1 LOI VIE PRIVEE

La loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel est d'application.

Avant que le responsable du traitement n'effectue un traitement automatisé, il doit déclarer ce traitement à la Commission sur la vie privée au moins un jour avant la mise en route du système.
(<http://www.privacycommission.be>).

4.2 LOI CAMERAS

Selon la loi caméras du 21 mars 2007, les magasins et les banques sont distingués comme **lieux fermés, accessibles au public**.

Les caméras peuvent seulement filmer la propriété propre.

Les images peuvent être conservées un mois, excepté si elles contribuent à faire la preuve ou identifier les auteurs des faits.

On doit aussi indiquer l'utilisation de caméras avec un pictogramme (AR 10 février 2008). Les pictogrammes doivent avoir une dimension de 30cm x 20cm.

5. DEDUCTIONS

Les indépendants ou titulaires de professions libérales qui sécuriseront leur locaux peuvent bénéficier des déductions légales : les déductions pour l'investissement pour la sécurisation (AR 17 août 2007) en une déduction des frais professionnels à 120% (code des impôts sur les revenus 192 – Art. 54).