Votre projet de vidéoprotection
Guide Méthodologique

Fiches thématiques

Comité de Pilotage Stratégique pour le développement de la vidéoprotection

Sommaire

LES FICHES THEMATIQUES

Les fiches sont organisées en quatre catégories, correspondant aux 4 principales étapes de la démarche de projet.

- **Analyse des besoins**
  - Fiche n°1 : 20 questions à se poser avant de lancer le projet
  - Fiche n°2 : La surveillance des parkings
  - Fiche n°3 : La prévention situationnelle
  - Fiche n°4 : Les besoins fonctionnels et techniques des forces de sécurité intérieure

- **Organisation du projet**
  - Fiche n°5 : Sources et moyens de financement pour les différents types d'opérateurs
  - Fiche n°6 : L'exploitation et accès aux images, protocoles d'exploitation et d'exportation
  - Fiche n°7 : La constitution du dossier de demande d'autorisation préfectorale
  - Fiche n°8 : Comment choisir un bureau d'études ou un cabinet conseil ?
  - Fiche n°9 : Le recrutement et la formation des opérateurs

- **Aspects techniques**
  - Fiche n°10 : Le panorama des matériels et des logiciels
  - Fiche n°11 : Les normes techniques
  - Fiche n°12 : Les traitements intelligents (LAPI, reconnaissance faciale, vidéogestion,..)
  - Fiche n°13 : 20 tests à réaliser à la réception du système

- **Vie du système**
  - Fiche n°14 : L'évaluation des résultats ?
  - Fiche n°15 : Comités et chartes d'éthiques
  - Fiche n°16 : Le dispositif national de suivi

1 FICHE N°1 : 20 QUESTIONS CLES A SE POSER AVANT DE LANCER LE PROJET

Fiche n°1

20 questions CLES à se poser avant de lancer le projet

Avant la mise en place d'un système de vidéo protection, le responsable du projet devra, après avoir suivi la démarche du guide et pour optimiser les travaux à venir, pouvoir répondre à 20 questions essentielles communes à la majorité des projets.

- **Stratégie**
  - Quel est l'objectif principal du système de vidéo protection? Existe-t-il des objectifs secondaires ?
  - Ces objectifs sont-ils clairement exprimés et partagés par l'ensemble des acteurs du projet ?
  - Ces objectifs ont-ils été validés par des personnes externes au projet et en particulier par les services de sécurité intérieure ?
  - Ces objectifs ont-ils permis de déterminer des critères de choix pour la détermination du lieu d'implantation des caméras ?
  - Ont-il permis de dimensionner un système optimal, sans tenir compte à ce stade des problématiques de coût ?
  - Les problématiques juridiques ont-elles été prises en compte, en particulier concernant le régime juridique applicable aux caméras et à l'exploitation du système ?
  - Quelle coordination, quelle mutualisation ou quels échanges peuvent être envisagés avec d'autres acteurs, ou d'autres projets ?
  - Des projets similaires réussis ont-ils été identifiés afin de permettre la validation des hypothèses de travail ?
- **Organisation**
  - Quel est le territoire sur lequel s'étend le projet ?
  - Quel est le besoin concernant l'exploitation des images (principalement visualisation directe ou exploitation différée,…)?
  - Qui exploitera les images ?
  - Quels sont les besoins en personnel pour réaliser cette exploitation et pour administrer les systèmes ?
  - Le retour sur investissement global du système de vidéo protection a-t-il été évalué ?
  - Quels seront les outils d'évaluation de l'efficacité du système mis en place ?
  - Le coût estimatif de mon installation a-t-il été optimisé et les aides au financement locales et nationales ont-elles été sollicitées ?
- **Technique**
  - Compte tenu des objectifs opérationnels retenus, puis-je déterminer les principales caractéristiques de mon système :
    - qualité et technologie des capteurs (caméras IP ou analogiques, résolution des caméras, protection des caméras, mobilité des caméras, …) ?
    - résolution et fluidité des images visualisées en direct et en différé ?
    - dimensionnement des moyens de transmission (bande passante)
    - dimensionnement des capacités de stockage en fonction

du nombre, de la qualité et de la durée de conservation des images collectées?

- L'architecture du système a-t-elle été conçue pour optimiser les coûts d'investissement (choix des technologies de transmission, mutualisation des supports de transmission, architecture de stockage centralisée ou répartie) et les coûts d'exploitation (mutualisation de moyens d'exploitation, automatisation des moyens de maintenance à l'aide de traitements automatisés, …)
- Est-elle évolutive pour pouvoir prendre en compte les évolutions technologiques ?
- La solution technique envisagée est elle ouverte (compatible avec des systèmes de fournisseurs différents) ou propriétaire ?
- Cette solution technique permet-elle d'intégrer simplement de nouvelles caméras en cas d'extension du système ?
- Les traitements intelligents seraient-ils susceptibles d'apporter une plus-value opérationnelle au système ?
- Quelles normes techniques mon projet doit-il respecter

Fiche n°2

La surveillance des parkings

2 FICHE N°2 : LA SURVEILLANCE DES PARKINGS

2.1 LA SURVEILLANCE DES PARKINGS OUVERTS AU PUBLIC

Les parkings représentent un endroit pouvant être à fort risque. D'où l'intérêt qu'y présente un système de vidéoprotection, pour garantir la sécurité des personnes mais aussi pour obtenir la rentabilité financière optimale.

En application du décret 97-47 du 15.01.1997 et de la circulaire du 30.05.1997, la vidéoprotection est une réponse possible à l'obligation de surveillance, en alternative à la surveillance humaine. Cette obligation de surveillance pèse sur les garages et sur les parcs de stationnement ouverts au public comprenant au moins 200 places et situés dans des espaces urbains de plus de 25 000 habitants.

La notion d'ouverture au public mérite d'être explicitée : en effet sont considérés comme tels les parcs de stationnement dont l'accès n'est pas nominatif ou réservé à certaines catégories d'usagers. Ainsi, ceux qui ne sont accessibles qu'à des abonnés, aux salariés d'une entreprise, aux locataires ou propriétaires d'immeubles à usage d'habitation ne sont pas considérés comme ouverts au public. Dans le cas d'un parking mixte, seule la partie ouverte au public est assujettie aux obligations spécifiques du décret de 1997 sous la condition que sa contenance soit égale ou supérieure à 200 places.

2.2 LA SURVEILLANCE DES PARKINGS PRIVES D'IMMEUBLES A USAGE D'HABITATION

- **Contrôler les accès aux parkings et les mouvements intérieurs afin de garantir la protection des véhicules et la sûreté des résidents.**

On peut distinguer deux grandes catégories de parkings privés d'immeubles à usage d'habitation : la **première** concerne ceux situés dans des immeubles collectifs à usage locatif relevant des articles L127-1 et R127-1 du Code de la Construction et de l'habitation et la **seconde** concerne tous les autres relevant soit du régime de la copropriété ou de celui des immeubles collectifs à usage locatif non situés dans les zones définies par les textes susmentionnés.

En ce qui concerne la première catégorie, les bailleurs sont assujettis à diverses obligations de gardiennage et de surveillance tant sur le plan technique qu'humain afin de prévenir les risques manifestes pour la sécurité et la tranquillité des locaux communs dont les parkings.

En ce qui concerne la seconde, il n'existe pas d'obligation réglementaire de surveillance des parkings sur le plan réglementaire.

Les parkings sont des lieux sensibles en termes d'insécurité, compte tenu du large panel d'actes de malveillance qui peuvent s'y dérouler, du détournement d'usage aux violences sur les personnes sans omettre le vandalisme et le vol de véhicules. De plus, la voiture constitue un bien précieux en termes d'usage et de coût que ce soit pour se rendre sur son lieu de travail ou pour ses divers déplacements, notamment dans des quartiers souvent excentrés et/ou mal desservis par les réseaux de transports en commun.

2.3 LA SURVEILLANCE DES PARKINGS PRIVES SOUTERRAINS

Les places de stationnement représentent un investissement financier non négligeable tant pour un locataire que pour un copropriétaire. Le résident n'utilisera donc le parking que s'il s'y sent en sécurité ; dans le cas contraire le taux de vacances sera important et il y aura donc une perte d'usage ou un manque à gagner, de plus cela risque naturellement d'accroître un stationnement extérieur plus au moins anarchique

D'une manière générale et pour un bon fonctionnement de la vidéoprotection le niveau d'éclairage des parkings est aussi très important pour l'utilisation de la vidéosurveillance et trop de parkings ont pour des raisons économiques des niveaux d'éclairement nettement insuffisants et non sécurisants.

Les niveaux d'éclairage ci-dessous sont préconisés par l'association française de l'éclairage (AFE).

Zone de parking	Niveau recommandé (en lux)
Rampe d'entrée	100 (nuit) et 300 (jour)
Contrôle et péage	150
Rampes et circulation verticale	15

Emplacement de stationnement	10
Circulation piétonne	20
Zones communes piétons / véhicules	100
Sas	40

2.3.1 CONCEPT DE SÉCURISATION :

Quel que soit le statut juridique du parking, il convient que les portes d'accès piétons et véhicules du parking soient équipées d'un système de contrôle d'accès personnalisé, limitant ainsi l'entrée aux seuls usagers d'un emplacement de stationnement. La technologie du contrôle d'accès des véhicules sera de préférence de « type anti-pass back » offrant une balance « une entrée pour une sortie » afin de limiter ainsi les détournements d'usage.

Les mesures complémentaires de prévention technique de la malveillance concernent principalement :

- la configuration des points d'entrée et de sortie, la plus ou moins grande étanchéité par rapport à la circulation générale sur la voie publique et aux tentatives de pénétration à pied ou au moyen d'un véhicule motorisé,
- le contrôle des mouvements de véhicules et des piétons en entrée–sortie,
- la surveillance humaine et/ou technique des véhicules sur leur lieu de stationnement,
- l'aspect architectural et visuel à l'intérieur du parc de stationnement, lisibilité, visibilité, niveau de l'éclairage, peinture claire aux murs et au plafond, places délimitées et numérotées, personnalisation des différents niveaux, acoustique, etc…

Un soin doit être apporté à la qualité des issues de secours en termes de fonctionnement et de résistance à l'effraction. Elles ne doivent pas pouvoir être utilisées pour pénétrer frauduleusement dans l'enceinte du parking.

L'implantation des caméras de surveillance se fait principalement aux points suivants :

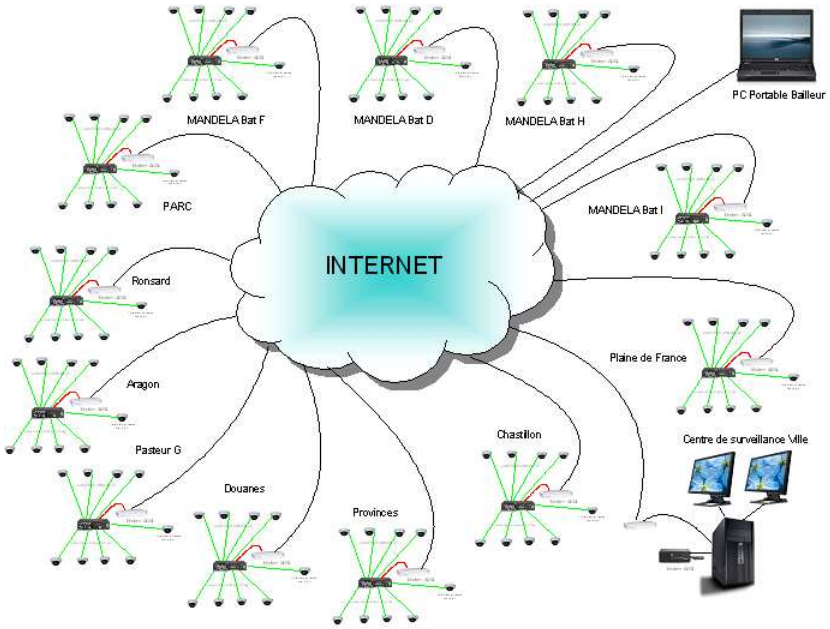
- Face à la porte d'accès véhicule : la caméra sera équipée d'un dispositif de type « peak limiter » pour permettre la lecture des plaques,
- Dans le parking face à chacune des portes d'accès piétons et des arrivées ascenseurs,
- Quelques caméras visibles ou discrètes judicieusement placées permettront de visualiser les comportements dans les allées du parking et de réaliser en cas de besoins un tracking vidéo,
- Aux issues de secours.

L'alimentation des caméras se fait depuis un local dont les ouvrants (portes et fenêtres) sont d'une qualité résistant à l'effraction. Ce dernier est implanté dans le parc de stationnement et les équipements fonctionnent sur onduleur avec une autonomie de 1H00.

Le stockeur numérique peut être logé dans ce local, installé dans une baie ventilée le protégeant des poussières.

2.3.2 EXPLOITATION

Ci-dessous un exemple de réalisation de surveillance de 12 parkings répartis sur une commune (Tremblay en France) pour le compte de SEMIPFA. L'exploitation se fait au moyen d'un logiciel graphique très simple d'exploitation et d'un coût modéré permettant de visualiser soit toutes les caméras du parking en multivision, soit une seule caméra en choisissant le point d'implantation désiré.



Fiche n°3

La prévention situationnelle

3 FICHE N°3 : LA PREVENTION SITUATIONNELLE

3.1 ÉLEMENTS DE DEFINITION

La théorie criminologique de prévention situationnelle s'analyse comme une prévention primaire du crime qui met l'accent sur la réduction des opportunités et place les services de police et de gendarmerie au cœur du dispositif. Cette théorie s'est développée dans les années 80 en ANGLETERRE à partir de recherches américaines et sous l'impulsion de RONALD V CLARKE, alors chef de l'unité de recherche et de planification du Home Office. Selon les tenants de cette théorie, le délit résulte autant de l'émergence d'une occasion que de la motivation de l'auteur. Une des approches les plus importantes est celle de "l'activité routinière" selon laquelle l'environnement physique et social de notre société crée des occasions de délit en réunissant dans un même espace et dans un même temps trois conditions de base :

L'exemple le plus fréquemment évoqué pour traduire ce que représente la prévention situationnelle, dans son approche classique, est celui de la théorie du « broken glass » de G. Kelling et J.Q Wilson. Cet exemple new-yorkais de réduction de la délinquance s'illustre autour du concept de fenêtres brisées selon lequel la production d'un cycle de violence découlerait d'un enchaînement d'actes en relation avec certains signes de désordres.

3.2 PRINCIPES DE LA PREVENTION SITUATIONNELLE

En réponse à cette dynamique, les techniques de prévention situationnelle visent à durcir les cibles selon un schéma décrit par Ronald Clark. Les travaux de ce professeur à l'université de Newark, aux États-Unis, décrivent quatre axes d'intervention, recouvrant seize techniques :

- **Augmenter l'effort des délinquants**
  - par la protection des cibles,
  - par le contrôle des accès,
  - par le découragement du délinquant,
  - ou encore le contrôle des « éléments facilitant » (cartes de crédit, armes à feu, identifiants téléphoniques),
- **Augmenter les risques pour le délinquant potentiel**
  - par le contrôle des entrées et des sorties,
  - par la surveillance formelle (dont radars),
  - par la surveillance par des employés (dont vidéosurveillance),
  - par la surveillance naturelle (fréquentation des lieux, éclairage…),
- **Réduire les gains**
  - par l'élimination des cibles,
  - par l'identification des biens,
  - par la réduction de la tentation,
  - par la limitation voire la suppression des profits estimés par le délinquant.
- **Empêcher la justification**
  - par la facilitation du respect de la loi,
  - par le contrôle des « désinhibiteurs » (alcool, drogues…),
  - par la mise en place de règles,
  - par la capacité à donner mauvaise conscience.

3.3 BILAN ET LIMITES DE LA PREVENTION SITUATIONNELLE

Plusieurs critiques peuvent être faites sur cette stratégie. Elles ne remettent toutefois pas en cause sa pertinence mais doivent être connues du décideur Une efficacité variable selon le profil des délinquants

Elles concerneraient les limites du champ préventif, ce type de prévention fonctionnant sur des délinquants occasionnels, mais beaucoup moins sur des délinquants d'habitude, surtout ceux affiliés à la grande délinquance, très actifs et recherchant en permanence de nouvelles stratégies.

Certaines de ces stratégies d'évitement de la vidéoprotection sont effectivement constatées dans les sites équipés. Cela reste cependant peu significatif et peut être compensé par d'autres techniques.

- **Un risque d'accroissement des inégalités devant l'insécurité.**

D'un côté, apparaîtraient les « victimes organisées », qu'il s'agisse de villes, d'entreprises, de commerces ou de particuliers, en mesure de se doter des moyens, notamment techniques, pour se protéger. De l'autre, les victimes potentielles, moins protégées et donc plus exposées. Enfin, l'un des risques est le développement non maîtrisé du marché privé de la sécurité.

C'est la raison pour laquelle tout projet de sécurisation doit être menée dans le cadre d'un partenariat local.

- **Une nécessaire complémentarité entre la prévention sociale et la prévention situationnelle**

Ces approches doivent être complémentaires. La technique ne remplace pas le dialogue et la prévention situationnelle ne doit pas conduire à une surprotection ou à une déshumanisation d'un espace.

La prévention situationnelle doit être utilisée à bon escient.

- **Une technique mal évaluée**

Les informations relatives au niveau d'insécurité sont globalement connues mais éparses et mal exploitées. Les retours d'expériences sur les événements et la pertinence des mesures de prévention sont rarement organisés et souvent négligés.

Il est essentiel de mettre en place des outils d'évaluation des actions de sécurisation mises en place.

- **Une expertise encore trop confidentielle**

Les théories et les savoirs de la prévention situationnelle demeurent l'affaire de spécialistes et leur diffusion reste faible. Ainsi, ce sujet n'apparaît-il pas dans le cursus de formation initial des aménageurs et concepteurs (écoles d'architecture, écoles d'ingénieur du bâtiment et des travaux publics), qui sont pourtant en première ligne dans la création d'espaces publics et privés.

- **Des dispositifs qui peuvent s'avérer coûteux, voire inaccessibles**

Les équipements de vidéosurveillance s'ils sont mal conçus et superflus par rapport au besoin présentent des prix élevés, voire prohibitifs.

3.4 PREVENTION SITUATIONNELLE ET « EFFET PLUMEAU »

- **L'effet « plumeau » constitue une réalité inévitable**

Compte tenu du partage des responsabilités territoriales entre les différents acteurs de la sécurité, et malgré les efforts de coordination des actions et de partage des informations menés au niveau local, la mise en œuvre de la prévention situationnelle ne peut s'inscrire que dans un espace donné et par nature limité. Dans ces circonstances, et à l'exception des bâtiments ou des sites pouvant être totalement sécurisés (clos, sous contrôle d'accès et détection d'intrusion avec réactivité en temps réel), le déplacement de la délinquance vers des lieux plus propices à son exercice semble inévitable.

- **Les différentes formes d'effet « plumeau »**
  - Déplacement géographique : les délinquants quittent la zone ou changent de lieu dans la même zone
  - Modifications dans les modes opératoires : adaptation des délinquants en réaction aux mesures mises en œuvre dans le cadre de la prévention situationnelle.

Exemple : l'interdiction d'occuper les halls d'immeuble induit un déplacement des trafics dans les étages et les caves.

- **Un effet qui peut être compensé**

Le phénomène de déplacement doit être compensé et canalisé par des mesures techniques, humaines et d'organisation (régionalisation et mutualisation en termes de partage de l'information dans le temps et dans l'espace) qui permettent d'assurer un suivi précis et pertinent de la trajectoire des délinquants et le traitement successif de ses manifestations.

4 FICHE N°4 : LES BESOINS FONCTIONNELS ET TECHNIQUES DES FORCES DE SECURITE INTERIEURE

Fiche n°4

Les besoins fonctionnels et technique des forces de sécurité intérieure

4.1 BESOINS FONCTIONNELS

4.1.1 LES USAGES POLICIERS DE LA VIDÉOPROTECTION

♦ **Identification des auteurs d'infraction**

- Identification en temps réel : l'opérateur détecte un événement, il avise immédiatement les services en charge de la sécurité qui jugent de la suite à donner aux faits observés. La réactivité de l'opérateur est déterminante.

  Dans le cadre d'une intervention, l'opérateur suit et guide, le cas échéant, l'unité d'intervention.

  Cela suppose que les services en charge de la sécurité disposeront d'un moyen de communication dédié. Par exemple, une ligne téléphonique ou un moyen radio approprié.

- Identification en temps différé : Les services de sécurité consulteront les enregistrements à des fins judiciaires ou de sécurité publique, afin d'obtenir des éléments permettant d'identifier un auteur ou d'orienter une enquête. Les possibilités d'identification dépendront beaucoup de la définition des images et de la qualité de l'enregistrement.
- En matière pénale la preuve peut être apportée par tout moyen : une image fait partie des éléments de preuve permettant d'établir la culpabilité d'une personne. Sa valeur probante est laissée à la libre appréciation du juge.

♦ **Dissuasion :**

- Présence visible des caméras dans les secteurs de délinquance avérés ou les territoires sensibles~~,~~
- Contrôle des points de fixation de la délinquance : lieux de regroupements, de troubles à la tranquillité publique, points de passage obligés...

♦ **Surveillance :**

- Identification, surveillance de certains individus recherchés, dans le cadre de procédures judiciaires : les services de police peuvent être amenés à solliciter les opérateurs pour l'identification de personnes recherchées,
- Identification de véhicules impliqués dans des procédures judiciaires,
- Surveillance constante à distance de quartiers éloignés, difficiles d'accès ou très sensibles,
- Protection des établissements sensibles.

◆ **Appui opérationnel à la gestion des événements de voie publique :**

- Surveillance du trafic routier,
- Aide à la décision en matière de service d'ordre ou de maintien de l'ordre (manifestations de voie publique, festivités, déplacements officiels…) Les images permettent au responsable du dispositif de mieux appréhender la situation, la réactivité du dispositif à la situation est ainsi améliorée,
- Vérification de l'adéquation des effectifs policiers à employer à la suite d'une demande d'intervention (appel 17),
- Appui des effectifs intervenants en zone difficile.

Pour répondre à tous ces besoins, les installations de vidéoprotection doivent donc être polyvalentes, réactives et évolutives. La qualité de l'enregistrement est très importante.

4.1.2 L'IMPORTANCE DE LA RÉACTIVITÉ DU SYSTÈME

L'efficacité et le pouvoir de dissuasion de la vidéoprotection dépendront en grande partie de la réponse apportée à la suite de la détection d'un événement considéré comme anormal. Le dispositif sera perçu comme très efficace si une intervention humaine (pas nécessairement policière) a lieu rapidement après le déclenchement d'un incident.

Pour maintenir un bon niveau de réactivité, il est nécessaire que les opérateurs aient un retour sur les signalements qu'ils auront faits aux services de police.

Concernant les forces de sécurité, cette réactivité sera conditionnée par plusieurs éléments importants :

- **L'existence d'un moyen de communication simple et permanent (CSV urbain principalement)**
  - Ligne téléphonique dédiée.
  - Communication aux opérateurs de numéros téléphonique « police » ou « gendarmerie » : standard.
  - Lien radio : un émetteur récepteur radio électrique peut être mis à disposition des responsables locaux de la police ou de la gendarmerie : embarqué avec les patrouilles de terrain, installation à proximité de l'agent chargé de recevoir les appels…
- **L'information des agents des forces de sécurité territorialement compétents**
  - Il est important que les forces de sécurité de tous niveaux amenés à intervenir dans la zone vidéoprotégée aient une bonne connaissance de l'installation :
    - Zones vidéosurveillées,
    - Durée d'enregistrement,
    - Implantation exacte des caméras,
    - Organisation du centre de surveillance vidéo : numéro d'appel, nom du responsable, horaires…

Cette information nécessite une formation régulière des agents des forces de sécurité, dans le cadre d'un partenariat entre l'exploitant et les services de sécurité concernés. Cette formation doit être régulièrement actualisée : mobilité des personnels, modification possible de l'installation…

- **La formation des opérateurs :**

- Connaissance de l'organisation des forces locales de sécurité,
- Connaissance sommaire de la procédure pénale et des organisations judiciaires,
- Connaissance des principaux modes opératoires des délinquants.

4.1.3 FACILITER L'ACCÈS AUX IMAGES :

Les services de sécurité doivent pouvoir accéder facilement aux images, quel que soit le site concerné. Il est donc important que le gestionnaire du système mette en place des conditions d'accès facilitant la consultation des images en temps réel ou en temps différé.

- **Accès aux images en temps réel**

Il est important de laisser aux services de sécurité la possibilité de prendre la main aux circonstances prévues au protocole signé au préalable avec le gestionnaire du système. Ces opérations contribuent à la motivation et à la formation des personnels.

- **Accès aux images en temps différé :**

Pour faciliter le travail de consultation des enregistrements il est important de centraliser l'exploitation de tous les enregistrements vers un poste unique de relecture. Ce poste de relecture sera de préférence situé à l'écart ou dans une salle distincte de la salle où travaillent les opérateurs.

4.2 EXIGENCES TECHNIQUES

Les systèmes de vidéosurveillance installés doivent être conformes à des normes techniques définies par l'arrêté du 3 août 2007 relatif aux normes techniques, à compter de l'expiration d'un délai de deux ans après la publication de cet arrêté (soit le 21 août 2009).

Ces normes ont pour but d'assurer une qualité minimum des images et de leur transmission de sorte qu'elles puissent servir effectivement à la lutte contre la délinquance.

Fiche n°5

Sources et moyens de financement pour les différents types d'opérateurs

5 FICHE N°5 : SOURCES ET MOYENS DE FINANCEMENT POUR LES DIFFERENTS TYPES D'OPERATEURS

La présente fiche n'a pas pour objet de présenter les modes classiques de financement utilisés pour l'acquisition de matériel ou de construction d'une infrastructure de réseaux (emprunt, crédit-bail, location financière).

Il s'agit de recenser les pratiques permettant un transfert ou un partage des coûts supportés par des personnes publiques ou des personnes privées lors de la création, la rénovation et l'exploitation d'un réseau de vidéoprotection.

Plusieurs départements et régions ont mis en place un dispositif de financement de la vidéoprotection. Pour pouvoir en bénéficier, les maîtres d'ouvrages peuvent se renseigner utilement auprès de ces collectivités. Le développement qui suit ne concerne que le financement par l'Etat.

5.1 AIDE PUBLIQUE SPECIFIQUE PAR L'ETAT

- le **Fonds interministériel de prévention de la délinquance :**

La loi du 5 mars 2007 dans son article 5 crée, au sein de l'Agence nationale pour la cohésion sociale et l'égalité des chances (l'Acsé), un fonds interministériel de prévention de la délinquance (FIPD).

Le FIPD est destiné à financer la réalisation d'actions de prévention de la délinquance mises en œuvre dans un cadre partenarial (CLS, plan d'action d'un CLSPD, CUCS, plan départemental de prévention de délinquance). Ces actions ne doivent pas être incompatibles avec le plan de prévention de la délinquance arrêté par le représentant de l'Etat dans le département. Les bénéficiaires du FIPD sont les collectivités territoriales, leurs groupements, les associations et les organismes publics ou privés. Le FIPD peut également financer des actions de prévention conduites par les services de l'Etat (études, actions de communication, formation…) à la condition que celui-ci n'intervienne pas en substitution des crédits de droit commun de chaque ministère s'agissant en particulier du fonctionnement de leurs services.

Le Comité interministériel de prévention de la délinquance (CIPD) fixe les orientations et coordonne l'utilisation des crédits de ce fonds. En application de ces orientations, le conseil d'administration de l'Acsé, quant à lui, approuve les programmes d'intervention correspondant et répartit les crédits entre les départements. L'Acsé est chargée du suivi et de l'évaluation de l'utilisation de ces crédits. Le préfet de département est le délégué territorial et l'ordonnateur secondaire de l'agence et chargé à ce titre d'organiser les appels à projets.

En référence au plan national de développement de la videoprotection sur la voie publique, le FIPD a été mobilisé dès 2007 pour financer 309 projets de videoprotection pour un montant de 13,4 millions d'euros. En 2008, 304 projets ont été financés pour un montant de 10,3 millions d'euros, ce qui représente environ 27% des crédits engagés sur le FIPD.

Comme en 2008, ce fonds est constitué en 2009 d'un montant prélevé sur le produit des amendes forfaitaires de la police de la circulation à hauteur de 35 millions d'euros (adopté en LFR 2008) ainsi que des reliquats de crédits de 2008 (2 millions d'euros).

Les orientations liées à l'utilisation du FIPD s'inscrivent globalement dans la continuité de celles fixées en 2008 avec la confirmation du soutien porté au développement de la videoprotection et un resserrement sur les actions de prévention à caractère éducatif et social les plus aptes à contribuer à la réduction de la délinquance et mises en œuvre dans un cadre partenarial.

L**es projets de vidéo-protection sur la voie publique, au profit des actions conduites principalement par des collectivités locales**, sont éligibles au FIPD à la triple condition suivante :

- réalisation d'une étude préalable, associant obligatoirement la direction départementale de la sécurité publique ou le groupement de gendarmerie ainsi que le SZSIC territorialement compétents ;

- justification de l'intérêt opérationnel du dispositif en termes de sécurité au regard du taux de délinquance du territoire concerné ou pour des motifs tenant à la surveillance du trafic routier ou à la protection de certains sites ;

- qualité technique de l'installation permettant un raccordement du centre de supervision urbain (CSU-CSV) aux services de sécurité publique dans des conditions de fonctionnement opérationnelles et conformes aux dispositions de l'arrêté du 3 août 2007 portant définition des normes techniques des systèmes de vidéosurveillance.

Comme pour les études préalables faisant appel à un prestataire extérieur, la participation de l'Etat via le FIPD aux frais d'installation ou d'extension des systèmes de videoprotection ne pourra excéder un taux de 50%. **Les dépenses de fonctionnement et de maintenance restent à la charge du propriétaire du dispositif.**

Pour leur part, les projets de raccordement des centres de supervision urbaine (CSU-CSV) des communes aux services de police ou de gendarmerie (déport d'images) peuvent être financés à hauteur de 100 % sur les crédits déconcentrés du FIPD. Ces dépenses incluent les travaux liés au raccordement, l'acquisition du matériel informatique nécessaire au déport d'images ainsi que la location de la ligne assurant la liaison, celle-ci étant financée la première année par le FIPD, puis par les services de police ou de gendarmerie compétents au cours des années suivantes.

Une circulaire du secrétaire général du CIPD précise chaque année les orientations des crédits (actions éligibles) et leurs conditions de mise en œuvre. Pour 2009, elle devrait être diffusée dans le courant du mois de janvier.

En tout état de cause, il appartient aux préfets de département de valider les projets qui pourront bénéficier d'un soutien du FIPD, compte tenu des orientations fixées par le CIPD et déclinées dans le plan départemental de prévention de la délinquance.

5.2 FINANCEMENT PRIVE DES SYSTEMES PUBLICS

- **La délégation de service public**

La délégation de service public, et plus particulièrement la concession, permet à une personne publique de confier à une autre personne publique ou privée, la construction d'installations destinées à un service public dont cette dernière assure l'exploitation contre rémunération substantiellement liée aux résultats de l'exploitation du service.

En matière d'exercice de pouvoirs de police, notamment sur la voie publique, la jurisprudence du Conseil d'État a fixé un principe d'interdiction des délégations.

Ainsi, à chaque fois que la vidéosurveillance est mise en œuvre pour une activité de police sur la voie publique, elle doit être gérée directement par l'autorité compétente qui peut seule obtenir l'autorisation préfectorale requise par l'article 10 de la loi du 21 janvier 1995.

De plus, les entreprises privées habilitées par arrêté préfectoral à exercer des prestations de vidéosurveillance ne peuvent remplir leur mission exclusivement dans un but de sécurité ou de gardiennage de biens meubles ou immeubles ainsi que pour la sécurité des personnes se trouvant dans ces immeubles.

Les personnes publiques ne peuvent donc recourir à une réalisation et l'exploitation de leur système par la voie d'une délégation de service public qu'à la double condition que le système:

- n'est pas institué pour l'exercice de pouvoir de police,
- ne sert qu'à la sécurité ou au gardiennage de biens meubles ou immeubles ainsi que pour la sécurité des personnes se trouvant dans ces immeubles

- **L'offre de concours**

L'offre de concours est un contrat en vertu duquel une personne qui a intérêt à la réalisation de certains travaux publics met, à la disposition de la personne publique, des moyens (financiers, immobiliers) facilitant, voire permettant, la réalisation des travaux.

Ce contrat peut être conclu lorsque, par exemple, pour des zones excentrées, il est sollicité des citoyens ou des entreprises l'établissement d'installation pour la vidéosurveillance sur les voies publiques ou des lieux ouverts au public.

L'offre de concours est un acte volontaire de la part de la personne participant à la réalisation du système. Il ne s'agit ni d'une taxe, ni d'une rémunération pour service rendu. Elle ne peut être conclue que pour des frais d'investissement.

Au risque d'être qualifiée de participation indue, l'offre de concours ne peut être obtenue dans le cadre de l'instruction d'une autorisation d'urbanisme de la part d'un pétitionnaire

- **Contrat de partenariat (Partenariat Public Privé)**

Le contrat de partenariat est un contrat par lequel une personne publique confie à un tiers, pour une période déterminée en fonction de la durée d'amortissement des investissements ou des modalités de financement retenues, une mission globale relative au financement d'investissements immatériels, d'ouvrages ou d'équipements nécessaires au service public, à la construction ou transformation des ouvrages ou équipements, ainsi qu'à leur entretien, leur maintenance, leur exploitation ou leur gestion, et, le cas échéant, à d'autres prestations de services concourant à l'exercice, par la personne publique, de la mission de service public dont elle est chargée.

L'équipement ainsi créé et entretenu est la propriété du partenaire privé qui le loue à la personne publique qui exerce directement sa mission de service public ou d'intérêt général. En fin de contrat, il peut être contractuellement prévu un droit d'acquisition de tout ou partie de l'équipement.

Le contrat de partenariat prévoit une analyse de la performance de la prestation fournie par le cocontractant de l'administration et permet de moduler l'étendue de sa rémunération ou d'adapter l'équipement au besoin.

Le recours au contrat de partenariat est limité au cas soit, d'urgence soit, de complexité du projet. Dans les deux cas, il convient que le contrat de partenariat présente un avantage économique pour la personne publique par rapport aux autres formes de contrats possibles de réalisation et de financement.

5.3 LA MUTUALISATION

- **Mutualisation de tout ou partie des systèmes.**

Pour les personnes privées, la possibilité de mutualisation des moyens de protection a été consacrée par le décret n° 97-46 relatif aux obligations de surveillance ou de gardiennage incombant à certains propriétaires, exploitants ou affectataires de locaux professionnels ou commerciaux. Les systèmes de vidéoprotection font partie de ces moyens et la mutualisation de réseau, de centre de supervision et des personnels est souvent pratiquée dans les ensembles commerciaux.

Pour les collectivités territoriales, outre le recours aux établissements public de coopération intercommunale dans les conditions de l'article L.5211-60 du code général des collectivités territoriales, la mutualisation de moyens et de personnels peut être opérée dans le cadre de convention ou d'entente.

- **Mutualisation des usages.**

Une installation de vidéoprotection repose nécessairement sur un réseau de collecte et de transmission. Ce réseau privé peut être construit à partir d'infrastructures telles que fourreaux ou fibres d'un réseau existant de communications électroniques.

Dans les zones d'activité, les infrastructures établies pour l'accueil des réseaux d'opérateur de téléphonie peuvent être mises à la disposition des structures créées entre les propriétaires ou exploitants des sites privés ou sur les voiries tertiaires gérées par des personnes privées.

Pour les collectivités locales qui mettent en place un des réseaux d'initiative publique une réflexion sur un tracé adapté aux besoins en matière de vidéoprotection peut précéder le déploiement. Il est à noter que si les installations de vidéoprotection ne sont pas éligibles au bénéfice de subventions européennes, en revanche l'établissement de réseaux de communications électroniques d'initiative publique peut bénéficier de fonds structurels européens et également d'éventuelles aides spécifiques votées aux niveaux régional et départemental.

6 FICHE N°6 : L'EXPLOITATION ET L'ACCES AUX IMAGES, PROTOCOLES D'EXPLOITATION ET D'EXPORTATION

Fiche n°6

L'exploitation et accès aux images, protocoles d'exploitation et d'exportation

6.1 L'ACCES AUX IMAGES

Tous les locaux abritant un enregistreur, un poste de pilotage ou un écran de visualisation doivent être protégés physiquement par un contrôle d'accès. Tous les systèmes informatiques doivent également être inaccessibles sans un nom d'utilisateur et un mot de passe. L'accès aux images est autorisé seulement :

- Aux personnes habilitées,
- Aux personnes ayant fait valoir leur droit d'accès à l'image, dans les conditions prévues par la loi.

Toute personne qui souhaite accéder aux images doit en formuler la demande auprès du chef de salle préciser le cadre de sa demande (motivations, date, plage horaire...). La demande acceptée, le chef de salle ou l'opérateur désigné par le chef de salle affiche la vidéo sur un moniteur. A cet effet, il est préconisé de disposer d'une salle dédiée à ce type de relecture ou de le faire dans le bureau du chef de salle par exemple.

Les images visées sont les images stockées dans un enregistreur numérique ou pour les installations les plus anciennes sur des cassettes vidéo. Ces images doivent faire l'objet d'une protection particulière.

Il appartient au responsable du système de fixer les conditions de protection des images. Aucune mesure particulière n'est imposée par la loi sur ces conditions et pour les systèmes soumis à la loi de 1995 il appartient à la commission départementale et au préfet de juger si les mesures de protection des images prises sont suffisantes ou non.

- **Une séparation des enregistrements et des images en temps réel**

Il est important de noter que la personne ne doit pas pouvoir visualiser d'autres vidéos (comme le mur d'images par exemple). Dans le cas d'un système supervisé il est préconisé de créer trois salles, chacune de ces salles ayant une utilisation particulière. Il s'agit là d'une organisation optimale pouvant être simplifiée au regard des contraintes spécifiques à chaque projet.

- Une salle d'exploitation

Cette salle est destinée au visionnage des images en temps réel par les opérateurs. Elle est équipée de postes de travail et d'un mur d'images. Il est préconisé que les opérateurs n'aient pas accès aux enregistrements ou a minima qu'ils n'aient pas la possibilité d'effectuer un transfert des images enregistrées de l'enregistreur vers un autre support. Le poste de travail doit donc être réduit à l'essentiel : un clavier, un écran, un téléphone. Tous les autres équipements sont installés dans une salle technique voisine.

- Une salle technique

La salle technique abrite tous les équipements techniques liés au système : ordinateurs, enregistreurs, serveurs, tableau électrique…

- Une salle de relecture

L'existence d'une salle spécifiquement dédiée à la relecture permet une sanctuarisation des enregistrements. En organisant de cette façon un système on se donne la possibilité de

contrôler de façon efficace les accès aux enregistrements. Par ailleurs, la relecture se fait souvent en présence des services de police et cette activité peut perturber le travail des opérateurs lorsqu'elle a lieu dans la même salle que l'exploitation.

- **Une protection de tous les locaux abritant des équipements et des images**

De façon générale les locaux dédiés à la vidéoprotection doivent être protégés, c'est-à-dire dotés d'une alarme anti-intrusion. Il est également recommandé d'installer un système vidéo à l'entrée du CSU. Tous les locaux, c'est-à-dire le CSU et les locaux techniques doivent être équipés de serrures de sûreté et de portes offrant des capacités de résistance à l'effraction suffisantes. Un système de contrôle d'accès permettant de définir des catégories d'usagers et des classes d'accès sera prévu et permettra de définir qui a accès à quelle pièce.

- **Une limitation des accès aux images**

Qu'il s'agisse des images en temps réel ou des enregistrements il convient de réduire au maximum le nombre de personnes ayant un accès aux images. Seul le personnel affecté à la vidéoprotection doit pouvoir pénétrer dans les locaux. Il est donc important de prévoir dans le règlement intérieur dans quelles conditions s'effectuent les travaux d'entretien et de maintenance des locaux ou les visites.

6.2 L'EXPLOITATION DES IMAGES

Les images enregistrées peuvent être :

- Visualisées pour réaliser une levée de doute par exemple,
- Imprimées pour permettre l'identification d'un individu,
- Exportées vers les services de sécurité.

Pour faciliter l'exploitation des images, il convient de formuler des demandes précises auprès du chef de salle. En effet, trop souvent les demandes sont imprécises notamment sur les tranches horaires ou le lieu de commission des faits. Cette imprécision est grande consommatrice de temps et distrait un opérateur de sa fonction essentielle pendant parfois plusieurs heures

6.2.1 CRITÈRES TECHNIQUES

Les images imprimées doivent l'être :

- sur un format suffisamment grand (format A5 au minimum),
- avec une résolution permettant de respecter la même qualité que celle affichée à l'écran.

En ce qui concerne les images exportées, la séquence précise doit être définie au préalable.

Il n'est pas imposé que la relecture de la vidéo puisse se faire avec un applicatif standard du marché. Dans certain cas où les vidéos pourraient mettre en péril la sécurité du site ou porter atteinte à la liberté d'aller et de venir des personnes filmées, il peut être nécessaire d'empêcher la relecture des vidéos via un applicatif standard du marché, l'enregistreur utilise alors un format propriétaire propre au constructeur. Il est indispensable dans ce cas,

de fournir le logiciel adéquat pour la relecture de la séquence (sur un autre support que celui contenant la vidéo).

Il est conseillé que le support utilisé pour l'exportation de la vidéo ne soit pas réinscriptible pour éviter que certaines personnes puissent effacer ou modifier les fichiers exportés (comme les CD-rom ou DVD - rom). Toutefois pour des volumes plus importants il peut être plus convenable d'exporter sur « clés USB » ou disques durs. Il faudra toutefois faire attention de limiter ce type de support pour éviter le risque de perte ou de modification des fichiers modifiés.

Dans certains cas particulier, il peut être recommandé de signer numériquement les vidéos afin de garantir leur authenticité. (watermarked)

6.2.2 LE CADRE JURIDIQUE

Jusqu'à l'entrée en vigueur de la loi n° 2007-297 du 5 mars 2007 relative à la prévention de la délinquance, l'accès aux images enregistrées ou non était limité aux cas de police judiciaire.

Dans le cadre des enquêtes, la communication s'effectue au visa des articles 60-1 et l'article 77-1-1 du code de procédure pénal applicables respectivement aux procédures de flagrance et enquêtes préliminaires.

En cas d'information judiciaire, les réquisitions sont formulées en application de l'article 99-3 du code de procédure pénal.

Ces textes font obligation à toute personne, tout établissement ou organisme privé ou public ou toute administration publique qui sont susceptibles de détenir des documents intéressant l'enquête, y compris ceux issus d'un système informatique ou d'un traitement de données nominatives, de remettre ces documents, notamment sous forme numérique, sans que puisse lui être opposée, sans motif légitime, l'obligation au secret professionnel.

Le fait de s'abstenir de répondre dans les meilleurs délais à cette réquisition est puni d'une amende de 3 750 Euros et commission rogatoire. Mais, il appartient toujours à l'autorité publique ou à la personne titulaire de l'autorisation préfectorale de s'assurer de la pertinence des images communiquées et d'en consigner la transmission.

La mise à disposition des données doit s'effectuer directement et matériellement entre les mains de l'autorité procédant à la réquisition. En cette matière, la mise à disposition par voie électronique n'est pas autorisée.

Désormais, l'accès aux images et aux enregistrements peut être réalisé en dehors d'enquête de police judiciaire mais sous des conditions strictes énoncées dans un arrêté préfectoral pris après avis de la Commission Départementale des systèmes de vidéosurveillance. En cas d'urgence et d'exposition particulière à un risque d'actes de terrorisme, l'arrêté peut être pris après information du Président de la Commission qui sera toutefois appelée à donner son avis lors de sa prochaine réunion.

Dans tous les cas, l'arrêté doit:

- comporter l'autorisation d'accès donnée aux agents d'un ou plusieurs services déterminés. L'habilitation et l'identification nominative des agents sont préalablement réalisées par les chefs de service ou d'unité concernés,
- Préciser la durée de cette possibilité d'accès,
- Préciser les modalités de transmission des images et d'accès aux enregistrements.

Ces dispositions peuvent être introduite dans l'autorisation initiale ou intervenir postérieurement par un arrêté en fonction de l'évolution des circonstances rendant nécessaire un accès des forces de l'ordre aux images.

6.2.3 LE CAS DES SYSTÈMES SOUMIS AU REGIME JURIDIQUE DE LA LOI DU 21 JANVIER 1995

L'exportation des images sur les systèmes soumis au régime juridique de la loi du 21 Janvier 1995 fait l'objet d'un arrêté du 3 août 2007 portant définition des normes techniques des systèmes de vidéosurveillance. Cet arrêté consultable au journal officiel, permet de fixer des contraintes minimales comme le fonctionnement continu de l'enregistrement lors de l'export, la non dégradation des images lors de l'export, afin de garantir que les images fournies aux force de polices et de gendarmerie sont bien les mêmes que celles enregistrées sur le système, et surtout la nécessité de fournir aux forces de police et de gendarmerie un logiciel permettant la relecture des images si celle-ci est impossible via un applicatif standard du marché.

- **Extrait : " Les flux vidéo stockés issus des caméras qui, compte tenu de leur positionnement et de leur orientation, fonctionnent principalement en plan étroit, à l'exclusion de celles de régulation du trafic routier, ont un format d'image supérieur ou égal à 704 x 576 pixels. Ce format pourra être inférieur si le système permet l'extraction de vignettes de visage d'une résolution minimum de 90 x 60 pixels. "**

  L'objet de l'article 2, cinquième alinéa, est de favoriser l'existence d'images d'une précision satisfaisante pour le travail des enquêteurs. Il pose donc le principe d'un niveau de qualité minimum des images stockées lorsqu'elles sont issues de caméras fonctionnant en plan étroit.

  L'équilibre recherché ici consiste à garantir un bon niveau de qualité des images seulement lorsque c'est nécessaire pour les forces de police et de gendarmerie, sans faire peser des contraintes techniques trop importantes sur les parties du dispositif qui concernent moins directement le travail d'investigation.

  Pour cela, on distingue deux grands types de caméras de vidéosurveillance, celles dont la fonction principale est d'analyser les informations sur les individus ou les objets présents dans le champ des caméras (qui sont dites fonctionner en plan étroit) et celles dont la fonction principale est de fournir une vue globale de la situation (qui sont dites fonctionner en plan large).

  Cette classification appelle deux remarques et mérite d'être illustrée par quelques exemples.

  Tout d'abord, il est entendu que les caméras qui constituent un dispositif de vidéosurveillance ont le plus souvent des missions multiples. Ceci est d'autant plus vrai que certaines caméras sont dotées de fonctions de zoom et d'orientation rapide qui leur permettent d'offrir un plan global et de passer l'instant suivant en plan rapproché. Néanmoins, il reste qu'à chaque caméra est le plus souvent assigné un objectif principal d'exploitation : levée de doute, gestion d'une file d'attente, surveillance d'un objectif sensible, contrôle des flux...

  Il est nécessaire que ces objectifs principaux soient précisés pour chaque caméra dans les dossiers transmis par les opérateurs. Le plus souvent ils doivent permettre de statuer sur la classification des caméras à plan large ou à plan étroit.

  Ensuite, il est légitime de s'interroger sur la corrélation éventuelle entre les caractéristiques techniques en termes de focale ou de zoom des caméras et leur usage en plan large ou plan étroit (telles que ces notions ont été définies ci-dessus). Compte tenu de la diversité des usages de la vidéosurveillance, ce lien ne semble pas être pertinent. En effet, une caméra destinée à garantir la sécurité d'un distributeur automatique de billets ou à sécuriser les entrées-sorties dans un bus peut, du fait de la faible distance à la cible, fonctionner avec une ouverture angulaire importante, alors qu'au sens de l'arrêté du 26 septembre 2006 il s'agit bien, compte tenu de la précision attendue de l'image, d'un fonctionnement en plan étroit. De la même manière, certaines caméras destinées à sécuriser des voies ferrées peuvent fonctionner avec une petite ouverture angulaire mais en plan large au sens de l'arrêté, si elles sont destinées à la régulation du trafic ferroviaire.

La résolution de 704 x 576 correspond au format dit 4 CIF, normalisé dans le domaine de la vidéo, compatible avec les performances de la majorité des caméras installées et constituant la norme haute en matière de définition d'image en attendant la généralisation des caméras dites à haute définition. La définition visée dans cet article concerne les images stockées sur le système d'enregistrement. Ceci implique que toute la chaîne vidéo doit afficher des caractéristiques compatibles avec ces formats d'enregistrement : la résolution des capteurs (caractéristiques techniques des caméras), le format d'image en sortie de caméra, le taux de compression des images lors du transfert et du stockage. Une autre conséquence est que les espaces de stockage doivent être compatibles avec les caractéristiques globales du système. Il est donc important que les spécifications techniques (définition, taux de compression, nombre d'images par seconde, durée de conservation des données, nombre de flux stockés) du système soient précisées ainsi que le calcul menant au dimensionnement des espaces de stockage.

Dans certains cas, il n'est pas nécessaire de disposer d'une image de 704 x 576 pixels pour offrir une résolution satisfaisante des sujets filmés. Les opérateurs ont donc toute latitude pour retenir un format inférieur pour peu que celui-ci propose, dans la zone nominale de prise de vue, une résolution permettant l'identification d'un visage. En particulier, des caméras numériques au format VGA (640 x 480 pixels) qui permettraient l'extraction sur les vidéos enregistrées de vignettes de visage de 90 x 60 pixels conviennent.

Il est certain que la diversité des situations occasionnera inévitablement des cas litigieux ou ambigus pour lesquels la proposition de classification plan large/plan étroit du soumissionnaire pourra apparaître discutable. Pour déterminer de façon pratique les caractéristiques minimales des images stockées, le tableau d'exemples proposé en annexe I doit permettre le plus souvent d'assimiler ces situations à un cas d'usage approchant déjà traité.

" Les autres flux vidéo stockés ont un format d'image supérieur ou égal à 352 x 288 pixels ".

Tous les autres flux vidéo issus des systèmes de vidéosurveillance visés par la loi du 21 janvier 1995, modifiée par la loi du 23 janvier 2006, doivent au minimum être stockés avec une résolution de 352 x 288 pixels, aussi appelé format CIF. C'est notamment le cas des images issues d'un dispositif de régulation du trafic routier.

" Une fréquence minimale de douze images par seconde est requise pour l'enregistrement des flux vidéo issus de caméras installées pour une des finalités mentionnées au II de l'article 10 de la loi du 21 janvier 1995 susvisée, à l'exclusion de celles de régulation du trafic routier, et qui, compte tenu de leur positionnement et de leur orientation, fonctionnent principalement en plan étroit et filment principalement des flux d'individus en déplacement rapide. "

Le nombre d'images par seconde constitue également un paramètre important lorsqu'il s'agit de chercher des éléments précis dans une scène vidéo en mouvement. Il convient pourtant de moduler les exigences en fonction des besoins opérationnels véritables pour ne pas surdimensionner le système de vidéosurveillance inutilement. C'est pourquoi l'exigence de disposer de 12 images enregistrées par seconde ne s'applique qu'aux caméras fonctionnant principalement en plan étroit (cf. article 2, alinéa 5) et parmi celles-ci exclusivement à celles destinées à surveiller des flux de personnes en " déplacement rapide ".

Cette notion fait explicitement référence à des situations où les individus filmés sont, sauf circonstances particulières, en train de marcher sans rencontrer d'obstacle lorsqu'ils traversent la zone de prise de vue. Il est question en particulier de déplacement rapide pour les caméras destinées à filmer un espace de transit dans les lieux publics (couloir de métro, hall d'aéroport, trottoir urbain...). En revanche ne sont pas considérées comme des déplacements rapides les images d'individus en train de franchir une porte ou un tourniquet de métro, ou stationnant dans un hall destiné à l'attente ou au recueil de bagages.

Les cas de figure les plus typiques ou susceptibles de poser problèmes sont évoqués en annexe 2 de l'arrêté du 3 août 2007.

" Pour l'enregistrement des autres flux vidéo, une fréquence minimale de six images par seconde est requise. "

Toutes les autres images visées par la loi du 21 janvier 1995 doivent au minimum être enregistrées à une cadence réelle de 6 images par seconde à partir d'une caméra dont bien entendu la fréquence d'acquisition des images sera d'au minimum 6 images par seconde. Ainsi, il ne serait donc être question de reconstruire artificiellement un flux à 6 images par seconde à partir par exemple d'une séquence initiale à 3 images par seconde. Il en est de même pour un enregistrement à 12 images par seconde.

" Le système de stockage utilisé est associé à un journal qui conserve la trace de l'ensemble des actions effectuées sur les flux vidéo. "

La traçabilité des actions effectuées sur le système est primordiale pour vérifier qu'aucun abus et qu'aucune action de malveillance n'ont été commis. Dans le cas des systèmes d'enregistrement analogique ou des systèmes de vidéosurveillance numériques de moins de huit caméras, un journal qui conserve la trace de l'ensemble des actions effectuées sur les flux (export, modification, suppression...) peut être tenu à la main.

" Pour les systèmes numériques, ce journal est généré automatiquement sous forme électronique. "

Pour simplifier l'opération de journalisation, qui peut être fastidieuse pour de gros systèmes, il faut que, pour les systèmes numériques, cette opération soit automatisée. Il conviendra donc de s'assurer que le système proposé intègre cette fonction et que l'opérateur prévoie dans son plan d'exploitation de la mettre en œuvre.

4. Les contraintes d'interopérabilité

L'arrêté du 03 août 2007 a pour objectif que les techniques de la vidéosurveillance puissent mettre en œuvre de façon concrète les dispositions que la loi du 21 janvier 1995 modifiée a édictées.

Les dispositions de l'article 3 de l'arrêté précité ont pour but de faciliter concrètement l'exploitation des systèmes par les services de police et de gendarmerie.

" Les flux vidéo sont exportés sans dégradation de la qualité. "

La transmission des films vidéo aux forces de police et de gendarmerie nécessite une opération dite " d'exportation ". Il est nécessaire que la qualité des images exportées soit maximale, ce qui implique que le système doit être en mesure d'exporter ses données sans perte de qualité.

Si, lors de l'opération d'exportation, il s'avère nécessaire de modifier le format ou le type de compression des flux vidéo, il conviendra alors de s'assurer que la compression des vidéos exportées ne dégrade pas leur qualité.

Il est donc important de connaître la méthode d'exportation des flux vidéo et, dans le cas où il ne s'agit pas d'une simple copie des données, les caractéristiques de la compression utilisée pour le stockage et l'exportation.

" Pour les systèmes de vidéosurveillance utilisant la technologie analogique, un dispositif détermine la liste des flux exportés, indiquant la date et l'heure des images filmées, leur durée, l'identifiant des caméras concernées, la date et l'heure de l'exportation, l'identité de la personne ayant réalisé l'exportation. "

Il est important de conserver une traçabilité des exportations pour assurer qu'aucun abus ne soit commis. La difficulté de cette mesure pour un système de vidéosurveillance analogique, et dans une moindre mesure pour les systèmes numériques de moins huit caméras, est parfois le manque d'automatisation du système. Il est alors nécessaire d'intégrer dans la procédure d'exportation de flux vidéo la constitution manuelle d'un journal des différentes opérations effectuées sur le système. Cette action de constitution d'un journal doit en particulier permettre de pouvoir identifier la ou les personnes qui ont exporté les flux vidéo.

" Pour les systèmes de vidéosurveillance utilisant la technologie numérique, un journal électronique des exportations, comportant les informations citées à l'alinéa précédent, est généré automatiquement. "

De même que pour les systèmes analogiques, la traçabilité des exportations est, pour les systèmes numériques, primordiale. L'avantage d'un système numérique est la possibilité d'automatiser des actions. Ainsi, pour assurer l'exactitude des informations contenues dans la liste des flux exportés, il suffit de créer un " journal " électronique constitué automatiquement par le système.

" Le système d'enregistrement reste en fonctionnement lors de ces opérations d'exportation. "

L'exportation de données ne doit en aucun cas diminuer les capacités d'un système de vidéosurveillance. En effet, il serait fortement dommageable que, lors de l'exportation d'images vidéo, un événement grave se produise et qu'il soit impossible d'enregistrer les flux vidéo y afférents. Le fait que le système d'enregistrement reste en fonctionnement lors des opérations d'exportation vise en particulier à interdire l'extraction des unités de stockage du système durant les phases d'investigation si cette action interdit la poursuite du fonctionnement normal du système. Il est donc important de vérifier que la procédure d'exportation soit conforme à cette exigence. Une méthode simple consiste à prévoir des supports de stockage supplémentaires afin de remplacer ceux qui seraient temporairement extraits du système.

" Le support physique d'exportation est un support numérique non réinscriptible et à accès direct, compatible avec le volume de données à exporter. Dans le cas de volumes importants de données à exporter, des disques durs utilisant une connectique standard pourront être utilisés. Pour les systèmes numériques de vidéosurveillance, un logiciel permettant l'exploitation des images est fourni sur support numérique, disjoint du support des données. "

Le système de stockage des enregistrements vidéo doit être doté de la capacité à exporter des films et des photos vers un support non réinscriptible, qui, en l'état actuel, sera le plus souvent du type graveur de CD ou de DVD. Tous les systèmes doivent donc disposer de cette fonctionnalité. Ceci implique notamment que les clés USB (qui constituent un support réinscriptible) ne peuvent être le seul support d'exportation sur un tel système.

Le support doit de plus être à accès direct, c'est-à-dire que les informations doivent être accessibles sans avoir à parcourir séquentiellement l'ensemble du support. En particulier, les cassettes DAT ne peuvent constituer un support d'exportation valable.

Toutefois, il est parfois nécessaire d'exporter une quantité importante de données. Dans ce cas exclusivement, il est autorisé d'utiliser des disques durs, qui permettent une plus grande capacité de stockage. Cette possibilité vient s'ajouter à la capacité d'export sur des supports non réinscriptibles, qui constituent dans tous les cas le moyen par défaut de transmission des données vers les forces de sécurité.

" Le logiciel permet :

" 1° La lecture des flux vidéo sans dégradation de la qualité de l'image ;

" 2° La lecture des flux vidéo en accéléré, en arrière, au ralenti ;

" 3° La lecture image par image des flux vidéo, l'arrêt sur une image, la sauvegarde d'une image et d'une séquence, dans un format standard sans perte d'information ;

" 4° L'affichage sur l'écran de l'identifiant de la caméra, de la date et de l'heure de l'enregistrement ;

" 5° La recherche par caméra, date et heure. "

Les flux vidéo sont exportés pour être traités par les services de police ou de gendarmerie. Les caractéristiques mentionnées doivent donc être intégrées dans le logiciel de lecture, fourni sur un support numérique séparé distinct de celui des images, par l'opérateur aux services enquêteurs en même temps que les images.

Fiche n°7

La constitution du dossier de demande d'autorisation préfectorale

7 FICHE N°7 : LA CONSTITUTION DU DOSSIER DE DEMANDE D'AUTORISATION PREFECTORALE

La demande d'autorisation préfectorale ne doit être sollicitée que pour les dispositifs visionnant la voie publique et les lieux ou établissements recevant du public et qui ne conduisent pas à des fichiers structurés avec données nominatives pour l'identification des personnes.

C'est le décret modifié n° 96.926 qui définit le contenu du dossier à déposer en Préfecture.

Cette fiche répond aux trois questions suivantes :

- Quel est le contenu du dossier ?
- Quel est le processus d'instruction ?
- Quel est le suivi du dossier ?

7.1 QUEL EST LE CONTENU DU DOSSIER ?

Dans un souci d'harmonisation du travail des commissions départementales et des services des préfectures en charge de la gestion de ces demandes, le contenu du dossier a été profondément simplifié par le décret modifié n° 96.926. qui précise :

- au premier alinéa de son article 1er , que la liste des pièces constitutives du dossier administratif et technique accompagnant la demande d'autorisation est exhaustive,
- au deuxième alinéa de l'article 3, que tout complément d'information sollicité par la commission départementale des systèmes de vidéosurveillance ne peut porter que sur les pièces du dossier de demande d'autorisation.

Le dossier à constituer sera différent selon que l'on se trouve dans le cadre d'une des quatre situations suivantes :

- Le dispositif de vidéosurveillance visionne la voie publique.
- Le dispositif visionne un lieu ou établissement recevant du public et comporte huit caméras ou plus.
- Le dispositif visionne un lieu ou établissement recevant du public et comporte moins de huit caméras.
- La demande porte sur la création d'un périmètre vidéosurveillé.

7.1.1 CAS N°1: LE DISPOSITIF VISIONNE LA VOIE PUBLIQUE

C'est le cas où le dossier est le plus complexe. Il va comporter :

- Le CERFA dont le modèle figure en annexe et qui rassemble les informations essentielles.

- Un rapport de présentation dont le but principal est d'exposer les finalités, c'est-à-dire les raisons justifiant la mise en œuvre du dispositif (le niveau de risque, par exemple de délinquance de proximité dans la zone concernée, et les moyens techniques qui doivent respecter les normes de l'arrêté du 3 août 2007).
  Les caractéristiques générales du système qu'il s'agisse des moyens d'acquisition (caméras fixes ou mobiles, nombre de caméras), de transmission des images puis de visualisation et de stockage.

- Le plan de masse :

  Ce plan doit permettre de vérifier la non visualisation de l'intérieur des immeubles d'habitation par les caméras visualisant la voie publique.
  Il doit indiquer : les bâtiments du pétitionnaire et les bâtiments appartenant à des tiers qui se trouveraient dans le champ de vision des caméras avec l'indication de leurs accès et de leurs ouvertures.

  Ce plan doit bien sûr être lisible et clair. Il est important de faire figurer sur ce plan une représentation des masquages qui seront programmés dans les caméras pour empêcher la surveillance des parties privées (la plupart des caméras actuellement sur le marché permettent de le faire).

- Le plan de détail

  Ce plan à l'échelle suffisante doit indiquer :

  - nombre et l'emplacement des caméras.
  - les zones couvertes par celles-ci.

-
-

  Il s'agit de vérifier que le champ de vision des caméras ne porte pas atteinte à l'intimité de la vie privée (cas de caméras qui visionneraient l'intérieur d'une cabine d'essayage).

- La description du dispositif prévu pour la transmission, l'enregistrement et le traitement des images.

  - Description des moyens d'enregistrement
  - Description des réseaux de transmission : fibre, cuivre, hertzien…,
  - Description des modalités d'exploitation des images : modalités de renvoi et d'exploitation des images en temps réel et différé :
    - Stockage local, avec ou sans possibilité de consultation à distance,
    - Centralisation vers un local technique.

  Si certaines de ces informations peuvent être renseignées dans les rubriques 4.5. et 7 du CERFA, concernant les dispositifs de voie publique, un document de description plus élaboré est recommandé.

- La description des mesures de sécurité qui seront prises pour la sauvegarde et la protection des images éventuellement enregistrées.

  Moyens techniques dédiés à la sécurisation des installations : portes blindées, vidéo, alarmes (anti feu, anti intrusion).

  - Procédures de sécurité dédiées à la sécurisation des installations.

  Un document spécifique n'est pas à priori nécessaire, ces informations devant figurer dans le CERFA à la rubrique 8 mais, s'agissant d'un dispositif de voie publique, un document plus complet est toutefois recommandé.

- Les modalités de l'information du public :

  Le but est de faire en sorte que toute personne susceptible d'être filmée en soit prévenue. Le dossier doit donc contenir :

- un modèle de l'affiche ou panonceau .Concernant la voie publique le panonceau qui sera utilisé doit contenir un pictogramme représentant une caméra.
- Une description des modalités : nombre d'affiches ou panonceaux, l'emplacement prévu de leur implantation. Cette description est prévue à la rubrique 9 du CERFA et le renseignement de cette rubrique suffit mais en cas de multiples implantations pour les dispositifs importants, un document décrivant de façon détaillée ce type d'information peut être apprécié.

- Le délai de conservation des images avec s'il y a lieu les justificatifs nécessaires.

  - Le délai maximum est d'un mois. Il n'y a pas de délai minimum mais si un dispositif apparaît justifié par le niveau de délinquance de proximité, il n'aurait guère de sens si les images n'étaient pas conservées le temps minimum pour s'assurer de l'ouverture d'une procédure judiciaire. (Celle-ci permettra de conserver ensuite les images le temps nécessaire). Les services de sécurité estiment en général à 7 jours le délai de sécurité.

  Cette information figurant dans le CERFA à la rubrique 5 qu'il faut obligatoirement compléter, aucun document sur ce point n'a besoin d'être joint au dossier.

- La désignation du personnel concerné par l'installation.

  - Désignation de la personne ou du service responsable du système,
  - Désignation de la personne responsable de la maintenance,
  - Indication sur la qualité des personnes chargées de l'exploitation du système et susceptibles de visionner les images.

  L'ensemble de ces informations doit être renseigné dans le CERFA en complétant les rubriques 2, 6, 10 et, le cas échéant 7. Il n'y a par conséquent aucun document à fournir. S'agissant de la voie publique une information complémentaire concernant les opérateurs (recrutement, formation…) sera bien sûr appréciée. (Une note explicative peut suffire).

- Les consignes générales données aux personnels d'exploitation du système pour le fonctionnement de celui-ci et le traitement des images.

  Si les indications principales figurent déjà dans le CERFA, s'agissant de la voie publique, il est recommandé de fournir une note d'information complémentaire répondant aux points suivants :

  - Règlement intérieur ou notes internes :
    - Personnel habilité à accéder aux images
    - Conditions d'accès du personnel chargé de la maintenance,
    - Conditions d'accès des visiteurs.
  - Horaires de fonctionnement.
  - Conditions d'accès des services en situation normale et en cas d'urgence.

- Les modalités du droit d'accès des personnes intéressées.

  L'information figure dans le CERFA. S'agissant de la voie publique, une information sur les règles internes mises en place pour permettre aux personnes intéressées d'accéder aux images enregistrées les concernant peut être appréciée, dans ce cas elle pourra faire l'objet d'une note complémentaire.

- La justification de la conformité du système de vidéosurveillance aux normes techniques de l'arrêté du 3 août 2007 :

  Deux situations se présentent :

- L'installateur est certifié dans les conditions fixées par arrêté du ministre de l'Intérieur.

Dans ce cas, le CERFA mentionne l'identité de l'installateur et son numéro de certification. L'installateur doit remettre au maître d'ouvrage une attestation de conformité ; elle suffit à en justifier et, dans ce cas, un rapport technique n'est pas requis.

(Précision : cette certification est assurée conjointement par l'AFNOR et le CNPP conformément à un règlement approuvé.)

- L'installateur n'est pas certifié

Le maître d'ouvrage joint au dossier le questionnaire (p.j. n°) rempli par l'utilisateur. Les services préfectoraux et la commission départementale apprécient si ces indications sont suffisantes dans le cas concerné.

7.1.2 CAS N°2 : LE DISPOSITIF DE VIDEOSURVEILLANCE VISIONNE UN LIEU OU ETABLISSEMENT RECEVANT DU PUBLIC ET COMPORTE HUIT CAMERAS OU PLUS

Le dossier comprendra les mêmes pièces et informations que ci-dessus **sauf l**e plan de masse (ce dernier est en effet justifié parce qu'il permet de savoir quelles zones privatives d'immeubles le dispositif pourrait visionner, il n'a donc de sens que si le dispositif visionne la voie publique où peuvent se trouver de tels immeubles).

Précision : Les modalités d'information du public sur l'existence du dispositif seront plus précises et comporteront la description du panneau d'information et de son ou de ses emplacements.

En ce qui concerne l'emplacement, chacun comprend qu'un panneau informatif devra être situé à l'entrée du lieu et le, cas échéant, du parking associé afin que les tiers choisissent en toute connaissance de cause d'y entrer ou non.

7.1.3 CAS N°3 : LE DISPOSITIF VISIONNE UN LIEU OU ETABLISSEMENT RECEVANT DU PUBLIC ET COMPORTE MOINS DE HUIT CAMERAS

Dans ce cas, qui, à la fois, présente a priori le moins de risques d'atteinte à la vie privée et correspond au plus grand nombre de demandes, le dossier sera simplifié.

Il ne comportera pas :

- Le rapport de présentation, l'exposé succinct des finalités, indications des risques et caractéristiques du système figurent déjà sur le CERFA,
- Le plan de masse exigé pour la seule voie publique,
- Le plan de détail indiquant nombre, implantation des caméras et zones couvertes par celles-ci. Le nombre de caméras est indiqué dans le CERFA.

Il est par conséquent recommandé de renseigner attentivement toutes les rubriques du CERFA et de joindre simplement le modèle d'affiche d'information du public ainsi que le questionnaire de conformité du système si l'installateur n'est pas certifié. S'il est certifié, l'indication dans le CERFA doit suffire mais l'attestation remise de conformité de l'installateur doit pouvoir être produite à tout moment.

7.1.4 CAS N°4 : LA DEMANDE PORTE SUR UN PERIMETRE VIDEOSURVEILLE

Lorsque le système de vidéosurveillance porte sur un ensemble immobilier ou foncier de grande dimension ou complexe, il peut être demandé la création d'un périmètre vidéosurveillé.

Cette possibilité nouvelle ouverte par le décret modifié n° 96.926 concerne des types de situations différentes :

A titre d'exemples :

- Sur la voie publique, il pourra s'agir d'une place centrale avec les rues qui y conduisent ou un centre piétonnier comportant des traverses ou de nombreuses petites rues,

- Dans un programme immobilier ce pourra être le fait d'un vaste projet devant comporter étude de sûreté ou d'un centre commercial comportant de nombreuses enseignes.

Dans ces cas, le nombre et l'implantation des caméras peuvent en effet être sujets à évolution.

Le dossier sera alors profondément différent.

- Le rapport de présentation devra établir non seulement les finalités, et, les risques que l'on devra réduire mais aussi, en fonction du site, l'intérêt de pouvoir adapter le nombre et l'implantation des caméras.

- Sera fourni un plan portant simple délimitation du périmètre ce document se substitue en fait aux plans de masse et de détail prévus pour les dispositifs de voie publique et/ ou pour ceux de huit caméras ou plus.

- Le CERFA ne comportera pas d'indication sur le nombre de caméras, ni sur leur emplacement, c'est la rubrique 4.2 qu'il faut renseigner.

Les autres informations : description du dispositif, mesures de sécurité pour la sauvegarde des images, modalités d'information du public, délai de conservation des images, désignation du personnel, consignes d'exploitation, modalités du droit d'accès, seront évidemment fournies.

Point commun aux quatre cas

Dans les quatre cas ci-dessus la liste des pièces et informations indiquées est limitative tant pour les Préfets que pour les commissions départementales.

En introduction du § traitant de la constitution du dossier, sont rappelés les deux alinéas du décret posant le principe du caractère limitatif des pièces ou informations à fournir. Par exemple, si le plan de détail (lorsqu'il est requis) est trop petit pour être lisible, la commission peut demander des précisions sur ce plan. S'il manque l'indication de l'emplacement des affiches ou panonceaux pour un établissement recevant du public, le dossier sera considéré comme incomplet et le préfet vous demandera de compléter cette information.

Les cas particuliers :

Ils sont visés par les articles 2 à 4 du décret :

Article 2 du décret n°96-926 du 17/10/1996

« La demande d'autorisation d'un système de vidéosurveillance mis en œuvre par un service de l'Etat est présentée par le chef de service responsable localement compétent. Dans le cas où des raisons d'ordre public et dans celui où l'utilisation de dispositifs mobiles de surveillance de la circulation routière s'opposent à la transmission de tout ou partie des indications mentionnées aux 2° et 3° de l'article 1er, le dossier de demande d'autorisation mentionne les raisons qui justifient l'absence de ces indications. »

Article 3 du décret n°96-926 du 17/10/1996

« Dans le cas où des raisons impérieuses touchant à la sécurité des lieux où sont conservés des fonds ou valeurs, des objets d'art ou des objets précieux s'opposent à la transmission par le pétitionnaire de la totalité des informations prévues aux 2° et 3° de l'article 1er, la demande d'autorisation mentionne les raisons qui justifient l'absence de ces informations. Le président de la commission peut déléguer auprès du pétitionnaire un membre de la commission pour prendre connaissance des informations ne figurant pas au dossier. »

Article 4 du décret n°96-926 du 17/10/1996

« La demande d'autorisation d'un système de vidéosurveillance mis en œuvre par un service, établissement ou entreprise intéressant la défense nationale est présentée par la personne responsable du système. Dans le cas où la protection des installations, du matériel ou du secret des recherches, études ou fabrications dont la sauvegarde est en cause s'oppose à la transmission de tout ou partie des informations prévues à l'article 1er (2° à 10°), le dossier de demande d'autorisation mentionne les raisons qui justifient l'absence de ces informations. Le préfet peut demander au ministre dont relève le demandeur de se prononcer sur les raisons invoquées. »

Il en résulte que le dossier peut être allégé pour des motifs d'ordre public (protection d'un bâtiment présentant une sensibilité particulière comme une préfecture par exemple), ou en cas de dispositifs mobiles (services de l'Etat), ou pour assurer la confidentialité des mesures de protection dans certains lieux (principalement les banques), ou pour des installations intéressant la défense nationale.

7.2 LA PROCEDURE

La demande d'autorisation préalable à l'installation d'un système de vidéosurveillance dans le cadre de l'article 10 de la loi du 21 janvier 1995 doit être déposée à la préfecture du lieu d'implantation ou, à Paris, à la préfecture de police.

- Cas particuliers :
  - La demande d'autorisation d'un système de vidéosurveillance mis en œuvre par un service de l'Etat est présentée par le chef de service responsable localement.
  - La demande d'autorisation d'un système de vidéosurveillance mis en œuvre par un service, établissement ou entreprise intéressant la défense nationale est présentée par la personne responsable du système.

Chaque préfecture dispose d'une personne qualifiée pour instruire le dossier. Si le dossier n'est pas complet, l'autorité préfectorale peut demander au pétitionnaire de la compléter. Elle lui délivre un récépissé lors du dépôt du dossier complet.

Lorsque le dossier est complet, il est examiné en commission qui émet un avis, favorable ou défavorable.

Le préfet prend ensuite une décision d'autoriser ou non le système. Sa décision est susceptible de recours.

Le silence gardé pendant plus de quatre mois sur la demande d'autorisation préalable à l'installation d'un système de vidéosurveillance vaut décision de rejet.

Le décret du apporte deux modifications à la procédure antérieure :

- Pour mieux assurer l'étude du risque d'insécurité auquel veut répondre le dispositif, le décret stipule que la commission départementale entend obligatoirement le chef de service de la police ou de la gendarmerie territorialement compétent.

La préfecture aura transmis à ce dernier, dès qu'il aura été complet, le dossier reçu et le référent sûreté l'aura étudié. Souvent, s'agissant d'un dispositif de voie publique ou d'un dispositif important, il aura été associé à sa conception. La commission sera donc mieux éclairée sans alourdissement de la procédure.

- Normalement, la commission départementale doit de prononcer dans le délai de 3 mois. Si, s'étant réunie, elle demande un délai supplémentaire d'un mois, ce délai est de

droit. Passé le délai de 3 mois, ou exceptionnellement de quatre mois, l'avis de la commission est réputé donné et le Préfet prend la décision qu'il lui paraît appropriée.

Si le silence de l'administration a abouti à un refus implicite et que le Préfet entend donner l'autorisation, il prend un arrêté rapportant le rejet implicite et donnant l'autorisation qui lui paraît justifiée.

7.3 SUIVI DE L'INSTALLATION

Le suivi comporte information de l'administration et possibilité de contrôle par celui-ci.

7.3.1 LES INFORMATIONS À DONNER À LA PRÉFECTURE

Préalablement à la mise en service, le bénéficiaire de l'autorisation doit informer le Préfet de la mise en place des caméras.

Dans le cas où a été donnée une autorisation de périmètre vidéosurveillé (et donc le nombre et l'implantation de caméras ne sont pas définis par l'autorisation), le bénéficiaire informera le Préfet, préalablement à la mise en service du nombre et de l'emplacement des caméras installées. Quand il les déplacera ou en installera de nouvelles, il en informera de nouveau le Préfet.

7.3.2 LE CONTRÔLE SUR PLACE

La commission départementale peut à tout moment exercer, sauf en matière de défense nationale, un contrôle sur les conditions de fonctionnement des dispositifs autorisés en application des mêmes dispositions. Elle émet, le cas échéant, des recommandations et propose la suspension des dispositifs lorsqu'elle constate qu'il en est fait un usage anormal ou non conforme à leur autorisation.

8 FICHE N°8 : COMMENT CHOISIR UN BUREAU D'ETUDES OU UN CABINET CONSEIL ?

Fiche n°8

Comment choisir un bureau d'études ou un cabinet conseil ?

En fonction de la taille des projets et des compétences dont il dispose ou ne dispose pas en interne, le maître d'ouvrage se dispense ou non des services d'un bureau d'études ou d'un cabinet conseil.

D'une manière générale :

- il est préférable de rédiger en interne avec les partenaires éventuels, l'étude du besoin, l'analyse juridique et éventuellement l'appréciation de l'acceptabilité.

  Si le maître d'ouvrage ne dispose pas des moyens humains nécessaires, il pourra envisager le recours à un consultant mais en sachant que celui-ci ne constitue qu'une aide qui ne le libère en rien de la conduite de l'étude et, bien sûr, de la réflexion sur ses orientations.

- Pour les choix techniques, et si le système de vidé protection est d'une ampleur significative, il est assez rare que le maître d'ouvrage dispose en interne de compétences spécialisées. Il aura plus intérêt à faire intervenir un bureau d'études, sur la base du cahier des charges fonctionnel qu'il aura élaboré en interne.

  Ce bureau d'études réalisera l'étude technique, éventuellement assistera le maître d'ouvrage dans l'analyse des offres des pétitionnaires puis dans le suivi des travaux.

Cette dépense peut sembler importante. Mais, pour un grand système, si le bureau d'études est bien choisi, l'apport d'idées nouvelles permettra une optimisation du système susceptible de générer une économie globale significative.

8.1 LE CHOIX D'UN CABINET

Plus de 400 cabinets ont été recensés dans la profession dite de « vidéosurveillance ». La **qualité** des prestations, la formation et le profil des intervenants dans ces structures est inégale. Le recours à une grille d'analyse permettant d'utiliser des critères objectifs qui permettront au décideur de faire le meilleur choix est donc impératif.

Critères d'analyse d'un cabinet :

Il est recommandé d'utiliser l'ensemble des critères suivant pour l'analyse.

- **Critère de complémentarité**

Il consiste à identifier les qualités et les **manques constatés** de l'équipe de Maîtrise d'Ouvrage qui sera mise en place pour le projet. En fonction de cette analyse, il faut rechercher et favoriser le cabinet qui complétera au mieux ces lacunes.

- **Critère de compétences requises pour le dossier :**

Quelles expériences et quelles références relatives aux deux grands postes suivants :

- **L'organisation** : quid des hommes, des structures en place ou à mettre en place , de la relation inter-service (PN, GN, PM, sécurité privée), des conventions à mettre en place…
- **La technique** :

- Technique **vidéo** : caméra, visualisation, enregistreur, IHM,
- Technique **voirie** : enfouissement des câbles, détermination de points hauts pour les transmissions radio,
- Technique **réseau** : haut débit, redondance et tolérance aux pannes, extensibilité, SAN, mutualisation de réseaux, maintenance, transfert de compétences et formations,
- Technique **spécifique :** parking, bus, métro, tram, centre commercial, antiterrorisme…,
- Technique **connexe** : détection incendie, création de local technique, contrôle d'accès au site, interfaçage avec logiciels existants…

Un cabinet conseil postulant doit pouvoir présenter des références détaillées sur des missions similaires. Il ne faut pas hésiter à contacter plusieurs anciens clients de cabinets conseil pour connaître leur avis sur la prestation fournie. Les références de l'entreprise et de l'équipe projet seront les critères déterminants.

- **Critère de prix :**

Les honoraires à la journée sont communément admis. En 2008, il s'agit environ 800 € HT par jour, hors frais. Ce montant constitue une bonne référence. Il s'agit d'une moyenne du coût des juniors et les seniors.

Il suffit pour obtenir « le bon prix » d'estimer précisément le nombre de jours d'assistance nécessaires in situ et dans l'entreprise, phase par phase, étape par étape, profil par profil.

On considère souvent qu'une pondération accordant 60% à l'aspect technique et 40% au prix est raisonnable.

- **Critère de compétences et de disponibilité des intervenants**

L'examen de ce critère consiste à

- Consulter attentivement les présentations des différents intervenants (CV à vérifier parfois).
- S'assurer que le responsable présent lors des négociations commerciales s'impliquera effectivement dans la réalisation de la mission. Le chef de projet doit être présent et disponible tout au long de la mission.

8.2 LES ETAPES D'ACCOMPAGNEMENT PAR UN BUREAU D'ETUDES

Lors du choix, le cabinet conseil devra remettre une note méthodologique. Cette dernière doit permettre de porter un jugement efficace sur la méthodologie proposée par le cabinet conseil. Elle fera l'objet d'une attention particulière.

8.2.1 L'AVANT PROJET, LE CONSEIL AMONT

Cette étape est déterminante puisqu'elle permet de fixer la teneur du projet, son périmètre, son budget global et son budget annuel. Les quatre blocs stratégique, organisationnel, juridique et technique doivent être appréhendés lors de cette étape. Comme nous l'avons vu précédemment, et si cela est possible, les blocs stratégie et juridique auront été élaborés au préalable en interne.

Deux comités doivent être créés :

- **Un comité de pilotage**, afin d'arrêter les choix stratégiques et financiers. Il assure la vision globale du dossier.
- **Un comité technique**, afin d'arrêter tous les choix d'ordre techniques. Il assure la vision de détail du dossier.

Une animation soignée de ces deux comités doit être assurée. Le nombre de jours prévus devra donc clairement correspondre à cette prestation. Cette animation pourra s'effectuer en deux temps :

- une étape d'avant projet sommaire (**APS**) où l'on s'attachera à envisager le maximum de solutions, de possibilités techniques et organisationnelles (afin de ne passer à côté d'aucune opportunité),
- puis une étape d'avant projet détaillé (**APD**) où l'on s'attachera au contraire à réduire le nombre de solutions étudiées en APS afin de cibler au mieux le cahier des charges, et donc le ou les entreprises qui traiteront le déploiement du dossier.

8.2.2 CCTP /DCE…

Lorsque l'avant-projet est mené correctement, cette étape est décisive pour le coût global et la bonne exécution de l'opération. Cette étape peut-être menée très rapidement en fonction de la compétence du cabinet. La description du dispositif à déployer et des travaux à effectuer seront donc précis. Le cahier des charges peut être plus ou moins ouvert En fonction de la parfaite connaissance du marché (intégrateurs et constructeurs susceptibles de répondre), pouvant même aller jusqu'à un dialogue compétitif.

Une « version 1 » du cahier des charges, déjà très complète et très professionnelle (chapitres ciblés sans copiés/collés cocasses, normes citées, travaux décrits,…) pourra donc être émise dans des délais courts.

Une version 2 et une version 3 sont à prévoir après lectures attentives et suggestions utiles de la part du Maître d'Ouvrage.

8.2.3 ANALYSE DES OFFRES

Si le maître d'ouvrage ne dispose pas en interne des moyens appropriés, il se fera aider par le bureau d'études pour l'analyse des offres.

Une grille doit être soigneusement bâtie dès l'étape d'avant projet. Elle doit intégrer tous les paramètres clés du dispositif déployé. Une pondération de chaque paramètre doit ensuite être débattue, en accord avec le comité de pilotage (validé lors de l'étape de rédaction de DCE). Voici un **exemple** de grille.

Critères d'évaluation	NOTATION		Commentaires
	Système de Notation	Note Attribuée	
Evaluation générale de l'entreprise			
Evaluation technique du système			
Conformité reseaux Conformité raccordement des caméras Conformité Energie Conformité Aménagement des locaux Conformité Caméras Conformité Ecrans Conformité Encodage des flux vidéos Conformité Enregistrement Conformité Contrôle d'accès Conformité Gestion des alarmes Conformité Poste informatique Conformité Superviseur vidéo Performance globale du système			
Spécifications relatives au déploiement			
Fonctionnement en mode projet Plan d'Assurance Qualité Plan d'acceptance et de tests systèmes Description de l'organisation de déploiement Proposition de Planning et crédibilité			
Evaluation de la maintenance et de l'assistance			
Maintenance Assistance téléphonique Télémaintenance Mise à niveau du firmware Mise à niveau logiciel			
Evaluation de la formation			
Note Technique et Organisationnelle de l'offre /20			

Note Financière /20 **(Montant de l'offre la moins disante / Montant de l'offre considérée x 20)**		Montant de l'offre la moins disante : Montant de l'offre considérée :

Note Finale /20 **(Note Technique et Organisationnelle de l'offre x coef1 + Note Financière x**	0

8.2.4 SUIVI DE TRAVAUX

Le suivi de travaux doit permettre de prendre toutes les dispositions nécessaires au bon déroulement des travaux de réalisation.

VISA : Le rôle du cabinet conseil est de valider les documents d'étude d'exécution des travaux, mais aussi, d'avoir un rôle actif d'accompagnement des utilisateurs et gestionnaires.

D E T : Direction de l'exécution des travaux :le cabinet conseil doit animer l'ensemble des réunions de suivi des travaux. Chaque réunion sera sanctionnée par un compte rendu et

diffusé immédiatement par e-mail à l'ensemble des participants du groupe de travail (étendu aux représentants du titulaire du marché).

Ce compte-rendu doit être sans ambiguïté sur les actions à effectuer pour chaque partie. Il pourra prendre la forme suivante (sous forme de colonnes) :

- **Article :** indexation du paragraphe
- **Objet :** explication précise du constat, de la remarque
- **Date consignée sur CR**
- **Date début action ou travaux**
- **Date achèvement action ou travaux**
- **Observations :** il peut être indiqué ici « RAPPEL » ou « RAPPEL N°2 »

8.2.5 RÉCEPTION

A O R : Assistance lors des opérations de réception et pendant la garantie de parfait achèvement

L'objectif de cette étape est l'encadrement de l'entreprise titulaire du marché pour la bonne réalisation des travaux.

Il est par ailleurs indispensable de vérifier la conformité des solutions déployées avec les exigences du DCE et de s'assurer de leur stabilité dans le temps.

V.A.B.F : Vérification d'Aptitude au Bon Fonctionnement

Un protocole de tests devra être défini, il pourra comprendre :

- Une vérification visuelle des ouvrages,
- La définition des fiches de tests, techniques et fonctionnelles, validés par le comité technique,
- La réalisation de l'ensemble de ces tests, essais techniques et fonctionnels,
- La validation du dossier des ouvrages exécutés (D.O.E).

Suivi des réserves éventuelles

Les réserves constatées devront être levées dans des délais consignés dans le compte-rendu.

V.S.R. : Vérification du Service Régulier

La stabilité des solutions déployées par le biais de nouveaux essais préalablement définis avec le Maître d'Ouvrage et le Conducteur d'Opération devra être constatée.

9 FICHE N°9 : RECRUTEMENT ET FORMATION DES OPERATEURS

Fiche n°9

Recrutement et formation des opérateurs

L'efficacité d'un système de vidéoprotection est avant tout liée à la réaction lors de la détection d'un fait anormal ou de la commission d'un délit, d'où l'importance de la fonction « opérateur ».

9.1 RECRUTEMENT :

C'est une phase essentielle à prévoir dès le début du projet. Il est nécessaire de déterminer :

- les heures d'exploitation du système de vidéoprotection
  - une exploitation en mode 24/24 nécessite un minimum de 5 personnes
- les tâches qui seront confiées à l'opérateur
  - trop de tâches différenciées ne permettront pas à l'opérateur de se concentrer sur sa mission principale de vidéo protection.
  - la télésurveillance des zones équipées d'alarmes est parfaitement compatible, mais sans que l'opérateur n'ait à quitter le local de vidéosurveillance.
- existe-t-il une ressource interne ou doit-on effectuer un recrutement externe ?

« Opérateur de vidéo protection » est un métier spécifique qui n'est pas encore reconnu par la fonction publique. En cas de recrutement interne une formation complète aux métiers de sûreté sera donc nécessaire hormis s'il s'agit de policiers municipaux. Les personnes à mobilité réduite peuvent effectuer ce métier à condition de bénéficier d'un poste de travail aménagé.

Un recrutement extérieur avec des fiches de poste précises permet d'attirer des candidats de la sécurité privée ayant très souvent une formation en vidéosurveillance soit en grande surface, soit en protection de site.

***Note** : Dans le cas d'un projet de vidéoprotection communale, le recrutement devra se faire en étroite collaboration avec les intervenants de la DGPP, de la DSIT et de la Direction des Ressources Humaines.*

Il s'agit ensuite de réaliser une fiche de poste par métiers qui listera :

- L'identification des tâches,
- Les objectifs qualitatifs à atteindre,
- Les règles déontologiques à respecter,
- Le travail en partenariat,
- Les contraintes propres à chaque environnement.

- **Organisation du recrutement**

Les phases de recrutement sont primordiales pour le bon fonctionnement du centre de supervision. Il est généralement préférable de procéder à un recrutement en trois étapes qui se traduiront pas trois prises de contacts différentes:

- 1er contact : information et tests écrits et oraux,
- 2ème contact : entretien avec les candidats pré-sélectionnés suite aux tests,
- 3ème contact : entretien final avant décision.

- **Critères de recrutement**

Les critères principaux devant être pris en compte lors des entretiens sont les suivants :

- Motivation
  - Poste contraignant avec des horaires décalés
- Autonomie
  - Souvent l'opérateur est seul pour accomplir sa mission, il doit savoir faire preuve d'initiatives
- Discipline
  - Ponctualité à la prise de service
  - Respect des consignes
  - Suivi des procédures
- Réactivité
  - Analyse rapide d'une situation
  - Sens de l'anticipation
- Elocution
  - En particulier au téléphone lors de la description d'un événement aux forces de police ou aux pompiers

9.2 FORMATION :

Il n'existe pas, pour l'instant, de formation nationale d'opérateur de vidéosurveillance Dans beaucoup de cas la seule formation consiste à savoir se servir de l'outil mis à disposition sur le plan technique, mais sans recevoir une formation de base « sûreté ».

Une formation d'opérateur de vidéoprotection doit comprendre plusieurs phases :

- Une formation théorique
  - Etude des fondamentaux d'une installation de vidéosurveillance et de télésurveillance
  - Rappels du rôle d'un opérateur et des bases réglementaires
- Une formation technique d'utilisation de l'outil
  - Etude de toutes les fonctionnalités du système et prise en main de l'installation – répétitivité obligatoire pour créer des automatismes-

- Une formation « opérationnelle » (trop souvent oubliée). Cette phase sera décomposée en cinq parties spécifiques
  - Découverte et étude à pied des zones à vidéosurveiller et des zones voisines avec indication des problématiques particulières de chacune,
  - Formation au « tracking » de jour et de nuit en utilisant le système,
  - Formation au compte rendu écrit et oral,
  - Exploitation en présence d'un personnel de terrain de la police nationale qui exprimera ses attentes particulières du système et qui fera bénéficier aux stagiaires de son expérience,
  - Retour d'expérience, contrôle et complément de formation après deux mois d'exploitation.
- Une formation maintenance de premier niveau permettant de résoudre des problèmes techniques simples tel que relancer le logiciel ou déterminer un défaut

La formation des personnels pour les phases techniques et opérationnelle doit être effectuée sur site pour mettre le personnel en situation et tenir compte des spécificités

Une formation complémentaire sera nécessaire pour les personnels en charge de l'exploitation des enregistrements qui sont en général différents des opérateurs.

La formation est la transmission d'un savoir et d'une expérience, aussi le formateur devra avoir une connaissance théorique et pratique de la vidéo protection.

9.3 ANNEXES

9.3.1 ANNEXE 1 / FICHE METIER

- Copie de la fiche métier d'opérateur de vidéosurveillance proposée par le centre national de la fonction publique territoriale.

9.3.2 ANNEXE 2 / CRITÈRES DE CHOIX D'UN PRESTATAIRE PRIVÉ

Dans certains cas il est possible de confier la supervision des images à un prestataire privé. Les avantages sont multiples : baisse significative du budget alloué, souplesse de fonctionnement, professionnalisme reconnu. … Comment choisir ce prestataire ? Quelques éléments permettant d'effectuer un choix sont proposés ci-après :

- Le prestataire retenu devra faire preuve de professionnalisme : respect des normes APSAD P3, réelle implication sur le sujet de la vidéo protection urbaine,
- Le prestataire devra avoir mis en place des formations spécifiques de façon à être capable de mettre à disposition des personnels dédiés à l'utilisation des moyens et à l'exploitation des images vidéos. L'objectif est d'avoir de réels spécialistes, identifiés et capables d'affiner leurs expertises en développant au mieux leurs sens mis à contribution (vue, ouïe) et de maîtriser les techniques de mise au repos de ces derniers.
- Le personnel assigné à la vidéo protection ne doit pas être sollicité pour faire une autre activité (gestion des bornes d'entrée / sortie, …). Pour minimiser les coûts, ils pourront être polyvalents sur d'autres opérations de télésurveillance (gestion des alarmes, ….) mais seront dédiés exclusivement à la vidéo surveillance urbaine lorsque qu'ils seront affectés à cette tâche lors de vacations spécifiques.
- Il faut établir des contrats spécifiques pour le recrutement des agents vidéos en intégrant très fortement une notion de confidentialité et de respect du secret et en précisant bien que le non respect de cette clause entraînerait immédiatement une mise à pied conservatoire et ferait l'objet d'un dépôt de plainte.
- A minima, demander le port d'un badge spécifique. L'objectif est de pouvoir identifier facilement qui fait quoi dans un PC de vidéoprotection. L'idéal serait de doter le personnel d'une tenue spécifique.
- Il faut prévoir un rapprochement fort avec les services de police ou de gendarmerie Le prestataire doit proposer de réaliser régulièrement des réunions de travail avec les services de police (municipales, nationale) et/ou les services de la Gendarmerie Nationale. L'ordre du jour pourrait être : Faits constatés, taux d'utilisation du matériel installé, nombre de recours à l'extraction de données, conseils pour optimiser l'utilisation, la communication et la synergie entre les services, arrestations réalisées en partie grâce à l'utilisation de vidéo, …).
- Mise en œuvre d'une démarche qualité (certification).

Fiche n°10

Le panorama des matériels et des logiciels

10 FICHE N°10 : LE PANORAMA DES MATERIELS ET DES LOGICIELS

L'architecture d'un système de vidéoprotection peut être modélisée selon les six blocs suivants : **acquisition, transport** (dont encodage et commutation)**, visualisation** (et pilotage)**, enregistrement**. Chaque bloc est abordé indépendamment d'un point de vue technique.

10.1 L'ACQUISITION DES IMAGES : LES CAMERAS

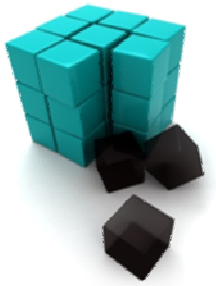
L'acquisition des images est réalisée par des caméras fixes ou mobiles, dans des conditions de jour et de nuit.

- **Caméras fixes**

Une caméra fixe ne surveille qu'une zone unique et sera parfaitement visible, elle indiquera donc clairement la direction dans laquelle elle est orientée. Pour une protection renforcée, ces caméras peuvent être placées dans des caissons spécialement conçus (comme des caissons anti-vandales).

Avantage	**Inconvénient**
Fiable (bonne durée de vie) Facile d'entretien	Visible Angle de vision réduit Généralement pas de zoom optique
Bloc Optique	
Résolution	640X480 ou 768 X 576
Zoom optique	Non pour la majorité
Sensibilité (lux)	De 1 à 0.5 (jour) à 0,04 (nuit)

Exemple d'utilisation : Surveillance d'un couloir, d'une entrée de parking, d'un point de passage obligatoire d'un site à surveiller, surveillance d'une zone



- **Caméras Minidômes (ou dôme fixe)**

Les caméras Minidômes, (ou dôme fixe), se composent d'une caméra fixe installée dans un caisson fixe de type dôme. Elles peuvent être orientées facilement dans n'importe quelle direction. Elles sont relativement discrètes car elles peuvent être intégrées dans un faux plafond ou un mur et il est difficile de les apercevoir et de déterminer la direction dans laquelle elles pointent.

Avantage	**Inconvénient**
Discrète Installation facile	Généralement pas de zoom optique
Bloc Optique	
Résolution	640X480 ou 768 X 576
Zoom optique	Non pour la majorité
Sensibilité (lux)	De 1 à 0.5 (jour) à 0,05 (nuit)

Exemple d'utilisation : Surveillance d'un passage obligé et, étroit.

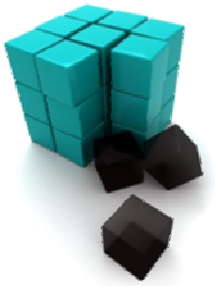
- **Caméras dôme fixe 360°**

Ces caméras sont des caméras qui filment les scènes à 360° et permettent ainsi d'avoir une vision globale de la scène en permanence. Ces caméras ne sont pas motorisées.

Avantage	**Inconvénient**
Visibilité global de la scène Relativement discrète Prix	Pas de zoom optique (reconnaisse ou identification difficile si éloignement important)
Bloc Optique	
Résolution	640X480 ou 768 X 576

Zoom optique	Non
Sensibilité (lux)	De 1 à 0.5 (jour) à 0,05 (nuit)

Exemple d'utilisation : Surveillance d'un hall, surveillance d'un bureau, surveillance d'une zone proche à 360°.



- **Caméras PTZ**

L'avantage des caméras PTZ tient à leurs fonctionnalités PTZ, c'est-à-dire à leurs options de contrôle panoramique/inclinaison/zoom. La caméra PTZ permet par exemple de suivre une personne dans un lieu. Beaucoup de caméras PTZ n'offrent pas de fonctions panoramiques à 360 degrés et ne sont pas conçues pour fonctionner en mode automatique. Des caméras fixes peuvent être montées sur des tourelles pour proposer des fonctionnalités semblables.

Avantage	**Inconvénient**
Contrôle panoramique/inclinaison/zoom Zoom optique puissant	Pas de rotation à 360° Ne surveille qu'une scène à la fois
Bloc Optique	
Résolution	640X480 ou 768 X 576
Zoom optique	De 3X à 36X
Sensibilité (lux)	De 2 à 0,7 (jour) / 0,05 (nuit)

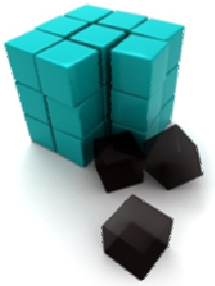
Exemples d'utilisation : surveillance d'une zone étendue non controlée, surveillance d'une rue, d'un carrefour.

Caméras dômes mobiles

Ces caméras possèdent les même carastéristiques que les caméras PTZ sauf qu'elles sont sont pourvues de fonctions panoramiques à 360 degrés. De plus de par leur intégration elle sont plus discrètes

Avantage	Inconvénient
Contrôle panoramique/inclinaison/zoom Rotation 360° Zoom optique puissant	Ne surveille qu'une scène à la fois
Bloc Optique	
Résolution	640X480 ou 768 X 576
Zoom optique	De 3X à 36X
Sensibilité (lux)	De 2 à 0,7 (jour) / 0,05 à 0,01 (nuit)

Exemples d'utilisation : surveillance d'une zone étendue non controlée, surveillance d'une rue, d'un carrefour.



- **Caméras Mégapixel**

Même si la caméra megapixel est aujourd'hui une caméra fixe ou dôme mobile, elle mérite une rubrique à part. Cette caméra permet d'atteindre des résolutions beaucoup plus importantes et donc une finesse d'image très intéressante pour de la reconnaissance ou de l'analyse d'image. Elle représente aujourd'hui l'avenir en terme de qualité d'image. A moyen ou long terme, tous les types de caméras seront « mégapixels »

Avantage	**Inconvénient**
Résolution très importante Possibilité d'analyse et de traitement très précis.	Nécessite une capacité de stockage et de bande passante plus importante
Bloc Optique	
Résolution	> 1280X960
Zoom optique	possible
Sensibilité (lux)	De 0,8 à 0,6 (jour) / 0,05 (nuit)

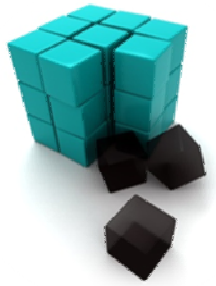
Exemples d'utilisation : surveillance d'une place, d'un grand hall surveillance d'une zone étendue

10.2 LE MEDIA DE TRANSMISSION

Le transport des informations (images, son …) est réalisé par la liaison entre la caméra et le local technique (ou point de concentration). Le type de liaison dépendra de la distance entre ces deux points, de la faisabilité technique et des coûts associés. Ils peuvent être résumés en quatre catégories différentes : Câble cuivre coaxial, Fibre optique, Câble cuivre multipaires, Liaison Radio. Selon le type de connectique disponible en sortie de cameras, des convertisseurs peuvent être nécessaires.

- **Câble cuivre Coaxial :**

Pour une distance inférieur à 300m des câbles coaxiaux de type KX6 seront utilisés. Pour une distance inférieur à 600m des câbles coaxiaux de type KX8 seront utilisés.



Caratéristiques	KX6	KX8
Normes et directives de référence		
Caractéristiques	UTE C93550	
Environnement (directives européennes)	R0HS et CEEE	
Caractéristiques techniques		
Impédance caractéristique	75 Ω	
Diamètre brut (± 5%)	6 mm	10 mm
Bande passante	1,5 Ghz	
Connectique	BNC, RG58	BNC, RG59
Distance d'utilisation	300 m	600 m

Note interface : Aucune interface spécifique n'est nécessaire dans le cas d'une caméra raccordée en coaxial. Côté points de concentration, ces câbles seront raccordés sur les équipements vidéos (matrice analogique ou encodeur), côté caméra, ils seront raccordés directement.

- **Câbles à fibres optiques**

Pour une distance maximale de 3 km en analogique bande de base ou 2 km en FastEthernet, la fibre optique multimode est préconisée. Pour une distance plus élevée (typiquement, jusqu'à 10 km), la fibre optique monomode s'impose. Les principales caractéristiques sont les suivantes :

Caratéristiques	Multimode 50/125 OM3	Monomode 9/125 OS1
Normes de référence		
Caractéristiques	ITU-T G651	ITU-T G652
Caractéristiques géométriques		
Diamètre du cœur (µm)	50 ±3	9,3 ±0,5
Diamètre de la gaine (µm)	125 ±3	125 ±1
Diamètre du revêtement primaire (µm)	250 ±10	245 ±10
Valeur de l'ouverture numérique	0,275 ±0,02	0,12 ±0,01
Excentricité du coeur (%)	< 6	< 6
Excentricité de la gaine (%)	< 2	< 2
Excentricité entre la gaine et le cœur (µm)	< 1.5	< 0,8
Caractéristiques de transmission		
Atténuation linéique assurée (dB/km)		
	< 3.2 à 850 nm	< 0,5 à 1310 nm
	< 1.0 à 1300 nm	< 0,4 à 1550 nm
Bande passante modale (Mhz.km)		
	> 200 à 850 nm	> 2 000 à 1310 nm
	> 500 à 1300 nm	> 5 000 à 1550 nm

Ces câbles devront respecter la directive de l'Union Européenne RoHS (Restriction sur l'usage de certaines substances dangereuses) et DEEE (Déchets d'équipements électriques et électroniques).

Note interface : Il faut, dans ce cas, utiliser une interface ***coaxial/fibre optique*** dans le cas d'une caméra analogique et **10BaseTx/100BaseFx** dans le cas d'une caméra IP.

- **Câbles multipaires cuivre**

Pour une liaison de moins 90 m entre le point de concentration et une ***caméra IP***, un câble 4 paires de catégorie 6 sera utilisé. Un câble de ce type peut également être utilisé pour la liaison de télémétrie d'une caméra analogique raccordée avec un câble coaxial vidéo (kx6, KX8). Ces câbles devront être conforme aux normes ISO / IEC 11801-2 et EN 50173-2.

Note interface : Aucune interface spécifique n'est nécessaire : Côté points de concentration, ces câbles seront raccordés sur des équipements de réseaux, côté caméra (IP), ils seront raccordés directement.

- **Radio**

Ces type de liaisons sont utilisées lorsque les distances sont relativement importantes et que les coûts en génie civil sont trop élevés.

Les liaisons radio utilisent des bandes de fréquences de 5,4Ghz ou 5,8Ghz. Une attention toute particulière sera apportée à la sécurisation des données (cryptage des données, contrôle d'association basé sur des adresses MAC, adresses IP autorisées, …) et à la capacité des liaisons à supporter le débit nécessaire au bon fonctionnement du système.

10.3 L'ENCODAGE

L'encodage qui prend en compte les normes vidéo ainsi que les normes de compression nécessite un développement spécifique.

10.4 LE PILOTAGE – LES INTERFACES

Les caméras sont pilotées via une IHM (Interface Homme-machine). Il s'agit, de piloter et d'exploiter, en temps réel, un système complexe sur le plan technique, avec des contraintes fortes sur les plans temporel et géographique.

Deux « types » d'IHM se partagent le marché :

- Des IHM dites « propriétaires » qui dialoguent parfaitement avec les équipements du même constructeur (systèmes globaux packagés) mais proposeront une interopérabilité limitée ou des pertes de fonctionnalités avec d'autres fabricants.
- Des IHM dites « ouvertes » qui permettent l'intégration d'éléments d'architecture provenant de différents fabricants, ouvrant ainsi le spectre du choix des équipements et favorisant la concurrence.

Lors du choix de l'IHM, les points suivants devront être étudiés :

- **La cartographie**

Les logiciels devront gérer une arborescence de plans utilisant un format couramment utilisé (.dxf, .dwg, mapx, …). Ces plans, qui ne concerneront que les zones de couverture des caméras, pourront être enrichis de différents champs (icônes, texte, …) afin d'améliorer la convivialité du système.

- **Visualisation d'une zone**

Pour faciliter la convivialité du système, l'opérateur visualisera la zone souhaitée par un simple « clic » de souris sur le plan correspondant. Le choix et le positionnement de la caméra se feront alors logiciellement, de manière automatique. Selon le logiciel proposé, il convient de faire attention à la précision de pointage et de positionnement de la caméra. Chaque logiciel ayant ces spécificités.

- **Mémorisation d'un cadrage**

Lors d'une opération de surveillance, en pilotant sa caméra l'opérateur peut repérer une zone à surveiller ponctuellement, de manière spécifique (ex : accident ou incident, événement divers). Le système doit donc permettre la mémorisation simple, du cadrage de la scène (position caméra + zoom) concernée. Un dispositif permettra de marquer sur les plans la zone correspondant au cadrage mémorisé. L'effacement du marquage doit pouvoir également se faire de manière simple. Enfin le système doit permettre une gestion dynamique de plusieurs centres d'intérêts.

- **Automatisation**

Afin de faciliter et automatiser des séquences d'exploitation (visualisation et/ou mémorisation), ces dernières seront gérées par le logiciel. Ces scénarii vidéo seront ceux préalablement paramétrés par le responsable d'exploitation. Ceux-ci pourront être déclenchés de la manière suivante :

- Choix de l'opérateur dans une liste, ou sur des boutons spécifiques,
- Apparition d'un événement d'alarme,
- Heure de déclenchement planifiée, dans un agenda journalier et hebdomadaire intégrant les jours fériés et des jours ou heures particulières.

Les séquences exécutables dans un scénario seront au minimum les suivantes:

- Affichage d'une caméra sur un moniteur (ou plusieurs caméras sur plusieurs moniteurs),
- Positionnement automatique d'une caméra et de son zoom,
- Durée d'affichage ou de mise en position pour chaque instruction,
- Mémorisation des images d'une ou plusieurs caméras,
- Choix de la vitesse et de la durée de l'enregistrement,
- Affichage d'un plan,
- Affichage de messages de consigne,
- Incrustation de textes dans l'image,
- Incrustation du nom de la zone visualisée.

- **Incrustations vidéos**

Afin de faciliter le repérage d'une image visualisée par une caméra mobile sur un moniteur, les incrustations vidéo indiqueront à la place du nom de la caméra, le texte correspondant à la zone visualisée.

- **Mode poursuite (de hand-over)**

Lorsqu'un opérateur pilote une caméra pour suivre un sujet qui se déplace, il est probable que celui-ci, à un moment ou un autre quitte le champ de couverture de la caméra pilotée. Si le sujet pisté entre, par-là même, dans le champ de vision d'une autre caméra, il est souhaité que le système dispose d'une fonction de pilotage qui appellera et positionnera automatiquement la caméra qui assure la couverture de la nouvelle zone concernée.

10.5 LA VISUALISATION

Il faut distinguer le(s) moniteur(s) associé(s) au poste de contrôle et les moniteurs du mur d'image dont la dimension est fonction de la distance entre l'opérateur et les écrans.

- **Poste de travail opérateur**

Concernant le poste de travail, il est préconisé d'avoir deux écrans par opérateur : Un écran avec la cartographie des différentes zones « vidéoprotégées » et un écran visualisant la caméra souhaitée.

Au niveau des caractéristiques des écrans opérateurs, il est aujourd'hui préférable de travailler sur un écran LCD 4/3 de 19 à 21'' avec :

- Une luminosité minimale de 300cd/m² et un contraste minimal de 1000/1
- Un temps de réponse minimal de 5ms
- Une résolution de dalle de 1280 X 1024 (19'') à 1600 X 1200 (21'')
- Une base réglable et inclinable

- **Murs d'images**

Nous pouvons trouver plusieurs types de murs d'images, ceux-ci peuvent être constitués de :

Plusieurs écrans LCD :

- diagonale de 21'' à 28'',
- luminosité minimum : 450 cd/m²,
- contraste minimum : 500 :1,
- temps de réponse maximum : 8 ms,
- résolution de la dalle : 1600 x 1200 (21'') jusqu'à 1920 x 1200 (28'').

Un ou plusieurs écrans LCD en multi fenêtrage :

- diagonale de 40'' à 60'',
- luminosité minimum : 450 cd/m²,
- contraste minimum : 7000 :1,
- temps de réponse maximum : 8 ms,
- résolution de la dalle de 1920 x 1080.

Un ou plusieurs systèmes de rétroprojection :

- diagonale de 50'' à 80'',
- contraste minimum 1000 :1,
- résolution de 1024 x 768.

10.6 L'ENREGISTREMENT

La fonction enregistrement a en charge le stockage des images fournis par les caméras. Il doit également permettre une recherche multicritères sur les données enregistrées (date, heure, identification caméra, événement déclenchant, zone géographique, …). L'enregistreur doit pouvoir être piloté depuis L'IHM.

Les capacités de stockage des enregistreurs dépendent :

- du nombre de caméras à enregistrer,
- du nombre de jours d'enregistrement,
- du temps d'enregistrement par jour (heure),
- du nombre d'images par seconde,
- de la qualité de l'image,
- du constructeur.

Les principales caractéristiques des enregistreurs doivent êtres les suivantes :

- Enregistrer des signaux vidéo à 25 Images/secondes en 4CIF,
- Ils doivent supporter plusieurs relectures simultanées,
- Etre tatoué "*Watermarked*".
- Enregistrer des signaux audio si besoin,
- Utiliser un système RAID5 pour éviter des dysfonctionnements matériels. Il devra permettre de remplacer un disque « à chaud » et le reconfigurer automatiquement,
- Une alimentation redondante afin d'éviter une possibilité de panne.

A Savoir

Watermarked signifie tatouage numérique. Il s'agit d'une technique permettant d'ajouter des informations de copyright ou d'autres messages à un fichier ou signal audio, vidéo, une image ou un autre document numérique.

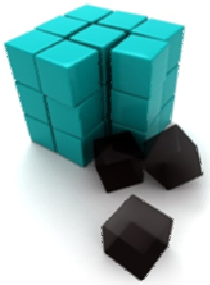
- **Enregistrement type DVR**

Les DVR (Digital Video Recorder) sont des équipements équipés de cartes d'acquisition permettant de numériser les vidéos

Les caméras analogiques sont donc raccordées directement sur l'équipement. Les DVR -utilisés avec des caméras analogiques.-assurent alors le rôle de commutation, encodage et enregistrement.

- **Enregistrement type NVR**

Les NVR (Network Video Recorder) sont des équipements dont le rôle est uniquement d'enregistrer les images provenant du réseau. Ce matériel est donc adapté aux systèmes utilisant des caméras IP ou des caméras analogiques avec encodeurs Il s'agit généralement d'un serveur générique équipé d'une grande capacité de stockage. Les fonctions de commutation et d'encodage sont réalisées par d'autres équipements. Ce type de matériel est adapté aux systèmes de grandes envergures du fait de sa grande capacité d'extension.



Fiche n°11

Les normes techniques

11 FICHE N°11 : LES NORMES TECHNIQUES

Il n'existe actuellement pas de norme technique à proprement parler pour encadrer la mise en place d'un système de vidéoprotection.

L'AFNOR mène actuellement une réflexion dans ce domaine mais aucun document n'est encore disponible.

Le décret du 03 août 2007 n'est pas une norme, mais il permet cependant de donner quelques recommandations et spécifications techniques sur une installation de vidéoprotection typique.

11.1 STANDARDS VIDEO

NTSC

NTSC ou National Television System Committee, c'est-à-dire « Comité du système de télévision nationale ») est une norme de codage de la vidéo en couleur mise au point aux USA en 1953.

Elle est destinée aux formats vidéo 525 lignes/60 Hz (30images/secondes). La résolution est en fait de 711 x 480, la différence entre le nombre de lignes (525) et la résolution verticale (480) est du au fait que 8% des lignes servent à la synchronisation de l'image.

Le NTSC est utilisé en Amérique du Nord, dans une partie de l'Amérique du Sud (NTSC-M) et de l'Asie dont le Japon (NTSC-J).

SECAM

Le SECAM, ou Séquentiel Couleur À Mémoire est une norme de codage de la vidéo analogique en couleur mise au point en France et diffusée à partir de 1967.

Elle est destinée aux formats vidéo en 625 lignes/50 Hz (25 images/secondes). La résolution est en fait de 720 x 576, la différence entre le nombre de lignes (625) et la résolution verticale (576) est du au fait que 8% des lignes servent à la synchronisation de l'image

Le format SECAM est utilisé en France, dans les pays de l'Est, en Afrique, les pays de l'ex-URSS et au Moyen-Orient, avec suivant les pays, des normes de télédiffusion spécifiques (notées par les lettres L/L', B/G et D/K ou K').

PAL

Le PAL est une norme de codage de la vidéo en couleur mise au point en Allemagne.

PAL ou Phase Alternate Line, c'est-à-dire alternance de phase suivant les lignes, lignes/50 Hz (25 images/secondes). La résolution est en fait de 720 x 576, la différence entre le nombre de lignes (625) et la résolution verticale (576) est du au fait que 8% des lignes servent à la synchronisation de l'image

Utilisé principalement en Europe de l'Est, mais également en Australie, et dans certaines régions d'Afrique et d'Amérique Latine.

Le signal PAL et SECAM ne varie que par le codage couleur. Il est donc possible de regarder un signal SECAM sur un moniteur PAL et vice-versa. Cependant, on ne pourra pas voir la couleur (l'image sera en noir et blanc).

11.2 COMPRESSION

En ce qui concerne les « normes » de compression vidéo, une présentation exhaustive est nécessaire :

La compression des images et des données vidéo peut suivre deux approches différentes : sans perte ou avec perte.

Dans le cas d'une compression sans perte, chaque pixel est maintenu intact. L'image obtenue après compression est donc identique à l'original. Cependant, l'inconvénient est que le gain, en termes de réduction des données, est très limité.

Voilà pourquoi plusieurs méthodes et normes de compression dites avec pertes ont été développées. Le principe fondamental est de réduire les éléments invisibles à l'œil humain et d'accroitre ainsi considérablement le taux de compression.

Les méthodes de compression suivent également deux approches différentes par rapport aux normes de compression : compression des images fixes et compression vidéo.

Important

Bien que chaque constituant du système s'appuie généralement sur des normes, il n'existe pas aujourd'hui de référentiel permettant de mesurer, en absolu, la qualité d'une image. Celle-ci est donc particulièrement subjective et peut varier sensiblement en fonction des individus émettant leur avis.

Ce point, très délicat à maîtriser, est un aspect important du volet technique car il représente un indice majeur de l'efficacité du dispositif.

11.2.1 NORMES DE COMPRESSION DES IMAGES FIXES

Toutes les normes de compression des images fixes ont la particularité de se concentrer sur une seule image à la fois. La norme la plus connue et la plus répandue est le JPEG.

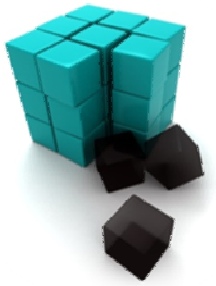
JPEG

Le JPEG a été normalisé au milieu des années 1980, à l'initiative du Joint Photographic Experts Group. Le JPEG permet d'obtenir le degré de compression souhaité : le taux de compression est paramétrable.

La compression sélectionnée est directement liée à la qualité de l'image voulue. Outre le degré de compression, l'image elle-même influence également le taux de compression obtenu. Par exemple, un mur blanc peut produire un fichier image de taille relativement petite (et un taux de compression élevé), tandis que le même degré de compression appliqué à une scène complexe et chargée produira un fichier de plus grande taille, avec un taux de compression plus faible.

JPEG2000

JPEG2000 est une autre norme utilisée pour la compression d'images fixes. Elle a été mise au point par le comité à l'origine de la norme JPEG. À des taux de compression peu élevés, la qualité JPEG2000 est similaire à la qualité JPEG. En revanche, quand on passe à des taux beaucoup plus élevés, JPEG2000 s'avère légèrement supérieur à JPEG.



11.2.2 NORMES DE COMPRESSION DES VIDÉOS

M-JPEG

Un système d'acquisition (caméra) saisit des images individuelles, et les compresse au format JPEG. Une caméra peut ainsi capturer et compresser (par exemple 25 fois par seconde) puis les envoyer pour lecture ou enregistrement. Lors de la lecture l'utilisateur percevra une vidéo en mouvement. C'est cette méthode que l'on appelle Motion JPEG ou M-JPEG. Chaque image individuelle étant compressée en JPEG, en fonction du taux de compression sélectionné par le système d'acquisition ou/et l'enregistreur.

H.263

La technique de compression H.263 est conçue pour une transmission vidéo à débit fixe. L'inconvénient du débit fixe est que l'image perd de sa qualité lorsque les objets sont en mouvement. La norme H.263 était initialement destinée aux applications de vidéoconférence et non à la surveillance où les détails ont plus d'importance que la régularité du débit.

MPEG

La norme MPEG (fondée par le Motion Picture Experts Group à la fin des années 1980) est la plus connue des techniques de transmission directe en vidéo.

Le principe de base du MPEG consiste à comparer entre elles deux images compressées destinées à être transmises sur le réseau. La première des deux images servira de trame de référence. Sur les images suivantes, seules seront envoyées les zones qui diffèrent de la référence. L'encodeur reconstruit alors toutes les images en fonction de l'image de référence.

Bien que plus complexe que la technique Motion JPEG, la compression vidéo MPEG produit de plus petits volumes de données à transmettre sur un réseau.

Il est noté qu'il existe différentes normes MPEG :

MPEG-1

Lancée en 1993 et destinée à l'archivage des données vidéo numériques. La plupart des encodeurs et des décodeurs MPEG-1 sont conçus pour un débit d'environ 1,5 Mbit/s en résolution CIF. MPEG-1 met surtout l'accent sur le maintien d'un débit relativement constant au détriment de la qualité d'image, laquelle est variable et comparable à la qualité vidéo VHS. En MPEG-1, la fréquence d'image est plafonnée à 25 (PAL) / 30 (NTSC) images par seconde.

MPEG-2

Approuvée en 1994, le MPEG-2 est destinée à la vidéo numérique de qualité supérieure (DVD), à la télévision haute définition (HDTV), aux supports d'enregistrement interactifs (ISM), aux systèmes d'émission vidéo numérique (DBV) et à la télévision par câble (CATV). Le format MPEG-2 vise à accroître la technique de compression de la norme MPEG-1 afin de couvrir des images plus grandes et de meilleure qualité, mais aux dépends d'un taux de compression plus faible et d'un débit d'images plus rapide. La fréquence est plafonnée à 25 (PAL) / 30 (NTSC) images par seconde, tout comme en MPEG-1.

MPEG-4

Le MPEG-4 représente une évolution substantielle par rapport au format MPEG-2. Les possibilités permettant de réduire le débit d'images de manière à atteindre une certaine qualité´pour une application ou une scène déterminée sont beaucoup plus nombreuses en MPEG-4. En outre, la fréquence n'est plus limitée à 25 ou 30 images par seconde. Il est à noter que les outils actuels permettant de réduire le débit ne concernent que les applications en temps réel car les besoins en termes de débit et de stockage sont beaucoup trop important. Finalement, la majorité´ des outils MPEG-4 destinés aux applications en temps réel sont les mêmes que ceux qui existent pour les formats MPEG-1 et MPEG-2.

H.264

La toute dernière norme de compression vidéo H.264, est appelée à devenir la norme vidéo de référence. Elle a déjà été intégrée avec succès dans le secteur de la vidéosurveillance, le H.264 offre de nouvelles possibilités en termes de réduction des frais de transport et de stockage et de renforcement de l'efficacité globale.

Le H.264 est le fruit d'un projet commun entre le Groupe d'experts en codage vidéo (VCEG) de l'International Telecommunications Union et le Groupe d'experts en images animées (MPEG) de l'ISO/IEC. L'ISO est l'Organisation internationale de normalisation et l'IEC est une organisation de surveillance des normes électroniques et électriques. Le H.264 est le nom employé par l'ITU-T, l'ISO/IEC préférant pour sa part opter pour l'appellation MPEG-4 Partie 10/AVC, la norme étant présentée comme un nouvel élément de sa série de normes MPEG-4.

Le H.264 est une norme ouverte sous licence, compatible avec les techniques de compression vidéo les plus efficaces d'aujourd'hui. Un encodeur H.264 peut réduire la taille d'un fichier vidéo numérique de plus de 80 % par rapport à la norme Motion JPEG et de 50 % par rapport à la norme traditionnelle MPEG-4, sans que la qualité d'image ne soit compromise. L'importance de ces gains rend le H.264 très intéressant pour les applications de vidéosurveillance.

Le H.264 devrait accélérer l'adoption des caméras mégapixel dans le secteur de la surveillance. Un des inconvénients actuels des caméras mégapixel est la taille importante des fichiers de données vidéo obtenus. Comme indiqué, le H.264 réduit la taille des fichiers, sans compromettre la qualité des images. Il est probable que cette technologie de compression hautement efficace trouve rapidement sa place dans des applications où les utilisateurs exigent à la fois une haute résolution et des fréquences d'image élevées, comme pour la vidéoprotection de certains lieux spécifiques.

11.3 DEBIT

Le débit ou Flux vidéo est composé d'une succession d'images, X images par seconde constituant l'illusion du mouvement. Le flux peut aussi se nommer frame rate ou FPS, Frames Per Second ou trames par seconde.

Les facteurs impactant sont les suivants :

- Résolution initiale (CIF) de l'image,
- Format de compression appliqué,
- Nombre d'images par seconde.

A paramètres constants, plus le débit est important plus une scène restituée en vidéo sera fluide.

Dans la réalité, il est plus fréquent de se heurter au débit de transmission comme contrainte à respecter, le coût du Kb/s ou du Mb/s restant élevé dans certain cas, notamment sur des distances importantes. Il convient alors de trouver le meilleur compromis entre la qualité de l'image, directement dépendante de la résolution et du format de compression, et le débit disponible.

Sur ce sujet, l'évolution des réseaux de transmission en termes de débit et les progrès constatés en permanence sur les techniques de compression vont dans le bon sens et permettent aux systèmes de vidéoprotection de se rapprocher des exigences des services d'investigation (Police technique, …).

11.4 LES FORMATS STANDARDS: CIF

Il s'agit tout simplement d'abréviations pour les dimensions d'image couramment utilisées. Ces valeurs optimisent certains des algorithmes de compression/décompression.

- CIF: Common Interchange Format (352 x 288)
- QCIF: Quarter CIF (176 x 144)
- SQCIF: Sub quarter CIF (128 x 96)
- 4CIF: 4 x CIF (704 x 576)
- 16CIF: 16 x CIF (1408 x 1152)

A retenir

La qualité d'une image, en numérique, est liée directement à sa résolution initiale (CIF) et au format de compression appliqué.

Le débit nécessaire pour transporter une image est la conséquence des choix de résolution et de compression. A l'inverse, il peut également être une contrainte à respecter, impactant les choix techniques et la qualité de l'image rendue.

Une image haute résolution, peu compressée dispose d'une qualité optimale mais nécessite un débit de transmission élevé (jusqu'à plusieurs dizaines de Mb/s).

Une image de faible résolution, très compressée sera de mauvaise qualité mais se contentera d'un débit de quelques kb/s.

Fiche n°12

Les traitements intelligents (LAPI, reconnaissance faciale, vidéogestion,..)

12 FICHE N°12 : LES TRAITEMENTS INTELLIGENTS (LAPI, RECONNAISSANCE FACIALE, VIDEOGESTION,..)

*« La **V**idéo**S**urveillance **I**ntelligente (VSI) est constituée des dispositifs intégrés à un système de vidéosurveillance permettant d'obtenir une action autonome du système selon des scénarii et contraintes prédéfinis »*

*« La **V**idéo**S**urveillance **I**ntelligente (VSI) est constituée des dispositifs intégrés à un système de vidéosurveillance permettant d'obtenir une action autonome du système selon des scénarii et contraintes prédéfinis »*

12.1 UN CONSTAT : « TROP D'INFORMATION TUE L'INFORMATION »

Il est difficile de surveiller les images issues de 250 caméras avec un nombre raisonnable d'opérateurs. En effet, l'œil humain ne sait détecter une situation atypique que sur 6 à 8 écrans au grand maximum. On parle donc parfois pour la salle de contrôle « d'écran éteint » ou « d'écran noir » : la probabilité de trouver un élément intéressant est voisine de zéro. Beaucoup d'événement ne sont pas détectés par les opérateurs, ce qui peut nuire à la crédibilité d'un système. Dans un cadre urbain, ceci peut être sévèrement critiqué par les citoyens et être relayé par la presse.

Pourtant, le nombre de caméras mises en service va progresser rapidement dans les années à venir du fait de l'engouement pour la vidéosurveillance, favorisé par la baisse des coûts des dispositifs (caméras, réseaux haut débit, enregistreurs…). Il est donc indispensable de positionner une intelligence artificielle dans les systèmes pour **scruter de manière systématique** les dizaines, les centaines voire les milliers de caméras mises en service.

12.2 STRATEGIE D'UTILISATION DE LA VSI DANS UN DISPOSITIF

L'intelligence artificielle est pertinente pour assurer un filtrage de **premier** niveau : cela consiste à positionner des seuils très sensibles de détection automatique de situations atypiques ou anormales. Les fausses alertes peuvent être nombreuses mais l'œil humain placé en **deuxième** niveau devient alors parfaitement adapté pour lever le doute et analyser la situation :

- Situation normale,
- Situation « à **vérifier** » : scrutation plus fine, plus précises, avec les caméras voisines…,
- Situation nécessitant une **intervention immédiate** sur site avec les procédures appropriées (procédures prédéfinies)

Attention ! : Des alarmes intempestives trop fréquentes peuvent lasser l'opérateur, avec le risque de manquer une situation critique.

Avec la multiplication des caméras, ce premier étage de détection automatique devient essentiel pour garantir **l'efficacité globale du dispositif**. Se passer de ce premier filtre revient à prendre le risque de ne pas détecter 90% des événements se déroulant dans le champ de surveillance des caméras.

Il existe actuellement une effervescence particulière sur le marché de la VSI : des dizaines de sociétés spécialisées voient le jour grâce aux avancées technologiques récentes en génie logiciel vidéo, rendues possibles grâce à la puissance phénoménale du hardware : microprocesseurs, mémoires, réseaux IP.

12.3 LES UTILISATIONS DE LA VSI

La VSI est pertinente quelle que soit la taille du dispositif :

- La VSI est pertinente pour les grandes installations :
  - Maintien de l'efficacité pour toutes les caméras installées,
  - Gestion autonome de certains sites ou de certaines tâches
- La VSI est pertinente pour les systèmes de taille modeste
  - Gestion autonome du système,
  - Réponse au problème du manque de personnel tout en conservant une efficacité satisfaisante.

La VSI peut être utilisée comme une aide précieuse dans de nombreux domaines :

- **Aide à la supervision et à la maintenance** d'un dispositif de vidéosurveillance, aide qui peut générer un retour sur investissement souvent rapide et important :
  - Surveillance de l'intégrité du système : caméras coupées, floutées, masquées, tournées ou réorientées progressivement jour après jour !…
  - Exemples : alors que la première vue est normale, la deuxième a été floutée (à l'aide d'un aérosol) et la troisième a été masquée…

  - Remplacement de l'opérateur en premier niveau d'analyse
- Aide à la gestion urbaine
  - Gestion du stationnement : payant, gênant, interdit, réservé…
  - Gestion des encombrants,
  - Gestion des travaux, des espaces verts…
- Détection de comportement atypique (maraudage dans un parking, tag sur un bâtiment)
- Détection d'intrusion
- Détection de perte de verticalité (chute) d'une personne
- Détection d'objets abandonnés ou enlevés
- Détection de graffiti
- Comptage de personnes (monodirectionnel ou bidirectionnel),

- Reconnaissance de véhicules (plaques, calandres…)
- Détection de vitesse, de direction,

12.4 LIMITES ACTUELLES DE LA VSI

Les précédents développements ont démontré l'intérêt d'utiliser l'outil d'intelligence artificielle dans l'exploitation d'un système de vidéosurveillance. Paradoxalement, ces systèmes ne sont pas ou peu déployés. Cette situation s'explique par un certain nombre de limites de cette technologie qui reste néanmoins très prometteuse :

- Limites éthiques et juridiques:
  - La scrutation automatique effectuée par « une machine » fait peur. Il s'agit là certainement d'un frein difficile à lever, puisque cette peur impacte le sentiment du non respect de la vie privée …
  - Reconnaissance de plaques : que reconnaître, quel croisement avec quel fichier ? qui peut faire quoi ?
  - Reconnaissance faciale : même question, s'agit-il de données nominatives ?…
- Limites techniques
  - Fiabilité de la reconnaissance de visages, des plaques : des progrès restent encore à accomplir dans ce domaine. Une bonne fiabilité suppose de dédier une caméra à une utilisation précise et efficace.
  - Problème de la définition de l'automatisme à mettre en place : qu'est-ce qu'un objet abandonné dans une gare ? qu'est-ce qu'un attroupement sensible ? qu'est-ce qu'un comportement atypique dans un parking…
  - Intégration de la VSI aux systèmes : dans la caméra ? à côté de la caméra, au central ?
  - Absence de norme : la VSI reste un produit mono-constructeur.

Pour vérifier qu'un système de VSI est utilisable il est très recommandé de mettre en œuvre des phases de tests avant la procédure d'achat puis après la mise en place du système d'étendre la phase de recette du système (un mois par exemple) afin de vérifier sur une longue période les fonctionnalités avancées.

Il faut enfin signaler que ce métier de la VSI est très récent. Le marché est composé de nombreuses sociétés souvent fragiles. On peut craindre des abandons d'activités, des rachats et donc potentiellement des parcs de produits difficiles à étendre ou à maintenir.

12.5 EXEMPLES

Cette partie vise à présenter quelles techniques présentes sur le marché et pouvant dès à présent être intégrées à un système. La liste n'est pas exhaustive.

EXEMPLE 1 : PERTE DE VERTICALITÉ

Cette application est peu utilisée à l'heure actuelle, alors qu'elle semble très intéressante et peu être utilisée pour de nombreux usages : maintien des personnes âgées à domicile, « maisons de retraites », établissements recevant du public, files d'attentes…

EXEMPLE 2 : DETECTION D'INTRUSION

Le piéton de la première image n'est pas détecté comme suspect, à l'opposé du personnage qui pénètre dans le parking sur la deuxième et troisième image.

Cette technique de détection d'intrusion a bien entendu d'innombrables applications et déclinaisons : passages à niveaux, tapis à bagages d'aéroports, sécurisation d'un périmètre…

EXEMPLE 4 : DÉTECTION AUTOMATIQUE DE PLAQUES

Les applications de cette technique sont particulièrement nombreuses : gestion d'accès, gestion et surveillance de la circulation, parkings publics et privés, hôtels... Cette technique est globalement fiabilisée même si des disparités de performance entre les produits peuvent être constatées.

EXEMPLE 5 : DÉTECTION DE TAG

Les tags coûtent cher aux propriétaires (collectivités, entreprises, maisons individuelles, transports en communs…). C'est un acte pourtant facile à détecter automatiquement et cette application de vidéosurveillance intelligente à un bel avenir car elle peut permettre de réaliser des économies significatives. Par exemple, si le nombre de tags baisse de 40% (chiffre constaté), le retour sur investissement du dispositif est rapide, tant sur le plan financier que sur le plan de la qualité de vie.

Cette technique peut également être utilisée dans le cadre de la lutte contre l'affichage sauvage : l'individu ci-dessous est détecté au moment où il s'éloigne de l'affiche qu'il vient de coller sur le mur.

EXEMPLE 6 : MESURE DE VITESSE

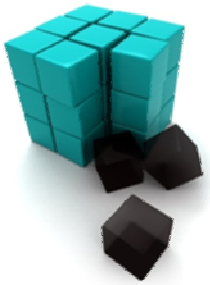
Cette technique est fiabilisée et peut connaître de nombreuses applications, la plus évidente étant la sensibilisation des automobilistes sur les portions de routes par exemples.

EXEMPLE 7 : DETECTION DE COLIS ABANDONNÉ

Un colis est abandonné. Le système détecte la situation et alerte l'opérateur. Il garde la trace de l'auteur du dépôt. Cette application n'est toutefois fonctionnelle que dans des environnements avec très peu de passages, comme par exemple l'entrée d'un site sécurisé… Cette technologie ne marche pas encore par exemple pour une utilisation dans des aérogares ou des gares.

EXEMPLE 8 : STATIONNEMENT GÊNANT

Le système est capable de détecter un véhicule stationné de façon gênante, ici sur un trottoir.



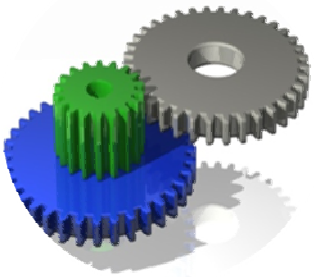
Fiche n°13

20 test à réaliser à la réception du système

13 FICHE N°13 : 20 TESTS A REALISER A LA RECEPTION DU SYSTEME

- **La transmission :**
  - Sur fibre optique : tests photométrique et réflectométrique,
  - Sur multipaire catégorie 6 (pour une liaison Ethernet) : certification catégorie 6 classe E,
  - Liaison radio : test de débit et de perte de trames (taux d'erreur binaire),
  - Vérification du repérage des câbles dans les chambres de tirage et les bâtiments.
- **Les caméras :**
  - Vérification de la stabilité du support,
  - Vérification de leur orientation.
- **L'Interface Homme Machine (IHM) :**
  - Validation des différents mots de passe, en fonction des profils utilisateurs,
  - Vérification du bon positionnement des caméras sur la carte et de leur intitulé,
  - Sélection des caméras sur la carte, avec un temps de réaction acceptable entre le choix de la caméra et son affichage sur l'écran,
  - Pilotage des caméras sur tous les axes + zoom :
    - Sans à coup,
    - Avec un temps de réaction acceptable entre le mouvement du joystick et le déplacement de la caméra.
  - Affichage des masques sur toutes les parties privatives, au bon niveau de zoom,
  - Validation du bon fonctionnement des différentes fonctionnalités :
    - Création de cycles,
    - Création de scénarios,
    - Mémorisation d'un cadrage,
    - Mode poursuite (positionnement automatique de certaines caméras lors du suivi d'un individu).
- **Le mur d'images :**
  - Validation de la qualité et de la fluidité de l'image,
  - Test de la modularité du mur d'images (multifenêtrage, positionnement de l'image).
- **Le réseau :**
  - Mesure du débit,
  - Tests de qualité de service (QoS).
- **L'enregistrement :**
  - Recherche d'une séquence enregistrée,
  - Vérification de sa qualité,
  - Vérification de l'effacement automatique des images, à l'expiration de la période définie.

- **L’exportation :**
  - Exportation d’une séquence sur un support externe,
  - Vérification de la qualité de l’enregistrement.



Fiche n°14

L'évaluation des résultats ?

14 FICHE N°14 : L'EVALUATION DES RESULTATS ?

14.1 EVALUATION DU FONCTIONNEMENT DU SYSTEME

L'évaluation comprend deux aspects :

- L'évaluation technique du système concernant son fonctionnement et son organisation,
- L'évaluation opérationnelle du système, c'est-à-dire son utilité et son efficacité.

Si le dispositif de vidéo protection mis en place constitue un investissement et un moyen de sécurité significatif, il est logique d'évaluer son fonctionnement (évaluation technique) et ses résultats (évaluation opérationnelle).

Pour un tout petit système (par exemple, une caméra dans un établissement ouvert au public), l'évaluation technique sera évidemment empirique. Le responsable sait si elle fonctionne.

Pour un système très complexe, en particulier dans le cas d'une collectivité territoriale utilisant très largement la vidéoprotection et si celle-ci fait encore débat, l'autorité pourra, une fois ou une autre, faire appel à un organisme extérieur, (un cabinet spécialisé) pour réaliser l'évaluation opérationnelle.

Dans tous les autres cas, de loin les plus nombreux, le responsable fera réaliser en interne les évaluations technique et opérationnelle, afin de piloter, le cas échéant de s'adapter, et par ailleurs, s'il le souhaite, de communiquer.

La présente fiche a pour but d'aider à cette démarche.

14.1.1 EVALUATION TECHNIQUE DU SYSTÈME

Cette évaluation peut être très utile lorsque l'on souhaite procéder à une extension du système. Elle permettra de faire un bilan approfondi du fonctionnement des installations.

Chaque élément du système sera étudié successivement, en prêtant particulièrement attention à la notion de continuité de service, fondamentale en sûreté.

- **L'acquisition**

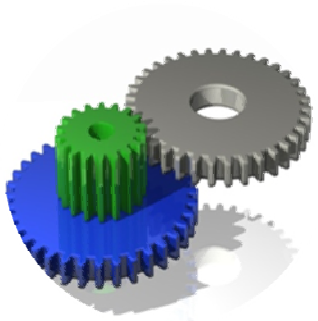
Il conviendra de faire le bilan pour chaque matériel déployé de sa pertinence au regard des besoins initiaux : qualité des images de jour et de nuit, fonctionnalités offertes, positionnement, implantation, support, alimentation… On procédera également à un bilan de fiabilité : combien de pannes rencontrées ? Quel délai moyen de remise en état ? à quel coût ?

- **Le réseau**

On procédera de la même façon que pour le poste précédent : adéquation du réseau aux besoins initiaux, qualité de service, fiabilité,…

- **L'enregistrement**

L'enregistrement est un des postes clés d'un système de vidéosurveillance. Les caractéristiques des enregistreurs doivent être précisément définies au regard des besoins



identifiés. Il conviendra de faire un bilan du fonctionnement de ces équipements (fiabilité, coût des remises en état) mais également de leur facilité d'utilisation : éventuelles difficultés rencontrées pour l'exportation, la relecture, la recherche d'images…

- **Poste d'exploitation**

Il est important de recueillir l'avis des utilisateurs (les opérateurs) qui utilisent quotidiennement le système.

- **Autres équipements**

Un système de vidéosurveillance est complexe et il n'est pas possible de lister ici tous les équipements à évaluer. De façon générale il faut faire un bilan des interventions de maintenance curative réalisées pour identifier les éventuels points faibles de l'installation. Il faut pour cela solliciter, le cas échéant, l'entreprise chargée de la maintenance.

Cette procédure d'évaluation devra également permettre d'évaluer la conformité du système avec les normes techniques en vigueur.

14.1.2 EVALUATION DE L'ORGANISATION DU SYSTÈME

Il s'agit d'évaluer l'organisation, les règles de fonctionnement, les procédures mises en place pour donner au système sa pleine efficacité.

- **Dans tous les cas**

Il faut solliciter les utilisateurs, en particulier les services de sécurité intérieure pour recueillir leurs remarques éventuelles sur le système : ont-ils eu facilement accès aux images ? Dans quels délais ? Quelles difficultés ou insuffisances ont été constatées ?

- **Dans le cas des systèmes supervisés**

La démarche d'évaluation est plus complexe car il faut évaluer le travail des opérateurs, l'organisation de leur travail et le respect des procédures.

14.2 EVALUATION OPERATIONNELLE DE LA VIDEO PROTECTION

Les préconisations ci-dessous concernent essentiellement les dispositifs des opérateurs ayant pour missions d'assurer la sécurité publique et de lutter contre la délinquance.

Elles sont néanmoins aisément transposables à l'évaluation de dispositifs des opérateurs privés (anticipation, cohérence entre le diagnostic et les futurs indicateurs, méthodologie rigoureuse de la remontée d'informations, implication de tous les acteurs dans le processus, analyse spécifique de l'activité, mesure de l'efficacité, localisation précise des événements…).

Généralités

Deux conditions sont essentielles à la réussite d'une évaluation :

- l'anticipation (après la mise en œuvre du dispositif il est trop tard) ;
- la capacité de localisation des crimes et délits « au numéro de rue près ».

Une enquête d'évaluation doit s'inscrire dans la durée et permettre une analyse qui rende compte de l'évolution de la criminalité sur une période relativement longue. Elle doit s'étendre sur les deux ou trois années qui suivent la mise en œuvre du dispositif et porter

non seulement sur les espaces équipés et mais également sur ceux non vidéoprotégés. Enfin, elle ne doit pas être globale mais permettre une analyse géographique (cartographie de caméras et de la délinquance) et par type de crime et délit.

Les indicateurs doivent toujours être en phase avec la stratégie et les objectifs fixés au dispositif. Ils doivent être approuvés sur la forme et sur le fond par l'ensemble des acteurs contribuant à leur gestion.

Le diagnostic initial est essentiel et doit être en parfaite cohérence avec les indicateurs qui seront ensuite exploités. Il doit s'étendre sur une période suffisamment significative.

En fonction de leur nature, les éléments d'information destinés à l'évaluation peuvent être fournis soit par le CSU, soit par les forces de police ou de gendarmerie (sans générer un surcroit de travail qui absorberait du potentiel humain au profit de cette seule mission)

Tous les acteurs contribuant à la remontée des informations doivent être informés en continu des enseignements tirés et des mesures prises ou envisagées.

Le dispositif d'évaluation peut s'organiser en deux séries d'indicateurs :

- les indicateurs permettant d'évaluer l'activité et l'utilité de l'outil pour les différents acteurs impliqués,
- les indicateurs permettant d'évaluer l'efficacité globale de la vidéoprotection.

Le pilote de l'évaluation, même si elle est externalisée, doit rester l'opérateur.

Le suivi des activités liées à la vidéoprotection ou générées par celle-ci

Les indicateurs d'activité peuvent porter sur :

- le nombre d'heures de travail des agents du CSU ;
- le nombre d'heures de visualisation effectuées par les services d'investigation ou de renseignement et par motif d'exploitation ;
- le taux d'utilisation des caméras télé opérables ;
- les échanges d'informations, dans les deux sens, CSU/services d'investigation ou de renseignement.

Les indicateurs faisant ressortir l'utilité peuvent être les suivants :

- interventions sollicitées par le centre de supervision par catégories d'intervenants (PN, GN, PM, pompiers, SAMU…) ;
- arrestations en flagrant délit dans le prolongement de l'activité du CSU ;
- appui à la sécurisation d'équipages en intervention;
- contribution à la gestion de l'ordre public (rassemblements manifestations…)
- surveillances ou filatures dans le cadre de l'exercice de la mission de police judiciaire ;
- réquisitions judiciaires par catégorie de requérant.

La mesure de l'efficacité de la vidéoprotection

Les indicateurs de perception et d'impact :

La perception de l'outil peut s'évaluer par *sondage*, mais aussi à partir de l'exploitation des *courriers* reçus par le maire et les responsables locaux de police et de gendarmerie ainsi que par le nombre et les motifs des demandes d'accès aux images. Les contacts informels avec les habitants et les commerçants restent les meilleurs « thermomètres », il s'agit surtout d'organiser, en amont, la remontée des informations et leur exploitation.

L'analyse de l'impact de l'outil sur les *coûts des dégradations* des bâtiments publics, du mobilier urbain, des différents actes de vandalisme et des tags constitue un bon indicateur et un excellent argument de promotion de la vidéoprotection.

Il convient également de conduire régulièrement des études qualitatives auprès des utilisateurs de la vidéoprotection : police national, police municipale, gendarmerie nationale, services spécialisés, transports publics, parquet …), mais aussi des responsables et des opérateurs des centres de supervision afin d'évaluer la qualité des images vues et stockées, les performances des outils d'exploitation, l'ergonomie et la fonctionnalité globale du dispositif et de son réseau.

Enfin, même s'il parait difficile d'y consacrer un indicateur, l'impact de la vidéoprotection sur les cibles et les modes opératoires des délinquants pourra éventuellement être recherché dans le cadre des auditions.

Les indicateurs de délinquance

Cette deuxième série d'indicateurs d'efficacité s'appuie essentiellement sur les chiffres officiels de la délinquance enrichis éventuellement des données fournies par les partenaires impliqués dans le dispositif (transporteurs, bailleurs, commerçants …). Pour ce faire, les renseignements en possession des services de police et de gendarmerie seront mis à disposition de la collectivité territoriale.

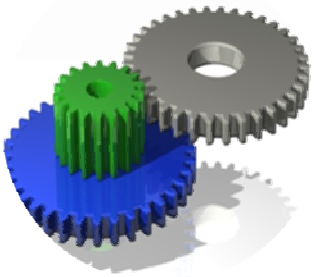
La police et la gendarmerie pourront notamment recenser les affaires élucidées grâce à ou avec la contribution de la vidéoprotection (à noter que le dispositif actuel de recueil statistique n'offre pas cette possibilité).

Il est nécessaire d'être en mesure d'apprécier l'évolution de tout ou partie de la délinquance sur le secteur vidéo protégé mais également sur les zones en périphérie du dispositif et sur l'ensemble de l'agglomération. La méthode pourrait également s'appliquer à une zone test située au sein de l'agglomération et présentant les mêmes particularités sociales, économiques, urbaines et délinquantes que la zone vidéo protégée afin de tenter d'isoler au mieux les effets de la seule vidéo protection (cf. le tableau infra).

Il sera utile de suivre l'évolution plus particulièrement les crimes et délits ayant motivé la mise en place du dispositif de vidéoprotection. Outre un suivi quantitatif des faits retenus, il sera également judicieux de s'intéresser à l'évolution du taux d'élucidation par type de crime ou délit dans la zone vidéo protégée.

Un exemple de tableau à renseigner pour le délit de « vol à la roulotte » est proposé, l'ensemble des infractions pouvant faire l'objet de cette même approche statistique.

Secteurs	Vol à la roulotte		Evolution en %	Taux d'élucidation	
	Moyenne 12 derniers mois	Décembre 2008		Moyenne 12 derniers mois	Décembre 2008
Ensemble de l'agglomération					
Zone vidéo protégée					
Zone périphérique					



Fiche n°15

Comités d'éthique et chartes de déontologie

15 FICHE N°15 : COMITES D'ETHIQUE ET CHARTES DE DEONTOLOGIE

La réglementation n'impose pas l'adoption d'une charte ni la création d'un comité d'éthique. Cette décision relève donc du maître d'ouvrage. Même si nos concitoyens ont profondément évolué dans leur regard sur la vidéoprotection, ils restent attachés à un contrôle de ces dispositifs afin d'assurer qu'il n'y a pas de dérapage. Cette sensibilité, mais aussi la nature de la matière elle-même qui touche aux libertés individuelles, confèrent tout leur intérêt aux chartes déontologiques et aux comités d'éthique qui en vérifient leur respect. A titre d'exemple, deux documents réalisés par des collectivités sont présentés ici.

15.1 CHARTE DEONTOLOGIQUE DE LA VIDEOSURVEILLANCE DE LA VILLE DE CLICHY LA GARENNE

Préambule

Souhaitant améliorer la sécurité des personnes et des biens, répondre davantage aux demandes sociales de sécurité et de prévention, et lutter contre le sentiment d'insécurité, la ville de Clichy la Garenne a décidé de s'investir dans la mise en place d'un dispositif de vidéosurveillance urbaine.

Cette démarche vient s'inscrire dans un cadre partenarial préexistant et matérialisé par la signature d'un Contrat local de sécurité en mars 1999 et par la mise en place d'un Conseil Local de Sécurité et de Prévention de la Délinquance. La ville, et ses partenaires, dans le cadre de la politique de la gestion de l'espace publique, la gestion des flux routiers et de la prévention de la délinquance, entendent ainsi lutter plus efficacement contre certaines formes de délinquance touchant directement la population et sécuriser certains lieux particulièrement exposés à de tels phénomènes. L'installation d'un système de vidéosurveillance apparaît comme un outil de compréhension des phénomènes, d'analyse et de maîtrise des territoires, ainsi que d'intervention et de réactivité de ses services et de ceux de ses partenaires.

Cette politique doit se concilier avec l'impératif du respect des libertés publiques et individuelles.

Les lieux d'implantation des caméras de vidéosurveillance répondent aux problématiques existantes sur certains espaces et respectent les impératifs législatifs fixés. Les principaux objectifs sont :

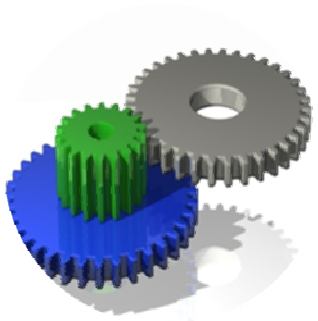
- La sécurité des personnes et des biens
- La régulation du trafic routier et la sécurité routière
- La protection des bâtiments publics et leurs abords
- La gestion de l'espace public

Par cette charte, la Ville de Clichy s'engage à aller au-delà des obligations législatives et réglementaires qui encadrent le régime de la vidéosurveillance afin de veiller au bon usage de ce système et garantir les libertés individuelles et collectives.

A/ Rappel des principes et des textes auxquels doit se conformer la Ville

La mise en œuvre du système de vidéosurveillance doit respecter les textes fondamentaux protecteurs des libertés publiques et privées :

- l'article 8 de la convention européenne des droits de l'homme et des libertés fondamentales qui dispose que toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance
- l'article 11 de cette convention, qui protège le droit à la liberté de réunion



et d'association

- la Constitution de 1958, en particulier le préambule de la Constitution de 1946 et la Déclaration des Droits de l'Homme et du Citoyen.

Le système de vidéosurveillance est soumis aux dispositions légales et réglementaires qui lui sont applicables : l'article 10 de la loi du 21 janvier 1995, la loi « informatique et libertés » du 6 janvier 1978 et le décret du 17 octobre 1996. La Ville applique également les dispositions issues de la jurisprudence administrative, judiciaire et européenne.

B/ Champ d'application de la charte

Cette charte s'applique aux espaces publics placés sous vidéosurveillance par la ville de Clichy conformément aux autorisations préfectorales.

Elle concerne l'ensemble des citoyens.

Les organismes privés et publics pourront s'inspirer de cette charte pour encadrer leur propre système de vidéosurveillance.

Les bailleurs sociaux qui souhaitent se raccrocher à ce dispositif devront accepter les règles définies par cette charte…

Article 1 : Principes régissant l'installation des caméras

1.1. L'autorisation d'installation

La procédure d'installation des caméras est soumise à une autorisation du préfet après avis de la commission départementale des systèmes de vidéosurveillance créée par la loi du 21 janvier 1995. Cette autorisation a été accordée par arrêté du Préfet des Hauts de Seine n°DAG/1/2005/166 du 11 mai 2005.

Toute modification présentant un caractère substantiel doit faire l'objet d'une déclaration dont l'absence peut justifier le retrait de l'autorisation.

1.2. Les conditions d'exploitation des caméras

La loi ainsi que l'arrêté préfectoral n° DAG/1/2005/166 du 11 mai 2005 précisent qu'il est interdit de filmer certains lieux : l'interdiction est relative pour les entrées d'immeubles, c'est à dire qu'elles ne doivent pas être filmées de façon spécifique. L'interdiction est totale pour l'intérieur des habitations. Il y a infraction à cette réglementation, lorsqu'on fixe, on enregistre ou on transmet, sans le consentement de l'intéressé, l'image d'une personne se trouvant dans un lieu privé. Cette infraction est punie de peine d'amende et d'emprisonnement par le code pénal.

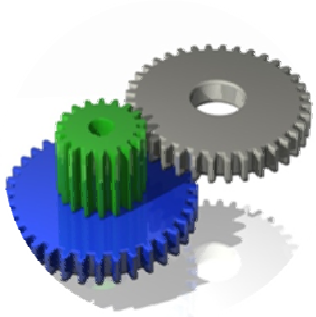
Chaque décision d'installation de nouvelle caméra fait l'objet d'une délibération du conseil municipal, après consultation du ou des conseils de quartiers concernés. Une demande d'autorisation au préfet doit également être formulée avant toute nouvelle installation de caméras non reprise par les autorisations préfectorales en cours.

Elle tient à disposition du public la liste des lieux placés sous vidéosurveillance.

1.3. L'information du public

La loi prévoit que le public doit être informé de manière claire et permanente de l'existence d'un système de vidéosurveillance et de l'autorité ou de la personne responsable de ce système.

La Ville s'engage à mettre en place un dispositif de signalisation dans chaque zone équipée de caméras de vidéosurveillance et qui devra être implanté de façon à être vu par chaque usager.



Le texte de la présente charte sera tenu à la disposition du public en Mairie, dans les mairies annexes, sur le site internet de la Ville et au poste de police municipale.

Article 2 : Conditions de fonctionnement du système de vidéosurveillance

2.1. Les personnes responsables de la vidéosurveillance

Le Maire de Clichy la Garenne, en tant qu'autorité représentant la commune de Clichy la Garenne, est le responsable du système de vidéosurveillance.

Le responsable de l'exploitation du système de vidéosurveillance est le Chef de la police municipale de Clichy la Garenne., sous l'autorité du Directeur de la Sécurité Publique Locale. Le responsable d'exploitation est le seul à avoir accès aux enregistrements et à décider de la sauvegarde des données sur un support amovible. Il devra également veiller à la destruction des enregistrements des images au delà du délai de 14 jours prévus par l'arrêté du Préfet des Hauts de Seine n° DAG/1/2005/166 du 11 mai 2005. Cependant, en cas d'absence de celui-ci, les personnes ayant reçu la délégation de la gestion du service de police municipale pourront remplacer le responsable d'exploitation dans ses fonctions et attributions. Ces personnes seront nominativement habilitées par le Maire de la ville de Clichy la Garenne.

L'ensemble du personnel du poste central de supervision est placé sous l'autorité du responsable d'exploitation, qui est ici le Responsable du service de la Sécurité Publique Locale, Chef de police municipale de Clichy la Garenne ; lui-même est placé sous la direction du responsable du dispositif à savoir le Maire de Clichy la Garenne.

2.2. Les conditions d'accès à la salle d'exploitation

La Ville assure la confidentialité de la salle d'opération grâce à des règles de protection spécifiques.

Un règlement intérieur regroupant les consignes données aux personnels d'exploitation du système et aux personnes habilitées à visionner les images sera rédigé et visé par ces derniers. Il comportera :

- les obligations liées à l'utilisation d'un système de vidéosurveillance
- le respect de la confidentialité des informations
- l'obligation d'information des autorités compétentes en cas de constatation d'une infraction

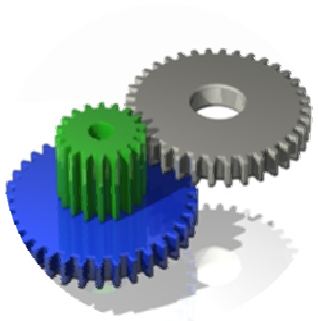
Un registre doit être tenu où sont inscrits les noms et qualités des personnes présentes dans la salle. Ce registre peut être consulté par les membres du Comité d'éthique.

L'accès à la salle d'exploitation est exclusivement réservé au personnel habilité. . Les agents d'exploitation devront s'assurer que les personnes qui pénètrent dans le poste, sont autorisées à le faire. Afin d'assurer ce contrôle, une liste visée par le Maire et le Responsable du service de la Sécurité Publique Locale, Chef de la police municipale de Clichy la Garenne, des personnes habilitées et pouvant accéder au poste central devra être mise à la disposition des opérateurs dans le poste d'exploitation.

Pour les personnes extérieures au service, il est interdit d'accéder à la salle sans une autorisation expresse. Cette autorisation est ponctuelle et ne peut être délivrée qu'après une demande écrite adressée au chef du centre de supervision urbaine. La demande doit être motivée et la personne autorisée s'engage par écrit à respecter les règles de confidentialité nécessaires.

Les membres du Comité d'éthique, peuvent être autorisés à procéder à des visites de courte durée de la salle d'exploitation, après une demande préalablement formulée auprès du Maire.

2.3. Obligations s'imposant aux agents d'exploitation chargés de visionner les images



La loi prévoit que l'autorisation préfectorale prescrit toutes les précautions utiles quant à la qualité des personnes chargées de l'exploitation du système de vidéosurveillance.

Les agents du système d'exploitation sont des agents assermentés et sont soumis au respect du secret professionnel et à l'obligation de discrétion des fonctionnaires territoriaux rappelée par l'article 26 de la loi du 13 juillet 1983, ainsi qu'aux dispositions sur la violation du secret professionnel fixées aux articles 226-13 et 226-14 du code pénal.

La Ville veille à ce que la formation de chaque agent comporte un enseignement de la réglementation existante et des principes inscrits dans la charte. Les agents sont tenus périodiquement informés des évolutions de la réglementation et des réactions suscitées par l'utilisation du système de vidéosurveillance.

Chaque agent du système d'exploitation signe un document par lequel il s'engage à respecter les dispositions de la présente charte et la confidentialité des images visionnées.

Il est interdit aux agents d'utiliser les images pour un autre usage que celui pour lequel elles sont autorisées, c'est à dire la garantie de la sécurité et de la salubrité publique. Il est en particulier interdit aux opérateurs de visualiser l'intérieur des immeubles d'habitation et de façon spécifique leurs entrées.

Le fait de procéder à des enregistrements de vidéosurveillance sans autorisation, de ne pas les détruire dans le délai prévu de 14 jours, de les falsifier, d'entraver l'action de la commission départementale, 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 est puni de trois ans d'emprisonnement et de 45000 Euros d'amende, sans préjudice des dispositions des articles 226-1 du code pénal (article 10, chapitre 11 de la loi vidéosurveillance n° 95-73 du 21 janvier 1995).

Le responsable de la salle d'exploitation porte, par écrit, à la connaissance du président du Comité d'éthique les incidents qui entrent dans le cadre du champ d'application de la charte.

Chaque personne habilitée qui sera par ailleurs soit officier de police judiciaire de la Police Nationale, soit agent de Police Nationale assermenté, sera informée de l'obligation de confidentialité absolue sur les informations dont elle aura eu connaissance par l'intermédiaire du système de vidéosurveillance, ainsi que des peines encourues en cas de manquement à la loi du 21 janvier 1995.

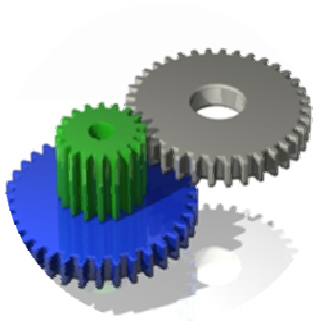
Article 3 : Le traitement des images enregistrées

3.1. Les règles de conservation et de destruction des images

Le délai de conservation des images tel que stipulé dans l'autorisation préfectorale est de 14 jours.

Trois types d'enregistrements ayant vocation à intervenir en cas de constatations d'infractions sont à distinguer :

- Les enregistrements de courte durée : C'est la possibilité pour l'opérateur de revisualiser la dernière heure d'images. L'accès par l'opérateur à la dernière heure d'images sauvegardées sera limité dans le temps ainsi que la durée de conservation de cette sauvegarde. Ces durées ne pourront excéder 4 heures. A la demande de l'opérateur, la séquence sauvegardée pourra être archivée pour être visualisée par le responsable d'exploitation (ou une personne ayant reçu délégation de la gestion du service de police municipale et dûment habilitée par le Maire) en différé, et éventuellement sauvegardée sur support amovible par le responsable d'exploitation en cas de constatation d'une infraction.
- L'enregistrement commandé par l'opérateur : L'opérateur aura également la possibilité de lancer l'enregistrement d'images d'une caméra sélectionnée. L'enregistrement prendra place sur le disque dur dédié du



poste de l'opérateur. Il sera soumis aux mêmes prescriptions que la sauvegarde de la dernière heure d'images, à savoir que l'accès et sa conservation ne pourront excéder plus de 4 heures. De même, à la demande de l'opérateur, la séquence enregistrée pourra être archivée pour être visualisée par le responsable d'exploitation (ou une personne ayant reçu délégation de la gestion du service de police municipale et dûment habilitée par le Maire) en différé, et éventuellement sauvegardée sur support amovible par le responsable d'exploitation.

- L'enregistrement automatique continu : Indépendamment des autres enregistrements, une sauvegarde de l'ensemble des images se fera par enregistrement numérique sur disques durs d'une capacité suffisante pour accueillir l'ensemble des données (images, informations…). Le délai de conservation de cet enregistrement ne pourra en aucun cas dépasser le délai de conservation fixé par l'arrêté préfectoral n° DAG/1/2005/166 du 11 mai 2005 à savoir 14 jours. La lecture des images enregistrées automatiquement se fera sur un poste informatique spécifique et dédié au seul responsable d'exploitation sans empêcher le stockage en continu des images des caméras. L'utilisation de ce poste informatique, ainsi que l'accès aux enregistrements en continu, seront sécurisés par un code d'authentification.

Passé ce délai, les fichiers seront automatiquement effacés et écrasés par une nouvelle période d'enregistrement.

Le poste central de supervision accueillera également, dans une armoire sécurisée, les sauvegardes des images qui auront pu être réalisées sur des supports amovibles en vue de leur transmission aux autorités policières ou judiciaires.

Le service d'exploitation tient à jour un registre mentionnant la visualisation (date, heure…) de l'enregistrement de courte durée (sauvegarde de la dernière heure des images) ainsi que la réalisation d'enregistrements commandés par l'opérateur. Devront y figurer impérativement les motifs de déclenchement de ces enregistrements ainsi que leur date de destruction. La destruction des enregistrements en continus devra également figurer sur ces registres, ainsi que la réalisation de copie sur support amovible avec leur date de remise aux autorités compétentes ou de leur destruction.

Les enregistrements réalisés, la date de destruction des images et le cas échéant, la date de leur transmission au parquet.

A la suite d'une infraction (dans la cadre d'une enquête de flagrance, d'une commission rogatoire…), le Commissaire de police chargé de la circonscription publique de Clichy la Garenne et le Procureur de la République de Nanterre sont habilités à saisir la sauvegarde de l'enregistrement vidéo (sur support amovible) après en avoir fait la demande écrite auprès de Monsieur le Maire de Clichy la Garenne.

Toute reproduction ou copie papier des enregistrements par le personnel est interdite.

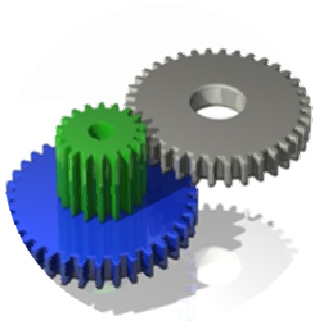
3.2. Les règles de communication des enregistrements

Seul un officier de police judiciaire territorialement compétent est habilité à se saisir du support comportant des enregistrements d'images vidéo après en avoir fait la réquisition écrite.

Un registre est tenu pour la délivrance des copies. Il mentionne le nom de l'officier de police judiciaire requérant, le sujet, la date et l'heure des faits contenus sur la copie. Le registre est signé par la personne à qui a été remise la copie.

3.3. L'exercice du droit d'accès aux images

Conformément à la loi du 21 janvier 1995, toute personne intéressée peut s'adresser au responsable d'un système de vidéosurveillance afin d'obtenir un accès aux enregistrements qui la concernent ou d'en vérifier la destruction dans le délai prévu. Cet accès est de droit.



Un refus d'accès peut toutefois être opposé pour un motif tenant à la sûreté de l'Etat, à la défense, à la sécurité publique, au déroulement de procédures engagées devant les juridictions ou d'opérations préliminaires à de telles procédures, ou au droit des tiers.

La personne qui souhaite avoir accès aux images la concernant doit faire sa demande dans le délai maximum des 14 jours durant lesquels les images sont conservées. Cette demande est adressée au Chef de la police municipale de Clichy la Garenne, ou en son absence, à la personne ayant reçu par délégation la gestion du service de police municipale. La personne demandeuse devra remplir une fiche précisant le lieu, la date et l'heure des images qu'elle désire visionner.

Le responsable d'exploitation sera chargé de traiter la demande et donc :

- soit de justifier de la destruction des enregistrements une fois le délai de conservation fixé par l'arrêté préfectoral expiré, par la présentation des registres (informatisé et/ou manuel) précisant les dates de destruction des enregistrements,
- soit de rechercher les images concernant la personne intéressée. Dans ce dernier cas, il devra vérifier préalablement à l'accès de la personne aux enregistrements :
- si celle-ci a un intérêt à agir, c'est-à-dire de s'assurer que la personne qui demande à accéder à un enregistrement est bien celle qui figure sur celui-ci ;
- et si cet accès, qui est de droit, ne constitue pas une atteinte à la sûreté de l'Etat, à la Défense, à la sécurité publique, au déroulement de procédures engagées devant les juridictions ou des opérations préliminaires à de telles procédures, ou au droit des tiers (respect de la vie privée).

Seulement dans ces cas, un refus d'accès pourra être opposé par le responsable. Dans tous les cas, la décision de refus doit être dûment motivée. Le refus de donner accès aux images peut être déféré au tribunal administratif par l'intéressé.

Après ces vérifications préalables, l'intéressé bénéficiant du droit d'accès, pourra visionner les images le concernant dans le local du poste de police municipale de la ville de Clichy la Garenne, indépendant du poste central d'exploitation et accueillant le poste du responsable d'exploitation. Aucune visualisation de l'intérieur du local ne pourra se faire de l'extérieur. Ce local sera sécurisé par un dispositif de contrôle d'accès et l'accès aux enregistrements sera contrôlé par un code d'authentification. L'existence de ce local, séparé de la salle d'exploitation, évitera toute entrée, de personnes voulant accéder aux images, dans le poste central de supervision et sauvegardera le droit à l'image et le respect de la vie privée des autres personnes filmées.

La personne autorisée à visionner les images la concernant peut être accompagnée d'un membre du comité d'éthique.

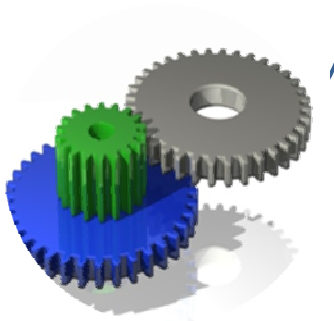
La loi prévoit que toute personne intéressée peut saisir la commission départementale prévue par la loi de 1995 de toute difficulté tenant au fonctionnement d'un système de vidéosurveillance.

Article 4 : Fonctionnement du Comité d'éthique

4.1. Composition

Le Comité d'éthique a été créé par délibération du conseil municipal 31 janvier 2006. Sa composition répond aux objectifs d'équilibre, d'indépendance et de pluralité. Il est composé de 5 élus représentant à la proportionnelle les différents groupes politiques du Conseil municipal et de 5 suppléants ainsi que de 5 personnalités morales (5 titulaires et 5 suppléants) désignées par le Maire sur proposition du C.L.S.P.D.. Le Maire de la Ville est membre de droit.

Fonctionnement et attribution



Il est chargé de veiller, au-delà du respect des obligations législatives et réglementaires, à ce que le système de vidéosurveillance mis en place par la ville ne porte pas atteinte aux libertés publiques et privées fondamentales.

Il formule des avis et recommandations au Maire sur les conditions de fonctionnement du système.

Le comité d'éthique se réunit 3 fois par an et émet un rapport annuel sur les conditions d'application de la charte déontologique. Ce rapport pourra faire l'objet d'une communication au Conseil Municipal

Il peut, à cet effet, demander au Maire de faire procéder à des études par des organismes ou bureaux d'études indépendants.

Il émet un avis sur les demandes qui pourraient être formulées par les organismes privés ou publics souhaitant adhérer aux principes de la charte déontologique.

4.2 Les modalités de saisine du collège

Le Comité d'éthique peut se saisir de toute question entrant dans le champ de sa compétence.

Le Comité d'éthique reçoit les doléances des citoyens qui estimeraient avoir subi un préjudice direct et personnel du fait d'un manquement aux normes en vigueur, à la charte ou à ses principes. Il en informe alors le Maire. Le Comité d'éthique émet à l'égard des parties concernées toute recommandation de nature à apporter une solution au litige.

Le Comité ne peut intervenir sur des faits faisant l'objet d'une procédure devant les tribunaux administratifs ou judiciaires ou devant une instance disciplinaire.

4.3 La Présidence du comité d'éthique

Le comité d'éthique de la vidéosurveillance des espaces publics est placé sous la Présidence du Maire de Clichy

Le Maire désigne parmi les membres, tous les 2 ans, un Président délégué qui assure la représentation et l'animation du comité d'éthique.

4.4 La qualité de membre

Le Maire de Clichy nomme les membres, sur proposition du C.L.S.P.D. sauf en ce qui concerne les élus qui sont désignés en Conseil Municipal.

La qualité de membre du comité d'éthique se perd :

- par décès,
- par perte de la qualité justifiant la qualité de membre,
- par démission adressée au Maire de Clichy,

La durée du mandat des membres ne peut excéder le mandat du Conseil Municipal en cours.

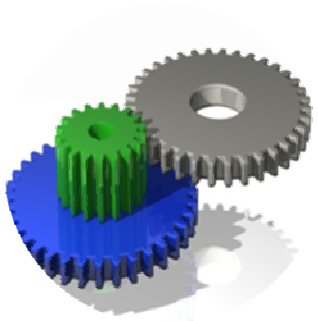
4.5 Les réunions

Le comité d'éthique de la vidéosurveillance des espaces publics se réunit une fois par trimestre.

Il peut être réuni exceptionnellement à la demande du Président ou d'au moins la moitié de ses membres, chaque fois que l'intérêt du comité l'exige.

Les convocations sont faites au moins huit jours à l'avance, par lettre adressée à chaque membre indiquant :

- le jour, l'heure et le lieu,



- l'ordre du jour.

Tout membre peut présenter des propositions pour compléter l'ordre du jour. Celles-ci devront parvenir au Président au moins quatre jours avant la réunion.

Le Président délégué peut inviter à titre consultatif toute autre personne.

Lors des réunions, il est dressé une feuille de présence signée par les membres en séance.

Secrétariat

L'administration est assurée par la Direction de la Sécurité Municipale de la Ville de Clichy

4.6 Les avis

Le comité d'éthique exprime des avis confidentiels signés du Président délégué et adressés uniquement au Maire de Clichy.

Les avis sont pris à la majorité des membres présents.

En cas d'égalité, la voix du Président délégué est prépondérante.

Seules les questions figurant à l'ordre du jour peuvent faire l'objet d'un avis.

4.7 Les modalités de saisine du comité d'éthique

Le comité d'éthique peut se saisir de toute question entrant dans le champ de sa compétence.

Le comité d'éthique reçoit les doléances des citoyens adressées par le Maire de Clichy qui estimeraient avoir subi un préjudice direct lié à la vidéosurveillance.

Le comité d'éthique ne peut intervenir sur des faits faisant l'objet d'une procédure judiciaire et se doit d'informer la justice de tout fait relevant de l'article 40. du Code de procédure pénale.

4.8 La déontologie des membres du comité d'éthique

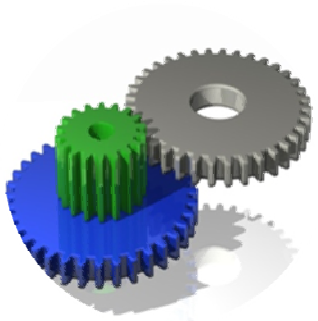
Les membres du comité d'éthique sont soumis pendant et après l'exercice de leurs missions au strict respect de la confidentialité attachée à leur fonction et au fonctionnement du système.

15.2 CHARTE DE LA VILLE DE LYON

Préambule

La vidéosurveillance est un outil au service de la politique de sécurité et de prévention de la Ville de Lyon dans le cadre du contrat local de sécurité. Ses objectifs sont de prévenir l'atteinte aux personnes et aux biens dans les quartiers de forte activité où la délinquance constatée est plus importante, d'augmenter le sentiment de sécurité des Lyonnais et des visiteurs et de sécuriser les bâtiments communaux et espaces publics exposés.

Cette politique doit se concilier avec l'impératif du respect des libertés publiques et individuelles.



Par cette charte, la Ville de Lyon s'engage à aller au-delà des obligations législatives et réglementaires qui encadrent le régime de la vidéosurveillance et à garantir aux citoyens un degré de protection supérieur.

A/ Rappel des principes et des textes auxquels doit se conformer la Ville

La mise en œuvre du système de vidéosurveillance doit respecter les textes fondamentaux protecteurs des libertés publiques et privées :

- l'article 8 de la convention européenne des droits de l'homme et des libertés fondamentales qui dispose que toute personne a droit au respect de sa vie privée et familiale, de son domicile et de sa correspondance
- l'article 11 de cette convention, qui protège le droit à la liberté de réunion et d'association
- la Constitution de 1958, en particulier le préambule de la Constitution de 1946 et la Déclaration des Droits de l'Homme et du Citoyen.

Le système de vidéosurveillance est soumis aux dispositions légales et réglementaires qui lui sont applicables : l'article 10 de la loi du 21 janvier 1995, la loi "informatique et libertés" du 6 janvier 1978 et le décret du 17 octobre 1996.

La Ville applique également les dispositions issues de la jurisprudence administrative, judiciaire et européenne.

B/ Champ d'application de la charte

Cette charte s'applique aux espaces publics placés sous vidéosurveillance par la ville de Lyon.

Elle concerne l'ensemble des citoyens.

Elle se veut exemplaire. Pourront y adhérer les organismes privés et publics souhaitant s'en inspirer pour encadrer leur système de vidéosurveillance.

Article 1 : Principes régissant l'installation des caméras

1.1. Les conditions d'installation des caméras

La loi énumère les cas dans lesquels il est possible d'installer des caméras de vidéosurveillance : il s'agit de la protection des bâtiments et installations publics et de leurs abords, de la sauvegarde des installations utiles à la défense nationale, de la régulation du trafic routier, et de la prévention des atteintes à la sécurité des personnes et des biens dans les lieux particulièrement exposés à des risques d'agression et de vol.

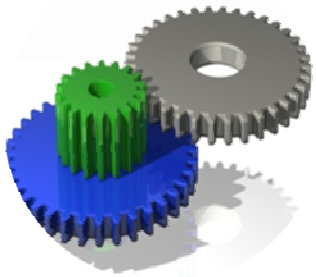
L'installation de caméras doit obéir au principe de proportionnalité : l'objectif de sécurité publique doit se concilier avec le respect des libertés publiques et individuelles.

La loi précise qu'il est interdit de filmer certains lieux : l'interdiction est relative pour les entrées d'immeubles, c'est à dire qu'elles ne doivent pas être filmées de façon spécifique. L'interdiction est totale pour l'intérieur des habitations. Il y a infraction à cette réglementation lorsqu'on fixe, on enregistre ou on transmet, sans le consentement de l'intéressé, l'image d'une personne se trouvant dans un lieu privé. Cette infraction est punie de peine d'amende et d'emprisonnement par le code pénal.

Chaque décision d'installation fait l'objet d'une délibération du conseil municipal, après consultation, pour avis, du ou des conseils de quartiers concernés.

La Ville s'engage à n'installer des caméras de vidéosurveillance que dans les cas de protection des bâtiments et installations publics et de leurs abords (télé surveillance des bâtiments communaux) et de prévention des atteintes à la sécurité des personnes et des biens dans les lieux particulièrement exposés à des risques d'agression et de vol.

Elle tient à disposition du public la liste des lieux placés sous vidéosurveillance.



1.2. L'autorisation d'installation

La procédure d'installation des caméras est soumise à une autorisation du préfet après avis de la commission départementale des systèmes de vidéosurveillance créée par la loi du 21 janvier 1995.

1.3. L'information du public

La loi prévoit que le public doit être informé de manière claire et permanente de l'existence d'un système de vidéosurveillance et de l'autorité ou de la personne responsable de ce système.

La Ville s'engage à mettre en place un dispositif de signalisation dans chaque site équipé de caméras de vidéosurveillance. Ce dispositif comporte la mention de l'existence du collège d'éthique de la vidéo surveillance et ses coordonnées. Ce dispositif devra être implanté de façon à être vu par chaque usager.

Avant ouverture de tout nouveau dispositif, la Ville procédera à l'information du public par voie de presse.

Le texte de la présente charte sera tenu à la disposition du public dans chaque mairie d'arrondissement et dans chaque poste de police municipale.

Article 2 : Conditions de fonctionnement du système de vidéosurveillance

2.1. Obligations s'imposant aux agents chargés de visionner les images

La loi prévoit que l'autorisation préfectorale prescrit toute les précautions utiles quant à la qualité des personnes chargées de l'exploitation du système de vidéosurveillance.

La Ville veille à ce que la formation de chaque agent comporte un enseignement de la réglementation existante et des principes inscrits dans la charte.

Les agents sont tenus périodiquement informés des évolutions de la réglementation et des réactions suscitées par l'utilisation du système de vidéosurveillance.

Chaque agent du système d'exploitation signe un document par lequel il s'engage à respecter les dispositions de la présente charte et la confidentialité des images visionnées.

Il est interdit aux agents d'utiliser les images pour un autre usage que celui pour lequel elles sont autorisées, c'est à dire la garantie de la sécurité et de la salubrité publique. Il est en particulier interdit aux opérateurs de visualiser l'intérieur des immeubles d'habitation et de façon spécifique leurs entrées.

La présence constante d'au moins deux opérateurs dans le centre de supervision est impérative. Le port d'un badge est obligatoire pour tous les opérateurs.

Le responsable de la salle d'exploitation porte, par écrit, à la connaissance du président du collège d'éthique les incidents qui entrent dans le cadre du champ d'application de la charte.

2.2. Les conditions d'accès à la salle d'exploitation

La Ville assure la confidentialité de la salle d'opération grâce à des règles de protection spécifiques.

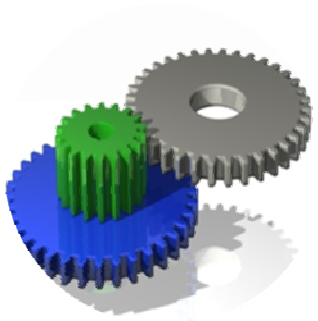
Un registre doit être tenu où sont inscrits les noms et qualités des personnes présentes dans la salle. Ce registre peut être consulté par les membres du collège d'éthique.

L'accès à la salle d'exploitation est exclusivement réservé au personnel habilité.

Pour les personnes extérieures au service, il est interdit d'accéder à la salle sans une autorisation expresse. Cette autorisation est ponctuelle et ne peut être délivrée qu'après une demande écrite adressée au chef du centre de supervision urbaine. La demande doit être

motivée et la personne autorisée s'engage par écrit à respecter les règles de confidentialité nécessaires.

Les membres du collège d'éthique peuvent procéder à des visites impromptues de la salle d'exploitation.



Article 3 : Le traitement des images enregistrées

3.1. Les règles de conservation et de destruction des images

La durée de conservation des images enregistrées est légalement fixée à un mois maximum sauf dérogation prévue par la loi dans le cas d'une enquête de flagrant délit, d'une enquête préliminaire ou d'une information judiciaire.

La Ville s'engage à conserver les images pendant une durée maximum de huit jours sous réserve de l'article 3.3 ci-après.

Le service tient à jour un registre mentionnant les enregistrements réalisés, la date de destruction des images et le cas échéant, la date de leur transmission au parquet.

La visualisation des enregistrements des images vidéo est autorisée par les opérateurs et le chef du centre de supervision urbaine dans le cadre de leur travail. Cependant, un agent de la police nationale a accès à cette visualisation sur demande écrite d'un officier de police judiciaire territorialement compétent.

Toute reproduction ou copie papier des enregistrements par le personnel est interdite.

3.2. Les règles de communication des enregistrements

Seul un officier de police judiciaire territorialement compétent est habilité à se saisir du support comportant des enregistrements d'images vidéo après en avoir fait la réquisition écrite.

Un registre est tenu pour la délivrance des copies. Il mentionne le nom de l'officier de police judiciaire requérant, le sujet, la date et l'heure des faits contenus sur la copie. Le registre est signé par la personne à qui a été remise la copie.

3.3. L'exercice du droit d'accès aux images

Toute personne intéressée peut s'adresser au responsable du centre de supervision urbaine afin d'obtenir l'accès aux enregistrements des images sur lesquelles elle figure, ou pour en vérifier la destruction.

La personne qui souhaite avoir accès à ces images dispose d'un délai de huit jours pour faire sa demande, par lettre avec accusé de réception, auprès du responsable du centre de supervision urbaine, à l'adresse suivante : Centre de supervision urbaine, 11 rue Pizay, Lyon 1er arrondissement.

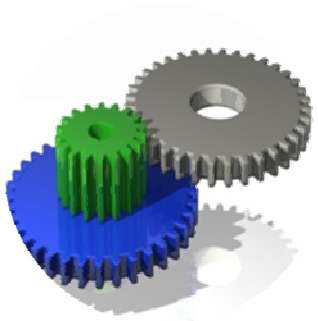
La réception de cette lettre proroge le délai de conservation des images dans la limite du délai maximum autorisé par la loi, soit un mois.

Le responsable du centre de supervision urbaine accuse réception de cette lettre. Il saisit sans délai le collège d'éthique et transmet une copie de la demande à la mairie d'arrondissement concernée.

La personne autorisé à visionner les images la concernant peut être accompagnée d'un membre du collège d'éthique.

La demande peut être rejetée afin de protéger le droit au respect de la vie privée des tiers. Elle peut également être refusée dans les cas où une procédure est en cours ou, pour des motifs de sûreté de l'Etat, de défense nationale ou de sécurité publique. Dans tous les cas, la décision de refus doit être dûment motivée. Le refus de donner accès aux images peut être déféré au tribunal administratif par l'intéressé.

La loi prévoit que toute personne intéressée peut saisir la commission départementale prévue par la loi de 1995 de toute difficulté tenant au fonctionnement d'un système de vidéosurveillance.



Article 4 : Dispositions visant au respect de la charte

4.1. Le collège d'éthique

Le collège a été créé par délibération du conseil municipal en date du 14 avril 2003. Sa composition répond aux objectifs d'équilibre, d'indépendance et de pluralité : il est composé d'élus répartis également entre majorité et opposition, de personnalités qualifiées représentant le monde du droit, de l'économie et de l'éducation, de représentants d'associations de défense des droits de l'homme.

Il est chargé de veiller, au-delà du respect des obligations législatives et réglementaires, à ce que le système de vidéosurveillance mis en place par la ville ne porte pas atteinte aux libertés publiques et privées fondamentales.

Il informe les citoyens sur les conditions de fonctionnement du système de vidéosurveillance et reçoit leurs doléances.

Il formule des recommandations au maire.

Il veille au respect de l'application de la charte d'éthique.

4.2. Evaluation du fonctionnement et de l'impact du système de vidéosurveillance

Le collège élabore chaque année un rapport sur son activité.

Il peut formuler au Maire toute recommandation sur les conditions de fonctionnement et l'impact du système.

Il peut, à cet effet, demander au Maire de faire procéder à des études par des organismes ou bureaux d'études indépendants.

4.3. Les modalités de saisine du collège

Le collège peut se saisir de toute question entrant dans le champ de sa compétence.

Le collège reçoit les doléances des citoyens qui estimeraient avoir subi un préjudice direct et personnel du fait d'un manquement aux normes en vigueur, à la charte ou à ses principes. Il en informe la mairie d'arrondissement concernée. Le collège émet à l'égard des parties concernées toute recommandation de nature à apporter une solution au litige.

Le collège ne peut intervenir sur des faits faisant l'objet d'une procédure devant les tribunaux administratifs ou judiciaires ou devant une instance disciplinaire.

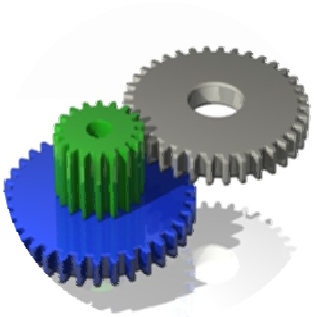
ANNEXE 1 : LISTE DES TEXTES APPLICABLES

Loi N°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés Article 10 de la loi N°95-79 du 21 janvier 1995 d'orientation et de programmation relative à la sécurité

Décret N°96-926 du 17 octobre 1996 relatif à la vidéosurveillance

Circulaire du 22 octobre 1996 relative à l'application de l'article 10 de la loi du 21 janvier 1995

Collège d'éthique de la vidéo surveillance des espaces publics - 21/07/04 8



Fiche n°16

Le dispositif national de suivi

16 FICHE N°16 : LE DISPOSITIF NATIONAL DE SUIVI

16.1 UNE VOLONTE DE L'ETAT DE PROMOUVOIR LA VIDEOPROTECTION

L'Etat souhaite encourager le développement de la vidéoprotection par le biais d'un plan national de développement de la vidéoprotection. Cette volonté de favoriser la généralisation de la vidéoprotection repose sur trois constats :

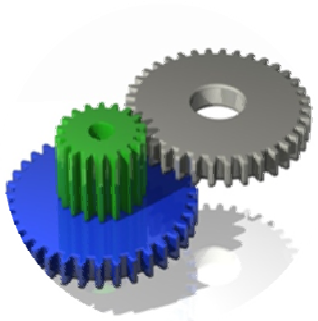
- L'efficacité de la vidéosurveillance pour améliorer de façon significative la sécurité quotidienne n'est plus à démontrer. Des expériences étrangères l'ont largement prouvée, notamment au Royaume Uni avec l'élucidation de meurtres d'enfants et de crimes terroristes. Des expériences locales en France le montrent quotidiennement.
- La France a pris du retard dans le déploiement de systèmes de vidéosurveillance : on évalue à 340 000 les caméras autorisées dans le cadre de la loi de 1995, dont seulement 20 000 sur la voie publique.
- L'opinion publique est désormais majoritairement acquise à cette technologie : deux enquêtes conduites par IPSOS en 2007 et 2008 l'illustrent : 71 % des Français dans l'un, 78% dans l'autre y sont favorables dans les lieux publics pour lutter contre l'insécurité et le terrorisme. 66 % des sondés se sentent davantage rassurés lorsqu'ils sont dans des lieux équipés de tels dispositifs. Et ils ne sont plus qu'un tiers à craindre que la vidéosurveillance ne réduise leur liberté ou menace leur vie privée.

Lors de son intervention à l'occasion de l'installation de la Commission Nationale de Vidéosurveillance, madame Michèle Alliot-Marie, ministre de l'Intérieur, a évoqué deux ambitions fortes :

- Sur un plan quantitatif : développer fermement et notamment en ce qui concerne la voie publique, tripler en deux ans le nombre de caméras afin de passer de 20 000 à 60 000.
- Sur un plan qualitatif :
  - des installations modernes, avec la possibilité pour les policiers d'accéder aux images des municipalités et des grands gestionnaires d'espaces publics : transports, centres commerciaux, enceintes sportives…,
  - une amélioration significative de l'élucidation des infractions,
  - une contribution nettement accrue à la prévention de la délinquance.

Trois structures sont chargées de concrétiser ces ambitions :

- **La Commission nationale de la vidéosurveillance,**
- **Le Comité de pilotage stratégique,**
- **Le comité interministériel de prévention de la délinquance.**



16.2 LA COMMISSION NATIONALE DE LA VIDEOSURVEILLANCE

La commission nationale de la vidéosurveillance a été installée le 9 novembre 2007.

La composition associe des parlementaires de la majorité et de l'opposition, représentant des Barreaux, des communes et des maires de France, des entreprises de sécurité, des chambres de commerce, directeurs d'administration centrale. Elle est présidée par Alain BAUER, criminologue.

C'est une instance dont le rôle est d'émettre des propositions visant :

- A améliorer la protection effective des libertés : liberté individuelle, droit à l'intimité de la vie privée, droit à l'image, droit à l'oubli, transparence...,
- A améliorer le fonctionnement des commissions départementales,
- A renforcer les droits de la personne humaine dans le cadre de la vidéosurveillance

16.3 LE COMITE DE PILOTAGE STRATEGIQUE

Le Comité de pilotage stratégique comprend des représentants des ministères et directions particulièrement concernés par la vidéo protection : Direction générale des Infrastructures, des Transports et de la Mer du MEEDDAT, Conseil Général des Technologies et de l'Information au ministère chargé de l'économie, direction générale de la Police nationale et direction générale de la Gendarmerie nationale au ministère de l'intérieur, secrétariat général du comité interministériel de Prévention de la délinquance.

Il est présidé par un inspecteur général de l'Administration, Mr Philippe Melchior.

Son rôle est de :

- proposer au gouvernement les mesures à prendre ;
- piloter leur mise en œuvre ;
- animer l'action des directions des ministères concernés.

16.4 LE COMITE INTERMINISTERIEL DE PREVENTION DE LA DELINQUANCE

Aux termes du **décret 2006-52 du 17 janvier 2006**, le Comité Interministériel de prévention de la délinquance fixe les orientations de la politique gouvernementale en matière de prévention de la délinquance et veille à leur mise en œuvre. Il coordonne l'action des ministères et l'utilisation des moyens budgétaires consacrés à la politique de la prévention de la délinquance.

Dans le domaine de la vidéoprotection, le Comité Interministériel de prévention de la délinquance fixe les orientations d'utilisation par les Préfets des crédits mis à leur disposition par le Fonds interministériel de même nom.

}